

**IMPLEMENTACIÓN DEL ÁREA DE SEGURIDAD DEL MODELO
FCAPS EN LA INFRAESTRUCTURA DE RED DE LA ALCALDÍA
DEL MUNICIPIO DE ENVIGADO**

ANDRÉS FELIPE ARROYAVE ARREDONDO

**INSTITUCIÓN UNIVERSITARIA DE ENVIGADO
FACULTAD DE INGENIERIA
TECNOLOGÍA EN GESTIÓN DE REDES
ENVIGADO
2013**

**IMPLEMENTACIÓN DEL ÁREA DE SEGURIDAD DEL MODELO
FCAPS EN LA INFRAESTRUCTURA DE RED DE LA ALCALDÍA
DEL MUNICIPIO DE ENVIGADO**

ANDRÉS FELIPE ARROYAVE ARREDONDO

**INFORME DE PRÁCTICA PARA OPTAR EL TÍTULO DE
TECNÓLOGO EN GESTIÓN DE REDES**

**ASESOR
LUIS FELIPE VILLAMIZAR TORRES
INGENIERO DE SISTEMAS**

**INSTITUCIÓN UNIVERSITARIA DE ENVIGADO
FACULTAD DE INGENIERIA
TECNOLOGÍA EN GESTIÓN DE REDES
ENVIGADO
2013**

DEDICATORIA

**A MIS PADRES,
MIS ABUELOS
MI HERMANA
TODA MI FAMILIA Y AMIGOS**

AGRADECIMIENTOS

EL AUTOR EXPRESA SUS AGRADECIMIENTOS A:

PRINCIPALMENTE LE AGRADEZCO A DIOS POR DARME LA OPORTUNIDAD DE VIVIR ESTA EXPERIENCIA ACADÉMICA QUE ACABA Y LA EXPERIENCIA LABORAL QUE EMPIEZA.

MIS PADRES Y MI HERMANA, QUIENES ME ACOMPAÑARON DURANTE TODO ESTE PROCESO DE APRENDIZAJE.

MIS ABUELOS, MIS PRIMAS SARA Y MANUELA POR LA COLABORACIÓN PRESTADA DURANTE TODO EL PROCESO.

A TODOS LOS PROFESORES DE TODOS LOS SEMESTRES: EMPEZANDO POR ANDRÉS, LINA Y VICTOR; Y TERMINANDO POR JACKSON, JOHN JAIRO Y LUIS SANTIAGO.

A FREDY CASTAÑO POR EL ACOMPAÑAMIENTO EN ESTOS 4 AÑOS Y MEDIO, Y POR SUPESTO A MI ASESOR, QUIEN DISPUSO DE MI TIEMPO PARA REALIZAR LAS ASESORIAS Y LAS VISITAS A LA OFICINA.

A FELIPE BURGOS, POR EL ACOMPAÑAMIENTO Y APRENDIZAJE QUE OBTUVE DE ÉL DURANTE MI PRÁCTICA COMO JEFE INMEDIATO, A TODOS LOS COMPAÑEROS DE LA LÍNEA 7000 Y DE LA DIRECCIÓN DE INFORMÁTICA DE LA ALCALDÍA DE ENVIGADO ESPECIALMENTE AL SEÑOR ALCALDE HÉCTOR LONDOÑO Y AL JEFE DE LA OFICINA LUIS FELIPE ROSSO, POR BRINDARME LA OPORTUNIDAD DE REALIZAR MI PRÁCTICA EN LA DIRECCIÓN DE INFORMÁTICA.

CONTENIDO

LISTAS ESPECIALES	8
GLOSARIO	9
RESUMEN	15
ABSTRACT	16
INTRODUCCIÓN	17
1. INFORME ASPECTOS GENERALES DE LA PRÁCTICA EMPRESARIAL EN LA ALCALDÍA DE ENVIGADO	18
1.1. Aspecto Generales de la Práctica	18
1.2. Centro de Práctica	18
1.3. Objetivo de la práctica	20
1.4. Justificación	20
2. ESPECIFICACIONES DE ACUERDO CON LA MODALIDAD (ÁMBITO) DE PRÁCTICA	20
2.1. Planteamiento del problema	20
2.2. Equipo de trabajo	20
2.3. Metodología de trabajo	21
2.4. Resultados esperados	21
3. SISTEMATIZACIÓN DE LA INFORMACIÓN DE ACUERDO CON LA MODALIDAD DE PRÁCTICA	22
3.1. Administración de las Redes Inalámbricas Institucional	22
3.2. Soporte Técnico en Redes	24

4. PROYECTO DE PRÁCTICA PARA LA AGENCIA O CENTRO DE PRÁCTICAS: IMPLEMENTACIÓN DEL ÁREA DE SEGURIDAD DEL MODELO FCAPS EN LA INFRAESTRUCTURA DE RED DE LA ALCALDÍA DEL MUNICIPIO DE ENVIGADO	24
4.1. Planteamiento del Problema del Proyecto de Práctica	27
4.2. Justificación del Proyecto de Práctica	27
4.3. Objetivos del Proyecto de Práctica (Objetivo General y Objetivos Específicos)	28
4.4. Diseño Metodológico del Proyecto de Práctica	28
4.5. Cronograma de Actividades del Proyecto de Práctica	30
4.6. Presupuesto (Ficha de Presupuesto) del Proyecto de Práctica	30
5. DESARROLLO DEL PROYECTO DE PRÁCTICA: IMPLEMENTACIÓN DEL ÁREA DE SEGURIDAD DEL MODELO FCAPS EN LA INFRAESTRUCTURA DE RED DE LA ALCALDÍA DEL MUNICIPIO DE ENVIGADO	32
5.1. Analizar documentación existente acerca de FCAPS y su área de seguridad	32
5.2. Registrar el conocimiento acerca de FCAPS	32
5.3. Diseñar un plan de seguridad del modelo FCAPS	32
5.4. Determinar un plan de seguridad para la Infraestructura de Red de la Alcaldía de Envigado	32
6. INCONVENIENTES EN EL DESARROLLO DE LA PRÁCTICA	33
7. CONCLUSIONES	33
8. RECOMENDACIONES	34
REFERENCIAS BIBLIOGRÁFICAS	35
ANEXOS	36
ANEXO A. Documentación recogida a cerca de FCAPS	41
ANEXO B. APARTES DE LA RESOLUCIÓN N° 2990 DE 2011. ALCALDÍA DE ENVIGADO	48

ANEXO C. APARTES DE LA RECOMENDACIÓN DE LA UIT-T M.3400. UNIÓN INTERNACIONAL DE TELECOMUNICACIONES	52
ANEXO D. EVIDENCIA FOTOGRÁFICA DE LA REALIZACIÓN DE LA PRÁCTICA EMPRESARIAL EN LA DIRECCIÓN DE INFORMÁTICA DE LA ALCALDÍA DE ENVIGADO.	55

LISTAS ESPECIALES

LISTAS DE TABLAS

TABLA 1. Aspectos Generales de la Práctica	18
TABLA 2. Tabla de número de usuarios que utilizan las redes inalámbricas de la Alcaldía de Envigado, semana del 1 al 5 de Abril del año en curso	23
TABLA 3. Presupuesto Global del Proyecto “Implementación del Área de Seguridad del Modelo FCAPS en la Infraestructura de red de la Alcaldía de Envigado”	30
TABLA 4. Descripción Gastos Personales “Implementación del Área de Seguridad del Modelo FCAPS en la infraestructura de red de la Alcaldía de Envigado”	31
TABLA 5. Descripción Gastos de Materiales y Suministros “Implementación del Área de Seguridad del Modelo FCAPS en la infraestructura de red de la Alcaldía de Envigado”	31
TABLA 6. Descripción Gastos de Equipo “Implementación del Área de Seguridad del Modelo FCAPS en la infraestructura de red de la Alcaldía de Envigado”	31
TABLA 7. Descripción Gastos de Otros “Implementación del Área de Seguridad del Modelo FCAPS en la infraestructura de red de la Alcaldía de Envigado”	32

LISTA DE FIGURAS

FIGURA 1. Estudio Organizacional de la Alcaldía de Envigado	19
FIGURA 2. Equipo de Trabajo de la Dirección de Informática	20
FIGURA 3. Página de inicio en el acceso remoto vía web de la controladora de la red inalámbrica de la Alcaldía de Envigado	22
FIGURA 4. Gráfico de número de usuarios que utilizan las redes inalámbricas de la Alcaldía de Envigado, semana del 1 al 5 de Abril del año en curso	23
FIGURA 5. Cronograma de Actividades	30
FIGURA 6. Fotografía de la consola de administración de la controladora inalámbrica de Aruba Networks	55
FIGURA 7. Fotografía de la consola de administración de los Access Points anexados a la controladora inalámbrica de Aruba Networks	55
FIGURA 8. Fotografía del rack que cubre las oficinas de Informática, Catastro y Sótano Municipal.	56
FIGURA 9. Fotografía del conector tipo PoE del AP presente en la Dirección de Informática, que cubre las áreas de Informática, Catastro y el Teatro Municipal.	56
FIGURA 10. Fotografía del Access Point que cubre las áreas de Informática, Catastro y Teatro Municipal.	57
FIGURA 11. Fotografía del practicante realizando la toma del número de usuarios conectados a la red inalámbrica de la Alcaldía de Envigado, mediante la consola de administración del Aruba Networks	57

GLOSARIO

AAA: (Autenticación, Autorización y Administración). AAA son siglas que se aplican en las herramientas de seguridad.

Acceso Remoto: Acceder desde una computadora a un recurso ubicado físicamente en otra computadora, a través de una red local o externa (como internet).

Administrador: Software que facilita el control de un entorno determinado, ya sea personal que facilita el control de un entorno determinado, ya sea personal o empresarial. Por extensión, se denomina administrador al encargado de realizar ese control.

Aplicación: Programa ejecutable capaz de realizar una función específica del mantenimiento del sistema (que lleva a cabo por medio de utilidades). Son aplicaciones los procesadores de texto, hojas de cálculo, bases de datos, etc.)

Archivo: Conjunto de datos estructurados que pueden recuperarse fácilmente y usarse en una aplicación determinada, Se utiliza como sinónimo de fichero.

Arquitectura: Término referente a la estructura general de un procesador, sistema operativo, ordenador, línea de sistemas, etc.

Back-up: Copia de seguridad de los archivos y aplicaciones en un soporte diferente del disco duro en el que se encuentran, con el fin de poder recuperar la información en caso de pérdida de esta.

Base de Datos: Conjunto de informaciones disponible para varios usuarios. Suele admitir la selección de acceso aleatorio y múltiples "vistas" o niveles de abstracción de los datos subyacentes.

Capacidad: La mayor velocidad de transmisión posible (fiable) que puede darse en un canal, un circuito o una pieza de equipo. La capacidad puede expresarse como la velocidad bruta o como el rendimiento neto.

COMPAQ: Compaq Computer Corporation era una compañía de computación fundada en 1982, actualmente es una marca de Hewlett-Packard. El nombre "Compaq" proviene de "Compatibility and Quality" (Compatibilidad y calidad).

Conexión: Punto donde se realiza un enlace entre dispositivos o sistemas. También conexión hace referencia al enlace completo. Una conexión puede ser alámbrica o inalámbrica, digital o analógica, virtual o real, etc.

Configuración: (Setup o setting en inglés) la configuración es una herramienta en los programas y en los sistemas operativos que sirve para configurarlos.

Cracker: Individuo con amplios conocimientos informáticos que desprotege/piratea programas o produce daños en sistemas o redes.

Cuello de botella: Límite en la capacidad del sistema que puede reducir el tráfico en condiciones de sobrecarga.

Cisco Systems: (Cisco Systems, Inc.) Compañía global con sede en San José, California (EE.UU.). Diseña y vende tecnología y servicios de red como ser: routers (enrutadores), switches (conmutadores), hubs, cortafuegos, productos de telefonía IP, software de gestión de red como CiscoWorks, equipos para Redes de Área de Almacenamiento.

Dato: Información en un formato que pueda ser procesado por u ordenado. La información se condensa digitalmente, de moda que un texto, imagen o sonido se pueda representar en la pantalla.

Dirección IP: Dirección de 32 bits del protocolo Internet asignada a un computador conectado a Internet. La dirección IP tiene un componente del propio computador y un componente de red. Este número tiene el formato de cuatro grupos de hasta tres dígitos, separados por un punto, por ejemplo "199.183.11.115".

