UNIVERSIDAD DE CHILE

Facultad de Derecho

Escuela de graduados

Elaboración de una medida tecnológica que permita garantizar y proteger el adecuado tratamiento de los datos personales en el Internet de próxima generación/IPv6.

Tesis para optar el grado de Magíster en
Derecho de la Informática y de las Telecomunicaciones.

Rubén Cañihua Florez

Profesor Guía: Dr. Jens Hardings Perl.

-2007-

Agradecimientos

Quiero agradecer sinceramente a todas aquellas personas que compartieron sus conocimientos y experiencias conmigo para hacer posible la conclusión de la presente tesis.

A la Dra. Lorena Donoso, quien como Directora Académica del CEDI, ha cumplido el papel mas relevante en mi formación del postgrado.

A mi tutor el Dr. Jens Hardings Perl por su asesoría siempre dispuesta, aun en la distancia, por sus ideas y recomendaciones respecto a la s investigaciones.

Gracias a mis compañeros del Magíster, por su gran ayuda cuando me enfrentaba con ciertos problemas.

Gracias a todos ellos.

A mis padres, por su gran ejemplo de superación, su consuelo y su valioso apoyo en todo momento desde los inicios de mis estudios de maestría.

A mis hermanos por ese optimismo que siempre me impulso a seguir adelante en días y noches de investigación.

INDICE DE CONTENIDOS

Pag.

CAPITULO PRIMERO

Presentación

CAPITULO SEGUNDO

Fundamentos generales y bases teóricas del protocolo de Internet IPv6

CAPITULO TERCERO

Análisis de implicancias del protocolo de Internet IPv6 en relación con la privacidad.

CAPITULO CUARTO

Implicancias del protocolo de Internet de IPv6 en relación a la protección de datos personales.

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

CAPITULO PRIMERO

PRESENTACION

1.1 Introducción

La extraordinaria celeridad con la cual las sofisticadas tecnologías de información vienen desdibujando el nuevo curso vital de nuestra era digital, hacen que sea necesario tomar la debida importancia del impacto que estas contraen con respecto a las ciencias reactivas del derecho, entendida esta, desde el ámbito de las posibles invasiones que se presentan en la privacidad y la vulneración de nuestros datos personales en el Internet, ya que enfrenta, un papel clave dentro de un escenario de regulación cual es, la búsqueda de determinar las soluciones mas competentes ante estos avances tecnológicos según la construcción de adecuadas condiciones de legalidad que le serán impuestas y que a su vez se encuentre vinculado a un tratamiento de la información ajustado a la mejora del desarrollo de los sistemas jurídicos, que sean potencialmente eficaces y dinámicos en la interpretación y su propia aplicación en la Legislación Chilena, acorde a los tiempos en que vivimos. Pues por tal circunstancia, en esta ocasión, me delimitare a exhibir específicamente el análisis de las principales implicaciones que conllevan en materia de la protección de datos personales y la privacidad con referencia al protocolo de Internet de próxima generación.

Como sabemos, el perfeccionamiento de las redes de computadoras de superior tecnología en la arquitectura de sus dispositivos Microchips

ensambladas con nanotecnologías moleculares[1], junto con los avances en el diseño de sofisticados programas con inteligencia artificial, redes neuronales y algoritmos genéticos aplicados a los campos del derecho[2], la robótica autómata[3]-[4], etc., hacen que nuestra realidad evolucione de forma acelerada, no respetando tiempo, ni espacio geográfico; viviendo en la actualidad en una nueva era de las telecomunicaciones, la era del ciberespacio[5], un ciberespacio virtual interpretado a través de la infraestructura de bits[6], y diseñada por la simbiosis de interrelación entre la maquina y lo humano; es así, que estas complejas comunicaciones enmarañadas de redes de redes interconectadas en todo el hemisferio en tiempo real hacen que día a día sea escasa la existencia de los puntos o nodos interconectados al Internet o las llamadas direcciones **IPv4**[7] a pesar incluso de los intentos de latencia de **NAT**[8] por prolongar la vida

---

[1] Microprocesadores de cilicio avanzados con conexiones moleculares discretas creadas por reacciones químicas a una escala billonesima, construidas por auto-ensamble con métodos de diseños análogos, según Bill Spence "un billón de veces más pequeño, un billón de veces más potente; transformando la concepción de la informática y los sistemas a una escala de nivel atómico para controlar y dominar la naturaleza". La nanotecnología es un campo de las ciencias aplicadas dedicado al control y manipulación de la materia a una escala menor que un micrómetro, es decir, a nivel de átomos y moléculas. El premio Nobel de Física Richard Feynman fue el primero en hacer referencia a las posibilidades de la nanociencia y la nanotecnología en el célebre discurso que dio en el Caltech (Instituto Tecnológico de California) el 29 de diciembre de 1959 titulado Al fondo hay espacio de sobra (*There's Plenty Room at the Bottom*).

[2] En la actualidad la Informática Jurídica y el Derecho Informático constituyen las áreas de avanzada del Derecho. Así pues "La informática jurídica estudia el tratamiento automatizado de: las fuentes de conocimiento jurídico, a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal (Informática jurídica documental); las fuentes de producción jurídica, a través de la elaboración informática de los factores lógico-formales que concurren en el proceso legislativo y en la decisión judicial (Informática jurídica decisional); y los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho (Informática jurídica de gestión)" (Perez Luño, Antonio Enrique. Manual de informática y derecho. Barcelona, Editorial Ariel, 1996, p.22) y el "Derecho informático o derecho de la informática es una materia inequívocamente jurídica, conformada por el sector normativo de los sistemas jurídicos contemporáneos integrado por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir de la informática y la telemática"(Perez Luño, Antonio Enrique. Manual de informática y derecho. Barcelona, Editorial Ariel, 1996, p.18).

[3] La robótica es una rama de la tecnología, que estudia el diseño y construcción de máquinas capaces de desempeñar tareas repetitivas o peligrosas para el ser humano. Las ciencias y tecnologías de las que deriva podrían ser: el álgebra, los autómatas programables, las máquinas de estados, la mecánica, la electrónica y la informática. La palabra robot fue acuñada por primera vez en 1920 por Karel Capek que proviene de la palabra checa "robota" (En la actualidad se presentan; Robonaut: Robot operador de la NASA, Ariel: Robot diseñado para salvar vidas, M2: Robot guía de la MIT, Locaas: Robot militar autómata de quirúrgica precisión del Dep. Defensa USA, Rimotech: Robot agente. P3: Robot de conducta humana de HONDA, Robart3: El robot guerrero del centro de guerra espaciales y navales de San diego-California financiada por Pentágono, DP: Robot dinámico Univ. Carolina del Sur, Kismet: Robot de emociones de la MIT…).

[4] Sistemas de tecnología de avanzada que toman decisiones por si mismos, sin intervención humana con la inteligencia artificial que dotan a la maquina para que piense por su propia lógica.

[5] Red de revistas científicas de América Latina y el Caribe – Emilia Bermudes y Gildardo Martinez Convergencia Nro. 26, 1405-1435 UNIVERSIDAD AUTONOMA DE MEXICO Pags. 11-31.

[6] Reacuérdese que un bit es la unidad mínima de información, y se trata de un valor que únicamente puede ser 0 ó 1. Así para almacenar 2 valores se tiene suficiente con un solo bits. Es bueno recordar que 1 byte es 8 bits.

[7] **IPv4:** Protocolo de Internet versión 4, es el actual protocolo con el que funciona Internet. Ref. RFC 791

útil frente a este agotamiento evidente, contando en la actualidad con solo **4.294.967.296** de direcciones IPv4, que se vienen extinguiendo por el natural crecimiento del Internet en todo mundo.

Ilustración 68. Estado del Arte de la extinción de direcciones Ipv4 por LACNIC[9].

Por ello pensando y preocupados por tal problemática de falta de direcciones entre otros factores[10], indicador clave para el funcionamiento de la red global, los científicos deslumbraron una solución tecnológica, por la cual, se creo el protocolo **IPv6**[11] diseñado por Steve Deering y Craig Mudge y adoptado por la IETF(*Internet Engineering Task Force)*[12] a través de los estándares internacionales de las RFCs(*Request For Comments*)[13] con lo que se precisa soportar un numero enorme de 340 sextillones o 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones con el fin de mejorar la calidad de vida de los usuarios y mantener la continuidad del futuro del Internet, por tal situación, organismos como la ICANN(*Internet*

---

[8] **NAT** (Network Address Traslation) traducción de direcciones de red que añade complejidad al despliegue de nuevos modelos extremo a extremo, inhibiendo el crecimiento de Internet y la innovación, incluyendo aquellos servicios como "siempre conectado" y "peer to peer" que quieren acceso seguro y constante a dispositivos. NAT es también conocido como el demonio de la innovación.

[9] LACNIC, anuncia oficialmente inminente agotamiento de direcciones Ipv4, http://portalipv6.lacnic.net/

[10] Factores de Existencia del protocolo IPv6(El IPngD *"IPng Directorate"* público el RFC 1550 de solicitud de requerimiento): a)IPv6 debería permitir la encapsulación de sus propios paquetes o de los de otros protocolos. b)IPv6 debería añadir clases de servicio para distinguir los tipos de datos transmitidos, tales como tráfico isócrono como audio y vídeo en tiempo real. c)IPv6 debe proporcionar direccionamiento multicast de forma que esté más completamente integrado con el resto de la pila que IPv4. d)IPv6 debe proporcionar autentificación y encriptación. e) IPv6 debería preservar las virtudes de IPv4: robustez, independencia de las características de la red física, alto rendimiento, topología flexible, extensibilidad, servicio de datagramas, direccionamiento unívoco a nivel global, protocolo de control integrado y estándares de libre distribución. f) La implementación debe suponer una transición sencilla. g)IPv6 debe coexistir con IPv4.

[11] **IPv6:** Protocolo de Internet versión 6, destinado a sustituir el protocolo Ipv4. Ref. RFC 2460.

[12] **IETF:** Organización internacional de normalización www.ietf.org es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería del Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad. Creada en EE.UU. en 1986.

[13] **RFCs:** Estándares internacionales para el Internet www.rfc.net, los RFCs describen todo el trabajo interno en Internet. Pero no todas las RFCs especifican estándares. Hay 5 clases de clasificaciones en las RFCs: Required(Requerido), Recommended(Recomendada), Elective, Limited de Use(Uso limitado) y Not Recommended(No recomendada). Si un documento comienza a ser considerado como un estándar, comienza a pasar por los diferentes estados de desarrollo, prueba y aceptación. Durante este proceso, estos procesos son formalmente llamados "Maturity Levels"(Niveles de Maduración). Hay tres niveles de maduración en los estándares de Internet: Proponed Standard(Propuesta), Draft Standard(Borrador) e Internet Standard.

Corporation for Assigned Names and Numbers)[14] y IETF unidos en conjunto estiman una inminente convivencia y transición tecnológica y en el futuro una completa adopción[15].

Por tal circunstancia, se percibe que la naturaleza de estas implicaciones tecnológicas[16] reales propicia a realizar un análisis pormenorizado de las condiciones de legalidad que implican su despliegue y como así mismo nos derivan un conjunto de aspectos legales nucleares a tratar en materia de:

1.- El derecho a la intimidad[17]/privacidad[18].

2.- Protección de datos personales.

Ofreciendo así nuestra investigación, una serie de consecuencias jurídicas en el despliegue e implantación del protocolo IPv6, las cuales en esta ocasión, las analizaremos y orientaremos a la búsqueda de perseguir un adecuado aseguramiento dentro del ámbito legal aplicable a efectos de que no vulnere la legislación ni los derechos fundamentales y libertades que se les son

---

[14] **ICANN:** Corporación de Internet para la asignación de nombre y números www.icann.org, organismo independiente sin ánimos de lucro creado el 18-09-1998 con el objeto de coordinar la asignación global de identificadores que deben ser únicos en Internet tales como el espacio de direcciones IP, el sistema de asignación de nombre de dominio y la definición de parámetros de los protocolo utilizados. Sustituye en estas funciones a la IANA.

[15] Objetivo principal de todas las Task Force's en la comunidad mundial www.ipv6tf.org

[16] Las nuevas tecnologías nos permiten transgredir fronteras nuevas, conocer información que antes era impensable y sobre todo, relacionar, almacenar, buscar y transmitir esta información. Sin embargo las señales de alerta se disparan ante los nuevos peligros que dichas tecnologías representan. Las tecnologías de la información y comunicación permiten nuevas maneras de inferencia en este ámbito protegido. Se trata de instrumentos que son infractores potenciales de la vida privada. Una nueva manera de violar la esfera privada de un sujeto consiste en la recogida, el almacenamiento y el control de sus datos. Un rasgo que incrementa el peligro de esta herramienta es que el control se puede hacer de manera prolongada en el tiempo, a menudo sin que la persona afectada se de cuenta de ello. Cada vez que navegamos por la red, compramos un libro o un billete de avio por Internet, visitamos una página Web, consultamos nuestras cuentas por medio del banco en línea, etc. Estos instrumentos nuevos representan realmente un riesgo y una amenaza para la privacidad, la intimidad, la defensa de una esfera de autonomía personal. Por lo tanto, hay que articular mecanismos nuevos de protección de la vida privada de las personas.

[17] El derecho a la intimidad es uno de los derechos fundamentales reconocidos en la mayoría de las cartas de derecho fundamentales y constituciones. Un derecho al cual difícilmente queremos renunciar según Miquel Peguera Poch, Albert Agustinoy Guilayn, Ramon Casas Valles, Agusti Cerrillo i Martinez, Ana M. Delgado Garcia, Jordi Herrera Joancomarti, Mark Jeffery, Oscar Morales Garcia, Rafael Oliver Cuello, Guillermo Ormanzabal Sanchez, Monica Vilasau Solana y Raquel Xalabarder Plantada "Derecho y nuevas tecnologías", Editorial UOC 2005, pag. 93.

[18] El Oxford English Dictionary define Privacy como, "estado o condición de estar retirados de la sociedad, de otros o del interés público". Si acudimos a la definición francesa que nos da Trésor de la Langue Francaise, vida privada es "lo que se sitúa en el nivel mas profundo de su vida psíquica, que permanece generalmente escondido bajo las apariencias, impenetrable a la observación externa, a veces al análisis del sujeto mismo".

reconocidos a los sujetos[19], considerando a este último como al hombre como sujeto protegido por el derecho a la privacidad, y que a su vez estos se manifiestan socialmente comunicándose[20] y que por tal circunstancia, dicha comunicación e información sobre la misma[21] debe ser protegida.

Por otro lado perceptiblemente también cabe la necesidad de prestar la debida atención a un punto especialmente delicado que es la denominada protección de datos personales analizada desde la perspectiva tecnológica[22] del protocolo Ipv6 con la necesidad de refrescar y empapar tecnológicamente pensamientos jurídicos a través de la técnica.

Encontrándonos entonces con un abanico de puntos legales a tratar, pero delimitaremos el desarrollo de la presente tesis, al contexto de la privacidad y protección de datos personales abordado desde la problemática del tratamiento de las direcciones de Internet para el caso de la existencia de "identificadores únicos" configurados en base al protocolo IPv6 que tienen la característica de no cambiar en el tiempo dejando así en el Internet rastros a modo de huellas[23]; para entender mejor, por ejemplo, cada vez que una persona accede al Internet, se podrá obtener una única autentificación realizándose así a través de ella un estudio detallado del perfil, gustos, etc, de esta persona[24] y en definitiva, efectuar un conjunto de rastreos de la navegación de los usuarios, saliendo a la luz preguntas como ¿Qué consecuencias legales concretas pueden existir?, ¿se vera la privacidad de los usuarios afectada por el IPv6?, ¿existen implicaciones en materia de protección de datos?, ¿será la dirección IP un dato

[19] El sujeto, la persona, se convierte en "dato", en un conjunto de información que puede llegar a ser muy preciada, tanto para el estado, para el poder, agentes externos, etc.

[20] Nuestro análisis deberá recaer sobre el ciudadano común, en oposición a los personajes públicos, sean artistas, deportistas, políticos o celebridades en general.

[21] E incluso no nos resulta difícil percibir que sus comunicaciones son aun mas relevantes que las simples informaciones. Y ello porque, mas que cualquier información destacada, las comunicaciones producidas por el hombre confieren un mayor peso a su personalidad. Conocer la voz de alguien significa menos que oírla. La comunicación en si misma tiene más trascendencia que una mera información. Por ello se hace necesario protegerla en grado igual o superior que para la información. Y eso es lo que se busca hacer.

[22] Victor Drummond, Internet, Privacidad y datos personales, Editorial Reus Madrid-España 2004, pag. 26

[23] Tal vez como consecuencia de esta situación, los juristas se encuentran perplejos ante las innovaciones tecnológicas y ante el intento de desvelar la sociedad de la información de la que formamos parte. Y, en cuanto se observa el nuevo mundo y se buscan soluciones para el ciudadano común, terceras partes controlan una observancia cada vez más cercana. Para nosotros el peligro de la vulneración de nuestros datos es único: el peligro de no existir.

[24] Cabe resaltar que la tecnología deja al ciudadano a merced de terceros, por lo que respecta a la manutención o manipulación de los datos e informaciones referidos a su persona.

personal? , ¿Qué esta permitido hacer con la información que se tiene acerca de los hábitos de navegación de un usuario?, etc.[25]; al obtener así un denominado autentificador único de Internet que permitirá identificar a cada persona por las redes desplegadas en el protocolo de Internet Ipv6. Ofrecido así, a que el enfoque propuesto se orientara a plantear realizar un análisis tecnológico jurídico, descifrado desde las ciencias de la computación, a efectos de analizar las condiciones de operatividad y legalidad del protocolo Ipv6.

En tal sentido, atendiendo al presente contexto, se precisa indicar que la naturaleza del despliegue actual que enfrenta el protocolo Ipv6 constituirá un entorno tecnológico y social nuevo que generara riesgos, además de sus beneficios; para la vida en el Internet de las personas que navegan o cuyos datos circulan por la red si no se toman a tiempo las medidas correctivas tecnológicas o jurídicas del caso, antes de su despliegue. Las peculiares características del Ipv6 junto con su especial fisonomía viene en gran medida marcada por la interactividad de las comunicaciones y la generación de un elevado número masivo de datos transaccionales o de conexión permanente que es utilizable para finalidades diversas en el trafico y el tratamiento de datos, percibiéndose contractualmente así, aspectos como:

- Los datos de navegación del usuario que son conservados e interceptados por el proveedor de acceso (datos de conexión asociados a la dirección Ipv6, con una exacta precisión a diferencia del actual protocolo de Internet que venimos utilizando Ipv4) que pueden permitir un seguimiento de la actividad detallada de un usuario(los webs visitados, la fecha y hora, los documentos telecargados, la participación en un espacio de discusión, los mensajes electrónicos enviados o recibidos; en síntesis una base de datos de trazabilidad de meta-data, potencialmente peligroso y además, muy atractivo para las empresas que recolectan datos con fines comerciales) durante todo el tiempo en que se conserven estos datos. Ello junto a la particular estructura

[25] Comision Europea, ConsulIntel, Ecija, Jordi Palet Martínez, Basar Kaisor(U. de Oxford), Francisco Javier Carballo Varques(U. de Cantabria), Alvaro Ecija Bernal(U. Autonoma de Madrid), Jennifer Gil Krokun(U. Complutense de Madrid), Antonio F. Gomez(U. de Murcia), Alberto Saiz Peña(U. de Alcala) y David G Mills(U. de Southampton) "IPv6: Aspectos Legales del Nuevo Protocolo de Internet", documento de la www.ipv6tf.org.

de Internet que permite el empleo de herramientas de búsqueda sofisticadas, agentes inteligentes y otros programas informáticos con tecnologías de avanzada[26], ofrecen particulares riesgos en la fase de recogida de datos personales.

