Documento Normativo para la Implementación de Políticas de Seguridad en la Red de Telecomunicaciones

Por MSc. Ing. Raymundo Pérez Sierra, Especialista B en Telemática,
Vicepresidencia de Desarrollo y Tecnología , ETECSA
raymundo.perez@etecsa.cu

I Introducción

Las últimas décadas han sido testigo de una evolución acelerada de las telecomunicaciones en el ámbito mundial, que se ha caracterizado por:

- El desarrollo de redes de datos desplegadas simultáneamente con las redes de telefonía básica que comparten los mismos recursos de transmisión.
- La incursión acelerada de la telefonía móvil, la cual ha detenido el crecimiento de la telefonía fija y, en algunos casos, comienza a sustituirla.
- La aceptación universal de Internet y de que las redes IP serán el soporte futuro de todos los servicios de telecomunicación.
- El desplazamiento de la inteligencia en la red fuera de los nodos de conmutación; primero, con las Redes Inteligentes y, posteriormente, con inteligencia en los bordes —pasarelas de media y control de acceso en el borde de la red—.

En este escenario se ha evidenciado una tendencia evolutiva hacia la integración de todos los servicios de comunicación en una única infraestructura de red IP, denominada comúnmente modelo Todo IP —*All-IP*—, proceso que ha mostrado las insuficiencias que tienen las soluciones IP tradicionales en temas como la capacidad, la Calidad del Servicio (CdS), la seguridad, la fiabilidad y la capilaridad. En consecuencia, el mercado de las telecomunicaciones se ha visto invadido por una gran variedad de equipos, técnicas, tecnologías y protocolos que, combinados adecuadamente, han propiciado el surgimiento de nuevos modelos de red que brindan todo tipo de servicios multimedia, tanto al usuario corporativo como al usuario residencial, a los que se les ha denominado modelos de Red de Próxima Generación o *Next Generation Network* (NGN).

En este contexto, el tema de la seguridad de las telecomunicaciones y las tecnologías de la información ha cobrado una importancia relevante. El aumento de la utilización de protocolos e interfaces abiertos, la diversidad de nuevos actores, la extraordinaria variedad de aplicaciones y plataformas y las implementaciones, no siempre probadas eficazmente, han conducido a una elevación del riesgo de un uso malintencionado de las redes [1], condicionando la presencia de un número importante de problemas de seguridad. Para enfrentar esta situación se requieren soluciones de seguridad completas y rentables que brinden una red protegida contra las amenazas malintencionadas o accidentales, en la que se garantice condiciones de alta disponibilidad, tiempo de respuesta apropiado, fiabilidad, integridad y escalabilidad, y se provea información exacta para la facturación. Precisamente, en aras de dar una respuesta a estos requerimientos, los esfuerzos de los grupos de normalización de reconocidas instituciones internacionales han estado dirigidos a neutralizar las amenazas a la seguridad en las áreas de infraestructura de telecomunicaciones, que abarcan desde los detalles de las especificaciones de los protocolos y aplicaciones hasta la gestión de las redes [1].

Específicamente significativo resultan, para este propósito, las últimas recomendaciones de la UIT-T enfocadas a los cambios que se están produciendo hacia la Red de Próxima Generación, tal como la Rec. X.805, debido a que no sólo proyectan las soluciones de seguridad para la infraestructura clásica de telecomunicaciones; sino también, para la nueva que ha emergido en el contexto actual.

Hasta el presente, ETECSA no cuenta con un documento rector específico que norme la implementación de políticas de seguridad en su red de telecomunicaciones. Por extensión, se aplican en la práctica los conceptos, medidas y regulaciones establecidos en el Manual de Seguridad Informática de la Empresa y otros documentos que, en esencia, fueron concebidos para los sistemas informáticos y de comunicaciones que conforman la Red de Datos de la Empresa o Red Corporativa. Por consiguiente, no contemplan las especificidades de la red de telecomunicaciones y su red de gestión. A partir de esta situación y considerando la insoslayable necesidad de garantizar una adecuada seguridad y protección de las redes de telecomunicaciones del país por su importancia estratégica, se emprendió la elaboración del Documento Normativo como contribución al aumento de la seguridad de la infraestructura tecnológica de la Empresa. Su antecedente fue un trabajo de maestría defendido en la Universidad Central "Marta Abreu" de Las Villas, que posteriormente fue actualizado y perfeccionado en dos versiones sucesivas entre los años 2005 y 2007, de las cuales se obtuvo este documento final (Figura 1).