Dirección URL: Formato de las direcciones de páginas Web que muestra el nombre del servidor en el que se almacenan los archivos del sitio, la ruta de acceso al directorio del archivo y su nombre.

DNS: (Domain Name System, Sistema de Nombres de Dominio) Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en el lenguaje natural a una dirección numérica IP.

Facebook: Facebook es un sitio web del tipo red social. Inicialmente era exclusivo de estudiantes universitarios, pero en septiembre de 2006 se amplió a cualquier persona que tenga correo electrónico. Facebook es uno de los sitios web más visitados del mundo.

Falla: En hardware y software, bug, agujero informático o vulnerabilidad.

Firewall: Software o hardware que limita ciertos tipos de acceso a una red o a sus recursos. Los firewall se utilizan para aumentar la seguridad de los sistemas informáticos a los que protegen de intrusiones no autorizadas.

Hacker: Nombre que se da en la jerga informática a un usuario con avanzados conocimientos que dedica mucho tiempo a trabajar con los computadores. Originalmente se utiliza el término para designar a una persona que escribe programas informáticos, troceando (hacking) el código digital. La palabra hacker se utiliza mucho para designar a las personas que rompen los sistemas de seguridad informáticos para causar daños, robar secretos o, simplemente para demostrar que pueden hacerlo.

HHTP: Es un conjunto de estándares que permite a los usuarios de la Web intercambiar información. Es el método que se utiliza para transferir documentos desde el sistema donde se almacenan las páginas hasta los usuarios individuales.

IEEE: (Institute of Electrical and Electronics Engineers. Instituto de Ingenieros Eléctricos y Eléctricos). Asociación estadounidense fundada en 1963 que se caracteriza por aportar tecnologías y desarrollos a la evolución de la informática y la electrónica, especialmente los estándares IEEE 802, para redes de área local, e IEEE 1394 para la conexión de periféricos externos mediante un canal de alta velocidad.

Informática: Ciencia que estudia el tratamiento automático de la información en computadoras, dispositivos electrónicos y sistemas informáticos. Proviene del francés *informatique* y fue acuñado por el ingeniero Philippe Dreyfus en 1962. Formó una conjunción entre las palabras “information” y “automatique”.

ISO: (International Standard Organization. Organización Internacional de Normalización). Fundada en 1947 reúne asociaciones de unos 90 países y su objetivo es establecer los estándares internacionales para la comunicación de datos.

ITU: (International Telecommunications Union - Unión internacional de telecomunicaciones). Organismo de las Naciones Unidas encargado de regular las telecomunicaciones entre las distintas administraciones y empresas operadoras.

LAN: (Local Area Network, Red de Área Local) Se trata de un conjunto de computadores conectados entre sí y geográficamente próximos. La ventaja de una LAN consiste en poder disponer de los recursos de varios computadores dentro de un grupo de trabajo.

Modelo: Representación de la realidad por medio de abstracciones. Los modelos enfocan ciertas partes importantes de un sistema (por lo menos, aquella que le interesan a un tipo de modelo específico), restándole importancia a otras.

Normalización: Redacción y aprobación de normas que se establecen para mejorar la compatibilidad, calidad y seguridad de dispositivos, sistemas y programas. Redacción y aprobación de normas que se establecen para mejorar la compatibilidad, calidad y seguridad de dispositivos, sistemas y programas.

Protocolo: Conjunto de reglas y normas que determinan cómo se realiza un intercambio de datos entre computadores.

Puerto de Datos: Interfaz por la cual pueden enviarse o recibirse datos. Esa interfaz puede ser física o de software (puerto de navegación http, puerto de IRC, etc.).

Puerto de Red: Interfaz para comunicar programa a través de una red.

QoS Quality of Service: Calidad de servicio. Es la posibilidad de saber la calidad o rendimiento de una red como internet con un determinado servicio.

Red: Sistema de elementos interrelacionados que se conectan mediante un vínculo dedicado o conmutado para proporcionar una comunicación local o remota (de voz, video, datos, etc.) y facilitar el intercambio entre usuarios con intereses comunes.

Redes de Computadores: Una red de computadoras es una interconexión de computadoras para compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico (alambrado) o inalámbrico. Algunos expertos creen que una verdadera red de computadoras comienza cuando son tres o más los dispositivos y/o computadoras conectadas.

Redes de Telecomunicaciones: (Telecommunications network) Una red de telecomunicaciones es una red de enlaces y nodos ordenados para la comunicación a distancia, donde los mensajes pueden pasarse de una parte a otra de la red sobre múltiples enlaces y a través de varios nodos.

Redes Inalámbricas: (Wireless network). En general, cualquier tipo de red que es inalámbrica. Pero el término suele utilizarse más para referirse a aquellas redes de telecomunicaciones en donde la interconexión entre nodos es implementada sin utilizar cables. Las redes inalámbricas de telecomunicaciones son generalmente implementadas con algún tipo de sistema de transmisión de información que usa ondas electromagnéticas, como las ondas de radio.

Router: (enrutador) Dispositivos que une entre sí dos redes, de forma que la información que no va dirigida a la otra red, no pasa a ella.

Servidor: En una red, ordenador que proporciona servicios a otras estaciones.

Seguridad Informática: La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

SHTTP: (Secure HTTP, HTTP Seguro) Protocolo HTTP mejorado con funciones de seguridad con clave simétrica. Se visualiza como `https://`

Sitio Web: Es un conjunto de páginas web afines, normalmente gestionadas por un único usuario.

Telecomunicación: (Telecommunication). Del griego tele, que significa "Distancia" o "Lejos". Comunicación a distancia. Tecnología que permite la transferencia de un mensaje de un punto a otro. La telecomunicación incluye formas de comunicación a distancia como radio, telegrafía, televisión, telefonía, etc.

TI: (Information technology, IT). Tecnologías de la información o simplemente TI, es un amplio concepto que abarca todo lo relacionado a la conversión, almacenamiento, protección, procesamiento y transmisión de la información. El concepto se emplea para englobar cualquier tecnología que permite administrar y comunicar información.}

URL: (Universal Resource Locator, Localizador Universal de Recursos) Dirección de Internet que apunta a un recurso concreto dentro de un servidor conectado a la red.

Virus: programa que infecta a una computadora, causando efectos indeseables.

VPN: VPN - Virtual Private Networks) Tecnología de redes que permite la extensión de una red de área local sobre una red pública o no controlada (como internet). Por ejemplo, crear una red entre distintas computadoras utilizando como infraestructura a internet. Evidentemente debe haber mecanismos de protección de los datos que se manejan.

WAN: (Wide Area Network, Rede de Área Amplia) Red de computadores conectados entre sí, dispersos geográficamente.

Wi-Fi: (Wireless Fidelity) Conjunto de estándares para redes inalámbricas basadas en las especificaciones IEEE 802.11 (especialmente IEEE 802.11b), creado para redes locales inalámbricas, pero también se utiliza para el acceso a internet.

RESUMEN

El Modelo FCAPS (Fault-Fallas, Configuration-Configuración, Accounting-Contabilidad, Performance-Desempeño, Security-Seguridad) de la Organización Internacional de Normalización (ISO, por sus siglas en inglés), es un modelo muy utilizado en empresas y redes de gran envergadura para una mejor gestión de dicha red. Abarca 5 principales áreas vitales para un correcto funcionamiento de dicha red: La Gestión de Fallas, la Gestión de la Configuración, la Gestión de la Contabilidad, la Gestión del Desempeño y la Gestión de la Seguridad. La ISO proporciona para cada área una descripción muy detallada de qué hacer en cada una para lograr una correcta Gestión de Redes.

ABSTRACT

The FCAPS model (Fault, Configuration, Accounting, Performance, Security) of the International Organization for Standardization (ISO, for its acronym in English), is a useful model for companies and networks large for better management of the network. It covers five main areas vital to the proper functioning of the network: The Fault Management, Configuration Management, Accounting Management, Performance Management and Security Management. The ISO provides for each area a very detailed description of what to do in each to ensure efficient network management.

INTRODUCCIÓN

El modelo de FCAPS implementado por la ISO y recomendado por la ITU, es un sistema de gestión de redes muy utilizado actualmente en redes de gran envergadura, desde redes de Mipymes que constan de pocos elementos de red, hasta redes de multinacionales con sedes en varias ciudades del mundo.

FCAPS abarca 5 grandes áreas, que al ser incluidas en éste modelo, son vitales para el correcto funcionamiento de las redes: Fallas, Configuración, Contabilidad, Desempeño y Seguridad.

Cada área se enfoca en actividades referentes a sus funciones, pero no trabajan por separado. Las 5 áreas deben trabajar juntas para poder lograr una excelente gestión de la red

1. INFORME ASPECTOS GENERALES DE LA PRÁCTICA EMPRESARIAL EN LA ALCALDÍA DE ENVIGADO

1.1. ASPECTOS GENERALES DE LA PRÁCTICA.

Nombre de Estudiante	ANDRÉS FELIPE ARROYAVE ARREDONDO
Programa Académico	TECNOLOGÍA EN GESTIÓN DE REDES
Nombre de la Agencia o Centro de Práctica	ALCALDÍA DE ENVIGADO
NIT.	890.907.106-5
Dirección	Carrera 43 A No. 38 sur 30
Teléfono	3394009
Dependencia o Área	Secretaría Administrativa – Dirección de Informática
Nombre Completo del Jefe del estudiante	Felipe José Burgos Ortega
Cargo	Profesional Universitario
Labor que desempeña el estudiante	Soporte Técnico en Redes Administración de la red inalámbrica interna.
Nombre del Asesor de práctica	Luis Felipe Villamizar Torres
Fecha de inicio de la práctica	Lunes, 25 de Febrero de 2013
Fecha de finalización de la práctica	Viernes, 23 de Agosto

Tabla 1 – Aspectos Generales de la Práctica

1.2 CENTRO DE PRÁCTICA.

ALCALDÍA DE ENVIGADO

Misión del Municipio

Nuestra misión es la promoción del desarrollo integral, la sostenibilidad y la competitividad del municipio, con el ánimo de contribuir al mejoramiento de la calidad de vida de la comunidad promocionando la generación de competencias en todos los individuos para que accedan a los beneficios del desarrollo y participen en su planeación y ejecución, mediante el óptimo uso de los recursos, un talento humano altamente calificado y la excelencia en la prestación de servicios.

Visión del Municipio

Nuestra visión consiste en lograr cada vez un mayor impacto social, fortaleciendo la calidad de vida, el civismo, la cultura y la educación de los ciudadanos, generando oportunidades de crecimiento y bienestar, basados en una organización moderna y en un talento humano especializado.

Objetivos de Calidad

- Satisfacer las necesidades de la comunidad envigadeña, mediante la formulación y ejecución del plan de desarrollo para el período de gobierno. (Directriz No. 01 de la Política de Calidad).
- Desarrollar y fortalecer procesos de automatización que faciliten la transparencia, el control, y el mejoramiento continuo con eficacia, eficiencia y efectividad. (Directriz No. 02 de la Política de la Calidad).
- Mejorar las competencias y desempeño del personal de la Administración Municipal. (Directriz No. 03 de la Política de la Calidad).
- Articular el sistema de gestión de la Administración con otros estándares nacionales e internacionales. (Directriz No. 04 de la Política de la Calidad).
- Cumplir con las competencias y normas legales vigentes aplicables al municipio mediante la ejecución del mandato legal de manera permanente. (Directriz No. 05 de la Política de la Calidad).

Estudio Organizacional



Figura 1 – Estudio Organizacional de la Alcaldía de Envigado

1.3. OBJETIVO DE PRÁCTICA

Implementar el área de seguridad del modelo FCAPS en la infraestructura de Red de la Alcaldía de Envigado

- Definir e implantar políticas de seguridad en redes LAN.
- Administración WIFI comunidad e institucional.
- Participación activa en las reuniones que le sean encomendadas
- Entrega de reportes de la información analizada.
- Presentar trabajos mensuales.
- Definir las mejores prácticas de administración de redes.
- Documentar y actualizar los procesos en lo referente a administración de redes.