- Concerniente a la normativa Chilena sobre la protección de la vida privada o protección de los datos personales Ley Nº 19.628[27], se enfrenta a 3 retos fundamentales: la vulnerabilidad, el carácter abierto de la red y la facilidad para realizar tratamientos invisibles (no conocidos por la persona concernida) sobre los datos relacionados con la selección contenidos o su identificación electrónica.
- Si la red es vulnerable tanto a los ataques de terceros como a los errores o accidentes que puedan ocurrir en la transmisión de la información ello se traduce, desde la perspectiva de la protección de datos personales, en la necesidad de adoptar especiales medidas de seguridad, como la norma Chilena Oficial NCh2777-ISO/IEC 17799:2000(Tecnología de Información – Código de practica para la gestión de seguridad de la información)[28] o la utilización de procedimientos técnicos de cifrado y control de acceso a los archivos o informaciones que contengan datos de carácter personal o, incluso, la especial responsabilidad de los agentes involucrados en los tratamientos de datos[29] realizados a través de la red.
- El carácter abierto y global del despliegue de Ipv6 en el Internet dificultara la sujeción de los tratamientos de datos personales a una normativa uniforme y generalmente aceptada por todos los países, obliga a acudir a la defensa de

---

26 

27 Ley Nº 19.628 Ley sobre protección de la vida privada o protección de datos de carácter personal, publicada en el diario oficial de 28 de agosto de 1999.

28 Norma Chilena Oficial NCh2777 – ISO/IEC 17799: 2000 denominada "Tecnología de la información – Código de Practica para la Gestión de Seguridad de la Información" que ha sido preparada por la División de Normas del Instituto de Normalización y aprobada por el Consejo del INN(Resolución Exenta Nº92), donde es establecen las recomendaciones sobre la gestión y la seguridad de la información; siendo una norma homologada de la Norma Internacional ISO/IEC 17799:2000 Information Tecnology – Code of practice for information secutity management.

29 Operaciones y procedimientos técnicos de carácter automatizado, que permiten la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

la vida privada de los usuarios. Perdiendo en la actualidad control, el interesado sobre sus datos.

- Los proveedores de acceso están situados en una posición privilegiada para el tratamiento de los datos de conexión relacionados con una determinada dirección Ipv6 y pueden asociar dicha dirección Ipv6 con el conjunto de datos personales relativos al usuario, que es su cliente, por ello están sujetos a unas reglas especiales de destrucción de los datos de tráfico.
- El principio fundamental que debe regir el tratamiento de datos transaccionales en Ipv4 o Ipv6 con el uso de Internet, dentro de los cuales quedan incluidos los archivos logs[30], cookies[31] y los clickstream date[32], es el del anonimato. El anonimato esta ligado por un lado a la libertad de expresión y también ligado a las facultades de control de los datos personales por un titular, entonces si es posible la comunicación anónima o en claro.

Motivado por tal situación y considerando el ámbito legal de la protección de datos personales en torno al cual giran las telecomunicaciones electrónicas, ya sean por espectros para cables o satélites, ser consideradas como una ponderable prioridad fundamental de investigación para quienes nos dedicamos a las nuevas tecnologías[33]-[34] y adoptamos como manifestaba Frossini una "conciencia tecnológica"[35], lograr pretender realizar un profundo análisis legal de las posibles vulneraciones que IPv6 podría conllevar con respecto a la privacidad y la protección de datos de los usuarios respecto a las implicancias

[30] Conocidos también como estadísticas del servidor, son la fuente de información primaria y fiable de conocimiento acerca de los usuarios actuales de nuestro sitio.
[31] Es un archivo pequeño que se salva en su ordenador. Ese archivo es escrito por el ordenador remoto que le está enviando la información a través de la World Wide Web.
[32] Es la información que los usuarios generan mientras se mueven de página en página y hacen clic en objetos dentro de un sitio Web, usualmente se almacena en archivos de registro.
[33] Miguel Angel Davara Rodríguez, "La protección de datos personales en el sector de las comunicaciones electrónicas", Universidad Comillas Madrid ISBN:84-932521-5-8.
[34] La Ley de Moore esbozada por Gordon en 1965 que sostenía la duplicación de periodos de tiempo de la capacidad de procesamiento de la información por los computadores; sin embargo, su vigencia, aun cuando contingente, también se ha mostrado idónea para dimensionar el crecimiento exponencial de la capacidad de almacenamiento de los sistemas, así como el volumen de fabricación de equipos. Sobre la extensión de la capacidad de almacenamiento, procesamiento y distribución de computadores, cf. Lucas Marin, Antonio, "La nueva sociedad de la información. Una perspectiva desde Silicon Valley" Editorial Trotta. Madrid, 2000, pp.59.
[35] Frossini, Vitorio. "Cibernetica, dirito e socierta"(1968). "Cibernética Derecho y Sociedad", trad. Salguero Talavera y Soriano Diaz. Ed. Tecnos. Madrid. 1982.

legales que estas conllevan derivadas de los principales RFCs[36] relacionadas con la privacidad y la proteccion de datos, con los que en la actualidad se construyeron la ingeniería del IPv6:

- RFC 2460: Internet *Protocol, Version 6 Specification* (Especificación de Protocolo Internet, versión 6).
- **RFC 2462: *IPv6 Stateless Address Autoconfiguration* (Configuración automática de direcciones sin estado en IPv6)**
- RFC 2374: *An IPv6 Aggregatable Global Unicast Address Format* (Formato agregable global de dirección de unidifusión IPv6)
- **RFC 3041: *Privacy Extensions for Stateless Address Autoconfiguration in IPv6* (Extensiones de privacidad para la configuración automática de direcciones sin estado en IPv6)**

Tomando como tema de investigación las **RFC 3041** y la **RFC 2462**, que pone en evidencia el problema latente en materia legal; manifestando que cualquier sistema de comunicación que se base o utilice una dirección fija o un "identificador único" tanto para recibir como enviar información, conlleva a problemas potenciales en la vulneración de los datos personales, poniendo en jaque una posible trazabilidad o búsqueda de la información por terceras partes o actores[37] en este caso utilizando el falseo de datagramas IP(*IP Spoofing*[38]), la

[36] **RFCs(Request for Comments):** Los RFCs describen todo el trabajo interno en Internet. Pero no todas las RFCs especifican estándares. Hay 5 clases de clasificaciones en las RFCs.

1.- Required(Requerido): Debe ser implementado en todas las maquinas.
2.- Recommended(Recomendada): Se estimula el que todas las maquinas las usen.
3.- Elective: El uso de esta RFC es opcional. No es ampliamente usada.
4.- Limited de Use(Uso limitado): No esta pensada para un uso general.
5.- Not Recommended(No recomendada): No esta aconsejada su uso.

Si un documento comienza a ser considerado como un estándar, comienza a pasar por los diferentes estados de desarrollo, prueba y aceptación. Durante este proceso, estos procesos son formalmente llamados "Maturity Levels"(Niveles de Maduración). Hay tres niveles de maduración en los estándares de Internet:

1.- Proponed Standard(Propuesta). Una especificación de propuesta, es generalmente estable, ha resuelto las conocidas alternativas de diseño, esta bien comprendida, ha recibido el visto bueno de la comunidad y parece u buen candidato a ser evaluado por la comunidad.

2.- Draft Standard(Borrador). Un borrador, debe ser entendido y reconocido como estable, tanto semánticamente como su base para poder ser desarrollada correctamente.

3.- Internet Standard: El estándar de Internet, (muchas veces nos referimos a el como un "Standard"simplemente) se caracteriza por un alto grado de madurez técnica y generalmente se reconoce como una ayuda al protocolo o al servicio que significa un beneficio para la Comunidad Internet. Cuando se publica un documento, se le asigna un número de RFC. Este número original, nunca va a cambiar. Si esta RFC requiera cambios, se publica una nueva RFC con un nuevo numero.

[37] Para determinar los términos con los que designan a la generalidad de los que actúan en la red nos planteamos los nombres de intervinientes, terceras partes, actores, agentes, participantes, entre otros. Ello por que es necesario considerar que muchas veces, una misma persona física o jurídica puede ejercer funciones distintas, lo

interceptación de datagramas IP(*IP Hijacking*[39]) y principalmente la escucha de datagramas IP(*Packet Sniffing*[40]) en nuestra comunicación en el Internet.

Por tal problemática se desea plantear una alternativa de solución desde un enfoque técnico jurídico en materia de ingeniería(configurada esta, sobre la diseño de la arquitectura de una medida tecnológica) orientada dentro de un contexto de la neutralidad[41] y el adecuado equilibrio del empleo de las herramientas informáticas[42], basado en una investigación de mas de 7 meses y

---

cual lleva a ejercer diferentes roles. De esta forma estaremos utilizando el termino actores, tomado prestado del francés acteurs, utilizado por la doctrina francesa en el marco del estudio de las nuevas tecnologías.

[38] Esta técnica se basa en la generación de paquetes IP con la dirección de origen falsa. Es muy usado cuando la "Victima" confía en determinadas direcciones IP, por ejemplo para la administración remota de maquinas. Eduardo Fernandez-Medina Paton, "Seguridad de las tecnologías de la información", "9.3.4.1.2 IP Spoofing" Pag.305.

[39] Consiste, en aprovechar fallos en el diseño del protocolo para interceptar una conexión ya establecida, suplantando la identidad de un usuario autorizado. Eduardo Fernandez-Medina Paton, "Seguridad de las tecnologías de la información", "9.3.4 Activos" Pag.305.

[40] En informática, un "packet sniffing" es un programa de captura de las tramas de red. Generalmente se usa para gestionar la red, aunque también puede ser utilizado con fines maliciosos.

Es algo común que, por topología de red y necesidad material, el medio de transmisión (cable coaxial, UTP, fibra óptica etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir esto el sniffer pone la tarjeta de red o NIC en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos de la OSI no son descartadas las tramas no destinadas a la MAC address de la tarjeta; de esta manera se puede obtener (sniffer) todo tipo de información de cualquier aparato conectado al internet como contraseñas, e-mails, conversaciones de chat o cualquier otro tipo de información personal (por lo que son muy usados por crackers, aunque también suelen ser usados para realizar comprobaciones y solucionar problemas en la red de modo legal).

[41] A la búsqueda de la neutralidad tecnológica, a pesar del problema que surge cuando aquello que pueden utilizar la tecnología de modo efectivamente mas productivo no lo hacen con neutralidad, a saber por ejemplo, que el terrorista norteamericano Unabomber, en su manifiesto denominado "El futuro de la sociedad industrial", publicado en una serie de periódicos de los EUA y también disponible en Internet, da la voz de alerta sobre la imposibilidad, debido al desarrollo de la tecnología, de conseguir la libertad y en consecuencia, la privacidad. Afirma que …La tecnología es una fuerza más poderosa que toda aspiración de libertad. No es posible establecer un compromiso duradero entre tecnología y libertad, porque la tecnología es de lejos la fuerza social más poderosa, usurpando frecuentemente la libertad a través de compromisos sucesivo… Comprendemos el análisis social, o mejor aun socio tecnólogo, propuesta por el autor del escrito y estamos de acuerdo con lo que respecta a la dificultad de que exista un equilibrio social en muchos sectores de la sociedad. Aun asi, recordamos que no se puede poner freno al desarrollo tecnológico por el recelo de lo que pueda ocurrir. Es preciso dejar claro, igualmente que cualquier acto de violencia propuesto por ese autor son merecedores de un total desprecio, pues aunque tengamos una opinión pesimista en relación con las nuevas tecnologías y con Internet a través de las redes Ipv4, no estamos de acuerdo con el radicalismo de tales opiniones.

Por otra parte, Yves Poullet acompaña este pensamiento, aunque metafóricamente, cuando afirma que "… la posibilidad de tener el consumidor a priori una transparencia completa, a través del sistema de cookies y de cibervinculos invisibles es alta y esta presente, y claramente demuestra que la tecnología no es neutral…" Texto original en "Cyberspace et Droit: Une revolution?", en el Centro de Recherches Informatique et Droit-Grid. Faculté de Droit Namur, www.droit.fundp.ac.be

[42] "En una sociedad como la que nos esta tocando vivir, en la que la información es poder y en la que ese poder se hace decisivo cuando convierte informaciones parciales y dispersas en información en masa y organizadas, la reglamentación jurídica de la informática reviste un interés prioritario. Se ha indicado que, en el plano de las relaciones entre el las Empresas, Estado y sus ciudadanos, la tecnología puede comportar el riesgo de hacer mas misteriosa e irresponsable la decisión política y que puede incluso eliminar cualquier tentativa de critica y alternativa a las decisiones a todos aquellos que se hallen fuera del circulo mágico que supone el dominio o, en el peor de los casos el monopolio de los bancos de información, a la par que, en el plano de las relaciones de los ciudadanos entre si se agravan las desigualdades de echo entre los detentadores y desposeídos del aparato informático, ya que en nuestra sociedad en ejercicio del poder económico, social y político, se funda en la

un conjunto de pruebas pre-experimentales en terreno, con el uso de la tecnología IPsec(Internet Protocol Security)[43] nos permitirá analizar e implementar herramientas legales en materia de protección, integridad, cifrado, flexibilidad, interoperatividad y autentificación de datos especializado; a efectos de ampliar la protección de estos derechos ajustados a las necesidades legales de los usuarios, concerniente al tratamiento de sus datos de carácter personal, o, expresado de otra forma, al amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento. Y a la par incorporar a la presente tesis, como otra alternativa de solución al estándar de la RFC 3041 que será circunscrita en el diseño de 2 nuevas arquitecturas o modos de extensión que brinden la adecuada protección al efecto.

1.2 Objetivos generales y específicos

1.2.1 Objetivos Generales.

Se plantea elaborar la arquitectura una medida tecnológica[44] destinada a proteger y evitar la vulneración de los datos personales por terceras partes que implícitamente ocasiona el protocolo de Internet Ipv6 dentro de su infraestructura de construcción con el denominado problema que presentan los identificadores únicos descritos en la RFC 2462 que originan la autentificación tendiente a la violación de la privacidad del titular de datos; a través de la modificación especializada de la RFC 3041 que genere un procedimiento de disociación[45]-[46] en la identificación del individuo en una extensión limitada que

---

disposición puntual y adecuada de informaciones.(…) " Perez Luño , Antonio "Los derechos fundamentales." Editorial Tecnos, Madrid, 1984.

[43] Ipsec: protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y, de esta manera, asegurar las comunicaciones Ref. RFC 2401.

[44] Toda técnica, dispositivos o componente que, en su funcionamiento normal es destinado a impedir o restringir actos referidos a información que no cuenten con la autorización del titular de los derechos.

[45] Dentro del concepto de la definición de la Ley Nº 19.628 sobre la protección de la vida privada o protección de datos de carácter personal, Articulo 2 letra l) que indica un procedimiento de disociación de datos es: "todo

permita ofrecer una solución alternativa orientada al resguardo de los bienes jurídicos[47] tutelados por la Ley Nº 19.628 en relación con el tratamiento de los datos personales del usuario, desde la óptica del análisis de las implicancias de su afectación dentro de los distintos encuadramientos normativos de la protección de la privacidad de cara con el avance tecnológico contractual que se enfrenta el nuevo protocolo que se viene desplegando; sobre la base de la configuración de un protocolo seguro[48]; que ofrezca las garantías de protección al momento de realizar el tráfico de datos en el Internet de próxima generación IPv6.

1.2.2 Objetivos Específicos.

1.- Realizar un profundo análisis legal de las posibles vulneraciones que IPv6 podría conllevar con respecto a la protección de datos personales planteadas a través de un estudio pormenorizado de las implicaciones que estas contraen, tomando como ejes centrales la RFC 2462(Configuración automática de direcciones sin estado en IPv6) y el RFC 3041(Extensiones de privacidad para la configuración automática de direcciones sin estado en IPv6); como así mismo la interpretación legal y su modo de funcionamiento de la RFC 2460(Especificación del protocolo IPv6), y la RFC 2374(Formato agregable global de dirección de unidifusión IPv6) frente a los riesgos de la velocidad del cambio tecnológico que se presentan en las nuevas redes de telecomunicaciones con el despliegue del protocolo de Internet en su versión 6.

---

tratamiento de datos de carácter personal de manera que la información que se obtenga no pueda asociarse a persona determinada o indeterminada".

[46] Comisión de las comunidades Europeas, "Primer informe sobre la aplicación de la Directiva sobre protección de datos(95/46/CE)", Bruselas, 15 de mayo de 2003, pp. 17-18.

[47] El bien juridico protegido en cualquier ordenamiento que posea una ley de protección de datos será la libertad informática o la autodeterminación informática, concluyente con la denominada intimidad informatica(Bajo Fernandez, Miguel. 1989. "Protección del honor y la intimidad", en comentarios a la legislación Penal, Tomo I, Madrid pp. 100-101") que abarca la reserva y control de la información de carácter personal en aras de la preservación de la propia identidad, dignidad y libertad, lo que se a dado en denominar "derecho de la tercer generación" (…Martinez Escribano Alonso, "Los Derechos fundamentales y las nuevas tecnologías en el trabajo".

[48] Referido a la utilización del protocolo Ipsec en relación con la implementación de un Criptoalgoritmo AH(Authentication Header) y un Sistema de bases de datos de políticas de seguridad en el ESP(Escapsulating Security Payload).

2.- Realizar un estudio descriptivo de las directivas internacionales en materia de protección de datos personales que obligan a los distintos responsables de los tratamientos de datos a adoptar medidas técnicas y organizativas necesarias que garanticen la confidencialidad[49] de la "información"[50] y su correcto tratamiento en materia de las medidas de seguridad, para orientarlo este ultimo a la opción de seguridad que ofrece el IPv6 en la denominada Ipsec que garantiza la autentificación en el origen de los datos, la integridad de la información transmitida y la confidencialidad[51] de la misma con respecto a la afectación de los agentes tratantes en la sociedad de la información contemporánea.

3.- Analizar e investigar desde la panorámica jurídica de la protección de los datos personales el diseño de la arquitectura de una medida tecnológica orientada a proteger y evitar la vulneración de las huellas sensibles de trazabilidad dejadas por el titular de datos a través de la modificación de un modelo marco equilibrado que regule la co-existencia "del único autentificador o

[49] Confidencialidad: Es la propiedad que asegura que solo aquellos que están autorizados tendrán acceso a la información. A menudo esta propiedad se conoce también con el nombre de privacidad según Miquel Peguera Poch, Albert Agustinoy Guilayn, Ramon Casas Valles, Agusti Cerrillo i Martinez, Ana M. Delgado Garcia, Jordi Herrera Joancomarti, Mark Jeffery, Oscar Morales Garcia, Rafael Oliver Cuello, Guillermo Ormanzabal Sanchez, Monica Vilasau Solana y Raquel Xalabarder Plantada "Derecho y nuevas tecnologías", Editorial UOC 2005, pag. 33.

