MIDDLEWARE DE SEGURIDAD PARA EL ACCESO A SERVICIOS IMS EN UN ENTORNO 802.11

EDGAR DE LA CRUZ ESPARZA

HERNÁN GEOVANNI TAIMAL

ANEXO A
IMPLEMENTACION DE REFERENCIA DE MIDSEG

UNIVERSIDAD DEL CAUCA
FACULTADA DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELEMÁTICA
POPAYÁN, MAYO DE 2009

TABLA DE CONTENIDO

LISTA DE FIGURAS

Anexo A

IMPLEMENTACION DE REFERENCIA DEL MidSEG

A.1. INTRODUCCION

Para los operadores de las redes de telecomunicaciones, la seguridad es una de las mayores preocupaciones a la hora de ofrecer servicios sobre su infraestructura de red, por consiguiente es importante controlar el acceso a sus recursos hardware de red. Desde el punto de vista de los usuarios la seguridad es importante ya que no estarán dispuestos a ser suplantados, a pagar por servicios no consumidos, ni mucho menos a que su información privada sea divulgada, manipulada o aprovechada por terceras partes [1][2]. De este modo, la seguridad en la comunicación puede ser un factor determinante para que un cliente prefiera una empresa prestadora de servicios de telecomunicaciones sobre otra [2]. El 3GPP define en el TS 33.203 la arquitectura de seguridad para IMS, la cual proporciona esquemas para la gestión de integridad, confidencialidad, autenticación y protección contra ataques de denegación de servicio. Esta arquitectura consta de cinco partes o asociaciones diferentes que garantizan seguridad en distintos puntos, los primeros dos permiten asegurar la comunicación entre el equipo de usuario (UE) y el primer punto de red IMS conocido como P-CSCF; los demás puntos hacen referencia a la protección entre las entidades internas de la red IMS o entre redes de distinto operador [3].

En el anteproyecto se definió como objetivo general proporcionar seguridad en la comunicación entre el UE y el P-CSCF de una red IMS sobre 802.11 por este motivo el trabajo se enfoca sobre los dos primeros puntos de la arquitectura de seguridad planteada para IMS. Como propósito del presente trabajo se tomó como referencia para WLAN la tecnología WiFi ya que esta presenta gran cantidad de problemas de seguridad que si son resueltos garantizarían su aplicación sobre otras no tan vulnerables a ataques. Como estrategia para cumplir con los objetivos específicos del proyecto se procedió a establecer una base inicial de conocimiento alrededor de la seguridad en la comunicación del UE y el primer punto de comunicación de una red IMS, a partir del conocimiento se procedió a diseñar e implementar un middleware de seguridad IMS para iniciar y establecer una comunicación segura entre el UE y el P-CSCF, que permita: autenticación mutua entre el UE y la red local (HN, Home Network) IMS, establecer asociaciones de seguridad entre el UE y el P-CSCF y proveer la autorización al UE para el uso de servicios. Finalmente se estableció el nivel de seguridad obtenido con el middleware construido a través de un servicio de prueba, haciendo uso de 802.11 como red de acceso al núcleo IMS.

Para el diseño e implementación del Middleware se partió de las características de seguridad y eficiencia identificadas en el interworking 3GPP-WLAN, estas características fueron utilizadas para realizar la caracterización y obtener los requisitos (funcionales y no funcionales) de la solución, con ellos se planteó la arquitectura de referencia para la solución denominada MidSEG, a partir de la arquitectura de referencia de MidSEG se realizó la implementación de las funcionalidades principales a lo cual se le denominó implementación de referencia del MidSEG, construida con el fin de evaluar la solución planteada y además servir como orientación a quienes deseen hacer una implementación comercial del MidSEG.

La implementación de referencia estuvo limitada por la imposibilidad de simular completamente el ambiente 3GPP, sin embargo el interworking WLAN-IMS se evaluó de la forma más completa y real posible. De aquí en adelante MidSEG será indistintamente tratado como la implementación de referencia.

En este documento se describe la metodología y las actividades que permitieron llevar a buen término el proyecto y se describe a MidSEG con un mayor detalle que el presentado en la sección 3.3 de la Monografía.

A.2. PLAN DEL PROYECTO

Con el propósito de llevar al mejor término cada uno de los objetivos se establecieron actividades para: sentar las bases teóricas, diseño, desarrollo y pruebas del proyecto. Además se tomó como referencia la metodología planteada en los documentos:

Modelo para la Investigación Documental, para adquirir la base conceptual.

Modelo para la Construcción de Soluciones, para el diseño, desarrollo e implementación de los prototipos de prueba.

Del "Modelo Integral para un Profesional en Ingeniería" [5].

A continuación se muestran a manera de tabla las actividades generales y específicas que se llevaron a cabo.

Tabla 1. Actividades generales y específicas.

Referencia	Actividad
1.	**Establecimiento de la base inicial de conocimiento sobre aspectos de seguridad entre el UE y la red IMS.**
1.1.	Estudio de la arquitectura de red IMS.
1.2.	Estudio de los aspectos de seguridad en la arquitectura de red IMS para el inicio y establecimiento de una comunicación segura entre el UE y el P-CSCF.
1.3.	Estudio del interworking WLAN-IMS y de su arquitectura de seguridad.
1.4.	Estudio de trabajos relacionados con la seguridad en el interworking WLAN-IMS.
1.5.	Revisión y actualización de alcances.
2.	**Diseño del middleware de seguridad IMS para iniciar y establecer una comunicación segura entre el UE y el P-CSCF.**
2.1.	Análisis de los requisitos funcionales y no funcionales.
2.2.	Definición de la arquitectura de referencia.
2.3.	Definición de las herramientas para la implementación del Middleware de Seguridad IMS.
2.4.	Revisión del diseño del middleware de seguridad.
3.	**Implementación del middleware de seguridad IMS.**
3.1.	Instalación e interconexión de las entidades funcionales de IMS, implementación de la señalización en cada subsistema haciendo uso del cliente WLAN.
3.2.	Implementación de la autenticación unificada y de la gestión de autorización para el acceso a los dominios WLAN, 3GPP e IMS.
3.3.	Implementación de la configuración dinámica a través de AKA/SIP de IPsec para los subsistemas SSW y SCSWI. Configuración de IKE para la comunicación IPsec entre el SSW y el SSP.
3.4.	Prueba y revisión de las capacidades operacionales del middleware de seguridad.
4.	**Establecimiento del nivel de seguridad y del rendimiento del Middleware**
4.1.	Diseño de pruebas.
4.2.	Aplicación de pruebas.
4.3.	Análisis de resultados.
5	**Prueba del Middleware con un servicio IMS de prueba.**
5.1.	Definición del servicio de prueba
5.2.	Diseño de pruebas.
5.3.	Aplicación de pruebas.
5.4.	Análisis de resultados.