ETECSA Grupo Seguridad Protección	DOCUMENTO NORMATIVO PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD EN LA RED DE TELECOMUNICACIONES	CÓDIGO: POL UNR-001-CI/GSP	
		REVISIÓN: 0	FECHA EMISIÓN: 25/09/06
		HOJA: 1	DE: 42

	Cargo	Nombre y apellidos	Firma
Realizado por:	Técnico C en Telemática UNR	Msc. Ing. Raymundo Pérez Sierra	
Revisado por:	Jefe de Grupo Seg. y Protección UNR	Ing. Oscar Estrada Marrero	
	Técnico en Normalización y Calidad UNR	Ing. Milagros M. Lescay Cordero	
Aprobado por:	Director Unidad de Negocios Red	Ing. Otto García García	
Distibuido a:			

Figura 1 Carátula del Documento Normativo. (Fuente: elaboración propia).

2 Características y contenido

2.1 Características del Documento Normativo

El Documento Normativo para la Implementación de Políticas de Seguridad en la Red de Telecomunicaciones (Tabla 1), como su nombre indica, posee un carácter normativo-metodológico y brinda una visión general acerca de los problemas de seguridad y sus posibles soluciones en los entornos de las redes de telecomunicaciones de nuestro país. También, pretende coadyuvar en la implementación de políticas y medidas de seguridad para aumentar la eficacia y seguridad de las telecomunicaciones y su gestión, que conlleva implícitamente un reforzamiento de la actividad de antifraude, basado en un conjunto de recomendaciones y normas elaboradas por los organismos de normalización internacionales, UIT-T e ISO, sobre la seguridad de la infraestructura de telecomunicaciones, los servicios y aplicaciones, así como la protección de la información por ellos soportada.

Contenido del Documento Normativo

1. Objetivos
2. Alcance
3. Términos, definiciones y acrónimos
4. Referencias
5. Responsabilidades
6. Desarrollo
   - Introducción
   - 6.1 Políticas de Seguridad para la Red de Telecomunicaciones
   - 6.1.1 La seguridad en las telecomunicaciones
   - 6.1.2 Vulnerabilidades, amenazas y riesgos en el entorno de las redes
   - 6.1.3 Requisitos del marco de seguridad en las redes
   - 6.2 Políticas de seguridad orientadas a la aplicación y cumplimiento de las dimensiones y requisitos de seguridad en la red
   - 6.3 Políticas de seguridad orientadas a garantizar las funciones de la gestión de seguridad en la red
   - 6.4 Políticas de seguridad orientadas a la protección contra las intrusiones no autorizadas en la red de comunicación de datos de la gestión
   - 6.5 Políticas orientadas a garantizar la compatibilización de los desarrollos e inversiones con la seguridad de la red
7. Anexos
8. Modificaciones

Tabla 1 Contenido del Documento Normativo. (Fuente: elaboración propia).

Su objetivo consiste en facilitar el análisis e implementación de políticas de seguridad en la red de telecomunicaciones de ETECSA, teniendo en cuenta sus características propias. Su alcance abarca las Unidades Organizativas que administren, operen y gestionen tecnologías, sistemas y redes de telecomunicaciones e incluye los siguientes componentes:

- Los elementos de infraestructura de las redes de telecomunicaciones sin incluir la Planta Exterior —dispositivos de transmisión, encaminadores, centros de conmutación, servidores y estaciones de trabajo—.
- Los sistemas gestores de los elementos de las redes de telecomunicaciones con sus componentes.
- Los servicios de red instalados en función de los usuarios —desde los básicos de transporte y conectividad hasta los de valor añadido—.
- Las aplicaciones de red a las que los usuarios tienen acceso, incluidas las propias de la gestión.
- La red de datos de la gestión.