[50] Como pone en evidencia Roszak, Th., El culto a la información. Folclore de los ordenadores y el verdadero arte de pensar, Critica, Barcelona,k 1988, la palabra "información", objeto de definiciones ambiciosas y universales, tiene sus orígenes en los mismos inicios de la moderna teoría de la información en el año 1948, precisamente "el mismo año en que Wienner produjo su estudio "Cybernetics", a través de la publicación por parte Claude Shannon de su innovador articulo "A Mathematical Theory of Communitacion", "que instauro una nueva disciplina: la teoría de la información, la ciencia de los mensajes", que ya se separo del concepto tradicional de la palabra "información", que "denotaba siempre una información lógica que expresaba un significado verbal y reconocible, generalmente lo que denominaríamos un hecho", para ofrecer una "definición técnica especial que la divorcio de su utilización racional", puesto que la información dejaba de esta "relaciona con el contenido semántico de las afirmaciones" para pasar a ser "una medida puramente cuantitativa de los intercambios comunicativos, en especial por que estos tienen lugar a través de algún cauce técnico que exige que ese mensaje sea codificado y luego descodificado, pongamos en su caso, en impulsos electrónicos…"pag 22-23. Justamente, "…desde su punto de vista, hasta un guiriguay podía ser "información" si alguien se tomaba la molestia de transmitirlo…". Por ello, como señalo el propio Shannon, "Debería tener muy en cuenta que (la información) es solo una medida de dificultad de transmitir las secuencias productivas por alguna fuente de información" (Warren Weaver, "The Mathematics of Communication", en Scientific American(julio 1949), pag. 12)"(th. Roszak Pag. 23 y 24). De forma que, "como dijo una vez el matemático Warren Weaver, "desde el actual punto de vista, dos mensajes, uno muy cargado de significado y el otro pura tontería, pueden ser equivalentes en lo que se refiere a la información"(pag.25). Por consiguiente, "que para el teórico de la información…(no) tiene importancia que lo transmitido sea un hecho, un juicio, una frase hecha y superficial, una enseñanza profunda, una verdad sublime o una obscenidad desagradable. Todas estas cosas son "información". La palabra adquiere una basta generalidad, mas para ello hay que pagar un precio; el significado de las cosas que se comunican queda nivelado, y lo mismo le ocurre a su valor" (pag.26). Por esta razón, considerándose, en definitiva, que "la información lo es todo", ENZENSBERGER, H.M. ha dicho: "El lema de "el arte por el arte" se encuentra aquí con un eco tardío en el principio "el medio por el medio" ("El evangelio digital"). Claves de la razón Practica, Numero 4. Julio-Agosto 2000, pag. 11).

[51] Hugo Adrian Francisconi, Ipsec en ambiente Ipv4 e Ipv6, Edición Carrol Godoy 2005 Argentina.

localizador de cada persona" con el protocolo de Internet tercera generación Ipv6 en el trafico de información durante el periodo de conexión al internet, dentro del contexto del cumplimiento de los limites legales de los estatutos de garantías y los derechos fundamentales que le asisten a los usuarios de las redes y servicios en sus acciones comunicativas, considerando también los estándares internacionales de la RFC 2411(*IP Security Document Roadmap*/Documento guía para Ipsec) y la *ISO/IEC 17799:2000 Information Tecnology – Code of practice for information secutity management (C*on su homologación en la Norma Chilena Oficial NCh2777 – ISO/IEC 17799: 2000 "Tecnología de la información – Código de Practica para la Gestión de Seguridad de la Información").

CAPITULO SEGUNDO

FUNDAMENTOS GENERALES[52] Y BASES TEORICAS DEL PROTOCOLO DE INTERNET IPV6.

[52] El objeto del presente capitulo es describir concretamente un esquema adecuado de los elementos teóricos y tecnológicos claves que serán requisitos necesarios para tener en mayor profundidad y comprensión los conceptos en torno al cual giraran las implicancias legales en materia de privacidad y la protección de datos personales que se analizaran y describirán en los posteriores capítulos de la presente tesis.

2.1 En que consiste el protocolo de tercera generación Ipv6.

Ipv6 sucesor por excelencia del protocolo Ipv4, es la versión 6 del Protocolo de Internet (IP)[53], un estándar del Nivel de red[54] encargado de dirigir y encaminar información a través de la Internet. Fue diseñada por Steve Deering y Craig Mudge y adoptada por el *Internet Engineering Task Force* en 1994 (cuando era llamado "IP Next Generation" o IPng) para dar una mejor solución global al problema que enfrenta Ipv4. Ipv4 soporta 4.294.967.296 (2^{32}) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos para cada coche, teléfono, PDA o tostadora; mientras que IPv6 soporta 340.282.366.920.938.463.463.374.607.431.768.211.456(2^{128} ó 340 sextillones) direcciones, cerca de $4,3 \times 10^{20}$ (430 trillones) direcciones por cada pulgada cuadrada($6,7 \times 10^{17}$ ó 670 mil billones direcciones/mm^2) de la superficie de La Tierra. Se espera que Ipv4 se siga soportando hasta por lo menos el 2025[55], dado que hay muchos dispositivos heredados que no se migrarán a Ipv6 nunca y que seguirán siendo utilizados por mucho tiempo. Ipv6 es la segunda versión del protocolo de Internet que se viene desplegando en la

---

[53] Protocolo de Internet(IP). Fue diseñado para interconexión de redes, IP se ocupa de la transmisión de bloques de datos, llamados datagramas de origen a destino, donde orígenes y destinos son *hosts* identificados por direcciones de una longitud fija. IP también se encarga de la fragmentación y reensamblado de datagramas, si éste fuera necesario.
El módulo internet usa las direcciones contenidas en la cabecera de los datagramas para hacer llegar a estos a sus destinos. Asimismo, existen otros campos en la cabecera que permiten gestionar la fragmentación y posterior reensamblado de datagramas, para poder transmitir a través de redes que trabajen con tamaños de paquete pequeños. El módulo Internet reside en cada *host* integrado en la Internet, y en cada *gateway* interconectando redes. Estos módulos siguen reglas comunes para interpretar las direcciones y para realizar la fragmentación/reensamblado de datagramas. Adicionalmente, estos módulos (especialmente en los *gateways)* están provistos de mecanismos para tomar decisiones sobre el enrutamiento de los datagramas. http://studies.ac.upc.edu/FIB/CASO/seminaris/1q0102/T6.doc Ricardo González Jareño, Elena Musté Gálvez y Borja Salanova de Cruells "Ipv6 Seminarios CASO" Universidad politécnica de Catalunya-España Departamento de Arquitectura de Computadores.

[54] Nivel de Red: Es el tercer nivel del modelo OSI y su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Ofrece servicios al nivel superior (nivel de transporte) y se apoya en el nivel de enlace, es decir, utiliza sus funciones.

[55] Según las estimaciones del *ALE("Address Lifetime Expectations")* que determinan hasta cuándo el problema será intratable y realizan las estimaciones actuales que fijan el agotamiento del espacio de direcciones al 2025. Pero cabe recordar sin embargo, por distintas fuentes que en el país China se estima al 2010 una infraestructura de Ipv6 según asegura Wu Jianping, profesor de la Universidad de Tsinghua y director del Comité de Expertos de CERNET2(Conecta 25 universidades, en 20 ciudades de todo el país y supondrá la red mas grande del mundo basada en el protocolo Ipv6). Así mismo también en la comunicación de la Comisión al Consejo y al parlamento Europeo sobre el Internet de nueva generación y las actuaciones prioritarias en la migración al nuevo protocolo de Internet IPv6(COM/2002/0096Final-52002DC0096) Europa estima convertirse en la economía basada en el conocimiento mas competitiva y muy dinámica del mundo al 2010 sometida por un completo despliegue del protocolo de Internet en su versión 6. En tal sentido se espera que las estimaciones del despliegue serán en algunos países antes del esperado 2025.

actualidad, para las principales troncales a nivel mundial(Ver 2.12.3. Estado del despliegue de Ipv6). La implantación del Ipv6 se inicio en 1996, desplegándose inicialmente con la red piloto 6bone Ipv6, que ahora en la actualidad cubre más de 50 países y 1.000 sitios. De hecho, el despliegue comercial del Ipv6 esta en curso, sobre todo en Japón y en particular en Asia[56]. De otro lado, también hubo un Ipv5, pero no fue un sucesor de IPv4; por que fue un protocolo experimental orientado al flujo de Streaming (Asignado a Internet Stream Protocol v2 ST2 en la RFC 1819)[57] que intentaba soportar voz, video y audio en tiempo real. Ahora, el nacimiento del protocolo Ipv6[58] no ha venido solo propiciado por la escasez de direcciones Ipv4 que existe en estos momentos, sino por que Ipv6 añade nuevas características y mejoras a su predecesor Ipv4 en materia de **Seguridad, Movilidad y Calidad de Servicio (QoS)**. Además por que en la actualidad las tablas de rutas de los routers de Ipv4 se están haciendo cada día más gigantescas, tanto en el **Multi-Homing[59]** como en la movilidad ocasionando

---

[56] Las comunicaciones de la próxima generación, "Despliegue del Ipv6 en el Mundo", Unión Internacional de telecomunicaciones, http://www.itu.int/itunews/issue/2002/03/ipv6deployment-es.html

[57] El Streaming es un término que se refiere a ver u oír un archivo directamente en una página web sin necesidad de bajárselo antes al ordenador o computador. Se podría describir como hacer click y obtener. En términos más complejos podría decirse que describe una estrategia sobre demanda para la distribución de contenido multimedia a través del internet. http://www.w3c.es/gira/paradas/presentaciones/Xabiel_conferencia.pdf Xabiel Garcia Pañeda, "Integración de Audio y Video en la Web" Universidad de Oviedo, La Universidad de Asturias, Departamento de Informática, Área de Ingeniería Telemática.

[58] Nace de la evaluación de 3 propuestas:

1.- CATNIP ("Common Architecture for the Internet") es un desarrollo de un viejo protocolo(TP/IX) que integra IPv4, Novell IPX y OSI CLNP("Connectionless Networking Protocol") y proporciona una infraestructura común. CATNIP se describe en el *RFC 1707 - CATNIP: Una arquitectura común para Internet*.

2.- TUBA("TCP and UDP with Bigger Addresses") también se basa en CLNP; en pocas palabras, sustituye a IPv4 en la pila TCP/IP. Enfatiza las redes multiprotocolo. La transición entre IPv4 a IPng se hace usando una estrategia de pila dual. TUBA se describe en el *RFC 1347 - TUBA("TCP and UDP with Bigger Addresses"), una simple propuesta para el direccionamiento y el encaminamiento en Internet*. Ver también el *RFC 1526 - Asignación de identificadores de sistema para hosts TUBA/CLNP* y el *RFC 1561 - Uso de ISO CLNP en entornos TUBA*.

3.- SIPP("Simple Internet Protocol Plus") es una combinación del trabajo de tres grupos de trabajo anteriores del IETF que dedicados al desarrollo de un IPng. SIPP se describe en el *RFC 1710 - SIPP("Simple Internet Protocol Plus White Paper")*.

1) IPAE("IP Address Encapsulation") determina que las extensiones de IPv4 lleven direcciones más largas, y como debe realizarse la transición de una versión a otra. 2) SIP("Simple Internet Protocol") SIP es una sustitución de IPv4 con una cabecera IP simplificada y direccionamiento de 64 bits. 3) PIP(""P" Internet Protocol") fue una nueva marca para un protocolo de Internet, diseñado con una amplia variedad de características avanzadas y usando direccionamiento de longitud variable. Universidad de Murcia-España Departamento de Ingeniería y tecnología de computadores http://ditec.um.es/laso/docs/tut-tcpip/3376fm.html "Descripción técnica del TCP-IP".

[59] **Seguridad:** Este fue otro de los requerimientos del diseño del nuevo protocolo: todas las aplicaciones se deben beneficiar de las facilidades de autenticación y encriptación de datos de forma transparente. El estándar escogido para esto fue IPsec.

Movilidad: Con esta funcionalidad podremos "saltar" de una red a otra sin apenas percibir ningún cambio. Si bien esto ya era posible con IPv4 de una manera mas bien ardua, en IPv6 fue una de los requerimientos del diseño. Esta característica es de gran importancia cuando entren en funcionamiento las nuevas redes de telefonía con tecnología UMTS.

Calidad de servicio (QoS): Si bien con IPv4 tenemos unos pocos bits para el control del tipo de servicio, ToS, con Ipv6 disponemos de campos más amplios para definir la prioridad y flujo
de cada paquete. Según el contenido de este campo, el router debe darle un trato más o menos especial.

problemas excesivamente complejos para satisfacer las necesidades de los usuarios de forma sencilla.

En estricto rigor según las fuentes de información de los estándares oficiales, la concepción del protocolo Ipv6 se especifica en el RFC 2460(Anexo) donde se establece lo siguiente:

"El IP versión 6 (IPv6) es la nueva versión del Protocolo Internet, diseñado como el sucesor para el IP versión 4 (IPv4) [RFC-791]. Los cambios del IPv4 al IPv6 recaen principalmente en las siguientes categorías:

- **Capacidades de Direccionamiento Extendida:** El IPv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico, un número mucho mayor de nodos direccionables, y una autoconfiguración más simple de direcciones. La escalabilidad del enrutamiento multienvío se mejora agregando un campo "ámbito" a las direcciones multienvío. Y se define un nuevo tipo de dirección llamada "dirección envío a uno de", usado para enviar un paquete a cualquiera de un grupo de nodos.
- **Simplificación del Formato de Cabecera:** Algunos campos de la cabecera IPv4 se han sacado o se han hecho opcional, para reducir el costo del caso común de proceso de tratamiento de paquete y para limitar el costo del ancho de banda, de la cabecera IPv6.
- **Soporte Mejorado para las Extensiones y Opciones:** Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.
- **Capacidad de Etiquetado de Flujo:** Una nueva capacidad se agrega para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares para lo cuál el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".
- **Capacidades de Autenticación y Privacidad:** Extensiones para utilizar autenticación, integridad de los datos, y (opcional) confidencialidad de los datos, se especifican para el IPv6.

Este documento especifica la cabecera IPv6 básica y las cabeceras de extensión IPv6 y las opciones inicialmente definidas. Aborda también cuestiones de tamaño del paquete, las semánticas de las etiquetas de flujo y las clases de tráfico, y los efectos del IPv6 en protocolos de capa superior. Los formatos y semánticas de las direcciones IPv6 son especificados separadamente en [ADDRARCH]. La versión IPv6 del ICMP, que a todas las implementaciones IPv6 se exige incluir, es especificada en [ICMPv6]."[60]

Tabla 41. Síntesis descriptiva de la RFC2460.

Multi-Homing: Esta funcionalidad se consigue con direcciones anycast. Una dirección anycast identifica a un conjunto de distintos interfaces, encontrándose estos, por norma general, en distintos nodos. Un paquete a una dirección anycast debe ser entregado a un solo miembro del conjunto. En principio, el paquete ser entregado al miembro mas cercano según el concepto de cercanías de los protocolos de encaminamiento, http://spisa.act.uji.es/~peralta/ipv6 Luis Peralta "Ipv6 @UJI" 2005, Universidad de Jaume España.

[60] **Terminología** estricta del Estándar de la RFC 2460

Nodo: Un dispositivo que implementa el IPv6.

Enrutador: Un nodo que reenvía paquetes IPv6 no explícitamente destinados hacia sí mismo.

Host: Cualquier nodo que no es un enrutador.

Capa superior: Una capa de protocolo inmediatamente encima del IPv6. Ejemplos son los protocolos transporte tal como el TCP y el UDP, protocolos control tal como el ICMP, protocolos enrutamiento tal como el OSPF, y protocolos internet o de capa inferior que están siendo "tunelizados" sobre (es decir, encapsulados dentro) IPv6 tal como el IPX, el AppleTalk, o el mismo IPv6.

Enlace: Una facilidad de comunicación o medio sobre el cual los nodos pueden comunicarse en la capa de enlace, es decir, la capa inmediatamente debajo del IPv6. Ejemplos son las Ethernets (simples o de puentes);
enlaces PPP; X.25, Frame Relay, o redes ATM; y "túneles" de capa internet (o superior), tal como los túneles sobre IPv4 o sobre el mismo IPv6.

Vecinos: Nodos conectados al mismo enlace.

Interface: Lo que acopla un nodo a un enlace.

Dirección: Un identificador de capa IPv6 para una interfase o un conjunto de interfaces.

Paquete: Una cabecera IPv6 más carga útil.

MTU de enlace: La unidad de transmisión máxima, es decir, el tamaño del paquete máximo en octetos, que puede transportarse sobre un enlace.

MTU de ruta: La MTU de enlace mínima de todos los enlaces dentro de una ruta entre un nodo origen y un nodo destino.

2.2 Principales aspectos y características.

2.2.1 Criterios de diseño[61].

a) Escalabilidad: Capacidad de identificar a 10^{12} estaciones y 10^{9} redes.

b) Flexibilidad topológica: Nueva arquitectura y encaminamiento.

c) Transición: Debe contemplarse el paso de Ipv4 a Ipv6.

d) Independencia de medio: LAN-MAN-WAN y AdB variados.

e) Configuración automática: De routers y hosts.

f) Operación Segura: El nivel de red debe proveer seguridad.

g) Movilidad: Capacidad para evolucionar ante nuevos servicios.

2.2.2 La cabecera del Ipv6.

La cabecera de un paquete IPv6 es, sorprendentemente, mas sencilla que la del paquete IPv4. IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, el doble que en IPv4, pero con muchas ventajas al haberse eliminado campos redundantes. Debido a que la longitud de la cabecera es fija, implica numerosas ventajas ya que facilita el procesado en router y conmutadores. Los nuevos procesadores y microcontroladores de 64 bits pueden procesar de forma más eficazmente este tipo de cabecera, ya que los campos están alineados a 64 bits; estos 40 bytes se componen de la siguiente forma:

1.- Versión (4 bits). Sirve para que el router se entere de que es un paquete IPv6.
2.- Dirección origen y de destino (128 bits cada una). Son las direcciones de los nodos IPv6 que realizan la comunicación.
3.- Clase de tráfico (8 bits). Para poder diferenciar entre servicios sensibles a la latencia, como VoIP, de otros que no necesitan prioridad, como trafico http.
4.- Etiqueta de flujo (20 bits). Permite la diferenciación de flujos de tráfico. Esto tiene importancia a la hora de manejar la calidad de servicio (QoS). Sirve para permitir tráfico con requisitos de tiempo real
5.- Siguiente cabecera (8 bits). Este campo permite a routers y hosts examinar con más detalle el paquete. A pesar de que el paquete básico IPv6 tiene cabecera de tamaño fijo, el protocolo puede añadir mas para utilizar otras características como encriptación y autenticación.
6.- Tamaño de payload (16 bits). Describe el tamaño en octetos de la sección de datos del paquete. Al ser este campo de 16 bits, podremos usar paquetes de hasta más de 64000 bytes.
Nota: El 3 y 4 son los que nos permiten una de las características fundamentales e intrínsecas de IPv6: Calidad de Servicio (QoS) y Clase de Servicio (CoS), y en definitiva un poderoso mecanismo de control de flujo, de asignación

[61] Enrique Alba Torres, "El protocolo de InterRed IP", Universidad de Málaga 2005, http://www.lcc.uma.es/~eat/courses/cdd-contents/tema4.pdf

de prioridades diferenciadas según los tipos de servicio.