A.3. MidSEG

Los requisitos funcionales y no funcionales para MidSEG son descritos en la sección 3.1.2 de la Monografia. Para facilidad del lector también se muestran a continuación:

Requisitos funcionales

- Controlar el acceso de paquetes a los dominios WLAN e IMS. De este modo el MidSEG protege las entidades de la red contra abusos y permite el tráfico, únicamente a usuarios registrados. Esta funcionalidad debe estar presente en cada uno de los tres dominios del interworking WLAN-IMS teniendo en cuenta que se ofrecen servicios de distinto tipo.
- Permitir al UE registrarse a la red WLAN, 3GPP o IMS. De esta manera MidSEG permite que el usuario escoja el tipo de acceso y obtenga el uso de los servicios conforme a su elección, por otro lado el operador tiene la posibilidad de realizar una diferenciación de usuarios y ejecutar el respectivo control de acceso.
- Obtener los desafíos de autenticación que permitan al UE autenticar las redes WLAN, 3GPP e IMS. De este modo, MidSEG evita que terceros suplanten a una o todas las redes.
- Unificar la autenticación del UE a los dominios WLAN, 3GPP e IMS, reutilizando la autenticación realizada por el núcleo IMS. Así, MidSEG evita la suplantación de un usuario legítimo, es decir garantiza que la comunicación de la red es con el usuario y no con alguien diferente.
- Actualizar el estado del usuario. MidSEG modifica el HSS como resultado de un registro satisfactorio con el fin de habilitar los servicios configurados en su perfil (p. Ej: Para una llamada entrante a un usuario, la red debe localizarlo haciendo uso del previo registro realizado), de la misma forma la red debe ser notificada cuando un usuario sale del sistema.
- Validar la integridad de los datos. MidSEG de esta forma garantiza la seguridad en la comunicación establecida entre el UE y el P-CSCF, evitando que alguien ajeno a la comunicación modifique, inserte o elimine información de acuerdo a su conveniencia.
- Cifrar la señalización. De esta forma, MidSEG permite garantizar la confidencialidad en la comunicación entre el UE y el P-CSCF. Cada usuario al momento de registrarse obtiene unas llaves de cifrado diferentes que permiten el establecimiento de asociaciones de seguridad, las cuales garantizan la privacidad en la comunicación y evitan que información confidencial llegue a manos de terceros.
- Proteger la red contra usuarios no autorizados. El MidSEG implementa esta funcionalidad para garantizar al operador la integridad de la infraestructura y la disponibilidad de la red para los usuarios legítimos.

Requisitos no funcionales

- Mejorar la eficiencia del sistema de autenticación en el interworking WLAN-IMS en cuanto al retardo, la sobrecarga de la red causada por las múltiples autenticaciones, el consumo de recursos de radio y de procesamiento. Todo esto se logra unificando la autenticación a los dominios WLAN, 3G e IMS.
- Seguridad en la señalización entre el UE y el P-CSCF, esto se logra con el establecimiento de SA entre: UE<->MidSEG y MidSEG<->P-CSCF
- Independiente de la tecnología WLAN utilizada (p. Ej: WiFi, Bluetooth, WiMax, etc.), esto se logra con La unificación de la autenticación a la capa de nivel de servicio y la utilización de IPsec.

A.3.1. Plan de la Implementación de Referencia

Teniendo en cuenta las recomendaciones realizadas en [1] para el desarrollo del proyecto: centrarse en la arquitectura, guiarse por los casos de uso y realizar mejoras de manera incremental. Se procedió a construir el MidSEG por subsistemas, tal como se especificó en la Arquitectura de Referencia (sección 3.2 de la Monografía). En la arquitectura de referencia se tienen tres subsistemas funcionales de MidSEG, el plan para su implementación consistió en desarrollar cada subsistema de manera independiente con la realización de pruebas en conjunto como las siguientes:

- Probar toda la funcionalidad de la señalización SIP de registro entre los subsistemas incluyendo el núcleo IMS.
- Probar la autenticación a los tres dominios sin seguridad.
- Probar la configuración dinámica de seguridad entre el SCSW y el SSW.

- Probar la configuración de seguridad entre el SSW y el SSP.
- Probar MidSEG en el ambiente completo WLAN-IMS.

En las secciones 3.5 y 3.6 de la monografía se muestran las pruebas y análisis de resultados sobre esta funcionalidad. A continuación se describe con detalle cada uno de los subsistemas.