La aplicación del Documento Normativo requiere tener en cuenta los resultados del análisis particular de riesgos en cada entorno, y las valoraciones económicas necesarias con la intención de alcanzar una correlación costo-beneficio adecuada en correspondencia con el valor de los activos y recursos que se pretenden proteger. Su observancia para el ámbito de las telecomunicaciones no exime del cumplimiento de las normas generales establecidas por los documentos rectores del país y de la Empresa, que se relacionan en las referencias del Documento.

2.2 La seguridad en las telecomunicaciones

La Recomendación X.805 de la UIT-T de 2003 "Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo", define el marco para la arquitectura y las dimensiones que garantizan la seguridad extremo a extremo de aplicaciones distribuidas [1], cuyos principios pueden ser aplicados a una amplia diversidad de redes independientemente de la tecnología de red y de la ubicación en la jerarquía de protocolos [2].

Esta arquitectura de seguridad fue concebida para abordar las exigencias generales de seguridad de proveedores de servicios, empresas y consumidores. Es adecuada para redes de voz, datos y convergentes, con tecnología inalámbrica, óptica o de cable [2]. La misma integra las particularidades de la gestión, control y uso de la infraestructura, los servicios y las aplicaciones de la red. Provee una perspectiva global, descendente y de extremo a extremo de seguridad de red, y puede ser empleada en elementos, servicios y aplicaciones de red para detectar, predecir y corregir vulnerabilidades de seguridad. La arquitectura en cuestión divide lógicamente un conjunto complejo de características de seguridad de red extremo a extremo en distintos componentes de arquitectura, lo cual permite considerar la seguridad de extremo a extremo de manera sistemática. Esto posibilita, a su vez, planificar nuevas soluciones de seguridad y evaluar la seguridad de las redes existentes.

La arquitectura de seguridad integra tres consideraciones esenciales para la seguridad extremo a extremo [2]:

1) ¿Qué tipo de protección se necesita, y contra qué amenazas?
2) ¿Cuáles son los diferentes conjuntos de equipos e instalaciones de red que es necesario proteger?
3) ¿Cuáles son las diferentes actividades de red que es necesario proteger?

La arquitectura de seguridad da respuesta a estas interrogantes al considerar tres componentes: dimensiones de seguridad, capas de seguridad y planos de seguridad, como se muestra en la figura 2.