Tabla 42. Descripción de la estructura del formato de cabecera IPv6.

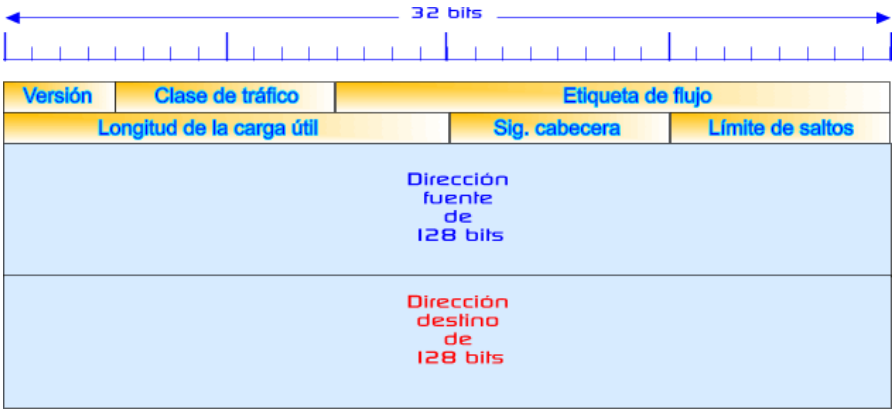


Ilustración 69. Estructura del formato de cabecera IPv6 de la RFC 2460[62].

2.2.3 Arquitectura de direccionamiento

Sin interrogante, el desarrollo más dramático proveído por Ipv6 es el aumento del tamaño en los campos de direcciones de 32 a 128 bits por dirección. Mientras el campo de 32 bits de Ipv4 produce 4,294,967,296 direcciones distintas, el campo de 128 bits de Ipv6 tiene considerablemente más: 340.282.366.920.938.463.463.374.607.431.768.211.456 en total. Pero antes de sumergirnos en esta estructura de direccionamiento y todos sus rigores, consideremos brevemente los formatos de direccionamiento de ipv4 para comparación.

a) Direccionamiento Ipv6 y modelos

Cualquier tipo de dirección se asigna a interfaces, no nodos. Es algo importante que no haya que olvidar. Todos los interfaces han de tener, por los menos, una dirección de enlace local (Link-Local) de tipo Unicast. Un mismo interfaz puede tener asignadas múltiples direcciones de cualquier tipo(unicast, anycast, multicast) o ámbito (scope). Direcciones unicast con ámbito mayor que el de enlace no

[62] Imagen fuente: Networking and Emerging Optimization de la Universidad de Málaga "Protocolo de Comunicación" http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/espipv6.html Ref. RFC 2460 Pag. 6, http://rfc.net/rfc2460.html

son necesarias para interfaces que no son usados como origen y destino de paquetes IPv6 hacia o desde los vecinos. Esto significa que para la comunicación dentro de una LAN no nos hacen falta direcciones IPv6 globales, sino que tenemos más que suficiente con direcciones de ámbito local. De hecho, es lo aconsejable para enlaces punto a punto. Respecto a los prefijos de subred, IPv6 sigue el mismo modelo que IPv4, es decir, un prefijo se asocia a un enlace, pudiendo haber varios prefijos en un mismo enlace.

b) Nomenclatura

i) Nomenclatura de las direcciones: Tenemos 3 formas comunes de representar direcciones IPv6 en texto:

- x:x:x:x:x:x:x:x donde cada x es el valor en hexadecimal de cada grupo de 16 bits de la dirección.
- x:x::x en el caso de que haya grupos contiguos de 16 bits todos 0. Una abreviatura que servir para hacer más cómodo el uso de direcciones.
- x:x:x:x:x:x:d.d.d.d, donde las x son los seis grupos de 16 bits en hexadecimal de mayor peso de la dirección y las d son los valores decimales de los cuatro grupos de 8 bits de menor peso de la dirección. Esta forma es a veces más conveniente a la hora de manejar entornos mixtos IPv6 e IPv4. Por ejemplo: 0:0:0:0:0:FFFF:129.144.52.38 y en su forma abreviada ::FFFF:129.144.52.38.

Representacin normal	Representacin abreviada	Tipo
1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A	unicast
FF01:0:0:0:0:0:0:101	FF01::101	multicast
0:0:0:0:0:0:0:1	::1	loopback
0:0:0:0:0:0:0:0	::	direccin no especificada

Tabla 43. Nomenclatura de direcciones Ipv6.

ii) Nomenclatura de los prefijos: La representación de los prefijos de direcciones con Ipv6 es similar a la que tenemos con CIDR con Ipv4, esto es: dirección-ipv6 / tamaño prefijo. Donde dirección-ipv6 es alguna de las notaciones vistas en la sección anterior y tamaño-prefijo es un valor decimal que especifica cuantos bits de la dirección

corresponden al prefijo. Por ejemplo, el prefijo de la UJI en hexadecimal es 3FFE33300002, que son 48 bits, lo podemos escribir como:

3FFE:3330:0002:0000:0000:0000:0000:0000/48 3FFE:3330:2:0:0:0:0:0/48 3FFE:3330:2::/48

Tabla 44. Ejemplo de direccionamiento UJI.

Si queremos escribir la dirección y el prefijo, no hace falta que escribamos los dos de forma explicita. Por ejemplo, una dirección IPv6 de la misma UJI con su prefijo asociado quedara 3FFE:3330:2:1:250:BAFF:FE7A:E67E/48.

Las direcciones ipv4 son típicamente representadas en notación con punto decimal. Así, una dirección de 32 bits es dividida en 4 direcciones de 8 bits, y cada sección es representada por un número decimal entre 0 y 255: Ejm, 128.138.213.13. Como las direcciones de ipv6 son de 128 bits de longitud, un método diferente de representación es requerido. Como se especifico el RFC 2373, la representación preferida es: x:x:x:x:x:x:x:x donde x representa 16 bits, y cada una de esas secciones de 16 bits es definida en hexadecimal. Por ejemplo: una dirección ipv6 podría ser de la forma: FEDC:BA98:7654:320:FEDC:BA98:7654:3210. Note que cada una de las secciones de 16 bits es separada por ":", y que cada 4 números hexadecimales son usado para representar cada sección de 16 bits. Si alguna sección contiene ceros al principio, esos ceros no son requeridos. Por ejemplo: 1080:0000:0000:000:0008:0800:200C:417A puede ser simplificada a: 1080:0:0:0:8:800:200C:417A. Si largas cadenas de ceros aparecen en una dirección, "::" Puede ser usado para indicar múltiples grupos de 16 bits de ceros, que mas luego simplifican la dirección de arriba : 1080::8:800:200C:417A. El uso de "::" es restringido a aparecer solo una vez en una dirección, aunque puede ser usado para comprimir o los ceros del principio o los subsiguientes en una dirección. Por ejemplo, una dirección "loopback" de: 0:0:0:0:0:0:0:1 podría ser simplificada a: ::1 Cuando las direcciones de ipv6 son expresadas en texto, es común delinearlas como dirección y longitud de prefijo: ipv6-address/prefix-length donde la dirección ipv6 es expresada en una de las notaciones listadas anteriormente, y la longitud de prefijo es un valor decimal que especifica el número de los bits más a la izquierda de la dirección comprimida en el prefijo. Por ejemplo: 12AB:0000:0000:CD30:0000:0000:0000:0000/60 indica que el prefijo de 60 bits (en hexadecimal) es 12AB00000000CD3. **i)Direcciones Unicast:** Un identificador para una interfase simple. Un paquete enviado a una dirección unicast es entregado a la interfase identificada por esa dirección. **ii)Direcciones Anycast:** Un identificador para un conjunto de interfases(Típicamente perteneciente a nodos diferentes). Un paquete enviado una dirección anycast es entregado por una de las interfases identificadas por esta dirección(la más cercana, según la medida de distancia del protocolo de ruteo). **iii)Direcciones Multicast.** Un identificador para un conjunto de interfases(típicamente perteneciendo a nodos diferentes). Un paquete enviado a una dirección multicast es entregado a todas las interfases identificadas por esta dirección[63].

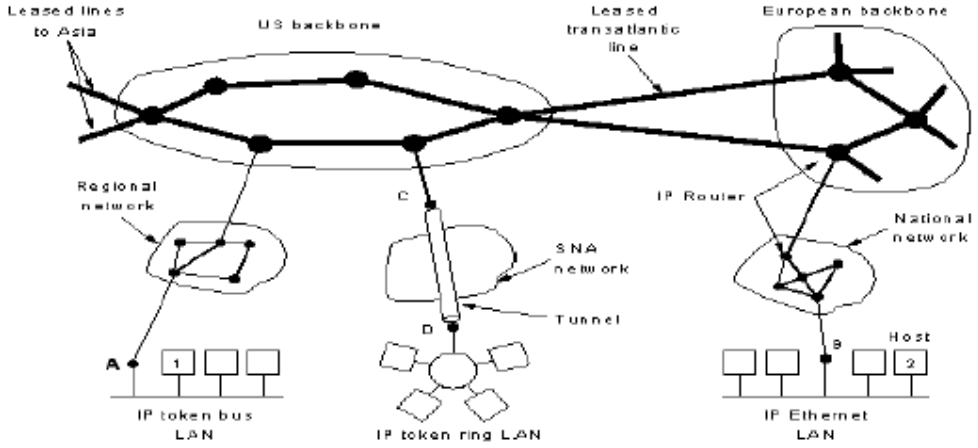
Tabla 45. Representación de los tipos de direcciones.

2.3 En que consiste el actual protocolo de Internet[64] Ipv4

[63] José Domínguez y Carlos Vicente "Introducción al Ipv6" Universidad de Oregon 2004 http://ws.edu.isoc.org/workshops/2004/CEDIA2/material/IPv6.pdf

[64] Curso de IG20 Redes de Ordenadores, "Estructura del Internet" Ingeniería Técnica en Informática de Gestión, Universidad Jaume I.

IPv4 es la versión 4 del Protocolo IP (Internet Protocol). Esta fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet. IPv4 es el principal protocolo utilizado en el Nivel de Red del Modelo TCP/IP para Internet. Fue descrito inicialmente en el RFC 791 elaborado por el Grupo de Trabajo en Ingeniería de Internet (IETF o Internet Engineering Task Force) en Septiembre de 1981, documento que dejó obsoleto al RFC 760 de Enero de 1980. IPv4 usa direcciones de 32 bits, limitándola a 2^{32} (4.294.967.296) direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs). Por el crecimiento enorme que ha tenido del Internet[65](mucho más de lo que esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones en muchos casos, ya hace varios años se vio que escaseaban las direcciones IPv4; de hecho en la actualidad LACNIC(Latin American and Caribbean Internet Addresses registry) ya anuncio oficialmente el inminente agotamiento de las direcciones de Ipv4[66](Sobre las estimaciones cientificas del connotado investigador Geoff Huston "Projected IANA Unallocated Address Pool Exhaustion:19/03/2010" y "Projected RUR Unallocated Address Pool Exhaustion:10/11/2010", http://www.potaroo.net/tools/ipv4) y se encuentra promoviendo la "campaña



[65] Que supera mas de los 50 millones con el uso de diversas tecnologías y 200 millones de hosts según Jordi Palet jordi.palet@consulintel.es "Evolución de las Redes basadas en el Protocolo IP, Facilidades y Ventajas de las Redes IP", European Ipv6 Task Force & Steering Comité IPv6 Forum, Education & Prmotion WG Co-Chair Consulintel, CTO/CEO, 2005, http://www.regulatel.org/eventos/cursos/INTERNET/PONENCIAS/Jordi%20Palet%20Martinez-%20Espana/01-%20Evolucion_ip_v2.pdf

[66] Centro de Información de Ipv6, en la conferencia de Prensa de LACNIC el 20 de junio del 2007-Montevideo, http://lacnic.net/ipv6/sp/

regional para lograr que antes del 1 de enero del 2011 se logre la total adaptación de las redes de la región a la nueva versión seis del protocolo IP(IPv6)".

IPv4 es un protocolo orientado hacia datos que se utiliza para comunicación entre redes a través de interrupciones (switches) de paquetes (por ejemplo a través de Ethernet). Tiene las siguientes características:

- Es un protocolo de un servicio de datagramas no fiable (también referido como de *mejor esfuerzo*).
- No proporciona garantía en la entrega de datos.
- No proporciona ni garantías sobre la corrección de los datos.
- Puede resultar en paquetes duplicados o en desorden.

Todos los problemas mencionados se resuelven en el nivel superior en el modelo TCP/IP, por ejemplo, a través de TCP o UDP. El propósito principal de IP es proveer una dirección única a cada sistema para asegurar que una computadora en Internet pueda identificar a otra.

En estricto rigor según las fuentes de información de los estándares oficiales, la concepción del protocolo Ipv4 se especifica en el RFC 791 donde se establece lo siguiente:

"Este documento especifica el Protocolo Internet Estándar del DoD(N.T.: Department of Defense, USA). Este documento está basado en seis ediciones anteriores de la Especificación del Protocolo Internet de ARPA, y el presente texto se basa en gran medida en ellas. Ha habido muchos colaboradores en este trabajo en términos de conceptos y texto. Esta edición revisa aspectos de direccionamiento, tratamiento de errores, códigos de opción, y de las características de seguridad, prioridad, compartimientos y manejo de restricciones del protocolo Internet.
1. INTRODUCCION
1.1. Motivación
El Protocolo Internet está diseñado para su uso en sistemas interconectados de redes de comunicación de ordenadores por intercambio de paquetes. A un sistema de este tipo se le conoce como "catenet" [1]. El protocolo internet proporciona los medios necesarios para la transmisión de bloques de datos llamados datagramas desde el origen al destino, donde origen y destino son hosts identificados por direcciones de longitud fija. El protocolo internet también se encarga, si es necesario, de la fragmentación y el reensamblaje de grandes datagramas para su transmisión a través de redes de trama pequeña.
1.2. Ámbito
El Protocolo Internet está específicamente limitado a proporcionar las funciones necesarias para enviar un paquete de bits (un datagrama internet) desde un origen a un destino a través de un sistema de redes interconectadas. No existen mecanismos para aumentar la fiabilidad de datos entre los extremos, control de flujo, secuenciamiento u

otros servicios que se encuentran normalmente en otros protocolos host-a-host. El protocolo Internet puede aprovecharse de los servicios de sus redes de soporte para proporcionar varios tipos y calidades de servicio.

1.3. Interfaces

Este protocolo es utilizado por protocolos host-a-host en un entorno Internet. Este protocolo utiliza a su vez protocolos de red locales para llevar el datagrama internet a la próxima pasarela ("gateway") o host de destino. Por ejemplo, un módulo TCP llamaría al módulo internet para tomar un segmento TCP (incluyendo la cabecera TCP y los datos de usuario) como la parte de datos de un datagrama internet. El módulo TCP suministraría las direcciones y otros parámetros de la cabecera internet al módulo internet como argumentos de la llamada. El módulo internet crearía entonces un datagrama internet y utilizaría la interfaz de la red local para transmitir el datagrama internet. En el caso de ARPANET, por ejemplo, el módulo internet llamaría a un módulo de red local el cual añadiría el encabezado 1822 [2] al datagrama internet creando así un mensaje ARPANET a transmitir al IMP. La dirección ARPANET sería deducida de la dirección internet por la interfaz de la red local y sería la dirección de algún host en ARPANET, el cual podría ser una pasarela a otras redes.

1.4. Operación

El protocolo internet implementa dos funciones básicas: direccionamiento y fragmentación. Los módulos internet usan las direcciones que se encuentran en la cabecera internet para transmitir los datagramas internet hacia sus destinos. La selección de un camino para la transmisión se llama encaminamiento. Los módulos internet usan campos en la cabecera internet para fragmentar y reensamblar los datagramas internet cuando sea necesario para su transmisión a través de redes de "trama pequeña". El modelo de operación es que un módulo internet reside en cada host involucrado en la comunicación internet y en cada pasarela que interconecta redes. Estos módulos comparten reglas comunes para interpretar los campos de dirección y para fragmentar y ensamblar datagramas internet. Además, estos módulos (especialmente en las pasarelas) tienen procedimientos para tomar decisiones de encaminamiento y otras funciones. El protocolo internet trata cada datagrama internet como una entidad independiente no relacionada con ningún otro datagrama internet. No existen conexiones o circuitos lógicos (virtuales o de cualquier otro tipo). El protocolo internet utiliza cuatro mecanismos clave para prestar su servicio: Tipo de Servicio, Tiempo de Vida, Opciones, y Suma de Control de Cabecera.

El Tipo de Servicio se utiliza para indicar la calidad del servicio deseado. El tipo de servicio es un conjunto abstracto o generalizado de parámetros que caracterizan las elecciones de servicio presentes en las redes que forman Internet. Esta indicación de tipo de servicio será usada por las pasarelas para seleccionar los parámetros de transmisión efectivos para una red en particular, la red que se utilizará para el siguiente salto, o la siguiente pasarela al encaminar un datagrama internet. El Tiempo de Vida es una indicación de un límite superior en el periodo de vida de un datagrama internet. Es fijado por el remitente del datagrama y reducido en los puntos a lo largo de la ruta donde es procesado. Si el tiempo de vida se reduce a cero antes de que el datagrama llegue a su destino, el datagrama internet es destruído. Puede pensarse en el tiempo de vida como en un plazo de autodestrucción. Las Opciones proporcionan funciones de control necesarias o útiles en algunas situaciones pero innecesarias para las comunicaciones más comunes. Las opciones incluyen recursos para marcas de tiempo, seguridad y encaminamiento especial. La Suma de Control de Cabecera proporciona una verificación de que la información utilizada al procesar el datagrama internet ha sido transmitida correctamente. Los datos pueden contener errores. Si la suma de control de cabecera falla, el datagrama internet es descartado inmediatamente por la entidad que detecta el error. El protocolo internet no proporciona ningún mecanismo de comunicación fiable. No existen acuses de recibo ni entre extremos ni entre saltos. No hay control de errores para los datos, sólo una suma de control de cabecera. No hay retransmisiones. No existe control de flujo.

Los errores detectados pueden ser notificados por medio del Internet Control Message Protocol (ICMP) (Protocolo de Mensajes de Control de Internet) [3] el cual está implementado en el módulo del protocolo internet."

Tabla 46. Síntesis descriptiva del estándar de la RFC791.