A.3.1.1. Subsistema Cliente de Seguridad WLAN-IMS

A.3.1.1.1. Diagrama de Casos de Uso del SCSWI

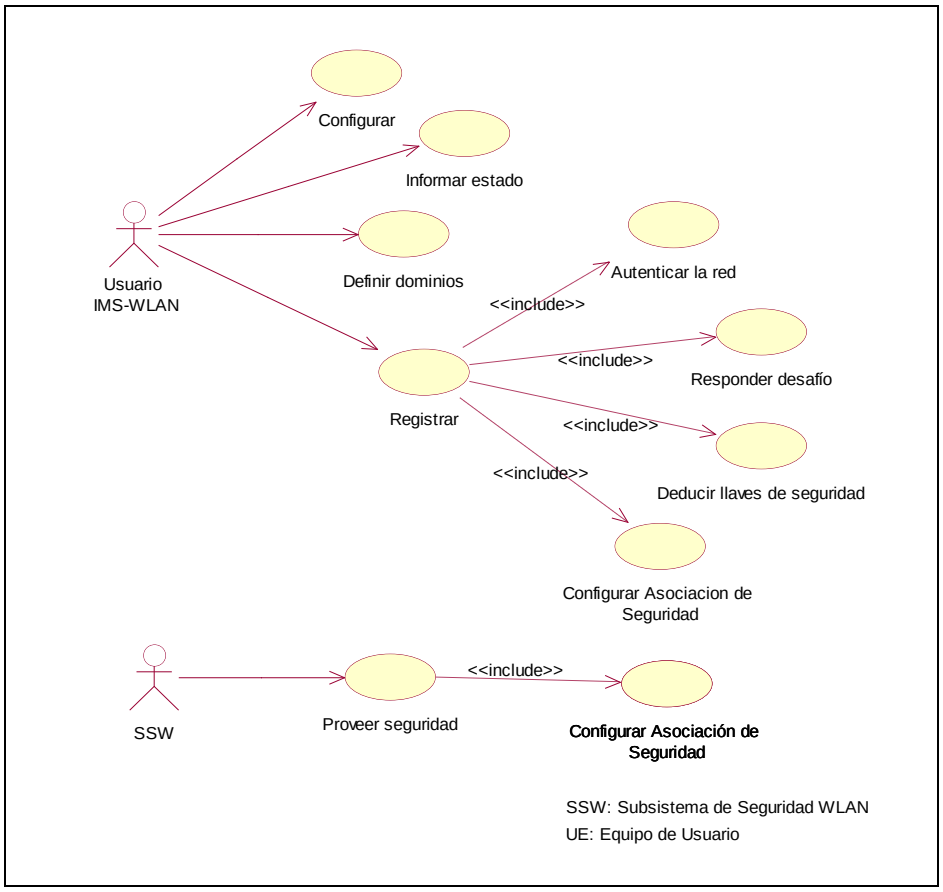

Figura 1. Diagrama de Casos de Uso del SCSWI.

A.3.1.1.1.1. Casos de Uso Iniciados por el Usuario WLAN-IMS.

Caso de uso definir dominios	
Iniciador	Usuario WLAN-IMS
Precondiciones	Aplicación sobre el equipo del Usuario WLAN-IMS iniciada.
Flujo principal	1. El Usuario WLAN-IMS elige sobre la interface de usuario los dominios a los que desea acceder. 2. Los dominios elegidos son configurados en el SCSWI.
Subflujos	Ninguno
Flujos alternativos	Ninguno
Flujos de excepción	1. Si el Usuario WLAN-IMS no elige ningún dominio. 2. Se configura por defecto el acceso al dominio WLAN en el SCSWI.
Postcondiciones	Dominios a registrar configurados en el SCSWI.
Notas	Ninguna

Caso de uso configurar

Iniciador	Usuario WLAN-IMS
Precondiciones	Aplicación sobre el equipo del Usuario WLAN-IMS iniciada.
Flujo principal	1. El Usuario WLAN-IMS ingresa en la interface de usuario sus datos de registro p. Ej: identidad pública, dirección ip local, puerto local, expires, servidor proxy, identidad privada, clave compartida, dominio de red al cual pertenece y protección de la interfaz de radio. 2. Se configura el SCSWI con datos suministrados.
Subflujos	Ninguno
Flujos alternativos	Ninguno
Flujos de excepción	1. Si el Usuario WLAN-IMS no ingresa valores como: identidad pública, identidad privada, dirección ip local, clave compartida o dominio de red al cual pertenece. 2. No se permite elegir la opción iniciar Registro. 1. Si el Usuario WLAN-IMS no ingresa valores como: puerto local, expires, servidor proxy o protección de la interfaz de radio. 2. Se configura el SCSWI con los valores por defecto para ellos.
Postcondiciones	Valores de registro configurados en el SCSWI.
Notas	Ninguna

Caso de uso informar estado	
Iniciador	Usuario WLAN-IMS
Precondiciones	Aplicación sobre el equipo del Usuario WLAN-IMS iniciada.
Flujo principal	1. El Usuario WLAN-IMS realiza una acción sobre la interface grafica p. Ej: iniciar el proceso de registro. 2. El SCSWI informa sus estados, los cuales son: “Sin Registro”, “Registrado”, “En Proceso” y “Error por Tiempo Excedido”. 3. La interface informa al Usuario WLAN-IMS el estado entregado por el SCSWI.
Subflujos	Ninguno
Flujos alternativos	Ninguno
Flujos de excepción	Ninguno
Postcondiciones	Ninguna
Notas	Ninguna

Caso de uso registrar	
Iniciador	Usuario WLAN-IMS
Precondiciones	Aplicación sobre el equipo del Usuario WLAN-IMS iniciada. Dominios a registrar configurados sobre el SCSWI. Valores de registro configurados sobre el SCSWI. Estado del SCSWI “Sin Registro”
Flujo principal	1. El Usuario WLAN-IMS elige la opción registrar en la interface grafica. 2. La interface informa al SCSWI. 3. El SCSWI inicia el proceso de registro elaborando un mensaje SIP REGISTER. 4. El SCSWI agrega como encabezados SIP los dominios elegidos y los algoritmos de seguridad para la protección de la interfaz de radio. 5. El SCSWI envía el mensaje SIP REGISTER al SSW. 6. El SSW responde con un mensaje 401 No Autorizado.

	7. El SCSWI aplica el algoritmo AKA para: autenticar la red IMS, verificar el número de secuencia, deducir las llaves de seguridad y generar la respuesta de autenticación. 8. El SCSWI configura una conexión IPsec para proteger la señalización de registro con el SSW haciendo uso de las llaves obtenidas en el punto anterior. 9. EL SCSWI agrega la respuesta como un encabezado de autenticación sobre el mensaje SIP REGISTER. 10. EL SCSWI envía el nuevo mensaje SIP REGISTER al SSW protegido por la conexión IPsec configurada. 11. El SSW responde con el mensaje SIP OK. 12. El SCSWI configura las conexiones IPsec con el SSW para proteger toda la señalización IMS y la interfaz de radio. 13. El estado del SCSWI cambia a "Registrado"
Subflujos	1. Al enviar el primer mensaje SIP REGISTER el estado "Sin Registro" cambia a "En Proceso" 2. Cuando llega el mensaje OK del SSW el estado cambia a "Registrado"
Flujos alternativos	1. Si ha existido un registro anterior con el mismo SSW, el primer mensaje SIP REGISTER se envía haciendo uso de la ultima configuración IPsec.
Flujos de excepción	1. El SSW no responde al mensaje SIP REGISTER enviado. 2. El SCSWI reenvía la solicitud de registro hasta cumplir con el tiempo estipulado en el valor expires. 3. El SCSWI deja de enviar la solicitud. 4. El SCSWI cambia al estado "Error por Tiempo Excedido"
Postcondiciones	Usuario WLAN-IMS registrado.
Notas	Ninguna

A.3.1.1.1.2. Casos de Uso Iniciados por el SSW

Caso de uso proveer seguridad	
Iniciador	SSW
Precondiciones	Usuario WLAN-IMS registrado. Existencia de una configuración IPsec anterior con el SSW, debida a un registro anterior.
Flujo principal	1. El SSW envía el mensaje 401 No Autorizado. 2. El mensaje SIP REGISTER que contiene la respuesta de autenticación es enviado inicialmente al componente IPsec del SCSWI. 3. El componente IPsec aplica el protocolo Encapsulating Security Payload (ESP) que proporciona confidencialidad, autenticación e integridad.
Subflujos	Ninguno
Flujos alternativos	Ninguno
Flujos de excepción	Ninguno
Postcondiciones	Ninguna
Notas	La seguridad con el protocolo ESP es provista a todo el trafico de señalización SIP proveniente de los servicios IMS, la protección para el resto de trafico sobre la interfaz de radio es protegida de acuerdo a la elección de seguridad del Usuario WLAN-IMS.