1.4 JUSTIFICACIÓN

Actualmente, en la Alcaldía de Envigado hay muy poco conocimiento a cerca de la Gestión de redes de telecomunicaciones; en la Institución Universitaria de Envigado se adquirió los conocimientos necesarios para transmitírselos a la Alcaldía por medio de su Dirección de Informática mediante el convenio realizado entre la Alcaldía y la Institución Universitaria para realizar la práctica empresarial. Se pondrá en función de la Dirección de Informática, todos los conocimientos adquiridos para poder suplir esa deficiencia con la que cuenta actualmente la Alcaldía.

2. ESPECIFICACIONES DE ACUERDO CON LA MODALIDAD (ÁMBITO) DE PRÁCTICA

2.1 PLANTEAMIENTO DEL PROBLEMA.

En la Alcaldía de Envigado, no se cuenta actualmente con una correcta Gestión de Redes, la gestión de FCAPS es muy descentralizada, cada área de FCAPS tiene un profesional universitario designado, y éstas áreas no están entrelazadas entre sí, y no va muy de acuerdo al estándar de la ISO, entidad que publica estándares a los que la Alcaldía se quiere acoger.

2.2 EQUIPO DE TRABAJO.



Figura 2 – Equipo de Trabajo de la Dirección de Informática

Se presta el servicio de la práctica en la sección de Redes y Telecomunicación a cargo del Profesional Universitario Felipe Burgos, en el área de Infraestructura bajo la supervisión del Profesional Universitario Alexander Heredia, en la Dirección de Informática de la Alcaldía de Envigado liderada por el Ingeniero Luis Felipe Rosso.

2.3 METODOLOGÍA DE TRABAJO.

Se aplicará la metodología de la retroalimentación en conceptos referentes a la Gestión de Redes y el modelo FCAPS, al igual que entrevistas con los usuarios directos de las aplicaciones y métodos de observación a los profesionales universitarios y técnicos de soporte, para adquirir también conocimiento de ellos.

2.4 RESULTADOS ESPERADOS.

Se espera para el final de la práctica empresarial en la Alcaldía de Envigado tener el área de seguridad del modelo de FCAPS planteada para su posterior evaluación e introducción en la red de la Alcaldía de Envigado.

3. SISTEMATIZACIÓN DE LA INFORMACIÓN DE ACUERDO CON LA MODALIDAD DE LA PRÁCTICA

En la Dirección de Informática, adjunta a la Secretaría Administrativa, de la Alcaldía de Envigado, la práctica empresarial se desarrolló principalmente alrededor de 2 temas centrales: Redes Inalámbricas y soporte técnico en redes.

3.1 Administración de las Redes Inalámbricas Institucional:

Las redes inalámbricas que ofrece la Alcaldía de Envigado se gestionan desde un controladora ARUBA, cuyo acceso remoto se realiza desde la red interna (cableada) de la Alcaldía, accediendo a la dirección: <http://10.1.1.100:4343>, desde donde se administran los 6 Puntos de Acceso (AP por sus siglas en inglés *Access Point*) ubicados en el Hall del Palacio, el Despacho del Señor Alcalde, el Recinto del Concejo Municipal y sus oficinas administrativas, en el Teatro Municipal (Dirección de Informática) y la Secretaría de Tránsito y Transporte; y los 2 AP Groups configurados, 'Palacio' y 'Tránsito'.

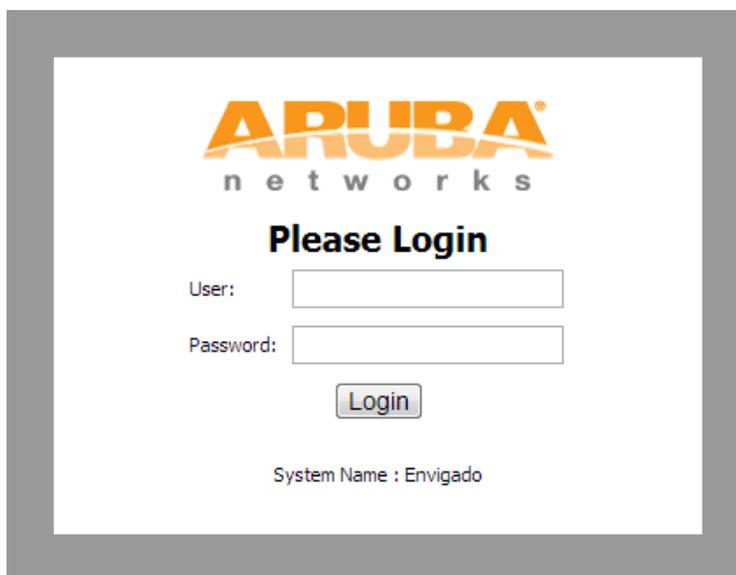


Figura 3 – Página de inicio en el acceso remoto vía web de la Controladora de la red inalámbrica de la Alcaldía de Envigado

Todos los días, y dentro del horario laboral (Lunes a Jueves de 7 am a 12 m y de 2 pm a 6 pm, Viernes de 7 am a 12 m y de 1 pm a 5 pm), se accede a este control remoto vía web de la controladora cada determinado tiempo y se toma fecha, hora, estado de los APs y cantidad de usuarios conectados a los Identificadores configurados del servicio (SSID por sus siglas en inglés *Service Set Identifier*) 'Visitantes' que cuenta con portal cautivo como medida de seguridad, y 'Funcionarios' que cuenta para su acceso de una contraseña de tipo WPA2-PSK.

NÚMERO DE USUARIOS QUE UTILIZAN LAS REDES INALÁMBRICAS DE LA ALCALDÍA DE ENVIGADO			
Fecha	Hora	No. De Usuarios	Estado APs
Lunes, 18 de Marzo	07:00 a.m.	9	up
	09:00 a.m.	24	up
	11:00 a.m.	34	up
	12:00 p.m.	38	up
	03:00 p.m.	35	up
	05:00 p.m.	36	up
	06:00 p.m.	16	up
Martes, 19 de Marzo	11:30 a.m.	37	up
	02:00 p.m.	42	up
	05:00 p.m.	31	up
	06:00 p.m.	15	up
Miércoles, 20 de Marzo	07:30 a.m.	8	up
	09:00 a.m.	30	up
	10:00 a.m.	34	up
	11:00 a.m.	35	up
	02:30 p.m.	31	up
Jueves, 21 de Marzo	07:00 a.m.	4	up
	08:00 a.m.	22	up
	11:00 a.m.	39	up
	02:00 p.m.	33	up
	03:00 p.m.	27	up
	05:00 p.m.	34	up
	06:00 p.m.	22	up
Viernes, 22 de Marzo	09:00 a.m.	33	up
	11:00 a.m.	44	up
	02:00 p.m.	41	up
	04:00 p.m.	39	up
	05:00 p.m.	21	up-Consejo (Recinto y oficinas) falla en ups

Tabla 2 – Tabla de número de Usuarios que utilizan las redes inalámbricas de la Alcaldía de Envigado, semana del 1 de Abril al 5 de Abril del año en curso.

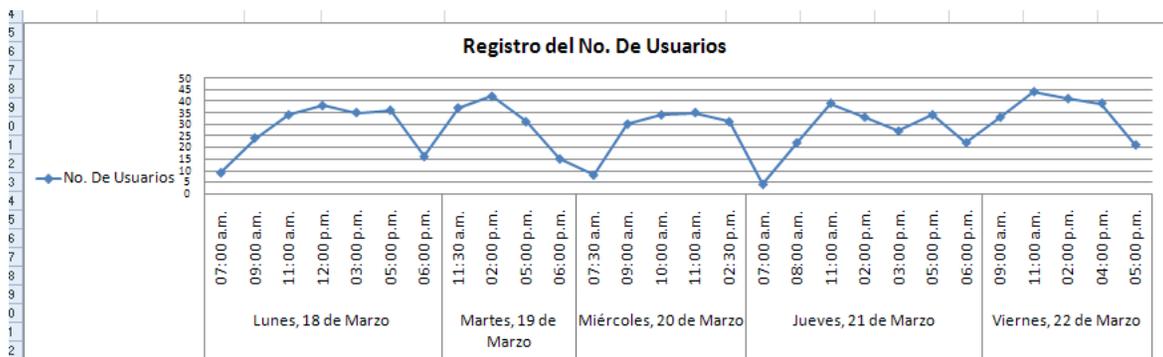


Figura 4 – Grafico de número de Usuarios que utilizan las redes inalámbricas de la Alcaldía de Envigado, semana del 1 de Abril al 5 de Abril del año en curso.

Como se puede apreciar en la Tabla 2 y Figura 4, y al llevar 3 meses tomando el informe (Marzo, Abril y Mayo), la cantidad de usuarios que acceden a las redes inalámbricas de la Alcaldía aumentan al llegar al medio día que son las horas de descanso, y al acercarse el fin de semana. Se puede concluir que los usuarios

utilizan principalmente las redes inalámbricas como “pausas activas” en sus horas de descanso, como por ejemplo escuchar música y accediendo a las redes sociales, que por políticas internas, éstas páginas están bloqueadas por el Fireware.

Mediante el uso de la controladora y su acceso remoto vía web, se recibió una capacitación dictada por un experto en el uso de esta plataforma, donde se aprendió temas como la creación y configuración de VLANs, configuración de los puertos en la controladora, creación de roles, perfiles de “Autenticación, Autorización y Contabilización” (AAA, por sus siglas en inglés *Authentication, Authorization, Accounting*), y AP Groups.

3.2 Soporte Técnico en Redes:

Otro punto que rodea la práctica empresarial es el Soporte Técnico que se presta a la Línea 7000 (Línea de Soporte de la Dirección de Informática), donde se puso al servicio de los compañeros los conocimientos en redes obtenidos en clase, como habilitar un punto de red, que no es más que verificar la existencia de una conexión desde el puesto de trabajo hasta un Patch panel ubicado en un rack y de ahí a un Switch, en el Switch se pedía colaboración al ingeniero Felipe Burgos, encargado de los Switches para la configuración del puerto asignado.

4. PROYECTO DE PRÁCTICA PARA LA AGENCIA O CENTRO DE PRÁCTICAS: IMPLEMENTACIÓN DEL ÁREA DE SEGURIDAD DEL MODELO FCAPS EN LA INFRAESTRUCTURA DE RED DE LA ALCALDÍA DE ENVIGADO

Las redes informáticas han ido evolucionando, y con ellas los riesgos de vulnerabilidad a ataques (de hackers, crackers), debido a esto y a la importancia de la información, las universidades y las organizaciones privadas y del estado han elaborado estrategias que permiten mantener seguras sus redes ante cualquier tipo de ataque que lleve como objeto el acceso a la información restringida.¹

El Modelo FCAPS cubre 5 áreas fundamentales en la Gestión de las redes: Fallas (Fault), Configuración (Configuration), Contabilidad (Accounting), Desempeño (Performance), Seguridad (Security). Fue introducido por la ITU, y es el modelo más recomendado por la ISO para la Gestión de Redes, abarcando los 5 aspectos más importantes que abarca la gestión de redes, donde cada uno de ellos se enfoca en funciones específicas, donde todas, con un correcto funcionamiento, llevan a una red a una gestión plena, y facilitan las funciones de su gestor.

¹ Seguridad en las redes LAN y WLAN de los laboratorios Universidad Minuto de Dios Sede García Herrerros (Girardot). TERREROS Daiver, NÚÑEZ Jorge. Corporación Universitaria Minuto de Dios. Facultad de Ingeniería. Girardot. 2008

Se propone para la Alcaldía de Envigado, la implementación de éste modelo para su infraestructura de red, más específicamente, el área de seguridad, con la definición y la implementación de políticas de seguridad en las redes que hacen parte de la infraestructura de red de la Alcaldía de Envigado.

La propuesta es cubierta por el Ejercicio Profesional de la Ingeniería dado por el Consejo Profesional Nacional de Ingenierías Eléctrica, Mecánica y Profesiones Afines (principalmente Ley 51 de 1986 y el Código de Ética Profesional – Ley 842 de 2003), en especial su artículo 31, que dicta los deberes generales de los profesionales, en su numeral b) *‘Custodiar y cuidar los bienes, valores, documentación e información que por razón de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados’.*

La Seguridad en toda organización es un ítem de vital importancia que no se debe tomar a la ligera. Por eso la Alcaldía, como ente territorial y organización del estado, al manejar información de interés público, debe tomarse la seguridad muy en serio, ya que constantemente puede ser blanco de ataques de personas inescrupulosas y mal intencionadas que quieren hacerse de esa información.