2.4 Principales aspectos y características

2.4.1 La cabecera Ipv4

La cabecera del Ipv4 se encuentra conformada por los siguientes campos:

a) Versión (4 bits): El campo Versión describe el formato de la cabecera. La versión más utilizada en la actualidad es la 4.
b) IHL (4 bits): Longitud de la Cabecera Internet (Internet Header Length), es la longitud de la cabecera en palabras de 32 bits y, por tanto, apunta al comienzo de los datos. El valor mínimo para una cabecera correcta es 5.
c) Tipo de Servicio (8 bits): El Tipo de Servicio proporciona una indicación de los parámetros abstractos de la calidad de servicio deseada. Estos parámetros se usarán para guiar la selección de los parámetros de servicio reales al transmitir un paquete a través de una red en particular.
d) Longitud Total (16 bits): La Longitud Total es la longitud del paquete, medida en octetos, incluyendo la cabecera y los datos. Todos los *hosts* deben estar preparados para aceptar datagramas de hasta 576 octetos (tanto si llegan completos como en fragmentos). Los datagramas de mayor tamaño solamente deben ser enviados si el emisor está seguro de que el receptor es capaz de tratar con este tamaño.
e) Identificación (16 bits): Es un valor de identificación asignado por el remitente como ayuda en el ensamblaje de fragmentos de un paquete.
f) Flags (3 bits): Son diversos indicadores de control.
g) Desplazamiento del Fragmento (13 bits): Este campo indica a qué parte del paquete pertenece este fragmento. La posición del fragmento se mide en unidades de 8 octetos (64 bits). El primer fragmento tiene posición 0.
h) Tiempo de Vida (8 bits): Este campo indica el tiempo máximo que el paquete tiene permitido permanecer en la red. Si este campo contiene el valor cero, entonces el paquete debe ser destruido. Este campo es modificado durante el procesamiento de la cabecera. El tiempo es medido en segundos, pero todo router que procese un paquete debe decrementar el TTL (Time To Live: Tiempo de Vida) al menos en una unidad, incluso si procesa el paquete en menos de un segundo. Por tanto, se debe pensar en el TTL sólo como un límite superior del tiempo durante el cual un paquete puede existir. La intención es hacer que los paquetes que, por algún motivo, no puedan ser entregados sean descartados silenciosamente.
i) Protocolo (8 bits): Este campo indica el protocolo de nivel de transporte usado en la parte de datos del paquete IP.
j) Suma de Control de Cabecera (16 bits): Dado que algunos campos de la cabecera cambian (p. ej. el tiempo de vida), esta suma es recalculada y verificada en todo lugar donde la cabecera sea procesada.
k) Dirección de Origen (32 bits): Incluye la dirección IP de origen.
l) Dirección de Destino (32 bits): Incluye la dirección IP de destino.
m) Opciones (longitud variable): Las opciones pueden o no aparecer en los paquetes. Deben ser implementadas por todos los módulos IP (*host* y routers) aunque es su tratamiento es opcional. Contiene las opciones solicitadas por el usuario que envía los datos y se diseñó para que las versiones posteriores del protocolo pudieran incluir información no considerada originalmente, para que los investigadores pudieran probar nuevos conceptos y para que aquella información que es utilizada en raras ocasiones no tuviera asignada unos bits determinados en la cabecera. Cada una de las opciones empieza con 1 byte que identifica la opción. Algunas de las opciones vienen seguidas de un campo de 1 byte para indicar la longitud de la opción y a continuación uno o más bytes de datos. Hay seis opciones (Seguridad, Encaminamiento Estricto Desde el Origen, Encaminamiento Libre Desde el Origen, Registrar la Ruta, Identificación de Secuencia, Marca de Tiempo) definidas actualmente, pero no todas son reconocidas por todos los dispositivos de encaminamiento:

- Seguridad: Permite añadir una etiqueta para indicar lo secreta que es la información que contiene el paquete.
- Encaminamiento estricto desde el origen: Es una secuencia de direcciones IP que sirve para indicar la trayectoria completa que debe seguir el paquete desde el origen hasta el destino.
- Encaminamiento libre desde el origen: Es una secuencia de direcciones IP que sirve para indicar que el paquete debe pasar obligatoriamente por esos dispositivos de encaminamiento y en ese orden, aunque también pueda atravesar por otros dispositivos de encaminamiento.
- Registrar la ruta: Sirve para indicar que los dispositivos de encaminamiento agreguen su dirección IP al campo de opción y de esta manera tener conocimiento de la ruta seguida por el paquete.
- Identificación de secuencia. Se utiliza cuando hay recursos reservados para un servicio, por ejemplo voz.

Sello de tiempo: En este caso, además de registrar las direcciones de los dispositivos de encaminamiento como se hacia en la opción registrar la ruta, se utilizan 32 bits para guardar una marca de tiempo expresada en milisegundos. Esta marca es usada en el presente proyecto. [67]

Tabla 47.Tabla de campos de la cabecera Ipv4.

[67] Juan Martinez Universidad Rey Juan Carlos - Grupo de Sistemas y Comunicaciones, Departamento de Ingeniería Telemática y Tecnología Electrónica "Protocolo de Internet" España-2005, http://gsyc.escet.urjc.es/~juaner/investigacion/pfc2/node8.html

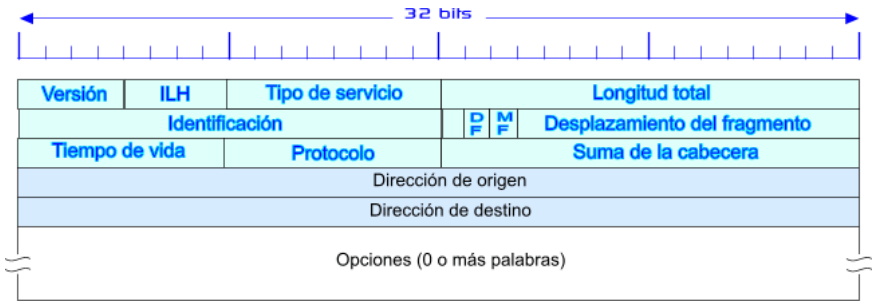


Ilustración 70. Estándar de la estructura del formato de cabecera IPv4[68].

2.4.2 Formato de direcciones Ipv4.

Para que en una red dos computadoras puedan comunicarse entre sí ellas deben estar identificadas con precisión Este identificador puede estar definido en niveles bajos (identificador físico) o en niveles altos (identificador lógico) dependiendo del protocolo utilizado. TCP/IP utiliza un identificador denominado dirección Internet o dirección IP, cuya longitud es de 32 bytes. La dirección IP identifica tanto a la red a la que pertenece una computadora como a ella misma dentro de dicha red.

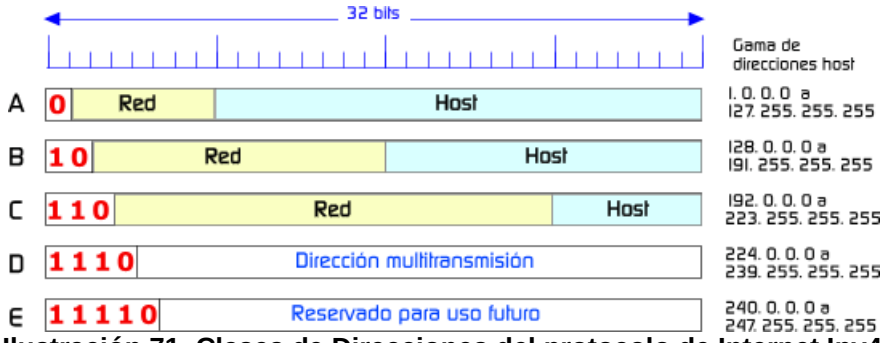


Ilustración 71. Clases de Direcciones del protocolo de Internet Ipv4.

Tomando tal cual está definida una dirección IP podría surgir la duda de cómo identificar qué parte de la dirección identifica a la red y qué parte al nodo en dicha red. Lo anterior se resuelve mediante la definición de las "Clases de Direcciones IP". Para clarificar lo anterior veamos que una red con dirección clase A queda precisamente definida con el primer octeto de la dirección, la clase B con los dos primeros y la C con los tres primeros octetos. Los octetos restantes definen los nodos en la red específica.

---

[68] Imagen fuente: Networking and Emerging Optimization de la Universidad de Málaga "Protocolo de Comunicación" http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/cabipv4.html

2.4.3 NAT (Traducciones de direcciones de Red)

NAT[69] en realidad no es un único método de traducción de direcciones, en realidad hay cuatro distintos: NAT Básico (Tradicional), NAT Bidireccional, Doble NAT y NATP. NAT es una solución a corto plazo, pero de uso muy extendido. Sin embargo su introducción en el despliegue de IPv4 ha introducido algunos problemas. Para decirlo de una forma rápida, NAT no inter-opera todo lo bien que debiera con protocolos ya definidos en IPv4. Ejemplos: RPC, FTP, X-windows... que no funcionan tan fácilmente de forma que permita su crecimiento, nuevos servicios y aplicaciones mejoradas, y en general la innovación. Además, estas técnicas hacen de Internet, las aplicaciones, e incluso los dispositivos mucho mas complejos, y esto supone también un incremento del coste[70].

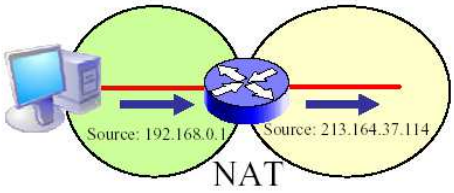


Ilustración 72. Traducción NAT[71].

La razón?
Estos protocolos incluyen, en algunos casos, información de la cabecera TCP/IP (que es la que NAT altera) dentro del intercambio de información entre equipos. NAT rompe, por tanto, el concepto universal en Internet: comunicaciones extremo a extremo.
La dirección IP ya no es un identificador único, una misma dirección IP puede, en realidad, ser utilizada por múltiples hosts con un servidor (dispositivo NAT) realizando la multiplexación. Todos los protocolos que he indicado anteriormente, junto con algunos otros (por ejemplo, Voz sobre IP, VoIP) se basan en este concepto de extremo a extremo.
Sin embargo, estos protocolos pueden, generalmente, resolverse con la introducción de ALG (Application Level

[69] Usemos un ejemplo para entender, sin tecnicismos, que es NAT. Supongamos que dos personas que hablan el mismo lenguaje, digamos Castellano, necesitan usar un determinado medio de comunicación, que sin embargo no permite el uso de Castellano. Para permitir dicha conversación, por tanto, necesitan usas traducciones situados juntos a cada uno de los dos participantes en dicha conversación, a cada lado del canal de comunicación. Es obvio que algunos matices de la comunicación se podrían perder con las traducciones. Esto es muy similar a lo que hoy ocurre con Internet con Ipv4: La falta de comunicaciones extremo a extremo impide que los servicios y aplicaciones tengan capacidad de sacas todo el provecho de la red, haciendo todo mucho más complejo e incrementando los costes de administración considerándose a NAT en la actualidad como un demonio de la innovación.
[70] Mientras que Ipv6 puede hacer que, a medio/largo plazo, cada dispositivo IP sea mas asequible, mas poderoso e incluso consuma menos energía(lo cual no es solo importante para la conservación ecológica, sino también para permitir baterías de mayor duración en dispositivos como teléfonos celulares).
[71] Julio Alba Soto(jalba satec.es) director de proyectos www.satec.es Requisitos de transición a IPv6-2004 pag. 8 http://www.6sos.net/pdf/boom_de_ipv6_cuando_los_servicios_lo_soporten_v2.pdf

Gateway). La idea general es que en el dispositivo NAT se introduce un Proxy que hace las modificaciones necesarias a la "carga" de los paquetes para que funcionen a través de un dispositivo NAT.
Por ejemplo, si en FTP el cliente utiliza el comando PORT para indicar el puerto en el que va a esperar la conexión de datos del servidor. El ALG de FTP lo que hará será inspeccionar el contenido de los paquetes enviados por el cliente, de forma que si ve una directiva PORT la modifique para que funcione tras la traducción.
También hay problemas generales por el uso de NAT en TCP/IP. Uno de ellos es el caso de que se utilice fragmentación de paquetes, como se comenta en el RFC 3027.Sin embargo, aún así, habrá protocolos que no funcionen ni con un ALG.
Esto sucede, por ejemplo, cuando el dispositivo NAT no puede modificar el contenido de los paquetes y éstos incluyen información dependiente de las cabeceras.
¿Cuando sucede esto?
Cuando se utiliza cifrado a nivel de aplicación, por ejemplo, o cuando, con IPsec se utiliza a nivel de red.
IPsec tiene dos métodos para garantizar estos servicios: AH y ESP .El primero de ellos garantiza la autenticidad de los paquetes TCP/IP y hace esto mediante la generación de un hash cifrado que "protege" la cabecera TCP/IP .
Esta información se incluye en todos los paquetes, así, si el servidor remoto observa que, tras descifrar el hash y compararlo con el que genera él del paquete son distintos, entonces descarta el paquete, porque alguien lo ha manipulado.
Claramente, AH no funciona con NAT. Si NAT modifica el paquete, y IPsec-AH se protege contra estas modificaciones, el resultado es interoperabilidad 0 (siempre y cuando claro, la operación de NAT se haga después de la de IPsec) ESP (Encapsulating Security Payload, RFC 2406) ofrece cifrado para el contenido del paquete IP.
De forma que garantiza la confidencialidad de la comunicación la cabecera IP se mantiene (en modo normal, no en modo túnel) sin embargo, el contenido se cifra. (Es decir, a partir de las opciones de IP, esto incluye la carga TCP/UDP/ICMP, etc.., el nivel transporte). ESP tiene problemas con NAT, aunque funciona en algunos casos (como es el modo túnel). Por la sencilla razón de que, como el contenido de los paquetes está cifrado, y el dispositivo NAT puede tener que cambiar esta información, los paquetes no salen "bien".
Por ejemplo, si cambia la dirección IP, cambia el CRC del paquete TCP y como el paquete está cifrado, el dispositivo NAT no puede (en principio) descifrarlo, volverlo a generar, y cifrarlo de nuevo.
O, en otro caso, si el dispositivo NAT tiene que cambiar el puerto TCP (cuando se usa NATP) el hecho de que no pueda modificarlo significa que el paquete no sale del dispositivo.
Por último, en IPSec hay que considerar IKE, que es el protocolo que se utiliza para el intercambio de claves entre los servidores que establecen el túnel de cifrado.
El hecho de que el intercambio de claves no funcione significa que ¡ni siquiera se puede establecer la comunicación IPSec.
Dos razones para que falle IKE:
1.- Algunas implementaciones de IKE sólo funcionan si origen y destino utilizan el puerto UDP 500 (por tanto si el dispositivo NAT cambia el puerto, nada que hacer)
2.- Si IKE utiliza como mecanismo de autenticación alguno de los propuestos basados en dirección IP, si ésta cambia, entonces estamos en la misma situación.
Esto resume un poco todos los problemas.
En realidad hay varios drafts del IETF (www.ietf.org) que hablan de los problemas de interoperabilidad de IPsec y NAT y sólo hay una propuesta que funcione, en todas las situaciones, extremo a extremo. Se conoce como NAT-T (Nat Traversal).
Existe una propuesta de implementación parcial basada en FreeSwan, que también se encuentra entre los estándares.
Como sustituto general de NAT, existe un draft, conocido como el protocolo RSIP (Realm Specific IP) que podría llegar a ofrecer conectividad extremo a extremo.
El protocolo es complejo, pero quizás se puede resumir en que es un NAT "acordado" es decir, los dispositivos que realizan la traducción de direcciones le comunican la dirección con la que va a salir al servidor origen.
De esta forma, cuando envíe paquetes al servidor remoto, puede "prepararlos" para que no sufran los efectos del cambio de dirección. Por ejemplo, puede calcular el CRC de los paquetes, en lugar de en base a su dirección actual, a la dirección final con la que sale. En cualquier caso RSIP no es todavía un estándar, pero que podría resolver, a corto, medio plazo, todos los problemas extremo-a-extremo en protocolos que no interoperen con NAT (IPsec incluido). Aunque esto significa cambiar las pilas de protocolos de los sistemas operativos, e introducir elementos de interconexión que incluyan este protocolo. NAT ha sido la "salvación" para IPv4 a corto plazo, no cabe la menor duda, y es el origen de su gran popularidad. Sin embargo, con el tiempo se han detectado problemas con muchos protocolos, el hecho de que IPSec sea uno de ellos no es de extrañar, ya que NAT rompe la premisa en la que se basa precisamente IPSec (y que intenta mantener) .
Actualmente IPSec no está tan extendido como podría estarlo, aunque la culpa no es sólo de NAT (los problemas de despliegue de las infraestructuras de claves públicas influyen) y, generalmente, uno se lo encontrará asociado a un dispositivo de NAT. De forma que la traducción de direcciones se haga antes que el cifrado.

Tabla 48. Ámbito de encuadramiento de la NAT.

A continuación se presentan los siguientes tipos de NAT[72]:

a) NAT full conexión. En el caso de la conexión completa o llena,(Full Cone) ver ilustración inferior, cuando la traducción se encuentra establecida, cualquier equipo que quiera alcanza al cliente detrás del NAT, necesita solo conocer la dirección y el puerto de donde el trafico esta siendo enviado. Por ejemplo un equipo detrás de un NAT con dirección 192.168.0.1 enviando y recibiendo en el puerto 5000, se ha traducido a la dirección externa 216.155.76.8 en el puerto 12345. Cualquier equipo de Internet puede enviar tráfico a esta IP externa y este tráfico será traspasado a la dirección cliente 192.168.0.1:5000.

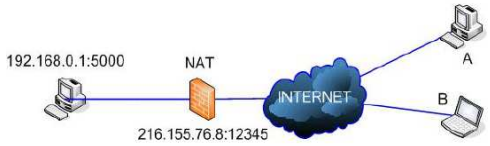


Ilustración 73. NAT Full conexión.

b) NAT conexión restringida. En este caso de la conexión restringida,(Restricted Cone) ver ilustración inferior, la IP y puerto externo son abiertos cuando el equipo de la red privada envía trafico saliente a una dirección IP especifica. Por ejemplo si el cliente envía paquetes hacia el equipo A, el NAT traduce la dirección privada 192.168.0.1.:5000 a la dirección pública 216.155.76.8:12345, dejando que solamente el equipo A pueda enviar trafico a esa dirección pública. El NAT bloqueara cualquier otro tráfico que venga de una dirección distinta. Por lo tanto el equipo B podrá enviar trafico hacia la red privada, solamente si antes el equipo que se encuentra detrás del NT a enviado a este equipo B.

[72] Heinz Waldemar Herlitz Gatica, TESIS "Transversabilidad en NAT-FIREWALL"Universidad católica de Temuco, Facultad de Ciencias 2005.

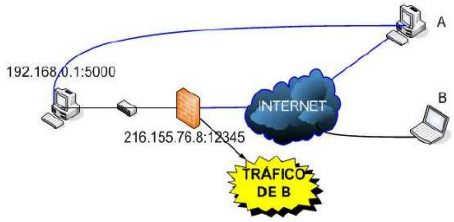


Ilustración 74. NAT conexión restringida.

c) NAT conexión restringida por puerto. Una conexión restringida por puerto,(Port restricted cone) ver ilustración inferior, es casi idéntica a la conexión restringida, pero en este caso el NAT bloqueara todo el trafico, a menos que el cliente haya enviado antes trafico a una IP y puerto especifico, solo entonces esa IP: PUERTO tendrán acceso a la red privada. Entonces en nuestro ejemplo si el cliente envía trafico al equipo B puerto 10101, el NAT solo permitirá tráfico proveniente desde 200.72.40.55:10101, ahora si el cliente envía a múltiples direcciones y puerto entonces estas direcciones podrán responder a clientes a la dirección 216.155.76.8:12345.