A.3.1.1.2. Diagrama de Clases de Análisis del SCSWI

En la Figura 2 se presenta el diagrama de clases de análisis para el SCSWI y está conformado por:

Paquete Aplicación

AplicacionPrueba: corresponde a la interfaz que permite, el ingreso de los parámetros de registro, el envío de alertas al Usuario WLAN-IMS y la configuración de seguridad para la interfaz de radio. Para hacer uso del MidSEG instancia la clase SCSWI.

Paquete Control

SCSWI: realiza la lógica de la aplicación para ello crea instancias de cada una de las clases principales de la aplicación. Instancia las clases: SipRegisterUA para manejar la señalización SIP de registro; AKA para obtener la respuesta al desafío, las llaves de cifrado e integridad; IPsec para realizar la configuración de SA y políticas para IPsec.

AKA: clase que hace uso del algoritmo Milenage para el cálculo de la respuesta esperada y deducción de llaves.

SipRegisterUA: Provee el soporte de SIP para la comunicación de registro. Esta clase contiene los atributos y métodos necesarios para el procedimiento de registro.

Paquete Transporte

IPsec: corresponde a la interfaz de configuración IPsec contiene dos vectores uno para las SA y otro para las SPD IPsec, sus funciones principales son: cargar la configuración actual de IPsec del sistema operativo (SO), guardar cambios de configuración de IPsec sobre el SO, agregar SA, borrar SA, agregar SPD y borrar SPD.

SA: corresponde a la clase que representa las SA y contiene los atributos necesarios para definir una nueva SA.

SPD: corresponde a la clase que representa a las políticas de seguridad de IPsec (SPD), contiene los atributos necesarios para definir nuevas SPD.