Los envigadeños, al entregarle información que para ellos es privada como números de teléfono, direcciones y números de identificación, desean que la Alcaldía y sus dependencias sean muy celosas con el manejo de esta información, teniendo en cuenta que hay personas ajenas a la Alcaldía y sus dependencias que desean tener acceso a esta información. Esta información debe tener acceso restringido para personas muy interesadas, teniendo en cuenta que los funcionarios autorizados, deben tener discreción con tal información².

Dentro de la propuesta que se hace con ésta práctica empresarial, están unas políticas con las que se propone reforzar todos los sistemas de seguridad con los que cuenta la infraestructura de red de la Alcaldía de Envigado, sistemas entre los que se destacan las Listas de Acceso, las Redes Privadas Virtuales o VPN's para cada dependencia y el hecho de que entre ellas no se pueden visualizar archivos como por ejemplo texto y videos.

El objeto de éstas políticas de seguridad es de brindar un complemento de seguridad a los sistemas ya implementados en éste ámbito en toda la infraestructura de red de la Alcaldía de Envigado.

Se deben tener en cuenta siempre los 3 pilares fundamentales que abarca la Seguridad Informática, como son la Disponibilidad, la Integridad y la Privacidad de la Información que se está manejando. En un Sistema de Información, los datos

²Ley Estatutaria 1266 de 2008. Congreso de la República. República de Colombia. Diciembre 31 de 2008. http://www.secretariassenado.gov.co/senado/basedoc/ley/2008/ley_1266_2008.html

que se manejan de ella, siempre deben contar con éstas características como mínimo.

Indiscutiblemente, una política de seguridad ha de satisfacer la normativa imperante en el país donde se aplica. Además de que se debe tener en cuenta que las políticas a implementar deben ser congruentes con la ley: como por ejemplo los derechos de propiedad intelectual y material.

Precisar una política de seguridad en red representa elaborar técnicas y planes que amparen los recursos de la red contra el daño y la pérdida. Una de las perspectivas posibles para confeccionar dicha política es reconocer lo siguiente:

¿Qué recursos está tratando de proteger? Se tratan de proteger los recursos físicos y lógicos como principalmente los usuarios, los servidores, equipos de cómputo, teléfonos, impresoras, escáneres, faxes, controladora de red inalámbrica, y la información, los datos como tales que se manejan en ellos.

¿De quienes necesita proteger la información? Se necesita proteger los recursos principalmente de personas ajenas y externas a la red, que desean tener acceso a ella y a los datos, la información que es manejada por los usuarios de la Administración Municipal. Igualmente se desea proteger la información de usuarios internos, que desean tener acceso a información restringida para ellos. Ambos usuarios, externo e interno, con fines maliciosos para dicha información.

¿Qué tan posibles son las amenazas? La Alcaldía de Envigado al ser una organización pública y un ente territorial que maneja información sensible y personal de todos los ciudadanos residentes en el Municipio de Envigado y que de una u otra manera guardan alguna relación con él, sobre ésta información recae una amenaza muy latente, tanto por la información que maneja, como lo vital que es para la Administración Municipal el sistema que corre sobre la infraestructura de red, ya que de éste depende su funcionamiento administrativo.

¿Qué tan importante es el recurso? Los recursos que se manejan la administración municipal, físicos y lógicos, son de vital importancia para la administración y su diario y normal trabajar, si la disponibilidad es nula en algún recurso, puede afectar sólo a un usuario, así como puede detener el funcionamiento de toda una dependencia, donde su trabajo es vital para el funcionamiento de otras dependencias.

¿Qué medidas se pueden implementar para proteger sus bienes de una manera económica y segura? Medidas como controles de acceso físicos y lógicos para los usuarios en las aplicaciones y equipos y a los que necesitan acceder debido a las funciones que deben realizar.³

³Introducción a la Seguridad en Internet y Aplicaciones. CONTRERAS Vega; OCHOA Rivera; SOLÍS Muñiz. Universidad Veracruzana - Universidad Autónoma de Chiapas.

4.1 PLANTEAMIENTO DEL PROBLEMA DEL PROYECTO DE PRÁCTICA.

Las organizaciones actuales, cuentan con un ambiente y un carácter cambiante y dinámico que es directamente proporcional a sus propósitos y objetivos. Estas organizaciones deben tener un soporte de red de telecomunicaciones suficientemente resistentes para soportar aquellos cambios que sufre la organización. Sin embargo, estos cambios, en ocasiones afectan negativamente a las redes de telecomunicaciones, generando alteraciones en la red y en los usuarios de tal.

El avance de las tecnologías y equipos tecnológicos es un desafío para las organizaciones, ya que deben estar a la vanguardia, para no poner en riesgo su red y sus equipos, ya sea de robo de información por parte de desconocidos, ruptura de seguridad, como daño en el mismo equipo, por obsoleto.

Al estar a la vanguardia, toda organización debe tener un modelo, donde se gestione la red como tal, donde se tenga, por ejemplo, control de su configuración, control de los fallos, control frente a la seguridad de la red y sus dispositivos. Para esto, la Organización Internacional de Normalización (ISO por sus siglas en inglés, *International Standard Organization*), propuso un modelo, donde están incluidos todos los aspectos claves en la gestión de una red y sus dispositivos. Éste modelo fue llamado FCAPS, por sus siglas en inglés (Fault, Configuration, Accounting, Performance, Security).

Las áreas de fallos, configuración, contabilidad, desempeño y seguridad, áreas que cubre el modelo FCAPS, deben ser de vital importancia para la Alcaldía, de donde deben surgir soluciones y buenas prácticas para una correcta gestión de la red, que le dé un seguimiento a las fallas, guarde back-ups de la configuración, lleve una contabilidad de sus elementos de red, lleve un reporte cada cierto tiempo del desempeño de sus equipos, y mantenga protegida toda la información sensible que maneja la red, además de una compaginar entre estos.

La Alcaldía del Municipio de Envigado, como organización (gubernamental) también debe estar a la vanguardia en los aspectos en el área de Gestión de Redes, ya que al ser una organización que forma parte del estado colombiano, maneja una información muy sensible de los ciudadanos que viven en el Municipio de Envigado, como por ejemplo teléfonos, direcciones y estratos sociales; que son necesarias para su funcionamiento, pero que a la vez, las personas de las que habla dicha información, son muy celosas con el manejo de esta.

4.2 JUSTIFICACIÓN DEL PROYECTO DE PRÁCTICA.

El informe de la Práctica Empresarial es de importancia para la Alcaldía de Envigado, por cuanto se implementará un modelo que pondrá a la Alcaldía del Municipio como organización a la vanguardia en el uso de tecnologías de punta, obteniendo como mejor resultado aumento de la seguridad, en el acceso a la

información y recuperación ante fallos, además de fortalecer la estrategia de inteligencia en negocios, un modelo de gestión de redes.

Algo muy latente en las redes de telecomunicaciones es el riesgo a sufrir fallas y ataques informáticos, lo que obliga a las organizaciones a estar a la vanguardia en temas de seguridad. Este informe además de tener implicaciones prácticas y reales, la Alcaldía y su Dirección de Informática, puede tomar medidas y presentar alternativas para mejorar las situaciones que se presenten en la red. Además, en cuanto a utilidad metodológica, es de importancia, ya que se crea un instrumento para aplicar en las infraestructuras de red y que sirve como referencia para trabajos futuros.

4.3 OBJETIVOS DEL PROYECTO DE PRÁCTICA (OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS).

Objetivo General: Proponer un modelo de Gestión de Redes basado en el área de seguridad del modelo FCAPS para la Alcaldía de Envigado.

Objetivos Específicos:

1. Analizar documentación existente acerca de FCAPS y su área de seguridad.
2. Registrar el conocimiento encontrado acerca de FCAPS.
3. Diseñar un plan de Seguridad del modelo FCAPS para la Alcaldía de Envigado.
4. Determinar un plan de seguridad para la Infraestructura de Red de la Alcaldía de Envigado.

4.4 DISEÑO METODOLÓGICO DEL PROYECTO DE PRÁCTICA.

La Unión Internacional de Telecomunicaciones, en su “Serie M: RGT y Mantenimiento de Redes: Sistemas de Transición, Circuitos Telefónicos, Telegrafía, Facsímil y Circuitos arrendados internacionales. Red de Gestión de Telecomunicaciones, Principios para una red de gestión de las telecomunicaciones. (Recomendación UIT-T M.3010)”, especifica que *hasta la fecha han sido identificadas las cinco áreas funcionadas de gestión*, áreas que en el mundo de la gestión de redes es reconocida por medio de las siglas FCAPS.

John Jairo Yúnez, en sus memorias de clase en la Institución Universitaria de Envigado, asegura que *la gestión de redes permite asegurar que la red opera eficientemente en todo momento, evitando problemas en las operaciones de los clientes*. Igualmente, José Rodríguez, basado en la “Introducción a la Gestión de Redes” de Carlos Vicente de la Universidad de Oregon, nos habla de una gestión de redes con muchos aspectos a cubrir, pero lo expresa de una manera amena, Vicente y Rodríguez presentan la gestión de redes como un proceso largo pero práctico y sencillo, que si se lleva correctamente, puede llegar a simplificar y favorecer el trabajo de un gestor de redes.

Alexander Clemm, en la guía de Cisco 'Network Management Fundamentals' define a FCAPS como e ABC de la Gestión. Cuando se habla del ABC de un objeto, se habla de que es una guía básica y de vital importancia para el tema a tratar. FCAPS, en efecto, es una guía a seguir que trata los temas más básicos pero igualmente vitales en lo que se refiere a la Gestión de Redes. El Doctor Peter J. Welcher en su 'Network Management Best Practices', cree por el contrario que mayoritariamente FCAPS es un modelo de cultura, una cultura no solo para el usuario, si no para el gestor de la red, quien debe llevar una cultura sana en lo que le compete como gestor, y que además la gestión de redes son todos los medios, todos los procesos que se realizan el gestor para *encargarse* de la red.

Antoni Barba en su 'gestión de red', habla de un modelo funcional basado en la recomendación de la ISO. Si bien el modelo FCAPS es un modelo presentado por la ISO, habla de un conjunto general de modelos, todos recomendados por la ISO, dándole, al parecer, un puesto privilegiado a FCAPS, mencionándolo en primer lugar en la lista de modelos mencionados por el propio autor, reconociendo que FCAPS es el más completo y complejo modelo que abarca de manera sencilla todos los aspectos que debe tener una gestión de redes.

Robbie Harrell, en la E-Guide de SearchNetworking.com "Network Management Fundamentals" define brevemente el modelo FCAPS como un *modelo categórico de objetivos de trabajo de gestión de redes*. Mientras que Guadalupe Orozco, en su monografía "La gestión de grandes redes y uso de OSPF", lo detalla como una herramienta *que permite controlar y monitorear todos y cada uno de los diversos aspectos inmersos en la gestión de redes*. Como se puede notar, cada autor trata de exponer su punto de vista de FCAPS, para unos, como Harrell es un '*modelo categórico*', teniendo en cuenta que un modelo se puede tomar como una plantilla para realizar algo, y Orozco lo toma ya como una '*herramienta*', dándole ya una utilidad más específica.

Pankaj Goyal, Rao Mikkilineni y Murthy Ganti en su artículo presentado en el año 2009 en la 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, concluyen que *en la práctica, algunos elementos del modelo FCAPS se han aplicado más ampliamente que en otros sistemas de gestión coordinadas. En general, las empresas aplican FCAPS de fallos y problemas de configuración. La función de seguridad ha dependido de otras herramientas que no están integradas al modelo general FCAPS. Esto es lamentable, porque los problemas de fallos, configuración y rendimiento pueden ser en realidad un problema de seguridad en el encubrimiento. Del mismo modo, los patrones de tráfico inusuales capturados por la gestión de contabilidad pueden indicar un problema de seguridad. Y finalizan sabiamente diciendo "La conclusión es que, aunque hay cinco elementos a FCAPS, un elemento puede influir en el éxito de otro elemento"*.