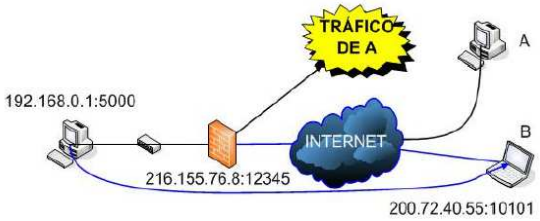


Ilustración 75. NAT conexión restringida por puerto.

d) NAT simétrico. El ultimo tipo de NAT simétrico, (Symmetric NAT) ver ilustración inferior, es diferente de los otros 3. Específicamente debido a que la traducción de la IP publica a la privada depende de la IP de destino donde ha sido enviado el trafico, Para nuestro ejemplo si el cliente envía trafico desde la dirección privada 192.168.0.1:5000 al equipo B, la dirección traducida seria la 216.155.76.8 con el puerto 12345, y si el equipo privado envía trafico a otra IP publica distinta la dilección traducida para ese equipo seria la 216.155.76.8 con el puerto 45678.

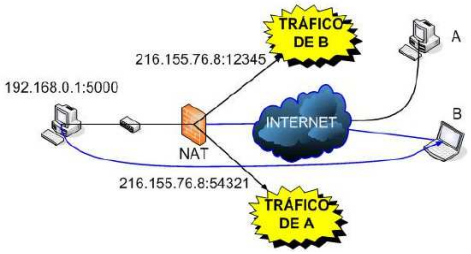


Ilustración 76. NAT simétrico.

2.5 Principales diferencias entre Ipv4 e Ipv6

Ipv4 tuvo que evolucionar para proporcionar lo que los usuarios demandaban (Mas direcciones, capacidades QoS, seguridad, movilidad IP, multicast y mas ancho de banda) por las causas de la proliferación de aplicaciones P2P y GRID, "Convergencia IP(VoIP y Triple Play)", aumento y diversificación de las amenazas a la seguridad, comercio electrónico, diversidad de dispositivos IP(PDAs, telefonía móvil, domótica, etc.) mostrando así, una marcada tendencia entre Ipv4 e Ipv6 la capacidad de servicios, como se muestra en la ilustración inferior:

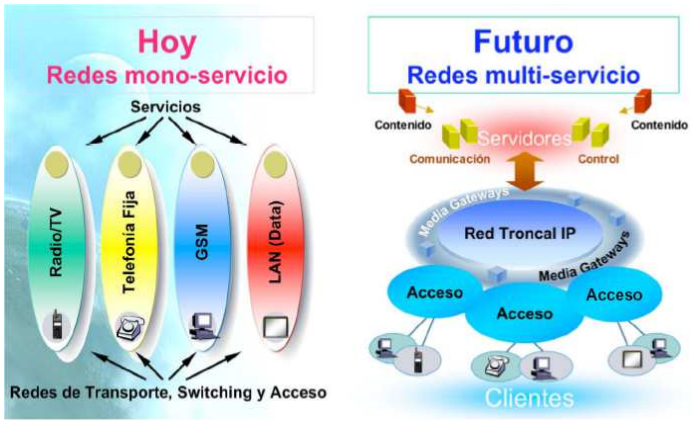


Ilustración 77. Estructura de Servicios[73].

El siguiente cuadro resume las principales diferencias funcionales entre los protocolos Ipv4 e Ipv6.

[73] Fuente: Jordi Palet, "Evolución de las redes basadas en el protocolo IP, facilidades y ventajas de las redes IP", European Ipv6 Task Force and Steering Comité IPv6 Forum, Education and promotion WG Co-chair Cónsulintel.,CTP-CEO.

Protocolo IPv4	Protocolo IPv6
Espacio de direcciones de 32 bits, es decir $2^{32} \sim 4.2x10^{9}$ direcciones IP posibles	Espacio de direcciones de 128 bits, es decir $2^{128} \sim 3.4x10^{34}$ direcciones IP posibles
Configuración Manual o Dinámica (*DHCP*)	Configuración "Plug & Play", Manual o Dinámica (*DHCPv6*)
Direcciones de Tipo *Unicast*, *Multicast* y *Broadcast*	Direcciones Tipo *Unicast*, *Multicast* y *Anycast*
Políticas de calidad de servicio se realizan a través del campo *Tipo de Servicio* (ToS) del paquete IP	Políticas de calidad de servicio se realizan a través de los campos *Etiqueta de Flujo* y *Clase de Tráfico*
Seguridad es algo opcional, a través del parche *IPSec*.	Seguridad extremo-a-extremo implementada en forma nativa
Protocolo no escalable	Protocolo escalable

Tabla 49. Cuadro de diferencias del protocolo Ipv4 e Ipv6[74].

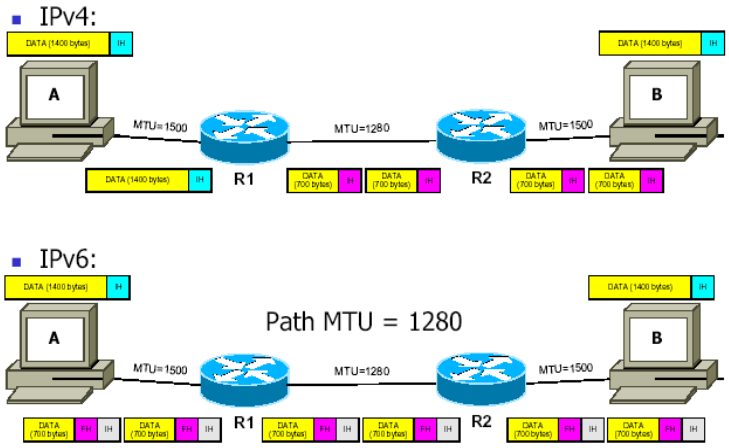


Ilustración 78. Ipv4 e Ipv6 Fragmentación y Reensamblado[75].

[74] Javier Rodríguez Albornoz, Rodrigo Guerra Diaz y Agustin Gonzáles Valenzuela, "Evaluación y comparación de los protocolos de Internet versión 4 y versión 6 en una red experimental WDM" Universidad Técnica Federico Santa Maria Departamento de Electrónica.

[75] Ing. Carlos Bercenilla c.a.barcenilla@ieee.org , "Ipv6", The Next Generation Internet Protocol, Universidad Tecnologica Nacional Facultad Regional La Plata.

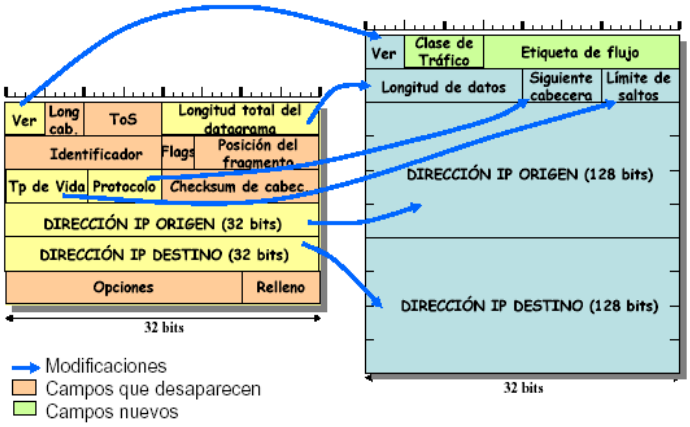


Ilustración 79. Diferencias de los formatos de cabecera se presenta Ipv4 e Ipv6[76].

2.6 En que consisten los protocolos TCP/IP.

Aunque el modelo de referencia OSI sea universalmente reconocido, el estándar abierto de Internet desde el punto de vista histórico y técnico es el Protocolo de control de Transmisión-Protocolo Internet (TCP/IP). El modelo de referencia TCP-IP tiene importancia histórica, al igual que las normas que permitieron el desarrollo de la industria telefónica, de energía eléctrica., el ferrocarril, la televisión y las industrias de videos. El TCP-IP es una colección de protocolos estándar de la industria diseñada para intercomunicar grandes redes. Las Siglas TCP/IP provienen de Transmisión Control Protocol-Internet Protocol. Vamos a intentar dar en esta parte, unos conceptos sobre TCP/IP, su terminología y explicar como la Internet Society crea el estándar Internet.

[76] Eva castro, "Diferencias de los formatos de cabecera entre Ipv4 e Ipv6", Universidad de Alcalá Departamento de Automática.

Direccionamiento	Direcciones 128 bits asignadas jerárquicamente
Encaminamiento	Jerárquico, agregación de rutas
Prestaciones	Cabecera simple, alineada a 64 bits
Versatilidad	Formato flexible de opciones
Multimedia	Identificador de flujos
Multicast	Obligatorio, control de ámbitos
Seguridad	Soporte a la autenticación/encriptado (IPsec)
Autoconfiguración	Configuración automática
Movilidad	Mejora de la eficiencia y seguridad
Multihoming	Facilita el cambio de proveedor de servicio

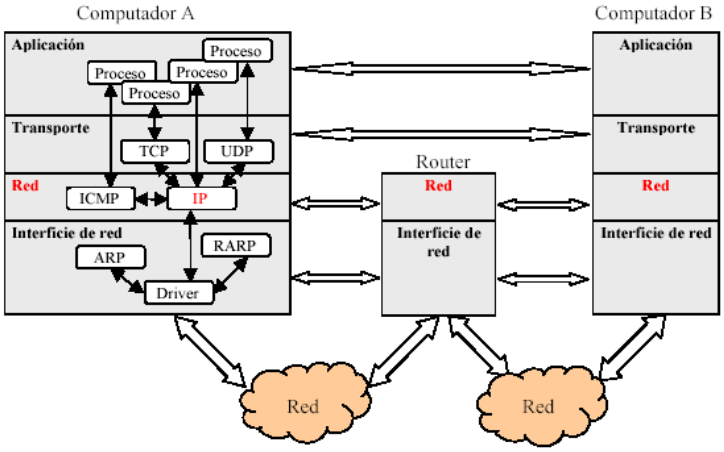


Ilustración 80. Arquitectura del TCP/IP[77].

2.6.1 Reseña Histórica

El TCP-IP fue originado con los experimentos de intercambio de paquetes dirigido por el U.S. Departamento of Defense Advanced Research Projects Agency (DARPA) durante la década de 1960 a 1970. Hay varios hitos importantes en la historia del TCP/IP.

1970: Los ordenadores de la advanced research Agency Network (ARPANET) comienza a utilizar el NCP (Network Control Protocol).
1972: La primera especificación Telnet, "ad hoc telnet protocol" se define como una RFC la 318.
1973: RFC 454. Se introduce el FTP(File Transport Protocol).
1974: El TCP(Transmisión Control Protocol) se especifica detalladamente.
1981: El estandar IP se publica en la RFC 791.
1982: la "defense Comunications Agency"(DCA) y ARPA establecen a la "Transmisión Control Protocol(TCP) y al internet protocol(IP)" como la colección de protocolos TCP-IP
1983: ARPANET cambia de NCP a TCP-IP.
1984: Se define el concepto de DNS(Domain Name System).

Tabla 50. Reseña histórica de la TCP/IP.

2.6.2 El modelo de capa de TCP-IP.

a) Capa de Red: La base de este modelo de capas de interfase de red. Esta capa es la responsable de enviar y recibir frames, los cuales son los

[77] Paul Artigas, Daved Carrera y Jordi Torres "T6 nivel IP- Xarxes de computador's i aplicaction's" Universidad Politécnica de Catalunya, Departamento de Arquitectura de computadores" UPC, 2006.

paquetes de información que viajan un una red como una “Unidad Simple”. La capa de red, envía frames a la red, y recupera frames de la red.

b) Capa de Internet: Esta capa encapsula paquetes en datagramas Internet y además esta capa ejecuta todos los algoritmos de enrutamiento (routing) de paquetes. Los cuatro protocolos de Internet son: Internet Protocol(IP), Address Resolution Protocol(ARP), Internet Control Message Protocol(ICMP) y Internet Group Management Protocol(IGMP).

- IP: Es el responsable del envío y enrutamiento de paquetes entre maquinas y redes.
- ARP: Obtiene las direcciones de hardware de las maquina situadas en la misma red física. Recordemos que la dirección física de cada tarjeta de red es única en el mundo. Dicha dirección “física” ha sido implementada vía hardware por el fabricante de la tarjeta de red, y dicho fabricante. Lo selecciona de un rango de direcciones único asignado a el y garantiza la unicidad de dicha tarjeta. Este caso es el más corriente y es el de las tarjetas de red Ethernet. Existe para otras topologías de red, igualmente una asignación única hardware de reconocimiento de la tarjeta.
-ICMP: Envía mensajes e informa de errores en el envió de paquetes.
-IGMP: Se utiliza para la comunicación entre routers (Enrutadores de Internet)

c) Capa de transporte: La capa de transporte, nos da el nivel de “sesión” en la comunicación. Los dos protocolos posibles e transporte son TCP(Transmisión Control Protocol) y UDP(User Datagram Protocol). Se puede utilizar uno u otro protocolo dependiendo del método preferido de envió de datos. El TCP nos da un tipo de conectividad “Orientado a conexión”. Típicamente se utiliza para transferencia de largas cantidades de datos de una sola vez. Se utiliza también en aplicaciones que requieren un “reconocimiento” o validación (ACK: acknowledgment) de los datos recibidos.

El UDP proporciona conexión de comunicación y no garantiza la entrega de paquetes. Las aplicaciones que utilicen UDP normalmente envían pequeñas cantidades de datos de una sola vez. La aplicación que lo

utilicé, es la responsable en este caso de la integridad de los paquetes y debe estableces su propios mecanismos para pedir repetición de mensaje, seguimiento, etc. No existiendo ni garantía de entrega ni garantía del orden de entrega en la maquina destino.

d) Capa de Aplicación: En la cima de este modelo, esta la capa de aplicación. Esta es la capa que las aplicaciones utilizan para acceder a la red. Existen muchas utilidades y servicios en la capa de aplicación, por ejemplo: FTP, Telnet, SNMP y DNS.

2.7 En que consiste el Modelo OSI

Durante las ultimas dos décadas ha habido un enorme crecimiento en la cantidad y tamaño de las redes. Muchas de ellas sin embargo, se desarrollaron utilizando implementación de Hardware y Software diferente. Como resultado, muchas de las redes eran incompatibles y se volvió muy difícil para las redes que utilizaban especificaciones distintas poder comunicarse entre si. Para solucionar este problema, la Organización Internacional para la Normalización (ISO) realizo varias investigaciones acerca de los esquemas de red. La ISO reconoció que era necesario crear un modelo de red que pudiera ayudar a los diseñadores de red a implantar redes que pudieran comunicarse y trabajar en conjunto(Interporatividad) y por lo tanto, elaboraron el modelo de referencia OSI en 1984. Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red hablen el mismo lenguaje o protocolo. Un protocolo es un conjunto de reglas que hacen que la comunicación en una red sea más eficiente. Una definición técnica de un protocolo de comunicaciones de datos es: Un conjunto de normas, o un acuerdo, que determina el formato y la transmisión de datos. La capa n de un computador se comunica con la capa n de otro computador. Las normas y convenciones que se utilizan es esta comunicación se denominan colectivamente protocolo de la capa n. Al principio de un desarrollo, las LAN, MAN y WAN eran en cierto modo caótico. A principios de la década de los 80 se produjeron tremendos aumentos en la cantidad y el tamaño de las redes. A medida que las empresas se dieron cuenta de que podrían ahorrar mucho

dinero y aumentar la productividad con la tecnología de Networking, comenzaron a agregar redes y a expandir las redes existentes casi simultáneamente con la aparición de nuevas tecnologías y productos de red.

a) Capa de Aplicación.

La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiera de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de dichos procesos de aplicación son los programas de hojas de cálculo, el procesamiento de texto y los de las terminales bancarias. La capada aplicación establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación e errores y control de integridad de los datos.

Nota: Si desea recordar la capa de aplicación o capa 7 en la menor cantidad de palabras posible, piense en los navegadores de Web.

b) Capa de Presentación.

La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.

Nota: Si desea recordar la capa de presentación o capa 6 en la menor cantidad de palabras posible, piense en un formato de datos común.

c) Capa de Sesión.

Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el dialogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase

de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

Nota: Si desea recordar la capa de sesión o capa 5 es la menor cantidad de palabras posible, piense en diálogos y conversaciones.

d) Nivel de Transporte.

La capa de transporte segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor. El limite entre la capa de sesión y la capa de transporte puede imaginarse como el limitara entre los protocolos de capa de medios y los protocolos de capa de host. Mientras que las capas de aplicación, presentación y sesión están relacionadas con aspectos de las aplicaciones, las tres capas inferiores se encargan del transporte de datos. La capa de transporte intenta suministra un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales.

Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte.

Nota: Si desea recordar de transporte o capa 4 en la menor cantidad de palabras posible, piense en calidad de servicio y confiabilidad.

e) Capa de Red.

La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hots que pueden estar ubicados en redes geográficamente distintas.

Nota: Si se desea recordar la capa de red o capa 3 es la menos cantidad de palabras posible, piense en selección e ruta, conmutación, direccionamiento y enrutamiento.

f) Capa de Enlace.

La capa de enlace de datos proporciona un transito de datos confiable a través de un en enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico). La topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo.

Nota: Si desea recordar la capa de enlace o capa 2 es la menor cantidad de palabras posible, piense en tramas y control de acceso al medio.

g) Nivel Físico.

La capa física defina las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares se definen a través de las especificaciones de la capa física. Nota: Si desea la capa de física o capa 1 es la menor cantidad de palabras posible, piense en señales y medios.[78]

Ilustración 81. Capas del modelo de referencia OSI[79].

2.8 Paralelo de la OSI con el TCP-IP

[78] Darwin Lamarck Santana Yuner, TESIS "IPv6, nueva generación del protocolote Internet", Universidad Nacional Pedro Henriquez Ureña, Facultad de ciencia y tecnología, Escuela de Informática, Santo Domingo-2004.

[79] Fuente: Curso de "REDES DE COMUNICACIONES", "Capitulo II, Modelo de referencia OSI", Universidad de Santiago de Chile, Facultad de Ingeniería, Departamento de Ingeniería Eléctrica, http://usach.jedicruces.cl/cap2.htm

Como sabemos, OSI("Open Systems Interconnection") es la estructura de protocolos en siete niveles propuesta por ISO e ITU-T ("International Telecommunication Union Telecommunication Standardization Sector") la arquitectura OSI se ha impuesto en los años 90 al contrario de lo que se opinaba en los 80, cuando se creía que el modelo OSI es el que triunfaría. Los protocolos TCP/IP están compuestos por cuatro niveles o capas, de forma que cada uno utiliza los servicios del nivel inferior y se crearon y normalizaron mucho antes de que se definiera el modelo de referencia OSI de la ISO. Ya a finales de los 80, muchas empresas y administraciones usaban TCP/IP, cuando todavía la torre OSI no estaba totalmente desarrollada. Pese a que los gobiernos apoyaban los estándares de OSI, desde mediados de los 80 se ha ido introduciendo TCP/IP en las administraciones, principalmente en el Departament of Defense de Estados Unidos, donde precisamente se creó. Otro de los motivos de su implantación es la popularización de Internet. Aun así, el modelo OSI es una buena idea de organización de protocolos, por lo que suele ser el más estudiado. No existe un modelo oficial de protocolos TCP/IP, al contrario que en OSI. Los protocolos se han ido definiendo anárquicamente, y a posteriori englobados en capas. Aunque OSI tiene muchos puntos a su favor, no ha logrado sustituir a la arquitectura TCP/IP como estándar en Internet[80].