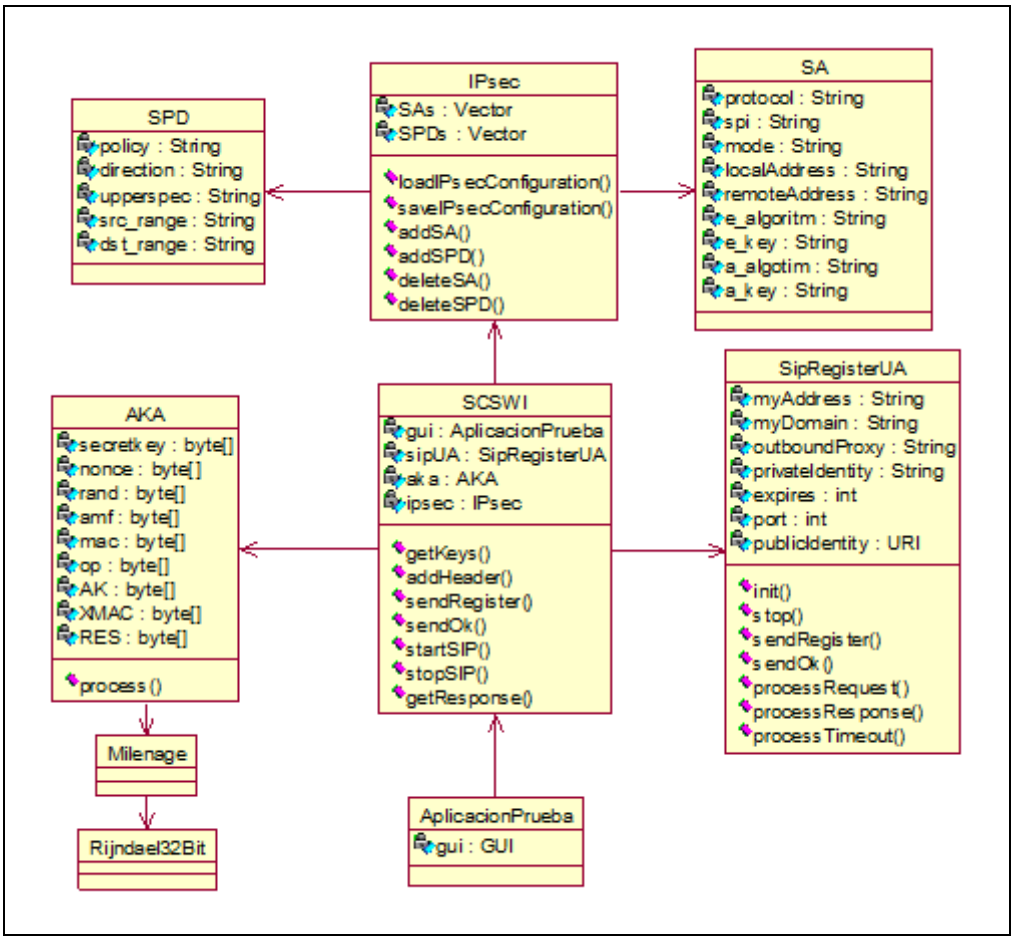

Figura 2. Diagrama de Clases de Análisis SCSWI

A.3.1.2. Subsistema de Seguridad WLAN

A.3.1.2.1. Diagrama de Casos de Uso del Subsistema

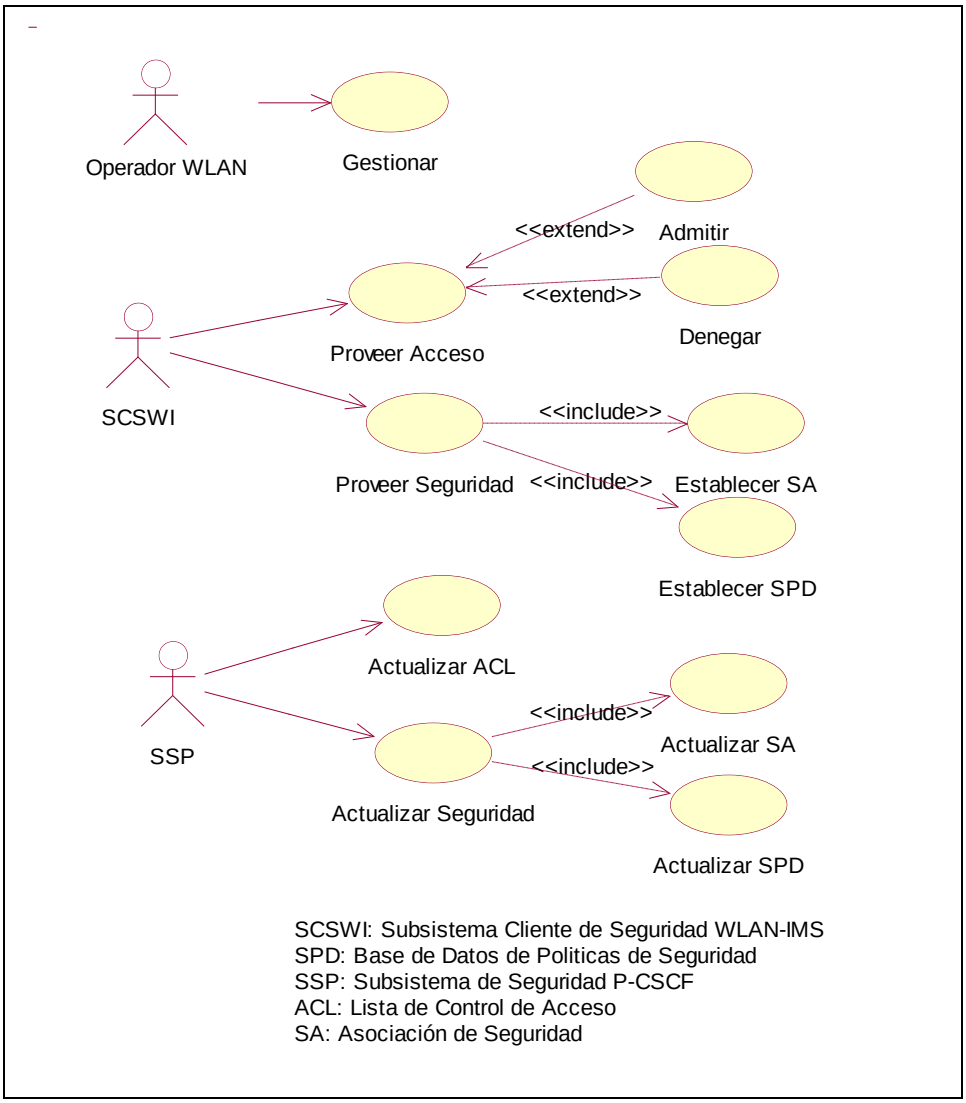

Figura 3. Diagrama de casos de uso del SSW.

A.3.1.2.1.1. Casos de Uso Iniciados por el Operador WLAN.

Caso de uso gestionar	
Iniciador	Operador WLAN
Precondiciones	Ninguna
Flujo principal	1. El operador WLAN ingresa los valores sobre el archivo de configuración. 2. El operador WLAN inicia la aplicación. 3. El operador WLAN escribe el comando “start” para iniciar el servidor. 4. El operador WLAN escribe el comando “stop” para detener el servidor. 5. El operador WLAN escribe el comando “exit” para salir de la aplicación.
Subflujos	Ninguno
Flujos alternativos	1. Con el servidor detenido, el operador cambia los valores sobre el archivo de configuración. 2. El operador WLAN escribe el comando “start” para iniciar el servidor. 3. El operador WLAN escribe el comando “stop” para detener

	el servidor. 4. El operador WLAN escribe el comando "exit" para salir de la aplicación.
Flujos de excepción	Ninguno
Postcondiciones	Ninguna
Notas	Ninguna

A.3.1.2.1.2. Casos de Uso Iniciados por el SCSWI.

Caso de uso proveer acceso	
Iniciador	SCSWI
Precondiciones	SSW iniciado.
Flujo principal	1. El SCSWI envía una solicitud de servicio a la WLAN o a IMS. 2. La solicitud ingresa como paquete IP al componente IPsec del SSW. 3. El componente IPsec comprueba el origen y dirige el paquete al componente Filtro TCP/IP-NAT. 4. El componente Filtro TCP/IP-NAT aplica las reglas configuradas en el componente ACL sobre el paquete. 5. Si el Usuario WLAN-IMS se encuentra registrado envía el paquete hacia la interfaz de red que permite alcanzar el destino del paquete.
Subflujos	Ninguno
Flujos alternativos	1. Si el Usuario WLAN-IMS no se ha registrado anteriormente al SSW, entonces el filtro aplica directamente las reglas de la ACL. 2. El SSW descarta el paquete. 1. El componente IPsec autentica a nivel IP al SCSWI y remite esta solicitud al componente Filtro TCP/IP-NAT. 2. El componente Filtro TCP/IP-NAT determina que el Usuario WLAN-IMS no se encuentra registrado, entonces descarta el paquete.
Flujos de excepción	1. El componente IPsec encuentra un error en la autenticación o integridad del paquete. 2. El SSW descarta el paquete.
Postcondiciones	Acceso provisto Acceso denegado
Notas	Ninguna

Caso de uso proveer seguridad	
Iniciador	SCSWI
Precondiciones	Usuario WLAN-IMS registrado. Existencia de una configuración IPsec con el SCSWI
Flujo principal	1. El SCSWI hace una solicitud SIP REGISTER al SSW con la respuesta de autenticación. 2. El SSW reenvía el mensaje al SSP 3. El SSP responde al SSW con el mensaje SIP OK. 4. El SSW envía la respuesta SIP OK primero al componente IPsec. 5. El componente IPsec aplica el protocolo Encapsulating Security Payload (ESP) que proporciona confidencialidad, autenticación e integridad.
Subflujos	Ninguno
Flujos alternativos	Ninguno

Flujos de excepción	Ninguno
Postcondiciones	Ninguna
Notas	La seguridad con el protocolo ESP es provista a todo el trafico de señalización SIP proveniente de los servicios IMS, la protección para el resto de trafico sobre la interfaz de radio es protegida de acuerdo a la elección de seguridad del usuario.