4.5. CRONOGRAMA DE ACTIVIDADES DEL PROYECTO DE PRÁCTICA.

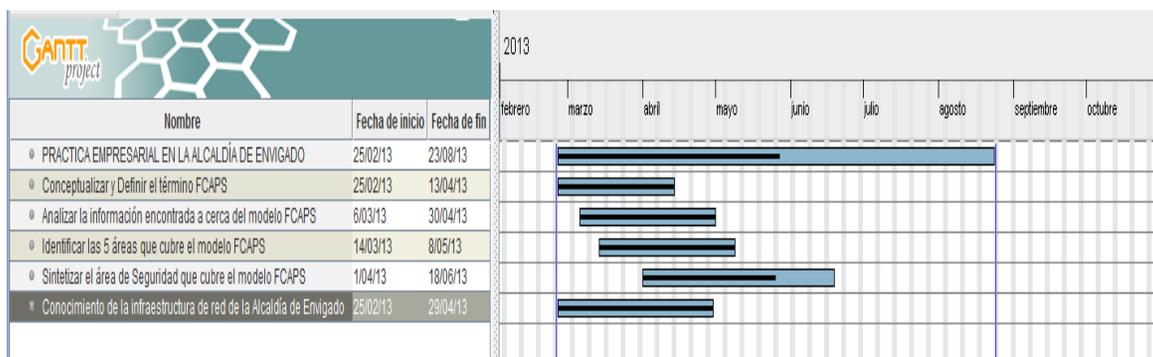


Figura 5 – Cronograma de Actividades

4.6 PRESUPUESTO (FICHA DE PRESUPUESTO) DEL PROYECTO DE PRÁCTICA

A continuación se presentan unas tablas descriptivas, explicando el uso del presupuesto inicial y la especificación de cada gasto durante la ejecución del proyecto.

PRESUPUESTO GLOBAL DEL TRABAJO DE GRADO				
RUBROS	FUENTES			TOTAL
	Estudiantes	IUE	Alcaldía de Envigado	
Personal	--	960.000	--	960.000
Material y suministros	15.000	--	7.500	22.500
Salidas de campo	76.800	--	--	76.800
Bibliografía	--	--	--	0
Equipos	1'500.000	--	1'500.000	3'000.000
Otros	1'500.000	--	4'000.000	5'500.000
TOTAL	3'091.800	960.000	5'507.500	9'559.300

Tabla 3 - Presupuesto Global del Proyecto "Implementación del Área de Seguridad del Modelo FCAPS en la Infraestructura de Red de la Alcaldía del Municipio de Envigado".

DESCRIPCIÓN DE LOS GASTOS PERSONALES.						
NOMBRE DEL PERSONAL	FUNCIÓN EN EL PROYECTO	DEDICACIÓN MESES	FUENTES			TOTAL
			Estudiantes	IUE	Alcaldía de Envigado	
ANDRÉS FELIPE ARROYAVE ARREDONDO	Autor – Practicante	6 meses	0	0	--	0
LUIS FELIPE VILLAMIZAR TORRES	Asesor	3 meses	0	960.000		
TOTAL	--	--	0	960.000	0	960.000

Tabla 4 – Descripción Gastos Personales “Implementación del Área de Seguridad del Modelo FCAPS en la Infraestructura de Red de la Alcaldía del Municipio de Envigado”

DESCRIPCIÓN DE MATERIALES Y SUMINISTROS				
MATERIAL	FUENTES			TOTAL
	ESTUDIANTES	IUE	Alcaldía de Envigado	
Papelería	15000	--	--	15000
Tinta	0	--	--	0
CD	3000	--	--	3000
TOTAL	18000	0	0	18000

Tabla 5 - Descripción Gastos de Materiales y Suministros “Implementación del Área de Seguridad del Modelo FCAPS en la Infraestructura de Red de la Alcaldía del Municipio de Envigado”

DESCRIPCIÓN EQUIPOS				
DESCRIPCIÓN EQUIPOS	FUENTES			TOTAL
	ESTUDIANTES	IUE	Alcaldía de Envigado	
Computador HP Pavilion Slimline.	1'500000	--	--	1'500000
Computador COMPAQ Presario PC	--	--	1'200000	1'200000
TOTAL	1'500000	0	1'200000	2'700000

Tabla 6 – Descripción Gastos de Equipo “Implementación del Área de Seguridad del Modelo FCAPS en la Infraestructura de Red de la Alcaldía del Municipio de Envigado”

DESCRIPCIÓN OTROS				
DESCRIPCIÓN OTROS	FUENTES			TOTAL
	ESTUDIANTES	IUE	Alcaldía de Envigado	
Servicios Públicos	1'500000	--	4'000000	5'500000
TOTAL	1'500000	0	4'000000	5'500000

Tabla 7 – Descripción Gastos de Otros “Implementación del Área de Seguridad del Modelo FCAPS en la Infraestructura de Red de la Alcaldía del Municipio de Envigado”

5. DESARROLLO DEL PROYECTO DE PRÁCTICA: IMPLEMENTACIÓN DEL ÁREA DE SEGURIDAD DEL MODELO FCAPS EN LA INFRAESTRUCTURA DE RED DE LA ALCALDÍA DE ENVIGADO

5.1. Analizar documentación existente acerca de FCAPS y su área de seguridad

Se analiza y clasifica como relevante e irrelevante, toda información de FCAPS y seguridad encontrada en la web. La relevante, se detalla en las referencias bibliográficas.

5.2. Registrar el conocimiento acerca de FCAPS

Se registra en un documento, que se puede encontrar en Anexos.

5.3. Diseñar un plan de seguridad del modelo FCAPS

Basándose en el conocimiento analizado, clasificado y registrador, se diseña un plan de seguridad según el modelo FCAPS publicado por la ISO.

5.4. Determinar un plan de seguridad para la Infraestructura de Red de la Alcaldía de Envigado

Se define un plan, acorde a FCAPS, para la Infraestructura de Red de la Alcaldía de Envigado

6. INCONVENIENTES EN EL DESARROLLO DE LA PRÁCTICA

Un suceso que se presentó durante el desarrollo de la práctica, pero no fue un inconveniente en ésta, fue la lentitud en la firma del Convenio de Prácticas por ambas partes, la Secretaría Administrativa de la Alcaldía de Envigado y la Institución Universitaria de Envigado. La Práctica Empresarial que se realizó en la Dirección de Informática de la Alcaldía de Envigado, adjunta a la Secretaría Administrativa, se inició el 25 de Febrero del año en curso, y el día 9 de Mayo se entregó a la Oficina de Jurídica de la Institución Universitaria de Envigado, debido a que una de las personas firmantes por parte de la Institución se encontraba incapacitada por un tiempo aproximado de un mes, lo que demoró un poco la firma del mencionado convenio.

Por momentos, un inconveniente en la realización de la práctica, fue la disponibilidad de equipos de cómputo en la oficina para realizar la redacción de los Informes Inicial y Final de la Práctica, debido a que los equipos se encontraban ocupados por los técnicos realizando sus propios deberes. De igual modo se respetaba ese momento en que los compañeros tenían en uso los equipos, y no se ocupaba hasta que ellos terminaran sus deberes, ya que ellos se encuentran menos tiempo en la oficina en comparación del practicante.

7. CONCLUSIONES

El Informe Final de Práctica se finaliza con un nuevo aprendizaje en lo que respecta a conocimientos de FCAPS y Seguridad en Redes de Telecomunicaciones, adquirido mediante consultas a compañeros de la Dirección de Informática y a páginas web con una dedicación y concentración que dieron al informe un feliz término.

El desarrollo del informe de práctica estuvo enmarcado de la adquisición de nuevos conocimientos y revisión de conocimiento ya adquirido en el tema que trata este informe, mejorando la disciplina del practicante para realizar una actividad específica, como también el compromiso y la responsabilidad para la presentación de informes y en general en puntualidad en temática relacionada.

8. RECOMENDACIONES

La Gestión de Redes, con el tiempo se ha ido convirtiendo en un área en todas las empresas de vital importancia, debido al crecimiento de sus redes internas y al crecimiento de las redes externas como el internet y todos sus servicios, aumentando también la cantidad de fallas que se presente en la red, el aumento de elementos de red, lo cual conlleva a un aumento de configuraciones, aumento del tráfico de la red, el aumento del consumo de recursos y de software y hardware que quiere atentar contra dicha red.

Estos aumentos son vigilados por un modelo que integra todos estos aumentos, monitoreándolos constantemente para el bienestar de la red.

Verdaderamente, el modelo FCAPS es el soporte que pueden tener tanto las grandes empresas como las Mipymes, ya que es un formato de gestión de redes muy versátil respecto a la red que se quiera gestionar.

Es un modelo versátil, ya que la red no siempre va a estar en un estado 'estable', siempre va estar bajo algún ataque, por ella va cruzar constantemente un tráfico propenso a colisiones de paquetes, y el modelo siempre se va a adaptar a estos cambios y tratará de devolverle ese estado de estabilidad a la red.

REFERENCIAS BIBLIOGRÁFICAS

BARBA, Antoni. Gestión de red. Edicions de la Universitat Politècnica de Catalunya, SL. Primera edición. CBS – Impressió digital. Barcelona, España. 1999.

BUSTAMANTE, Rubén. Seguridad en Redes. Monografía. Ingeniero en Electrónica y Telecomunicaciones. Estado Libre y Soberano de Hidalgo, México. Universidad Autónoma del Estado de Hidalgo.

ESCOBAR, John Jairo. 02-Generalidades de la gestión. [Diapositivas]. Envigado. Gestión de Redes de Telecomunicaciones. Institución Universitaria de Envigado. 2011

GOYAL, MIKKILINENI y GANTI. FCAPS in the Business Services Fabric Model. En: 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises. 2009

HARRELL Robbie. Network Management Fundamentals. SearchNetworking.com

INTERNATIONAL TELECOMMUNICATION UNION – TELECOMMUNICATION STANDARDIZATION SECTOR. SERIE M: RGT y Mantenimiento de Serie M: RGT y Mantenimiento de Redes: Sistemas de Transición, Circuitos Telefónicos, Telegrafía, Facsímil y Circuitos arrendados internacionales. Red de Gestión de Telecomunicaciones, Principio para una red de gestión de las telecomunicaciones. Recomendación UIT-T M.3010. Ginebra, Suiza, 2000. 9 p.

SARABIA, Guadalupe. La gestión de grandes redes y uso de OSPF. Monografía. Licenciada en Sistemas Computacionales Administrativos. Xalapa-Enriquez, Veracruz. Universidad Veracruzana. Facultad de Contaduría y Administración. 33 p.

TERREROS, Daiver y NULEZ Jorge, Seguridad en las Redes LAN y WLAN de los Laboratorios Universidad Minuto de Dios Sede García Herreros (Girardot). Proyecto. Tecnólogo en Redes de Computadores y Seguridad Informática. Girardot, Cundinamarca. Corporación Universitaria Minuto de Dios. Facultad de ingeniería. 2008

UNTIVEROS, Sergio. Metodologías para Administrar Redes. AprendeRedes.com

VICENTE, Carlos. Introducción a la Gestión de Redes. [Diapositivas]. Universidad de Oregon.

ANEXO A. Documentación recogida a cerca de FCAPS

Las Áreas Funcionales de Gestión

La ISO clasifica las tareas de los sistemas de gestión en cinco áreas funcionales:

- Gestión de Configuración.
- Gestión de Prestaciones.
- Gestión de Seguridad.
- Gestión de Fallos.
- Gestión de Contabilidad

FCAPS

Es el modelo y framework de red de gestión de telecomunicaciones de ISO para la gestión de redes. FCAPS es un acrónimo de Fault, Configuration, Accounting, Performance, Security (Falla, Configuración, Contabilidad, Desempeño, Seguridad) que son las categorías en las cuales el modelo ISO define las tareas de gestión de redes. En algunas redes Contabilidad se reemplaza con Administración

Fault Management & Real Time Monitoring, Detección de problemas en tiempo real en redes, servidores, aplicación, segmentos y enlaces, para que posterior a su detección se realizar un análisis detallado de las posibles causas.

Configuration, Automatización de los procesos de configuración y control de la operación de la red. Los cambios de hardware y software, incluyendo la inserción de equipos y programas, modificaciones a los programas existentes, remoción de programas y sistemas obsoletos, entre otros.

Accounting, Contabilizar los recursos de red y a su vez de TI (Hardware y Software).Procesos como inventario del equipamiento y sus programas de forma automatizada.