Ventajas	Inconvenientes
-Inter-funcionamiento e interconexión de equipos de distintos fabricantes. -Economías de escala, globalizando el mercado para evitar la dependencia no deseada de un solo fabricante y conseguir abaratar los precios de los equipos.	-Complejidad para satisfacer los intereses particulares múltiples y variados de los distintos clientes y fabricantes. Las soluciones a la medida de cada usuario quedan descartadas en favor de la estandarización. -Inmovilismo tecnológico, que redunda en la imposibilidad de aplicar inmediatamente los continuos avances tecnológicos en un campo tan dinámico como el de las telecomunicaciones.

Tabla 51. Problemas sobre la normalización.

- OSI define claramente las diferencias entre los servicios, las interfaces, y los protocolos.

  - Servicio: lo que un nivel hace
  - Interfaz: cómo se pueden acceder los servicios

[80] Arturo Azcorra <azcorra@it.uc3m.es>, Álvaro Ramos <arc@it.uc3m.es> Asignaturas de "Redes de comunicaciones –Redes de computadoras" y "transmisión de datos" Proyecto PROMETEO Universidad Carlos III de Madrid, http://www.it.uc3m.es/~prometeo/rsc/problemas/por_temas/Tema1/normas.html <www@it.uc3m.es>.

- Protocolo: la implementación de los servicios

- TCP/IP no tiene esta clara separación.

- Porque OSI fue definido antes de implementar los protocolos, los diseñadores no tenían mucha experiencia con donde se debieran ubicar las funcionalidades, y algunas otras faltan. Por ejemplo, OSI originalmente no tiene ningún apoyo para broadcast.

- El modelo de TCP/IP fue definido después de los protocolos y se adecuan perfectamente. Pero no otras pilas de protocolos.

- OSI no tuvo éxito debido a:

  - Mal momento de introducción: insuficiente tiempo entre las investigaciones y el desarrollo del mercado a gran escala para lograr la estandarización
  - Mala tecnología: OSI es complejo, es dominado por una mentalidad de telecomunicaciones sin pensar en computadores, carece de servicios sin conexión, etc.
  - Malas implementaciones.
  - Malas políticas: investigadores y programadores contra los ministerios de telecomunicación.
  - Sin embargo, OSI es un buen modelo (no los protocolos). TCP/IP es un buen conjunto de protocolos, pero el modelo no es general.

En la imagen se pueden apreciar los 5 niveles de la arquitectura, comparados con los siete de la torre OSI.

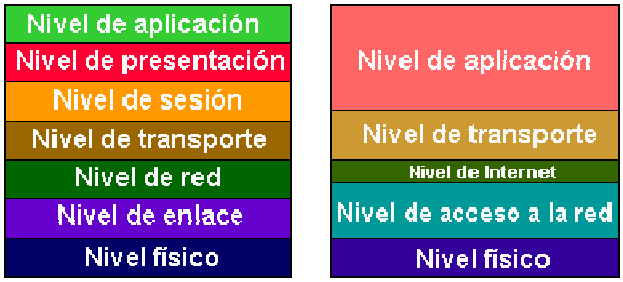


Ilustración 82. Paralelo entre el modelo OSI y la arquitectura TCP/IP.

Debido a esta correspondencia entre OSI y TCP/IP, por ejemplo, el nivel IP del modelo TCP/IP puede ir sobre protocolos diseñados para la torre OSI.

Capa	Descripción
Medio de Transmisión	Soporte material (físico) de la transmisión.
Capa Física	Transmisión de bits. Voltajes, tiempos, ...
Capa de Enlace de Datos	Control de errores. Control de flujo. En redes de difusión: control de acceso al canal.
Capa de Red	Controla las operaciones de la subred. Determinar el camino de los paquetes. Control de congestiones. Calidad de servicio (retrasos, tiempos transmisión, ...)
Capa de Transporte	Partir datos en unidades más pequeñas y pasarlos a la capa de red. Asegurarse de que llegan al receptor. Es una capa de fin a fin, desde fuente a destino.
Capa de Sesión	Establecer sesiones entre máquinas. Control de diálogos, gestión de *tokens* y sincronización.
Capa de Presentación	Sintaxis y semántica de la información transmitida.
Capa de Aplicación	Protocolos de usuario.

Capa	Descripción
Capa Ordenador-Red	No se especifica mucho, solo que debe permitir el envío de paquetes IP a la red.
Capa de Internet	Red sin conexión basada en conmutación de paquetes. Inyectar paquetes a la red con caminos independientes. Pueden llegar paquetes en orden diferente. Define el protocolo IP (*Internet Protocol*).
Capa de Transporte	Permite llevar una conversación entre peers. Protocolo TCP (*Transmission Control Protocol*): Orientado a conexión y fiable. Fragmenta los mensajes para la capa de internet y los ensambla en destino. Control de flujo. Protocolo UDP (*User Datagram Protocol*). No fiable. Sin conexión, para aplicaciones que no necesitan secuenciación TCP o control de flujo. Cuando se necesita rapidez.
Capa de Aplicación	Protocolos de usuario.

Tabla 52. Descripción del paralelo del modelo OSI y la arquitectura TCP/IP.

OSI	TCP/IP
-Conceptos centrales en OSI: Servicios, interfaces, protocolos -TCP-IP originalmente no distinguió entre estos 3 conceptos: Después se ha res-estructurado. -OSI oculta mejor los protocolos. Se pueden realizar cambios fácilmente. -OSI se definió antes que los protocolos en particular. Modelo más general.	-En TCP-IP los protocolos definieron primero. El modelo fue una descripción de los protocolos. -OSI soporta comunicaciones: Con o sin conexión en la capa de red. Solo conexión en capa de transporte (visible al usuario). -TCP-IP soporta comunicación basada: Sin conexión en la capa de red. Ambas en la capa de transporte (da opción al usuario).

Tabla 53. Diferencias de la OSI vs TCP/IP.

OSI	TCP/IP

-Mala planificación: Estándares tarde. tcp/ip estaba ya siendo utilizado. -Mala tecnología: Elección de capas no de acuerdo a criterios técnicos. Capas sesión y presentación casi vacías. Capas de enlace de datos y red demasiados llenos. Modelo complejo. Redundancia de funciones en varias capas. -Mala implementación: Complejidad del modelo: primeras implementaciones ineficientes y lentas. -Mala política: Imposición de organismos oficiales.	-No distingue claramente entre: Servicio, interfaz y protocolo. -No es un modelo general. No puede describir otras pilas de protocolos. -La capa de ordenador-red no es una capa en el sentido del termino: Es una interfaz entre la red y la capa de enlace de datos. No distingue la capa física y de enlace de datos. -Protocolos implementados ad-hoc, difíciles de reemplazar.

Tabla 54. Criticas de la OSI y el TCP/IP.

2.9 Modelos de transición del protocolo Ipv6.

Las técnicas y tecnologías de la transición del protocolo Ipv6 se establecen en el RFC 2893.

2.9.1 Transición modo túnel.

El túnel IPv6 sobre IPv4 es la encapsulación de paquetes IPv6 con un encabezado IPv4 para que los paquetes IPv6 puedan ser enviados sobre infraestructura IPv4. Dentro del encabezado IPv4:

- El campo de protocolo de IPv4 es puesto a 41 para indicar que es un paquete IPv6 encapsulado.
- Los campos origen y destino son asignados para direcciones IPv4 para los extremos del túnel. Los extremos del túnel son configurados manualmente como parte de la interfase del túnel o están automáticamente derivados desde la interfase transmisora, la dirección del próximo salto de la ruta en cuestión o de las direcciones IPv6 fuente y destino en la cabecera IPv4.

Ilustración 83. Paquetes para túnel IPv6 sobre IPv4.

Para el túnel IPv6 sobre IPv4, la unidad de transmisión máxima (MTU) de la trayectoria IPv6 para el destino es típicamente 20 bytes menos que el MTU de la trayectoria IPv4 del destinatario. Sin embargo, si el MTU de la ruta IPv4 no se almacena para cada túnel, existen instancias donde los paquetes IPv4 necesitan ser fragmentados en un enrutador intermedio IPv4. En este caso, el paquete IPv6 sobre IPv4 transmitido sobre el túnel debe ser enviado con la bandera de no fragmentación en la cabecera del encabezado IPv4, es decir esta bandera es puesta a 0.

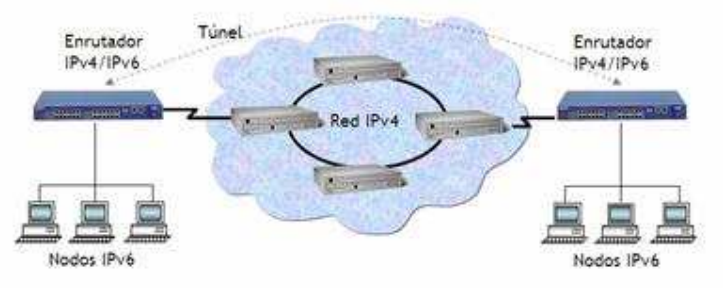


Ilustración 84. Túnel IPv6 sobre IPv4.

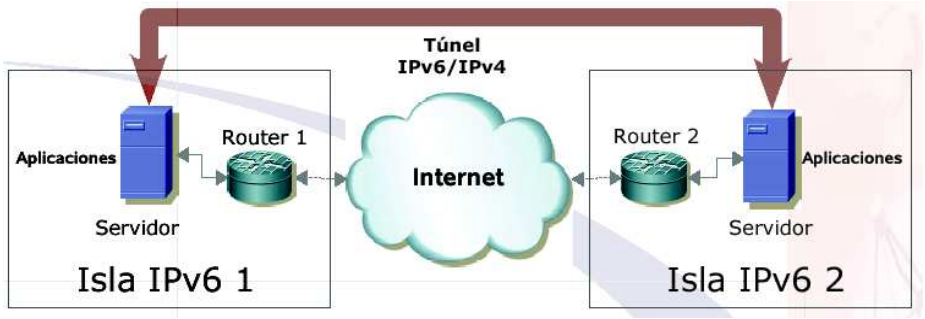


Ilustración 85. Tunel IPv6/IPv4[81].

Las transiciones en modo túnel se clasifican en:

a) Túneles automáticos: En este tipo de túnel la dirección IPv6 debe ser una dirección IPv4 compatible, donde los 32 bits de más bajo nivel son la dirección IPv4, 0::/96 + dirección IPv4. Cuando el túnel esta hecho por un *host* IPv6/IPv4 que tiene un paquete que enviar a través de una red tipo IPv4, este sigue las siguientes reglas:
o Si el destino del paquete es una dirección IPv4 o una dirección IPv4 mapeada2, se envía el paquete usando IPv4 ya que el receptor no es compatible con IPv6. Si el destinatario está en la misma subred se envía el paquete se usa IPv6 por que el receptor si es compatible con IPv6.
o Si el destino no esta en la misma subred pero hay al menos un *router* por defecto que es compatible con IPv6, o hay una ruta configurada a un *router* de este tipo, el paquete es enviado a este *router* usando IPv6. Si el destinatario es un nodo con una sola dirección IPv6 que esta conectado en un área IPv4 en la cual no hay una ruta IPv6, el destino es

[81] Derlis Zarate, Centro Nacional de Computación Universidad Nacional de Asunción "Implementación del servicio de sincronización horaria coordinada sobre Ipv6" http://www.cnc.una.py/cms/cnc/content/presentacion-ipv6.pdf

inalcanzable.

b) Túneles manuales: Un túnel manual puede ser de un *router* a otro *router* o de un *host* a un *router*. En el túnel manual el punto final del túnel no es el punto final del paquete, a diferencia del anterior túnel que si lo es, además que en el túnel manual se indica el camino por donde va a ir el paquete. Este tipo de túnel es usado normalmente entre sitios que intercambian información regularmente. El *host* emisor y el *router* retransmisor ambos se configuran de tal forma que la ruta además de contar con el siguiente salto, tiene una dirección de "fin de túnel"(que es siempre IPv4 compatible). El proceso de encapsulación es de la misma forma que el túnel automático, excepto que la dirección de destino IPv4 no es derivada de los 32 bits de más bajo nivel de la dirección de destino IPv6 sino de los 32 bits de bajo nivel de la dirección del final del túnel. En este caso, las direcciones de destino y origen no necesitan ser IPv4 compatible.

c) 6to4: Se trata de encapsular paquetes IPv6 dentro de paquetes IPv4, el punto donde ocurre esto es una interfaz IPv6, este punto es referido como una pseudo-interfaz. Los *routers* que soportan una pseudo-interfaz 6to4, son normalmente los *routers* fronteras, entre un dominio IPv6 y una red IPv4.

d) 6over4: La motivación de este método es permitir a *host* IPv6 aislados establecer un enlace físico, el cual no esta directamente conectado a un *router* IPv6, volviéndose así un *host* IPv6 funcional. Este mecanismo usa un dominio IPv4 que soporta *multicast* de IPv4, como un enlace local y virtual creando así una "*Ethernet* virtual". El mecanismo define un *set* de direcciones IPv4 que son usadas en el descubrimiento de vecindario (*Neighbour/router discovery*). Un dominio IPv4 está totalmente interconectado por subredes IPv4, dentro del mismo alcance local *multicast*, hay al menos 2 nodos IPv6 que lo conforman. Los *host* que usan este método no requieren direcciones IPv4 compatibles ni configuración de túneles. De esta manera IPv6 gana considerablemente independencia de los enlaces subyacentes y puede avanzar saltando subredes IPv4.

e) Tunel Broker: El túnel *Broker* es un mecanismo de túnel semi-automático. El túnel *Broker* puede ser visto como un proveedor de servicio, que ofrece conectividad a través de un túnel IPv6 sobre IPv4. Al cliente se le asigna una dirección fuera del rango de direcciones del proveedor, la cual puede ser una simple dirección o un prefijo de la red, el túnel creado se encuentra entre el cliente y servidor, mediante el túnel el cliente puede conectarse a Internet IPv6. El túnel *Broker* es conveniente para pequeños sitios IPv6 o *host* IPv6/IPv4 aislados en una red IPv4 la cual desea conectarse a la red IPv6. Los prerrequisitos para el uso del túnel es que cada cliente tenga al menos una dirección global y enrutable IPv4. EL procedimiento del túnel es el siguiente:
1. El host IPv6/IPv4 (Dual stack) se conecta al Tunnel Broker web server para pedir el túnel.
2. El Tunnel Broker web server envía el script al host IPv6/IPv4, el cual es usado para crear el túnel entre el host IPv6/IPv4 y el tunnel Broker tunnel Server.
3. El host IPv6/IPv4 corre el script, y el túnel es establecido.
4. El host IPv6/IPv4 obtiene conectividad IPv6 a través del tunnel Broker tunnel server.

f) ISATAP (*Intra- Site Automatic Tunnel Addressing Protocol*): Proporciona conectividad IPv6 *unicast* entre *hosts* IPv6 a través de una Intranet IPv4. Es una alternativa a usar dentro de un sitio. ISATAP conecta automáticamente *host* IPv6 o *routers*, los cuales son llamados nodos ISATAP, dentro de un sitio IPv4 por medio de un túnel automático el cual usa los sitios de infraestructura IPv4 como una NBMA (*Nonbroadcast multi-access*) de la capa de enlace. La dirección ISATAP soporta configuración manual y autoconfiguración. La dirección IPv4 no necesita ser globalmente única. Puede combinarse con el uso de cualquier prefijo IPv6, incluso 6to4.

g) Teredo: Teredo es una tecnología de transición que provee asignación de dirección y túneles automáticos *host* a *host* para tráfico *unicast,* cuando un *host* IPv6/IPv4 está localizado detrás de uno o varios NATs (*Network Address Translators*). 6to4 es igual, presta conectividad a direcciones *unicast* a través de un Internet IPv4 pero 6to4 necesita un *router* frontera, este *router* posee un dirección IPv4 pública. En algunas oficinas usan una configuración NAT IPv4 para conectarse a Internet, en la mayoría de las configuraciones de NAT, el dispositivo que provee la funcionalidad de NAT no es capaz de interactuar con un *router* 6to4. El "tunneling" en los *host* presenta un problema para NAT, cuando un paquete IPv6 es encapsulado con IPv4 tiene en el campo de protocolo (*Protocol*) en la cabecera IPv4 el número 41 (cabecera IPv6), en la mayoría de los NATs solo traslada tráfico TCP (*Transmission Control Protocol*) o UDP (*User Datagram Protocol*) y debe configurarse manualmente para trasladar otros tipo de protocolos, o tener editores de NAT instalados que realicen la traducción. Teredo resuelve el problema, este mecanismo encapsula el paquete IPv6 en mensajes UDP (*User Datagram Protocol*) que contiene tanto la cabecera de UDP como la de IPv4.

h) DSTM (*Dual -Stack Transition Mechanism*): Este túnel es diferente a los anteriores los cuales están basados en IPv6 sobre IPv4, DSTM esta basado en IPv4 sobre IPv6, levando trafico IPv4 sobre redes IPv6, y también provee un método para asignar una dirección IPv4 a nodos IPv6/IPv4. DSTM esta conformado por tres componentes:

- Servidor DSTM, el cual mantiene temporalmente las direcciones IPv4.

• Gateway DSTM, el cual es responsable de encapsular y de desencapsular paquetes IPv4 sobre paquetes IPv6. Un host IPv6/IPv4, el cual es llamado nodo DSTM y quiere comunicarse usando IPv4.

Tabla 55. Tipos de transición en modo túnel.

2.9.2 Transición modo traducción.

Requieren traducción de cabeceras los nodos sólo IPv6 para inter-operar con nodos sólo IPv4. Lo llevan a cabo los routers IPv6/IPv4 situados en las fronteras entre áreas IPv4 e IPv6. El tráfico que cruza la frontera se clasifica en:

1.- Tráfico de un área IPv4 que entra en un área IPv6 o el tráfico de un área IPv6 que entra en un área IPv4.

2.- Cada uno de estos tipos se puede describir como:

- Terminal.- dirigido a un nodo dentro del área.
- Tránsito.- dirigido a un nodo fuera del área.

Los routers traductores tienen que seleccionar de forma adecuada la dirección IP, además de mapear correctamente las direcciones a traducir:

- Las direcciones IPv4 se obtienen tomando los 32 bits de orden inferior de la dirección IP. Si la dirección de fuente o el destino son sólo IPv6, la cabecera es intraducible.
- Las direcciones de origen IPv6 debe ser una dirección IPv4 compatible, donde los 32 bits de más bajo nivel son la dirección IPv4, 0::/96 + dirección IPv4.
- Las direcciones de destino IPv6 debe ser una dirección IPv4 mapeada, donde los 32 bits de más bajo nivel son la dirección IPv4, ::ffff/96 + dirección IPv4.
- Es una dirección IPv6 compatible con IPv4 para el tráfico terminal, una dirección IPv6 mapeada a IPv4 para el tráfico de tránsito. En consecuencia, los traductores de cabeceras deben conocer los límites de su área.

Hay un caso especial: el tráfico IPv6 "tunelizado", si los traductores de cabeceras lo tratasen como tráfico IPv4 normal, el resultado sería un paquete IPv6 encapsulado en otro paquete IPv6. Por ello, los traductores han de examinar el número de protocolo de los datagramas IPv6, y si es

41(IPv6), desencapsularían el paquete en vez de traducir la cabecera IPv4.