A.3.1.2.1.3. Casos de Uso Iniciados por el SSP

Caso de uso actualizar seguridad	
Iniciador	SSP
Precondiciones	Estado de registro del SCSWI "En Proceso"
Flujo principal	1. El SSP envía el mensaje 401 No Autorizado al SSW, el cual contiene las llaves de seguridad. 2. El SSW extrae las llaves de seguridad y las elimina del mensaje. 3. El SSW reenvía el mensaje 401 No Autorizado al SCSWI. 4. El SSW configura las llaves de seguridad para la señalización de registro. 5. El SCSWI responde con nuevo mensaje SIP REGISTER que contiene el encabezado de autenticación. 6. El SSW reenvía el mensaje al SSP. 7. El SSP responde con el mensaje OK. 8. El SSW reenvía el mensaje OK al SCSWI. 9. El SSW configura las llaves de seguridad tanto para la señalización de IMS como para la interfaz de radio.
Subflujos	Ninguno
Flujos alternativos	Ninguno
Flujos de excepción	Ninguno
Postcondiciones	Estado de registro del SCSWI "Registrado"
Notas	Ninguna

Caso de uso actualizar ACL	
Iniciador	SSP
Precondiciones	Estado de registro del SCSWI "En Proceso"
Flujo principal	1. El SSP envía el mensaje OK como confirmación a la autenticación del Usuario WLAN-IMS, en el mensaje se agrega un encabezado con la autorización a los dominios registrados. 2. El SSW extrae los encabezados del mensaje. 3. El SSW configura la ACL de acuerdo a lo indicado en el encabezado. 4. El SSW reenvía el mensaje OK al SCSWI.
Subflujos	Ninguno
Flujos alternativos	Ninguno
Flujos de excepción	Ninguno
Postcondiciones	Estado de registro del SCSWI "Registrado"
Notas	Ninguna

A.3.1.2.2. Diagrama de Clases de Análisis del SSW

En la Figura 4 se presenta el diagrama de clases de análisis para el SSW. El cual está conformado por:

Paquete Control

SSW: realiza la lógica de la aplicación para ello crea instancias de cada una de las clases principales de la aplicación. Instancia las clases: SipProxy para procesar la señalización SIP de registro y reenviarla al SSP; IPsec para realizar la configuración de SA y SPD; Filter para configurar los filtros tras la autorización de acceso enviada por el SSP; Db_Manager como modelo de acceso a datos.

SipProxy: Provee el soporte de SIP para la comunicación de registro. Esta clase contiene los atributos y métodos necesarios para el reenvío de la señalización al SSP.

Db_Manager: representa el modelo de acceso a datos necesario para el manejo de los parámetros de registro del Usuario WLAN-IMS y para las conexiones IPsec establecidas con un SCSWI.

Parameters: representa los parámetros persistidos temporalmente para realizar el registro de un Usuario WLAN-IMS.

IPsecConnections: corresponde a las conexiones establecidas con un determinado UE.

Paquete Transporte

IPsec: corresponde a la interfaz para la configuración de IPsec contiene dos vectores uno para las SA y otro para las SPD IPsec, sus funciones principales son: cargar la configuración actual de IPsec del sistema operativo (SO), guardar cambios de configuración de IPsec sobre el SO, agregar SA, borrar SA, agregar SPD y borrar SPD.

SA: corresponde a la clase que representa las SA y contiene los atributos necesarios para definir una nueva SA.

SPD: corresponde a la clase que representa a las políticas de seguridad de IPsec (SPD), contiene los atributos necesarios para definir nuevas SPD.

Filter: corresponde a la interfaz de configuración del filtro para el control de acceso.

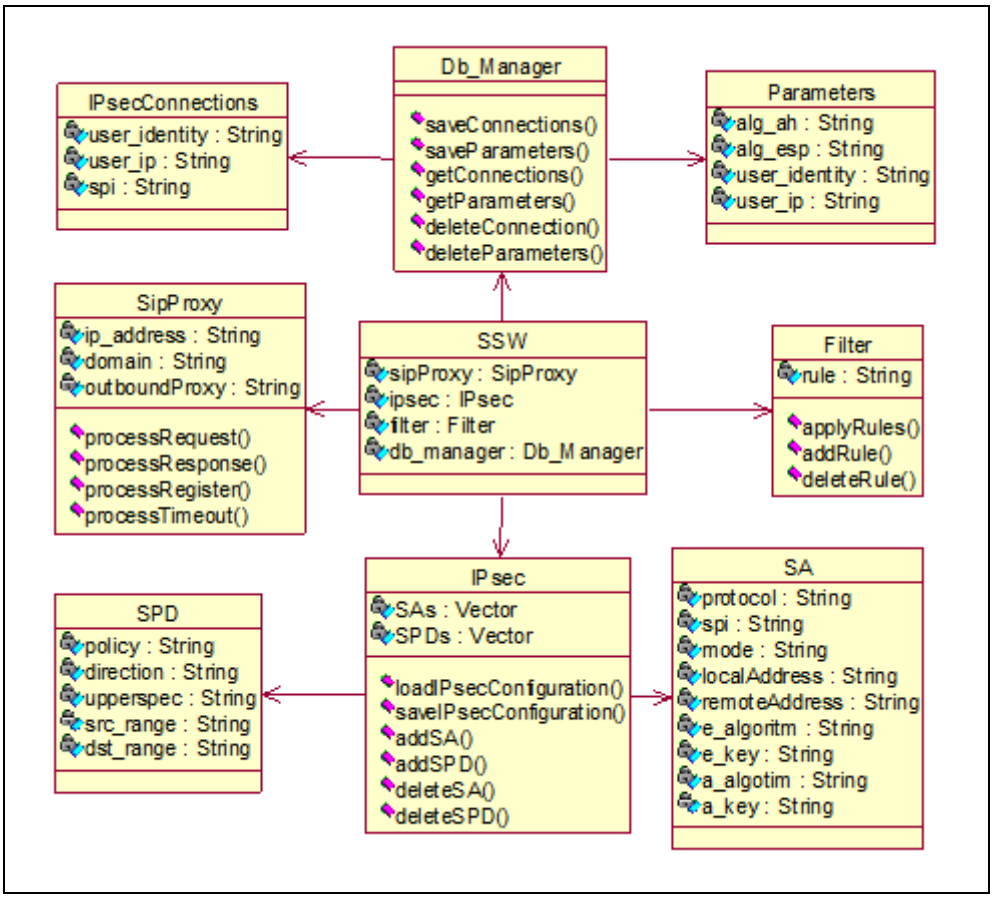

Figura 4. Diagrama de Clases de Análisis del SSW.