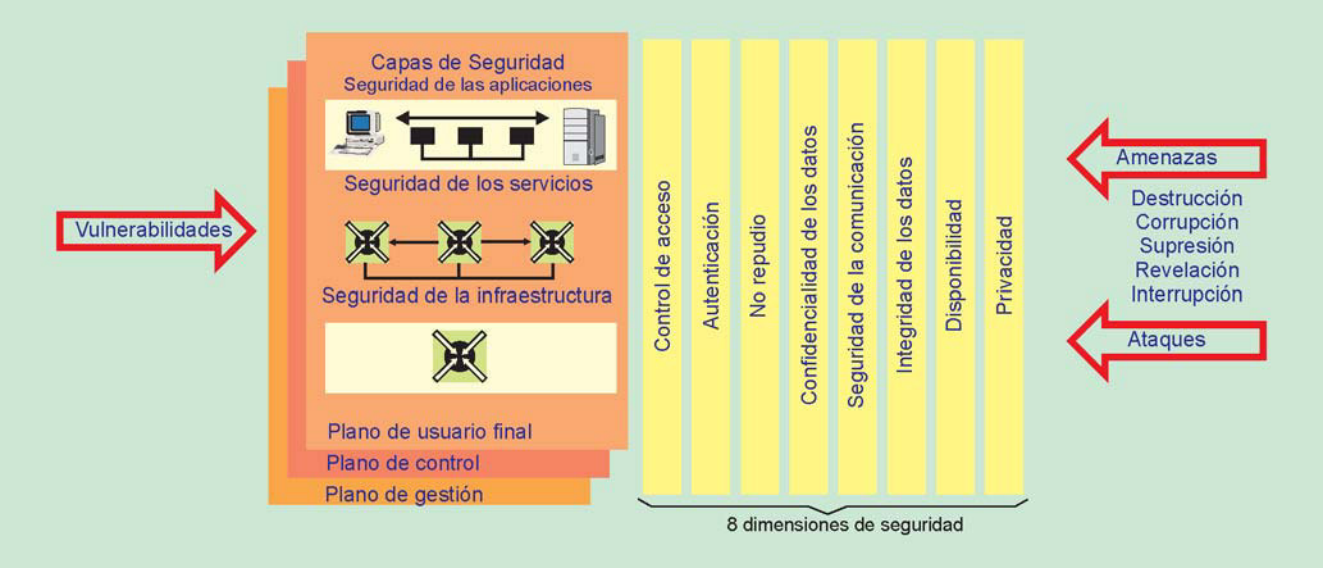

Figura 2 Arquitectura de seguridad. (Fuente: Recomendación UIT-T X.805).

Este enfoque arquitectural soporta un método de aplicación que consiste en la intersección de cada plano de seguridad —gestión, control y usuario final— con cada capa de seguridad —seguridad de la infraestructura, de los servicios y de las aplicaciones— y, de este modo, determinar un escenario específico (módulo) para cada intersección —en total 9— en el que se implementan, consecuentemente, las dimensiones de seguridad para contrarrestar las amenazas de seguridad latentes en cada uno de estos escenarios, propios de las redes de telecomunicaciones (Figura 3)[1]. En la gráfica se muestra el escenario de gestión en la capa de infraestructura al que se aplican las dimensiones de seguridad.

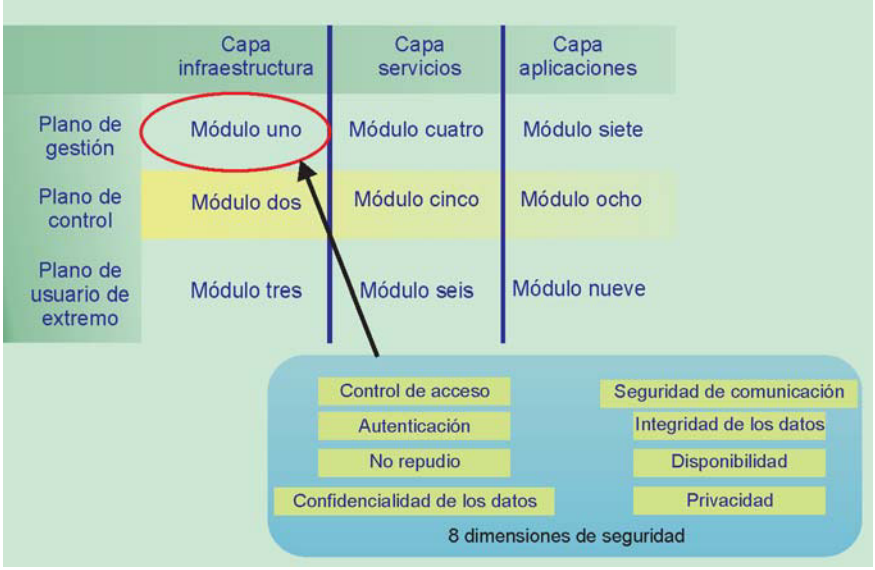

Figura 3 Aplicación de la arquitectura de seguridad. (Fuente: Recomendación UIT-T X.805).

De particular importancia resulta la posibilidad que brinda la arquitectura para abordar el planeamiento de la seguridad de la Red de Gestión de Telecomunicaciones, que incluye sus actividades, de modo íntegro, en el plano de gestión. El contenido y alcance de las dimensiones de seguridad, para este caso, son descritas como Requisitos Funcionales de Seguridad en las Recomendaciones de la UIT-T específicas para la Red de Gestión de las Telecomunicaciones —Rec. M.3016 y otras— recogidas en las referencias y que también sirvieron de base para la elaboración del Documento Normativo.

2.2.1 Vulnerabilidades, amenazas y riesgos en el entorno de las redes

Una **vulnerabilidad de seguridad** es un defecto o debilidad en el diseño, implementación o funcionamiento de un sistema que podría ser utilizado para violar su seguridad y no constituye un riesgo, amenaza o ataque. Existen cuatro tipos de vulnerabilidades [2]:

- vulnerabilidad **modelo de amenaza**: consecuencia de la dificultad para prever amenazas futuras.
- vulnerabilidad **diseño y especificación**: derivada de errores o descuidos en el diseño del protocolo que lo hacen inherentemente vulnerable
- vulnerabilidad **implementación**: resultante de errores en la implementación del protocolo.
- vulnerabilidad **funcionamiento y configuración**: efecto de la utilización errónea de opciones en las implementaciones o de políticas insuficientes de instalación.