Performance, Monitorear el desempeño de elementos como; la infraestructura de red, aplicaciones y comunicaciones LAN, WAN y HighSpeed. Mediante históricos y tendencias es posible el detectar problemas como cuellos de botella y los problemas potenciales se identifican mediante un veraz “capacity planning”. Una parte considerable de los esfuerzos en este nivel se enfocan en identificar las mejoras que puedan dar paso a optimizar el desempeño de la red, aplicaciones así como de los sistemas más críticos. Permitiendo detectar fallas de forma pre-activa, eliminando los problemas potenciales y así alcanzar los SLA's.

Security la red y todos los elementos conectados a la misma deben ser protegidos contra la acción de los hackers, usuarios no autorizados así como de sabotaje físico y/o electrónico. La confidencialidad de la información debe ser

garantizada mediante reglas, políticas y sistemas de seguridad como Firewalls, IDS, HIDS y NIDS.

La **F** en **FCAPS** discute las áreas de administración asociadas con la administración de fallas. Doce tareas de administración son identificadas en el modelo FCAPS como necesarias para un sistema de "fault management":

- Detección de falla.
- Corrección de falla.
- Aislamiento de la falla.
- Recuperación de la red.
- Manejo de alarmas.
- Filtrado de alarmas.
- Generación de alarmas.
- Borrado de correlación.
- Pruebas de diagnóstico.
- Error de registros.
- Manejo de errores.
- Estadísticas de errores.

Configuration Management

Es el concepto de asegurar una consistencia, repetición, y auditable configuración en todos los equipos de la red, basados en una política de configuración. Considera las siguientes tareas de administración:

- Recursos de inicialización.
- Aprovisionamiento de red.
- Auto-descubrimiento.
- Copia de seguridad y restauración.
- Shut down de recursos.
- Gestión del cambio.
- Pre-provisión.
- Inventario/gestión de activos.
- Copia de configuración.
- Configuración remota.
- Automatización de distribución de software.
- Iniciación de Job, tracking, y ejecución.

Accounting Management (contabilidad de gestión)

La siguiente lista destaca las ocho consideraciones para las herramientas que permiten a la contabilidad de gestión:

- Realizar un seguimiento de servicio o el uso de los recursos.
- Costo de los servicios.
- Contabilidad límite.
- Uso de las cuotas.
- Auditorías.
- Reporte de Fraudes.

- Combine los costos de múltiples recursos.
- Apoyo a diferentes modos de Gestión del Rendimiento.

Performance Management

Gestión del rendimiento implica la vigilancia efectiva del tiempo de respuesta de la gestión proactiva de las actualizaciones necesarias para apoyar a sus usuarios. Cuando se mira un sistema de gestión del rendimiento, se buscan los siguientes rasgos:

- Utilización y tasas de error.
- El performance y recolección de datos.
- Niveles consistente de performance.
- Realización de análisis de datos.
- Reporte de problemas.
- Capacidad de planificación.
- Generación de informes de rendimiento.
- Mantener y examinar los registros históricos.

Security Management (Gestión de la Seguridad)

Considere las siguientes actividades fundamentales para un eficaz sistema de gestión de seguridad:

- Acceso restrictivo a los recursos
- Registros de acceso
- Protección de datos
- Control de los derechos de acceso de usuario
- Seguridad de auditoría de registro
- Seguridad de alarma / Reporte de eventos
- Tenga cuidado de las violaciones de la seguridad y los intentos
- Seguridad de información relacionada con las distribuciones

Varias organizaciones han centrado su atención en el área de la gestión de Red y han reconocido la necesidad de desarrollar arquitecturas de gestión y fundamentalmente la necesidad de la estandarización en esta área buscando la interoperabilidad entre las diferentes soluciones. La ISO (Organización Internacional de Estandarización) a través de uno de sus grupos de trabajo agrupa las actividades de gestión (OSI Management) dentro de cinco áreas funcionales, comúnmente referenciadas por sus siglas en ingles (FCAPS):

- **Gestión de Fallos (Fault Management):** Comprende el conjunto de actividades que permiten la detección, aislamiento y corrección de operaciones anormales. Entre sus funciones se encuentran las de detectar fallas, aceptar y actuar ante notificaciones de error, ejecutar pruebas diagnósticas, etc.
- **Gestión de Configuración (Configuration Management):** Incluye registrar la configuración actual de los elementos de la red así como

efectuar cambios en la configuración e identificar los elementos de la red (asignarles nombres, direcciones, etc.)

- **Gestión de Contabilidad (Accounting Management):** Actividades que permiten que se establezcan tasas y se identifiquen costos relacionados con el uso de los elementos que conforman la red, permite además imponer límites de costos e informar a los diferentes usuarios de los costos en que incurrir.
- **Gestión de Rendimiento (Performance Management):** Actividades encaminadas a la detección de cambios en el rendimiento de la red, recolectando datos que pueden ser utilizados por otras áreas funcionales.
- **Gestión de Seguridad (Security Management):** Actividades relacionadas con asegurar la red de un comportamiento incorrecto de los usuarios, accesos no autorizados, etc.

Varios son los factores que indican los beneficios que aporta la actividad de la gestión de redes para la empresa, esos factores se derivan de los propios objetivos de la actividad:

- **Control de los recursos estratégicos corporativos.** Como se ha mencionado anteriormente, las computadoras y las redes de computadoras constituyen en la actualidad recursos vitales; sin un control adecuado éstos recursos no son capaces de aportar un beneficio real a la empresa.
- **Disminución de los tiempos de inactividad.** Los tiempos de inactividad (por fallas, bajo rendimiento, etc.) en una empresa que ha informatizado sus procesos puede traer consigo consecuencias negativas desde el punto de vista financiero, viéndose afectada la calidad de los productos y servicios que brinda. La gestión de redes juega un rol importante en el mantenimiento de la disponibilidad de los elementos que conforman la red.
- **Control de los costos.** Contribuye a que las necesidades esenciales de los usuarios finales puedan ser satisfechas a un costo razonable.

1.2.1. ADMINISTRACIÓN OSI

Este modelo posee arquitecturas para definir sus características y son las siguientes:

1.2.1.1. Arquitectura Funcional

Define una serie de funciones descritas en la norma ITU-M.3400 llamadas Áreas Funcionales de los Sistemas de Gestión o SMFA (Systems Management Functional Areas)³, más comúnmente conocido por FCAPS (Fault, Configuration, Accounting, Performance, Security).

Aquí las tareas de administración son separadas en cinco categorías permitiendo una mejor organización. No requiere de la implementación de algún protocolo en específico, sin embargo SNMP y CMIP son los más comúnmente utilizados.

1.2.1.1.1. Gestión de Fallas

Una falla es un evento perjudicial que causa la anormalidad de un servicio y perjudica el rendimiento de la red, por lo que su detección y corrección inmediata son indispensables.

Su objetivo es reconocer, aislar, corregir y registrar los problemas que ocurren en la red, un monitoreo continuo, el establecimiento de alarmas y un análisis de tendencias que permitan predecir posibles errores garantizando la disponibilidad de la red y notificando de manera automática al administrador cuando exista algún problema.

El procedimiento para el manejo de fallas se puede establecer como el siguiente:

- Monitoreo continuo de componentes de red.
- Identificación exacta de la ubicación de la falla.
- Aislamiento de la falla para que la red opere sin interferencia.
- Reacción ante la falla estableciendo acciones para su resolución.
- Asignar los recursos suficientes para su resolución.
- Proveer una solución (probar en todos los subsistemas importantes y grabar esta solución para una futura referencia).
- Notificación, creación de reportes de estado y seguimiento de la reparación.

1.2.1.1.2. Gestión de Configuración

Proceso mediante el cual se inicializa, identifica, configura y se controla las operaciones diarias de los dispositivos que conforman la red. Su objetivo radica en obtener información para establecer ajustes y modificaciones de configuración tanto de hardware como software, nuevos elementos, modificaciones de sistemas existentes, eliminación de componentes obsoletos, generación de reportes y gestión de cambios dentro de la red.

Involucra también el entendimiento del contexto en el cual un dispositivo particular está operando, de los sistemas que trabajan en conjunto y el efecto que causa un sistema en otro. Se incluyen detalles de la topología de la red y un mapa físico de la misma.

En esta gestión se debe tener en cuenta los siguientes aspectos:

- Un acceso rápido a la información sobre configuraciones.
- Un inventario continuamente actualizado de los elementos de la red y de la configuración de los recursos.
- Facilidad en el acceso remoto a los dispositivos.
- Simplificación de la configuración de los equipos.

1.2.1.1.3. Gestión de Análisis de datos (Accounting)

Proceso de recolección de información proveniente de los recursos utilizados, desde equipos de interconexión hasta usuarios finales.

Se realiza con el fin de obtener los cobros correspondientes a los clientes del servicio mediante tarifas establecidas. Este proceso, también llamado tarificación es muy común en ISPs. Además permite obtener el tiempo que un administrador gasta ayudando a individuos o departamentos particulares.

Otros propósitos de Accounting son el analizar el tráfico, visualizar el porcentaje de utilización de la red globalmente o en forma individual de los diferentes dispositivos, lo que permite administrar los recursos y facilitar el planeamiento de capacidad de la red.

1.2.1.1.4. Gestión de Rendimiento

Provee información del desempeño y de la calidad del funcionamiento de la red actual, recolecta y analiza datos de rendimiento con el fin de asegurar que las prestaciones estén acorde con las necesidades de los usuarios.

La recolección de información permite establecer un historial estadístico de sucesos, permitiendo tomar medidas preventivas y correctivas ante posibles puntos conflictivos que degraden la calidad de los servicios prestados.

Umbral de rendimiento son utilizados para el manejo de alarmas, habitualmente realizado por la gestión de fallas, otorga un nivel de severidad en función de la falla encontrada. Entre los parámetros que se analizan y controlan están: rendimiento, utilización, tráfico, tasa de error, tiempo de respuesta, cuellos de botella, latencia, entre otros.

1.2.1.1.5. Gestión de Seguridad

Proceso mediante el cual se controla el acceso a los recursos de la red y se protege la información para evitar alteraciones de cualquier índole. Puede ser conseguida mediante la implantación de controles, políticas, procedimientos o funciones de software, dividiendo a los recursos dentro de áreas autorizadas y no autorizadas.

La gestión de seguridad se ocupa de los siguientes puntos:

- Identificación de la información que se quiere proteger y su ubicación.
- Identificación de los puntos de acceso a la información.
- Protección y mantenimiento de los puntos de acceso a la información.

ANEXO B. Apartes de la Resolución N° 2990 DE 2011. Alcaldía de Envigado.



ALCALDÍA DE ENVIGADO
AVANCEMOS con toda SEGURIDAD

Secretaría Administrativa

RESOLUCION N° 2990 (31 de agosto de 2011)

"Por medio de la cual se reglamenta el uso de la Tecnología y los Software Implantadas en el Municipio de Envigado"

EL ALCALDE MUNICIPAL DE ENVIGADO, en uso de sus facultades constitucionales y legales, en especial las conferidas por la ley 603 de 2000 y

CONSIDERANDO:

- A. Que mediante Resolución 1669 del 6 de Mayo de 2010, se reglamentó el uso de la Tecnología y los Software Implantados para el Municipio de Envigado.
- B. Que toda entidad oficial, debe darle cumplimiento a la Ley 603 de 2000, por medio de la cual se reglamentan los derechos de autor y la propiedad intelectual.
- C. Que de acuerdo con las exigencias del entorno, temas de seguridad Informática, nuevas tecnologías y renovación tecnológica, es necesario reglamentar el uso de la tecnología y software Implantados en el Municipio de Envigado.
- D. Que es necesario preservar íntegra y veraz la Información del Municipio de Envigado, con estrategias de seguridad que ayuden a conservarla.
- E. Que dicha resolución establecía las siguientes políticas: Usuario de la Información, uso de contraseñas y acceso a Windows, manejo de la Información, novedades de personal, secretarios de despacho e Interventores, mesa de ayuda, uso de hardware y software, copias de seguridad y almacenamiento, traslado de equipos y elementos tecnológicos, instalación de periféricos, control de virus, uso de Internet y correo electrónico, seguridad en la red de datos, acceso área de servidores, compra de equipos de cómputo, apagado de equipos, cierre de sesiones y otras disposiciones, escala de faltas y sanciones.
- F. Que la Alcaldía Municipal y la Secretaría Administrativa a través de la Dirección de Informática, establecen las nuevas políticas para el uso de tecnología y software, y

RESUELVEN:

- ARTÍCULO 1°:** Actualizar la resolución que existe actualmente sobre la reglamentación del uso de la tecnología y software Implantados en el Municipio de Envigado.
- ARTÍCULO 2°:** Dar cumplimiento a la Ley 603 de 2000, por medio de la cual se regulan los derechos de autor y la propiedad intelectual y se asume el compromiso de la legalidad del software en todas las áreas y servicios de la Institución.
- ARTÍCULO 3°:** Preservar íntegra y veraz la Información, a través del buen uso en temas de seguridad informática, exigencias del entorno, nuevas tecnologías y renovación tecnológica.
- ARTÍCULO 4°:** Establecer como nuevas políticas, para el uso de la tecnología y el software en el municipio de Envigado, las siguientes:

10. INTERNET Y CORREO ELECTRÓNICO

La Entidad suministra a sus funcionarios y contratistas, el acceso a Internet y el uso de un correo electrónico que se encuentra asociado al usuario de red, como herramienta para el uso exclusivo de sus funciones laborales.