A.3.1.3. Subsistema de Seguridad P-CSCF

A.3.1.3.1. Modelo de Casos de Uso del Subsistema

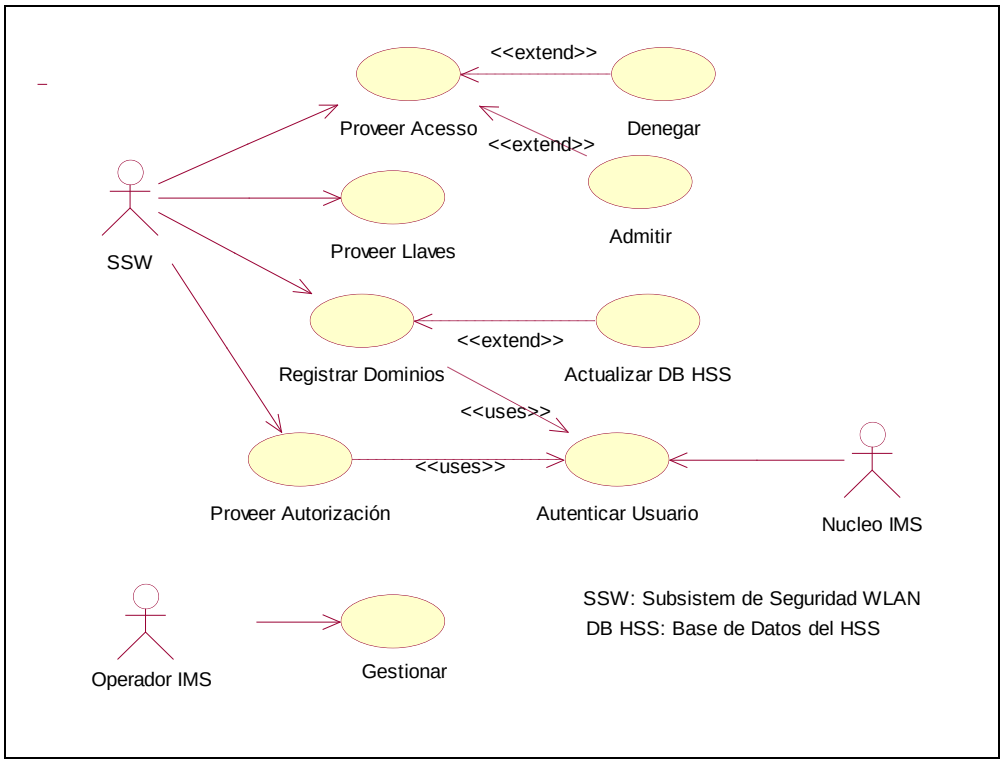

Figura 5. Diagrama de Casos de Uso del SSP.

A.3.1.3.1.1. Casos de Uso Iniciados por el SSW.

Caso de uso proveer acceso	
Iniciador	SSW
Precondiciones	SSP iniciado.
Flujo principal	1. El SSW envía una solicitud de servicio a IMS para un Usuario WLAN-IMS. 2. La solicitud ingresa como paquetes IP al componente IPsec del SSP. 3. El componente IPsec comprueba el origen y dirige el paquete al componente Filtro TCP/IP. 4. El componente Filtro TCP/IP aplica las reglas sobre el paquete. 5. Si el SSW encuentra dentro de los permisos para la prestación de servicios IMS se envía el paquete hacia la interfaz de red que permite alcanzar el destino del paquete.
Subflujos	Ninguno
Flujos alternativos	Ninguno
Flujos de excepción	3. El componente IPsec encuentra un error en la autenticación o integridad del paquete. 4. El SSP descarta el paquete.
Postcondiciones	Acceso provisto Acceso denegado
Notas	Ninguna

Caso de uso proveer llaves	
Iniciador	SSW
Precondiciones	Estado de registro del SCSWI “En Proceso”
Flujo principal	1. El SSW envía al SSP un mensaje SIP REGISTER proveniente del SCSWI.

	2. El SSP responde con el mensaje 401 No Autorizado al SSW, el cual contiene las llaves de seguridad. 3. El SSW extrae las llaves de seguridad y las elimina del mensaje.
Subflujos	Ninguno
Flujos alternativos	Ninguno
Flujos de excepción	Ninguno
Postcondiciones	Ninguna
Notas	Ninguna

Caso de uso registrar dominios	
Iniciador	SSW
Precondiciones	Estado de registro del SCSWI "En Proceso"
Flujo principal	1. El SSW envía al SSP un mensaje SIP REGISTER proveniente del SCSWI, el cual contiene los dominios que el Usuario WLAN-IMS desea registrar. 2. El SSP retira los dominios a registrar y reenvía el mensaje al núcleo IMS. 3. El núcleo responde con el mensaje 401 No Autorizado y el SSP lo reenvía al SSW 4. El SSW responde con el mensaje de autenticación del Usuario WLAN-IMS 5. El SSP reenvía este mensaje al núcleo IMS 6. El núcleo IMS responde con el mensaje OK indicando que el Usuario WLAN-IMS fue correctamente autenticado. 7. El SSP registra los dominios en el HSS
Subflujos	Ninguno
Flujos alternativos	Ninguno
Flujos de excepción	Ninguno
Postcondiciones	Ninguna
Notas	Ninguna

Caso de uso proveer autorización	
Iniciador	SSW
Precondiciones	Estado de registro del SCSWI "En Proceso"
Flujo principal	1. El SSW envía al SSP un mensaje SIP REGISTER proveniente del SCSWI. 2. El SSP reenvía el mensaje al núcleo IMS. 3. El núcleo responde con el mensaje 401 No Autorizado y el SSP lo reenvía al SSW 4. El SSW responde con el mensaje de autenticación del Usuario WLAN-IMS 5. El SSP reenvía este mensaje al núcleo IMS 6. El núcleo IMS responde con el mensaje OK indicando que el Usuario WLAN-IMS fue correctamente autenticado. 7. El SSP elabora el encabezado de autorización y los agrega al mensaje OK proveniente del núcleo IMS. 8. El SSP reenvía el mensaje al SSW 9. El SSW retira el encabezado de autorización y configura las reglas del ACL.
Subflujos	Ninguno
Flujos alternativos	Ninguno
Flujos de excepción	Ninguno
Postcondiciones	Ninguna
Notas	Ninguna