Una **amenaza de seguridad** [2] es una violación potencial de la seguridad, que puede ser **activa —**cuando existe la posibilidad de un cambio deliberado y no autorizado del estado del sistema— o **pasiva** —cuando hay amenaza de revelación no autorizada de la información sin que se modifique el estado del sistema—. Ejemplos de amenazas activas son la usurpación de identidad y la negación de servicio; y de amenaza pasiva, la escucha clandestina para robar contraseñas no cifradas.

Un **riesgo de seguridad** [2] ocurre cuando se combinan una vulnerabilidad y una amenaza de seguridad. Las consecuencias de los riesgos de seguridad son las pérdidas y corrupción de datos, la pérdida de privacidad, el fraude, el tiempo fuera de servicio y la disminución de la confianza del público.

Aunque las amenazas cambien, siempre habrá vulnerabilidades de seguridad durante la vida de un protocolo. Si se trata de protocolos normalizados, los riesgos de seguridad relacionados pueden ser significativos y de escala global, por lo que es importante entender e identificar sus vulnerabilidades para poder contrarrestar las amenazas que se derivan.

2.2.2 Requisitos del marco de seguridad en las redes

Los requisitos necesarios para contar con un marco de seguridad de red genérico se originan de las siguientes fuentes [3]:

- **Los usuarios/abonados** deben confiar en la red y los servicios que ofrece, incluso, su disponibilidad en caso de catástrofes.
- **Las autoridades** exigen un nivel de seguridad mediante normas y leyes, con el fin de garantizar la disponibilidad de los servicios y la protección de la privacidad.
- **Los operadores de red y los proveedores de servicios** necesitan seguridad para salvaguardar su funcionamiento e intereses comerciales y cumplir con sus obligaciones ante sus usuarios.

Es conveniente que los requisitos de seguridad de las redes y servicios de telecomunicaciones se basen en normas de seguridad internacionalmente aceptadas, puesto que así se incrementa la interoperatividad y se evita la duplicación de esfuerzos. Debido a la gran cantidad de combinaciones posibles de las características de seguridad, se espera que haya perfiles de seguridad que cubran una amplia gama de servicios de redes de telecomunicaciones. Gracias a la normalización, podrán reutilizarse más fácilmente las soluciones y productos; esto implica lograr la seguridad de una manera más rápida y a un menor costo.

Los servicios y mecanismos de seguridad que pueden suministrarse a las redes de telecomunicaciones o a los proveedores de servicios tienen que ver con la protección contra ataques malintencionados, por ejemplo, la negación de servicio, la escucha clandestina, la simulación, la manipulación de mensajes —modificación, retardo, supresión, inserción, reenvío—, el repudio o la falsificación [3]. Esta protección incluye la prevención, detección y recuperación tras ataques, medidas para prever cortes de servicio debido a eventos naturales, así como la gestión de la información relativa a la seguridad. Es necesario prever disposiciones que permitan la intercepción legal cuando las autoridades correspondientes así lo demanden.

2.3 Políticas de seguridad en las redes de telecomunicaciones

Las políticas de seguridad en las redes de telecomunicaciones —posibles de implementar, incluyendo la red de gestión de telecomunicaciones con su red de comunicación de datos— constituyen los capítulos esenciales del Documento Normativo que se presenta y se orientan en cuatro direcciones fundamentales, a saber:

- La implementación y aseguramiento de las dimensiones y requisitos de seguridad en la red de telecomunicaciones.
- La garantía de las funciones de la gestión de seguridad en la red.
- La protección contra las intrusiones no autorizadas a la red.

- La compatibilización de los desarrollos e inversiones con la seguridad de la red.