Cada usuario tiene la responsabilidad de utilizarlos de una manera productiva para sus funciones dentro de la Administración, por eso:

- a. El usuario recibirá capacitación en el manejo de las carpetas personales (PST) para la administración de los correos tanto entrantes como salientes que desee conservar y que serán almacenados en el disco duro del equipo de trabajo.
- b. El almacenamiento máximo en el servidor de correo manejará los siguientes tamaños:
General 80Mb
Directivos 100Mb.
- c. Se podrán enviar mensajes que no superen el tamaño de 10MB
- d. Se permitirán en envío de correo con archivos adjuntos con las siguientes extensiones: comprimidos con contraseña (ZIP, RAR, ARJ), JPG, JPEG, GIF, BMP, TIF, XLS, DOC, PPT.
- e. Las cuentas de correo son de carácter personal e intransferible.
- f. El correo electrónico se utilizará únicamente para el intercambio de información corporativa. Este medio no se utilizará para el envío de videos, cadenas, chistes, música, así como tampoco para ofrecer servicios personales como ventas, arrendamiento, clasificados, y demás contenidos no laborales.
- g. Se prohíbe transmitir información cuyo contenido sea ilegal, peligroso, invasor del derecho a la privacidad, pornográfico, ofensivo a terceros o violatorio de derechos de autor, marcas o patentes.
- h. Cuando se trate de alguna fecha especial, la Oficina de Comunicaciones será la única encargada de enviar masivamente los textos de conmemoración o felicitaciones a través del correo corporativo.
- i. No se permite utilizar el correo electrónico, la publicación Web o cualquier otro medio de difusión electrónica de la información para realizar manifestaciones o adquirir compromisos en nombre de la Administración Municipal sin tener la competencia o autorización para ello.
- j. Es responsabilidad de los usuarios de correo electrónico el depurar periódicamente la información.
- k. Se suspenderá el servicio de correo electrónico a los funcionarios que no hagan uso del servicio por más de dos (2) meses, lo mismo que aquellos que sean desvinculados de la entidad.
- l. Prohibido suplantar a otra persona a través del correo electrónico, hacer declaraciones falsas, falsificar la identidad de alguna persona en los encabezados de los mensajes.
- m. Es responsabilidad de la Dirección de Informática la administración y control del correo electrónico.
- n. Está prohibido el ingreso de correos electrónicos con archivos de video (AVI, MPEG, WMV, ASF, FLV), de audio (MP3, WMA, MIDI, MP4), ejecutables (EXE, INI, COM, VBS), librerías del sistema (DLL), archivos de bases de datos (MDB), entre otros.
- o. Está prohibido ingresar a sitios como: páginas de contenido pornográfico, emisoras de radio y televisión, páginas de videos y películas online, redes sociales (Facebook, Twitter, y otros), mensajería instantánea (chat en Hotmail, Gmail, Yahoo, y otras), o cualquier otro sitio que coloque en riesgo la seguridad de la información de la Institución o de sus funcionarios.

Las personas que por sus funciones necesitan tener habilitado estos servicios deben de tener autorización de su jefe inmediato mediante el diligenciamiento de la "Plantilla sobre creación de usuarios de red, correo, Internet, Intranet y aplicaciones".

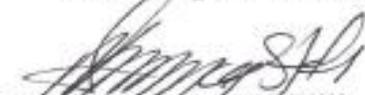
- d. La responsabilidad, el diseño de la hoja de estilo y del diseño gráfico de la página estará a cargo de Oficina Asesora de Comunicaciones que contará con el apoyo de la Dirección de Informática.
- e. Las Directrices del diseño obedecerán a requerimientos de las entidades públicas del orden nacional y departamental con las competencias que les otorgan la Constitución y la Ley.
- f. Todas las Dependencias de la Administración acogerán el diseño que para tal fin apruebe el Comité de Gobierno en Línea, encargado de atender las necesidades de publicación y comunicación de tipo Institucional de la Administración. Así mismo, para un mayor Impacto, guardará un orden lógico que servirá para un mayor entendimiento por parte de la ciudadanía, de acuerdo con las disposiciones del Comité.
- g. Existirá solo un Portal Web Institucional para la Administración Central Municipal que contendrá el que hacer de la entidad.
- h. La contratación de servicios externos para el diseño de éste Portal Web Institucional solo estará a cargo de la Dirección de Informática.
- i. Será responsabilidad de cada dependencia mantener actualizado el contenido de la Información de su competencia, para ello la Dirección de Informática reportará a cada una, sus responsabilidades de actualización permanente en el Portal.
- j. De conformidad con nuestro Sistema de Gestión Integral, será obligación de cada dependencia dar respuesta oportuna a las quejas, reclamos y sugerencias que sean interpuestas por la comunidad.
- k. Cuando estén automatizados los trámites, será obligación de cada dependencia, retroalimentar de manera oportuna y permanente la información que sea requerida por el sistema.
- l. En cada dependencia de la Administración, se deben tener los funcionarios responsables de la actualización de contenidos, quienes serán capacitados por la Dirección de Informática. Los nombres y cargos de éstos se reportarán a dicha oficina, con copia a la Secretaría de Control Interno.
- m. Los contenidos que se publiquen en el Portal Institucional deben ser de acuerdo con los estándares de estilo y manejo gráfico, definidos por la Administración y avalados por la Oficina Asesora de Comunicaciones.
- n. La publicación de boletines, noticias y campañas en el portal solo estará a cargo de la Oficina Asesora de Comunicaciones, pero, cada dependencia de conformidad con lo establecido en el Sistema de Gestión Integral, suministrará los contenidos a dicha Oficina.
- o. Será obligación por parte de los funcionarios responsables en cada dependencia del Portal Institucional, suministrar a la Oficina Asesora de Comunicaciones, la información de los eventos programados a lo largo del año. Estos datos serán suministrados con quince (15) días de anticipación, para informar oportunamente a la comunidad.
- p. La configuración de seguridad del hardware, software y redes del Portal Institucional debe garantizar disponibilidad, confidencialidad e Integridad de la Información.
- q. Todos los funcionarios de la Administración deben hacer uso responsable y seguro de los contenidos y servicios sobre el Portal Institucional, de los canales de acceso y de los equipos que lo soportan.
- r. Los trámites y servicios que se ofrezcan en el Portal Institucional deben atender a lo dispuesto en las directrices a nivel Institucional y del Gobierno Nacional.
- s. La transferencia de Información a través de los servicios del Portal Institucional debe ser implementada bajo condiciones de seguridad.
- t. Todos los funcionarios que generen, actualicen o hagan uso de los contenidos o los servicios ofrecidos por el Portal Institucional deben atender las disposiciones nacionales vigentes en materia de derechos de autor.
- u. El Portal Institucional debe funcionar de manera permanente.

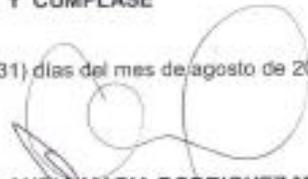
13. SEGURIDAD EN LA RED DE DATOS

- a. Por política de seguridad en red de datos de una dependencia no se podrá acceder a la máquinas de otra dependencia, esto estará restringido, cuando se necesite compartir información con funcionarios de otras áreas, lo podrán realizar a través del servidor de archivo solicitando los permisos respectivos para ingresar a la carpeta de su intereses, dichos permisos deben ser autorizados por el secretario de despacho o jefe sección y solicitados al área de seguridad y servidores de la Dirección de Informática utilizando la mesa de ayuda en la herramienta EPX Suite, otra manera será enviando los documentos por el correo electrónico institucional.

COMUNIQUESE Y CUMPLASE

Dada en Ervigado a los treinta y un (31) días del mes de agosto de 2011.


JENY ANDREA HERNÁNDEZ MAYA
Alcaldesa Municipal (E)


CLAUDIA MARÍA RODRIGUEZ MONTOYA
Secretaria Administrativa


LUIS FELIPE ROSSO RICAUTE
Jefe Oficina Dirección de Informática

Premio Nacional Alta Gerencia

Carrera 43 38 Sur 35 Palacio Municipal
PBX: 339 40 00 extensión 4002
adminis
www.



**pdfMachine - is a pdf writer that produces quality PDF files with ease!
Get yours now!**

"Thank you very much! I can use Acrobat Distiller or the Acrobat PDFWriter but I consider your product a lot easier to use and much preferable to Adobe's" A.Sarras - USA

ANEXO C. Apartes de la Recomendación UIT-T M.3400. Unión Internacional de Telecomunicaciones.

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

M.3010

(02/2000)



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

SERIE M: RGT Y MANTENIMIENTO DE REDES:
SISTEMAS DE TRANSMISIÓN, CIRCUITOS
TELEFÓNICOS, TELEGRAFÍA, FACSIMIL Y
CIRCUITOS ARRENDADOS INTERNACIONALES
Red de gestión de las telecomunicaciones

Principios para una red de gestión de las telecomunicaciones

Recomendación UIT-T M.3010

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE M

RGT Y MANTENIMIENTO DE REDES: SISTEMAS DE TRANSMISIÓN, CIRCUITOS TELEFÓNICOS, TELEGRAFÍA, FACSIMIL Y CIRCUITOS ARRENDADOS INTERNACIONALES

Introducción y principios generales de mantenimiento y organización del mantenimiento	M.10–M.299
Sistemas Internacionales de transmisión	M.300–M.559
Circuitos telefónicos Internacionales	M.560–M.759
Sistemas de señalización por canal común	M.760–M.799
Circuitos internacionales utilizados para transmisiones de telegrafía y de telefotografía	M.800–M.899
Enlaces Internacionales arrendados en grupo primario y secundario	M.900–M.999
Circuitos internacionales arrendados	M.1000–M.1099
Sistemas y servicios de telecomunicaciones móviles	M.1100–M.1199
Red telefónica pública Internacional	M.1200–M.1299
Sistemas internacionales de transmisión de datos	M.1300–M.1399
Designaciones e Intercambio de Información	M.1400–M.1999
Red de transporte Internacional	M.2000–M.2999
Red de gestión de las telecomunicaciones	M.3000–M.3599
Redes digitales de servicios Integrados	M.3600–M.3999
Sistemas de señalización por canal común	M.4000–M.4999

Para más información, véase la Lista de Recomendaciones del UIT-T.

6 Campo de aplicación

Se indican a continuación ejemplos de redes, servicios de telecomunicación y tipos principales de equipo que pueden ser gestionados por la RGT:

- redes públicas y privadas, incluidas las RDSI de banda estrecha y de banda ancha, (incluido el ATM) redes móviles, redes telefónica privadas, redes privadas virtuales y redes inteligentes;
- la propia RGT;
- terminales de transmisión (multiplexores, transconectores, equipos de modulación de canal, jerarquía digital sincrona, etc.);
- sistemas de transmisión digitales y analógicos (cable, fibra, radio, satélite, etc.);
- sistemas de restauración;
- sistemas de operaciones y sus periféricos;
- ordenadores principales, procesadores frontales, controladores de agrupaciones, servidores de ficheros, etc.;
- centrales digitales y analógicas;
- redes de área (ampliada, metropolitana o local);
- redes con conmutación de circuitos y de paquetes;
- terminales y sistemas de señalización, incluidos los puntos de transferencia de las señales (STP, *signal transfer points*) y bases de datos en tiempo real;
- servicios portadores y teleservicios;
- centralitas privadas, accesos a centralitas privadas y terminales de usuario (cliente);
- terminales de usuario RDSI;
- soporte lógico proporcionado por o asociado a servicios de telecomunicación; por ejemplo: soporte lógico de conmutación, directorios, bases de datos de mensajes, etc.;
- aplicaciones de soporte lógico de la RGT;
- sistemas soporte asociados (módulos de prueba, sistemas de alimentación de energía, unidades de acondicionamiento de aire, sistemas de alarmas de edificios, etc.).