A.3.1.3.1.2. Casos de Uso Iniciados por el Operador IMS

Caso de uso gestionar	
Iniciador	Operador IMS
Precondiciones	Ninguna
Flujo principal	1. El Operador IMS ingresa los valores sobre el archivo de configuración. 2. El Operador IMS inicia la aplicación. 3. El Operador IMS escribe el comando "start" para iniciar el servidor. 4. El Operador IMS escribe el comando "stop" para detener el servidor. 5. El Operador IMS escribe el comando "exit" para salir de la aplicación.
Subflujos	Ninguno
Flujos alternativos	1. Con el servidor detenido, el Operador IMS cambia los valores sobre el archivo de configuración. 2. El Operador IMS escribe el comando "start" para iniciar el servidor. 3. El Operador IMS escribe el comando "stop" para detener el servidor. 4. El Operador IMS escribe el comando "exit" para salir de la aplicación.
Flujos de excepción	Ninguno
Postcondiciones	Ninguna
Notas	Ninguna

A.3.1.3.2. Diagrama de Clases de Análisis Esenciales del Sistema

A continuación se presenta el diagrama de clases de análisis para el SSP el cual esencialmente está conformado por:

Paquete Control

SSP: realiza la lógica de la aplicación para ello crea instancias de cada una de las clases principales de la aplicación. Instancia las clases: SipProxy para procesar la señalización SIP de registro y reenviarla al P-CSCF; IPsec para realizar la configuración de SA y SPD; Filter para configurara los filtros tras la autorización de acceso enviada por el SSP; Db_Manager como modelo de acceso a datos.

SipProxy: Provee el soporte de SIP para la comunicación de registro. Esta clase contiene los atributos y métodos necesarios para el reenvío de la señalización al P-CSCF.

Db_Manager: representa el modelo de acceso a datos, necesario para obtener las llaves CK e IK del HSS y para guardar el registro a los dominios solicitados por el Usuario WLAN-IMS.

User_keys: representa las llaves asignadas a un Usuario WLAN-IMS.

User_realm: corresponde a la relación de un Usuario WLAN-IMS con los dominios que tiene registrados.

Paquete Transporte

IPsec: corresponde a la interfaz para la configuración de IPsec contiene dos vectores uno para las SA y otro para las SPD IPsec, sus funciones principales son: cargar la configuración actual de IPsec del sistema operativo (SO), guardar cambios de configuración de IPsec sobre el SO, agregar SA, borrar SA, agregar SPD y borrar SPD.

SA: corresponde a la clase que representa las SA y contiene los atributos necesarios para definir una nueva SA.

SPD: corresponde a la clase que representa a las políticas de seguridad de IPsec (SPD), contiene los atributos necesarios para definir nuevas SPD.

Filter: corresponde a la interfaz de configuración del filtro para el control de acceso.

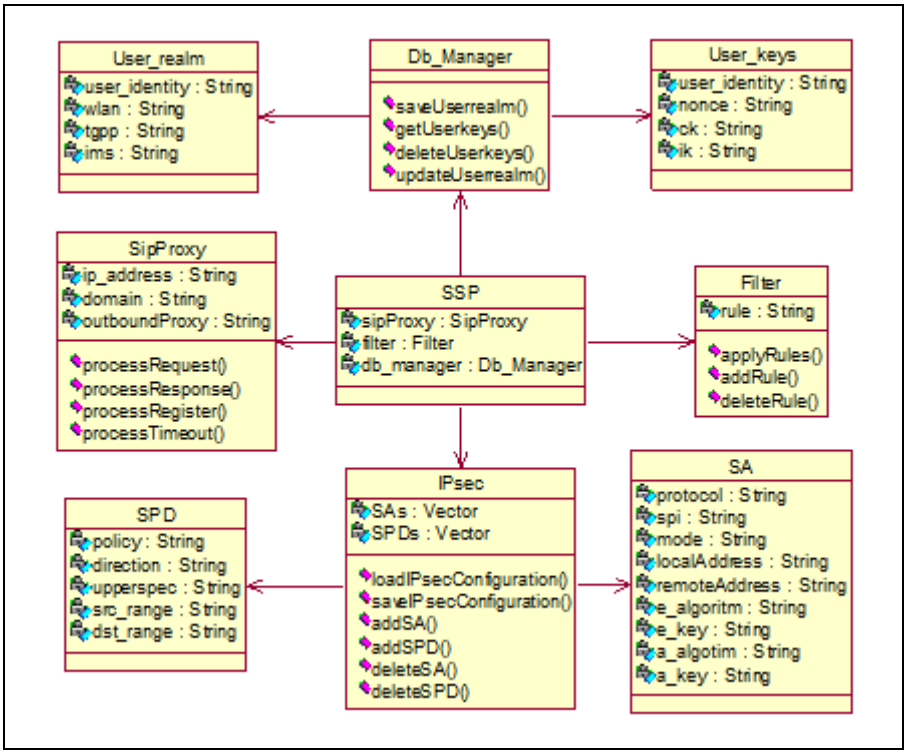

Figura 6. Diagrama de Clases de Análisis del SSP.

Bibliografía

[1] Jorge Ramió Aguirre, “SEGURIDAD INFORMÁTICA”, Madrid, España, 2002.
[2] Siler Amador Donado, Miguel Angel Niño, Andres Flechas. “Seguridad Computacional”, Universidad del Cauca 2002.
[3] Carlos Silva Ponce de León, “Seguridad de las Redes y Sistemas de Telecomunicaciones Críticos”, Revista de Telecomunicaciones No 116, Octubre/Diciembre de 2008.
[4] 3GPP TS 33.203, "3G security; Access security for IP based services", Release 8, Junio 2008.
[5] Carlos Serrano. “Modelo Integral para el Profesional en Ingeniería”. Popayan: Editorial Universidad del Cauca, 2005.
[6] CITEL. ”REDES DE PRÓXIMA GENERACIÓN”, disponible en http://www.citel.oea.org/sp/ccp1-tel/Carpetas%20Tecnicas/carpeta1-r5_e.pdf, 30 de Marzo de 2009
[7] IBM España, “Las propuestas de IBM para el desarrollo de la Sociedad de la Información”, Enero de 2004.