El contenido de estos capítulos se resume a continuación:

Conjunto de políticas para la aplicación y cumplimiento de las dimensiones y requisitos de seguridad en la red

La aplicación de las dimensiones de seguridad contempladas en la Recomendación UIT-T X.805 [4], así como el cumplimiento de los requisitos y servicios de seguridad expresados en la Recomendación UIT-T M.3016 [5] que se resumen en este acápite; es un proceso que necesariamente debe enfrentarse a partir del enfoque de arquitectura de seguridad concebido en la Recomendación UIT-T X.805, bajo el cual deben aplicarse estas dimensiones y requisitos por cada plano y capa de seguridad de esta arquitectura.

En este capítulo se abordan las dimensiones y requisitos de seguridad en la red según las recomendaciones referidas: control de acceso, autenticación, no repudio, confidencialidad de la información, seguridad de la comunicación, integridad de la información, disponibilidad y privacidad.

También se brinda una panorámica sobre algunos mecanismos de seguridad más utilizados.

Conjunto de políticas para garantizar las funciones de la gestión de seguridad en la red

En este capítulo se contemplan las políticas de seguridad encaminadas a garantizar las funciones de la gestión de seguridad en la red de telecomunicaciones y redes de datos, en correspondencia con lo que se establece en la Recomendación UIT-T M 3400 y la Norma ISO/IEC 17799, agrupadas en los siguientes aspectos [6-7]:

- Control de acceso físico.
- Análisis del riesgo con el personal —selección y capacitación—.
- Respuesta a incidentes y anomalías de seguridad.
- Seguridad del equipamiento e instalaciones —Sistema Integral de Protección, Aseguramiento Energético y Sistema de Alarma Ambiental—.
- Detección de anomalías indicadoras de quebrantamientos de la seguridad, fraude o robo del servicio.
- Salva de la información de gestión, datos empresariales y de usuarios, configuraciones de red y de elementos de red.
- Respuesta y recuperación ante quebrantamientos de la seguridad y ante desastres.

Conjunto de políticas para la protección contra las intrusiones no autorizadas a la red

Este sección tiene como objetivo específico lograr una adecuada protección de los elementos de red, sistemas, aplicaciones e información contra posibles ataques externos e internos a la red de comunicación de datos de la gestión, incluyendo los códigos maliciosos, mediante la aplicación de un grupo de políticas de seguridad concebidas a partir de la Recomendación UIT-T M 3016 [5], Norma ISO 17799 [7] y documentos rectores nacionales y de ETECSA [1-2], [8-14].

Estas políticas abarcan los siguientes elementos de seguridad de las redes:

- Organización, administración y control jerarquizados de los recursos informáticos en toda la red.
- Sistema de protección para evitar posibles intrusiones en los elementos de la red.
- Medidas para contrarrestar los programas maliciosos y otras formas de intrusión.
- Pasarela segura en la red de datos de la gestión —en el caso de ETECSA, denominada GESNET— como vía de conexión de los elementos de la Red de Gestión con la Red Corporativa u otras redes externas.
- Confidencialidad, integridad y no repudio del flujo de datos entre los nodos y sistemas de la red de datos de la gestión.

Conjunto de políticas para la compatibilización de los desarrollos e inversiones con la seguridad de la red

El propósito esencial de este apartado es garantizar que todo nuevo desarrollo y todas las inversiones tecnológicas, incluido el aseguramiento de programas asociado, sean compatibilizados internamente con los intereses de la seguridad de la red de telecomunicaciones.

3 Resultados y discusión

En el proceso de elaboración, actualización y perfeccionamiento del Documento Normativo, se tuvieron en cuenta los resultados obtenidos en dos Talleres Nacionales de Seguridad de la Red de Telecomunicaciones, celebrados en diciembre de 2003 y mayo de 2005, y convocados por la Unidad de Negocios Red de ETECSA en esos años. Ahí participaron otras Unidades Organizativas involucradas con el fin de levantar las vulnerabilidades existentes en esta red. Al mismo tiempo, se consideró la puesta en vigor por la UIT-T en el 2003 de la Recomendación X. 805 sobre la "Arquitectura de seguridad para sistemas de comunicaciones de extremo a extremo"[4] no disponible para la versión original del documento, así como los resultados de visitas y controles realizados a diferentes centros de gestión del país y los análisis conjuntos sobre el tema realizados con personal de operación y gestión de algunos de estos centros,

fundamentalmente el Centro de Supervisión y Gestión Nacional (CSGN).