Además, una RGT puede ser utilizada para gestionar:

- entidades distribuidas y servicios ofrecidos agrupando elementos de la lista precedente;
- recursos relacionados con los procesos que un PTO emplea en la operación de equipos, redes y servicios. Ejemplos de estos recursos gestionados son: las órdenes de servicio de reparación de equipos, las fichas de anomalías generadas por quejas de los clientes, contrato del cliente para la prestación de servicio, acuerdos de nivel de servicio, datos históricos, etc.

En lo sucesivo, se considerará que todos los equipos, programas de aplicaciones y redes, o agrupamientos de equipos, soporte lógico de aplicaciones y redes como los indicados en la lista precedente, así como todo servicio obtenible de una combinación de los elementos de dicha lista, son conceptos pertenecientes al entorno de las telecomunicaciones.

7 Objetivos básicos para la RGT

El objetivo en cuanto a especificaciones de la RGT es proporcionar un marco de gestión de telecomunicaciones. Introduciendo el concepto de modelos genéricos de red para gestión será posible ejercer una gestión general de equipos diversos mediante el empleo de modelos genéricos de información y de interfaces normalizados.

8 Recomendación M.3010 (02/2000)

Una RGT tiene por objeto soportar una amplia variedad de áreas de gestión que abarcan la planificación, instalación, operaciones, administración, mantenimiento y suministro de redes y servicios de telecomunicaciones. En la Recomendación M.3200 [10] se describe el alcance de la gestión a través de los dos conceptos principales siguientes: sectores gestionados de las telecomunicaciones y servicios de gestión de la RGT. El primero se relaciona con el agrupamiento de recursos de telecomunicaciones que se selecciona para ser gestionado en conjunto y el segundo con el conjunto de procesos necesarios para lograr objetivos comerciales, es decir, objetivos de gestión de la RGT.

La especificación y el desarrollo de la gama y funcionalidad de las aplicaciones requeridas para soportar las áreas de gestión citadas son un tema de incumbencia local que no será tratado en estas Recomendaciones. No obstante, el UIT-T proporciona algunas ideas al respecto, clasificando para ello la gestión en cinco grandes áreas funcionales de gestión (véase la Recomendación X.700 [1]). Estas áreas soportan el alcance de gestión que figura en la Recomendación M.3020 [9]. Presentan un marco a través del cual los servicios de gestión apropiados pueden atender las necesidades comerciales de los PTO. Hasta la fecha han sido identificadas las cinco áreas funcionales de gestión siguientes:

- gestión de la calidad de funcionamiento;
- gestión de fallos;
- gestión de la configuración;
- gestión de la contabilidad;
- gestión de la seguridad.

La clasificación del intercambio de información dentro de la RGT es independiente del uso que se haga de dicha información.

La RGT debe percibir las redes de telecomunicaciones y los servicios como colecciones de sistemas cooperantes. La arquitectura es el concepto que orquesta la gestión de distintos sistemas a fin de obtener un efecto coordinado con respecto a la red. La introducción de la RGT ofrece a los PTO la posibilidad de lograr una diversidad de objetivos de gestión, en particular la aptitud para:

- minimizar los tiempos de reacción de gestión ante eventos de la red;
- minimizar la carga causada por el tráfico de gestión cuando se utiliza la red de telecomunicaciones para cursarlo;
- posibilitar la dispersión geográfica del control sobre aspectos de la operación de red;
- proporcionar mecanismos de aislamiento para minimizar los riesgos de seguridad;
- proporcionar mecanismos de aislamiento para localizar y contener los fallos de red;
- mejorar la asistencia de servicio y la interacción con los clientes.

ANEXO D. Evidencia fotográfica de la realización de la Práctica Empresarial en la Dirección de Informática de la Alcaldía de Envigado

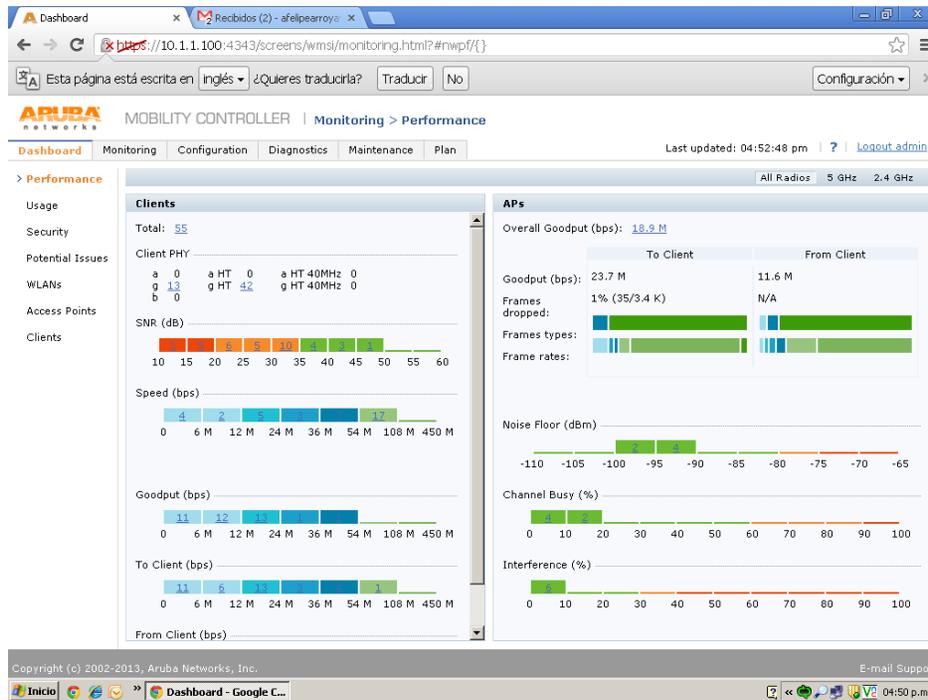


Figura 6. Fotografía de la consola de administración de la controladora inalámbrica de Aruba Networks.

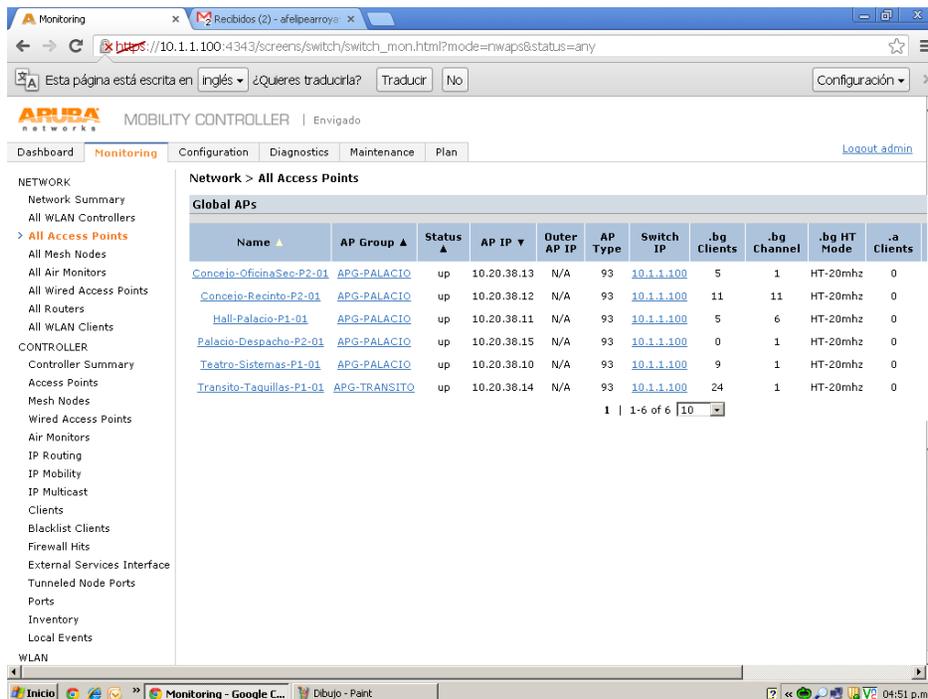


Figura 7. Fotografía de la consola de administración de los Access Points anexados a la controladora inalámbrica de Aruba Networks.



Figura 8. Fotografía del rack que cubre las oficinas de Informática, Catastro y Sótano Municipal.



Figura 9. Fotografía del conector tipo PoE del AP presente en la Dirección de Informática que cubre las áreas de Informática, Catastro y Teatro Municipal.



Figura 10. Fotografía del Access Point que cubre las áreas de Informática, Catastro y Teatro Municipal.

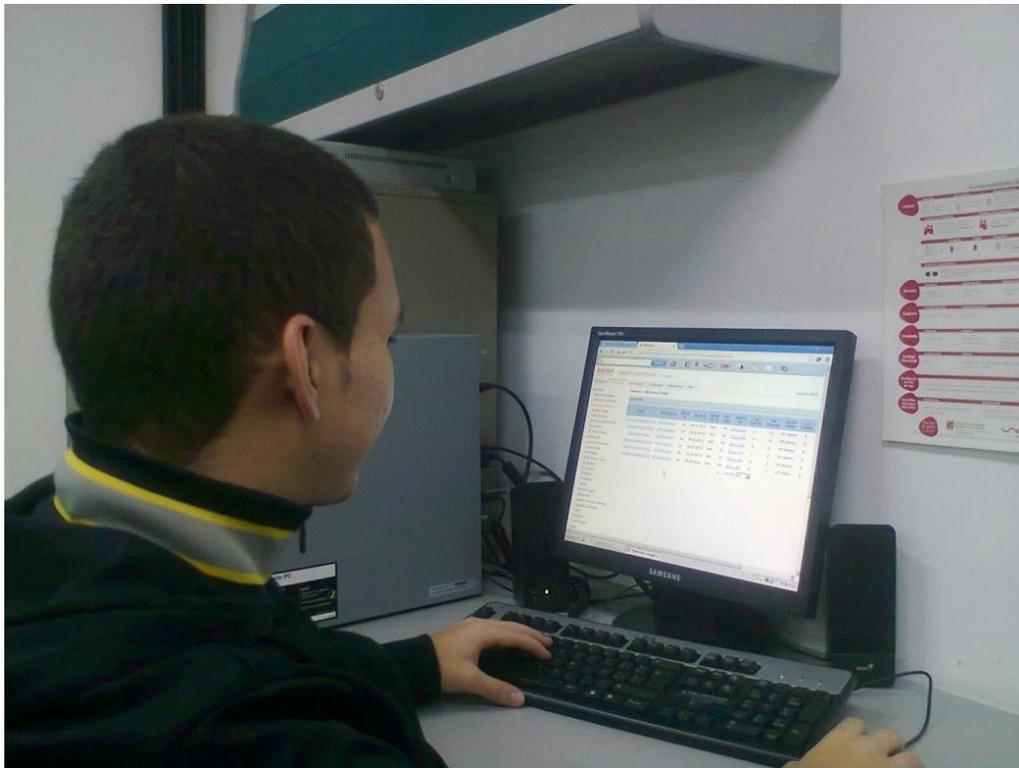


Figura 11. Fotografía del practicante realizando la toma del número de usuarios conectados a la red inalámbrica de la Alcaldía de Envigado, mediante la consola de administración del Aruba Networks

ANDRÉS FELIPE ARROYAVE ARREDONDO
ESTUDIANTE

LUIS FELIPE VILLAMIZAR TORRES
ASESOR DE PRÁCTICA INSTITUCIÓN UNIVERSITARIA DE ENVIGADO

FELIPE JOSÉ BURGOS ORTEGA
JEFE INMEIATO ALCALDÍA DE ENVIGADO–DIRECCIÓN DE INFORMÁTICA