El Documento Normativo fue sometido a la consideración de especialistas y entidades afines de la Empresa y aprobado, posteriormente, por el Consejo de Dirección de la misma Unidad en marzo de 2006. En estos momentos, se encuentra en proceso de valoración y puesta en vigor en el Nivel Corporativo.

Desde su segunda versión en el 2005, fue un documento de consulta y aplicación práctica cotidiana en la Unidad Organizativa mencionada, lo que se ha materializado en la elaboración de documentos internos —Instrucción 1 del 30/5/2005: Sobre el proceso de compatibilización de las inversiones con Seguridad y Protección en la Unidad de Negocios Red—, en actividades de compatibilización y pruebas de aceptación de nuevas tecnologías desde finales del 2005 y hasta su disolución, tales como centrales C&C08 Huawei, SoftSwich/Core NGN Huawei, NGN Ericsson, Red Inteligente OSP2.4 Alcatel, Outdoors Ericsson, ZTE y Huawei, y en visitas y controles realizados a diferentes centros de gestión de telecomunicaciones del país. Con la nueva estructura de la Empresa, desde noviembre de 2008, este Documento continúa aplicándose en el Departamento de Investigación y Desarrollo de la Dirección de Tecnología de la Vicepresidencia de Desarrollo y Tecnología (VPDT), durante el cumplimiento de las funciones relativas a la observancia de los requisitos de seguridad en las nuevas tecnologías en proceso de prueba y aceptación.

4 Conclusiones

El Documento Normativo para la Implementación de Políticas de Seguridad en la Red de Telecomunicaciones tiene un valor de uso significativo debido a que, tomando como punto de partida un grupo de recomendaciones y normativas emitidas por organismos internacionales adaptadas a las características de nuestro escenario, establece una metodología para las acciones a realizar con vista a la protección de las redes de telecomunicaciones de Cuba. En ese sentido puede concluirse afirmando que:

1- Este documento sintetiza los aspectos normativos internacionales acerca de la seguridad de las redes de telecomunicaciones, con una proyección hacia las nuevas generaciones de redes y adecuado a las características y condiciones del escenario del país.

2- Su puesta en vigor a nivel empresarial pondría a ETECSA en condiciones propicias para dar un impulso importante al fortalecimiento de la seguridad de la red de telecomunicaciones del país.

5 Referencias bibliográficas

[1] Resolución DDAR 01/2005 de ETECSA - Manual de Seguridad Informática.

[2] Resolución PE 03 de 2004 de ETECSA - Manual de Seguridad y Protección de la Información Oficial.

[3] UIT-T/Dic 2003 - La seguridad de las telecomunicaciones y las tecnologías de la información. Visión general de asuntos relacionados con la seguridad de las telecomunicaciones y la implementación de las Recomendaciones UIT-T existentes.

[4] Recomendación UIT-T X.805 (2003) Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo.

[5] Recomendación UIT-T M.3016.1 (2005) - Seguridad para el plano de gestión: requerimientos de seguridad.

[6] Recomendación UIT-T M.3400 (2000) - Funciones de gestión de la RGT.

[7] ISO/IEC 17799: 2000, Information Technology. Code of Practice for Information Security Management.

[8] Resolución PE 06 de 2004 de ETECSA - Compendio de Medidas Organizativas en el Sistema de Seguridad y Protección Física.

[9] Decreto Ley 199/99 del Consejo de Estado sobre la Seguridad y Protección de la Información Oficial.

[10] Resolución 6 de 1996 del MININT - Reglamento de Seguridad Informática.

[11] Resolución 204 de 1996 del SIME - Reglamento sobre la Protección y Seguridad Técnica de los Sistemas Informáticos.

[12] Resolución 39 de 2002 del MIC sobre Políticas de Seguridad Informática del MIC.

[13] Recomendación UIT-T M.3010 (2000) - Principios para una RGT.

[14] Recomendación UIT-T M.3016.0 (2005) - Visión general de la seguridad en la red de gestión de las telecomunicaciones.