Los mecanismos de traducción se clasifica en:

a) SIIT (Stateless IP/ICMP Translator): Algoritmo de traducción de cabeceras entre IPv4 e IPv6, incluye traducción de ICMP, es la base de diversos métodos de transición (Ej. AT-PT). La traducción es limitada a la cabecera IP, y no describe un método para asignar temporalmente una dirección IPv4 a un nodo IPv6, no mantiene estado (*Stateless*). SIIT no especifica como se realiza la conversión entre direcciones IPv4 e IPv6. Limitaciones:

- La traducción de IPv4 a IPv6 puede producir fragmentaciones.
- Traducción de cabeceras de extensión IPv6.
- No especifica cómo se traducen direcciones.
- A veces es necesario traducir cabeceras de aplicación.
- Aplicaciones que transportan direcciones IP como: DNS, FTP, etc.

La traducción es limitada a la cabecera IP, y no describe un método para asignar temporalmente una dirección IPv4 a un nodo IPv6, no mantiene estado (*Stateless*). El traductor esta operando en un modo sin estado (*Stateless*), lo cual significa que la traducción necesita ser hecha para cada paquete. Este mecanismo usa las direcciones IPv4 mapeadas a IPv6 ::FFFF:a.b.c.d donde a.b.c.d es una dirección IPv4, para describir el destino que no es compatible con IPv6.

b) NAT-PT (Network Address Translation- Protocol Translation): Método de Transición que combina, SIIT para la traducción de cabeceras y NAT para la traducción de direcciones IPv6 e IPv4. NAT en IPv6 es muy similar al NAT de IPv4, pero no es idéntico, en IPv4 se cambia de una dirección IPv4 a otra dirección IPv4, en IPv6 se refiere a cambiar de un dirección IPv6 a una dirección IPv4 y viceversa.

Hay dos variantes de NAT-PT:

- NAT-PT Básico.
- NAT-PT.

El NAT-PT Básico.- para paquetes de salida de un dominio versión 6, la dirección de rigen IP y los campos de suma de comprobación (*Cheksum*) en los protocolos TCP, UDP e ICMP son cambiados. Para paquetes de entrada la dirección de destino IP y la suma de comprobación (*Cheksum*) son cambiadas.

NAPT-PT.- extiende la noción un paso más allá, por que también traslada el identificador de transporte (por ejemplo en TCP y UDP el número de los puertos). Esto permite que varios identificadores de transportes de distintos *hosts* versión 6 seas multiplexados dentro de un solo identificador de transporte de dirección IPv4.

c) SOCKS Gateway*:* Socks *Gateway* esta basado en un mecanismo de *gateway* IPv6/IPv4 que permite una comunicación heterogénea entre nodos IPv6 y nodos IPv4, esta basado en el protocolo Socks. Esta basado en un mecanismo que pone fin a dos conexiones terminadas IPv4 e IPv6 en la capa de aplicaciones. En todas las aplicaciones de comunicación es un requisito obtener información de la dirección de destino para empezar la comunicación. Sin embargo es teóricamente imposible en las comunicaciones heterogéneas obtengan la información correcta, por que una aplicación IPv4 no puede tratarse con una dirección IPv6. Este prepara un espacio de dirección de 4 bytes para almacenar la información de la dirección y no puede guardar una dirección IPv6 en ese espacio, este es un problema crítico causado por las diferencias en la longitud de dirección.

d) BIS *(*Bump in the Stack*):* Este mecanismo inserta módulos que curiosean los datos que fluyen entre un modulo TCP/IPv4 y el modulo del controlador de la tarjeta de red y cambia de IPv4 a IPv6 y viceversa dentro del *host* y ellos mismo hacen la traducción. Cuando ellos se comunican con otro *host* IPv6, las direcciones IPv4 son asignadas a los *host* IPv6 internamente, pero la dirección IPv4 nunca fluye fuera de ellos. Desde que la asignación se lleva automáticamente usando el protocolo DNS (*Domain Name Service*), los usuarios no necesitan saber si la tarjeta de red es una tarjeta IPv6. Eso les permite a los *host* comunicarse con *host* IPv6 usando las aplicaciones existentes en IPv4, así parece como si ellos fueran un *host* IPv6/IPv4 (*Dual Stack IP*) con aplicaciones para IPv4 e IPv6. También pueden coexistir con otros transductores por que sus papeles son distintos.

e) BIA (Bump in the Application)

BIA es una técnica similar a BIS. Inserta un traductor de aplicaciones entre el *socket* de aplicaciones y el modulo TCP/IP del *host dual stack*. Cuando la aplicación IPv4 quiere comunicarse con un *host* IPv6, BIA detecta la función del socket de la aplicación IPv4 e invoca la función del socket de aplicación IPv6 para comunicarse con el *host* IPv6 y viceversa. Para apoyar la comunicación entre la aplicación IPv4 y la tarjeta del *host* IPv6 la dirección IPv4 será asignada a través de resolvedor de nombres de extensión en BIA.

f) TRT (Transport Relay Translator): Conceptualmente este mecanismo es exactamente igual que NAT-PT excepto que la traducción esta hecha en la capa de transporte en lugar de la capa de red. Si un cliente IPv6 y un servidor IPv4, se comunican utilizando TCP, TRT se ubica entre el cliente IPv6 y el servidor IPv4, terminando la sesión de TCP de IPv6 del cliente IPv6. Al mismo tiempo, origina una sesión TCP de IPv4 con el servidor IPv4 y copia los datos recibidos de cada una de la sesiones del otro. Si el cliente IPv6 y el servidor IPv4 se comunican usando UDP, TRT se ubica entre el cliente IPv6 y el servidor IPv4, recibiendo los datagramas UDP del cliente IPV6 y trasladándolos a ellos a datagramas UDP IPv4, y enviándolos al servidor IPv4.

g) ALG (Application Layer Gateway): Es un mecanismo que permite a los usuarios detrás de un *firewall* o detrás de un *gateway* NAT usar aplicaciones que no pueden atravesar si no es a través del *firewall* o del *gateway* NAT, un ejemplo común para un ALG es Proxy HTTP como "*squid*" o "*wwwoffle*". En redes IPv6 solamente, la funcionalidad de ALG puede usarse para habilitar a los *host* en subredes solamente IPv6, para establecer las conexiones a los servicios en un mundo IPv4 solamente.

Tabla 56. Tipos de mecanismos de traducción.

2.9.3 Transición modo doble pila(Dual Stack IP)

La pila dual IP dual es una implementación de la pila de protocolos TCP/IP que incluyen ambas, una capa de Internet IPv4 y una capa de Internet IPv6. Este es un mecanismo utilizado por nodos IPv6/IPv4 para que nodos IPv4 se puedan comunicar con nodos IPv6. Una pila dual IP contiene una simple implementación de protocolos de capa host-a-host tales como TCP y UDP. Todos los protocolos de capas superiores en una implementación de pila dual IP pueden comunicarse sobre IPv4, IPv6 o IPv6 en túnel en IPv4.

Ilustración 86. Arquitectura de pila dual IP[82].

El modelo Dual Stack soporta IPv6 e IPv4 en un mismo nodo (*host* o *router*) lo que significa que en este nodo se implementan ambos protocolos, son también llamados nodos IPv6/IPv4. Este nodo puede enviar y recibir paquetes IPv6 ó IPv4 dependiendo del tipo de sistema con el cual establece la comunicación. Este nodo posee una dirección de 128 bits y una dirección de 32 bits, estas direcciones no necesariamente están relacionadas.

La siguiente ilustración muestra un nodo IPv6/IPv4 que está estableciendo comunicación con un sistema IPv6 e IPv4 en un mismo enlace.

[82] Evelio Martínez Martínez, "El protocolo del Internet de la nueva generación" publicado en la Revista RED, http://www.eveliux.com/index.php?option=content&task=view&id=18

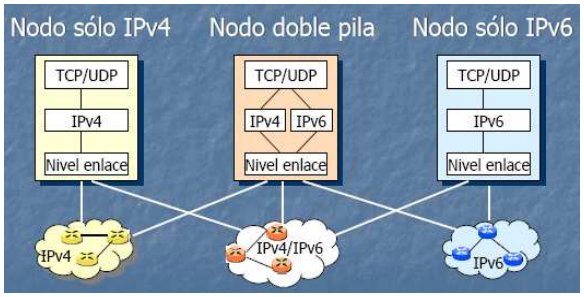


Ilustración 87. Nodos Ipv4/Ipv6

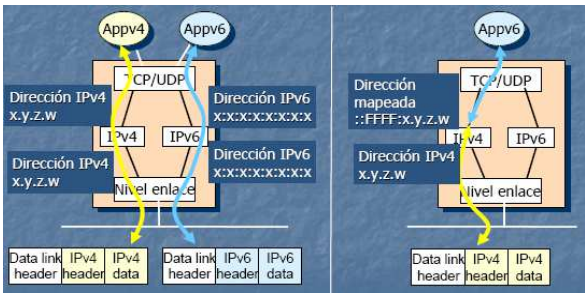


Ilustración 88. Aplicaciones terminales[83]

Un nodo IPv6/IPv4 puede usar autoconfiguración sin estado (Stateless) o con estado (Statefull) para obtener su dirección IPv6. También puede usar cualquier método para obtener su dirección IPv4, este método puede ser DHCP (Dynamic Host Configuration Protocol), BOOTP (Bootstrap Protocol) o configurarlo manualmente. Cuando un nodo IPv6/IPv4 desea comunicarse con otro sistema, este necesita conocer la compatibilidad de ese sistema y que tipo de paquete este debe enviar. El DNS (Domain Name System) juega un papel importante, para averiguar esta información.

- Los nodos solamente IPv4 tienen un registro tipo A que contiene una dirección IPv4.
- Los nodos IPv6/IPv4 que pueden interoperar con nodos solamente IPv4 es decir poseen un registro AAAA que contiene una dirección IPv4 compatible con IPv6 y un registro tipo A que contiene su dirección IPv4.
- Los nodos solamente IPv6 que no puedan interoperar con nodos solamente IPv4 por que tienen un registro tipo AAAA que contiene su dirección IPv6.
- Los nodos IPv6/IPv4 toman la decisión acerca de que protocolo base usar, según la información que devuelva el DNS, la incorporación del registro AAAA en el DNS es un prerrequisito para la interoperabilidad entre sistemas IPv6 e IPv4.

[83] Eva M.Castro eva@gsyc.escet.urjc.es "Portando aplicaciones a Ipv6", Grupo de Sistemas y Comunicaciones(GSyC), Departamento de Informática, Estadística y Telemática (DIET); Universidad Rey Juan Carlos(URJC), http://gsyc.es/~eva/publicaciones.html

2.10 En que consiste el protocolo IPsec.

Anterior a la ubicuidad de Internet, especialmente de la Web(Internet), las compañías que querían que las redes LAN trascendieran más allá del ámbito de la oficina e incluyeran a los trabajadores y centros de información de otros edificios, ciudades, estados o incluso otros países, tenían que invertir en hardware y servicios de telecomunicaciones costosos para crear redes amplias de servicio, WAN. Sin embargo, con Internet, las compañías tienen la posibilidad de crear una red privada virtual que demanda una inversión relativamente pequeña de hardware y utiliza el Internet global para la conexión entre los puntos de la red. Las LAN tradicionales son redes esencialmente restringidas, por lo cual se puede intercambiar información entre las computadoras usualmente sin pensar en la seguridad de la información o preocuparse mucho por ella.

Sin embargo, con las VPNs la situación es preocupante porque el Internet público es intrínsecamente abierto e inseguro. Por lo tanto, las VPN se implementan usando protocolos especiales como el protocolo de tunelización punto a punto, PPTP o IPSec, que le permitan al remitente encriptar los paquetes de información y permitir UNICAMENTE al receptor autorizado desencriptar la información que esté "sellada" con un identificador único que además comprueba que la transmisión se hace desde una fuente confiable. Cuando un empleado se conecta a Internet, la configuración de las VPN les permite hacer un túnel hacia la red privada de la compañía y navegar en la red como si estuvieran en la oficina. De este modo se protege y se da integridad a la información enviada a través de ese túnel que se realiza en Internet. IPSec es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP, entre otros).

Por fin existe un estándar que aborda las carencias en cuanto a seguridad del protocolo IP. Dichas carencias son muy graves y, tal como se ha constatado en los últimos años, afectan a la infraestructura misma de las redes IP. Todas las soluciones anteriores se basaban en soluciones propietarias que

dificultaban la comunicación entre los distintos entornos empresariales, al ser necesario que éstos dispusiesen de una misma plataforma. La falta de interoperabilidad ha sido el principal freno para el establecimiento de comunicaciones seguras, dado que no se ve factible la migración a una determinada plataforma en función de una colaboración empresarial puntual.

Entre las ventajas de IPSec destacan que está apoyado en estándares del IETF (Grupo de Trabajo en Ingeniería de Internet) y que proporciona un nivel de seguridad común y homogénea para todas las aplicaciones, además de ser independiente de la tecnología física empleada. IPSec se integra en la versión actual de IP (IP versión 4) y, lo que es todavía más importante, se incluye por defecto en IPV6. Puesto que la seguridad es un requisito indispensable para el desarrollo de las redes IP, IPSec está recibiendo un apoyo considerable: todos los equipos de comunicaciones lo incorporan, así como las últimas versiones de los sistemas operativos más comunes. Al mismo tiempo, ya existen muchas experiencias que demuestran la interoperabilidad entre fabricantes, lo cual constituye una garantía para los usuarios. Otra característica destacable de IPSec es su carácter de estándar abierto. Se complementa perfectamente con la tecnología PKI (*Public Key Infrastructure*), aunque establece ciertos algoritmos comunes, por razones de interoperabilidad, permite integrar algoritmos criptográficos más robustos que pueden ser diseñados en un futuro.

Entre los beneficios que aporta IPSec, cabe señalar que:

a) Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.
b) Facilita el comercio electrónico de negocio a negocio, al proporcionar una infraestructura segura sobre la que realizar transacciones usando cualquier aplicación. Las extranets son un ejemplo.
c) Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el costo de líneas dedicadas.
d) Ofrece al "Teletrabajador" el mismo nivel de confidencialidad que dispondría en la red local de su empresa, no siendo necesaria la limitación de acceso a la información sensible por problemas de privacidad en tránsito. Cuando se cita la palabra "seguro" no se refiere únicamente a la confidencialidad de la comunicación, también se refiere a la integridad de los datos, que para muchas compañías y entornos de negocio puede ser un requisito mucho más crítico que la confidencialidad. Esta integridad es proporcionada por IPSec como servicio añadido al cifrado de datos o como servicio independiente. Al momento de incorporar nuevas tecnologías existen factores importantes a considerar como beneficios, aplicaciones, servicios, etc. En el caso de IPSec las características a considerar serian:

1) Aplicaciones de IPSEC: Redes Privadas Virtuales sobre Internet entre sucursal y oficina central, PC remoto accede en forma segura a la compañía a través de Internet y Conectividad extranet e intranet con partners.
2) Beneficios: Si se implementa IPSEC en un firewall o router provee seguridad fuerte a todo el tráfico que atraviesa el perímetro, IPSEC está debajo del protocolo TCP/UDP y por lo tanto es transparente para las aplicaciones (no se requiere modificarlas) y es transparente para los usuarios finales.
3) Servicios IPSEC: AH: Authentication Header. Formato del paquete de autentificación., ESP: Encapsulating Security Payload. Formato del paquete ESP para encriptación y autentificación opcional. En la ilustración que se muestra a continuación se bosqueja a groso modo en ejemplo de aplicación importante:

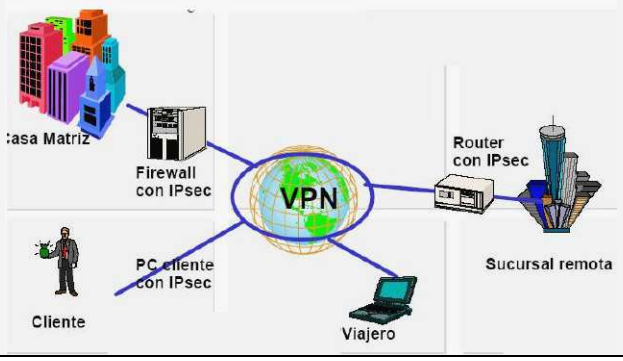


Ilustración 89. Beneficios del protocolo Ipsec.

2.10.1 Introducción

Las innovaciones que trae consigo Ipsec son, sin duda, extremadamente valiosas para el ciudadano común, y mas aun para quien las observa desde una posición superior.

IPSec (Internet Protocol Security) es un conjunto de extensiones de la familia del protocolo IP. Es un estándar de la IETF (Internet Engineering Task Force) definido en el RFC 2401. Provee servicios criptográficos de seguridad como autenticación[84], integridad[85], control de acceso y confidencialidad[86]. IPSec es, en realidad, un conjunto de

[84] Autenticación: Es la propiedad que hace referencia a la identificación. Se trata del nexo de unión entre la información y el emisor de esta información según Miquel Peguera Poch, Albert Agustinoy Guilayn, Ramon Casas Valles, Agusti Cerrillo i Martinez, Ana M. Delgado Garcia, Jordi Herrera Joancomarti, Mark Jeffery, Oscar Morales Garcia, Rafael Oliver Cuello, Guillermo Ormanzabal Sanchez, Monica Vilasau Solana y Raquel Xalabarder Plantada "Derecho y nuevas tecnologías", Editorial UOC 2005, pag. 33. Es necesario que la "Identidad" del acceso no pueda ser suplantada.

[85] Integridad: Es la propiedad que asegura la no alteración de la información. Esta alteración puede ser por ejemplo, insertar, borrar o sustituir información según Miquel Peguera Poch, Albert Agustinoy Guilayn, Ramon Casas Valles, Agusti Cerrillo i Martinez, Ana M. Delgado Garcia, Jordi Herrera Joancomarti, Mark Jeffery, Oscar Morales Garcia, Rafael Oliver Cuello, Guillermo Ormanzabal Sanchez, Monica Vilasau Solana y Raquel Xalabarder Plantada "Derecho y nuevas tecnologías", Editorial UOC 2005, pag. 33.

[86] Confidencialidad: Es la propiedad que asegura que solo aquellos que están autorizados tendrán acceso a la información. A menudo esta propiedad se conoce también con el nombre de privacidad según Miquel Peguera Poch, Albert Agustinoy Guilayn, Ramon Casas Valles, Agusti Cerrillo i Martinez, Ana M. Delgado Garcia, Jordi Herrera Joancomarti, Mark Jeffery, Oscar Morales Garcia, Rafael Oliver Cuello, Guillermo Ormanzabal Sanchez, Monica Vilasau Solana y Raquel Xalabarder Plantada "Derecho y nuevas tecnologías", Editorial UOC 2005, pag. 33.

estándares para integrar en IP funciones de seguridad basadas en criptografía[87]. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de *hash* (MD5, SHA-1) y certificados digitales X509v3. En la ilustración se observa como IPSec es el resultado de la complementariedad de varias de estas técnicas.

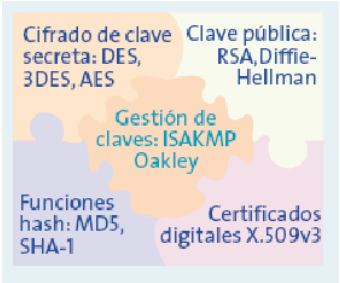


Ilustración 90. Tecnologías utilizadas en IPSec.

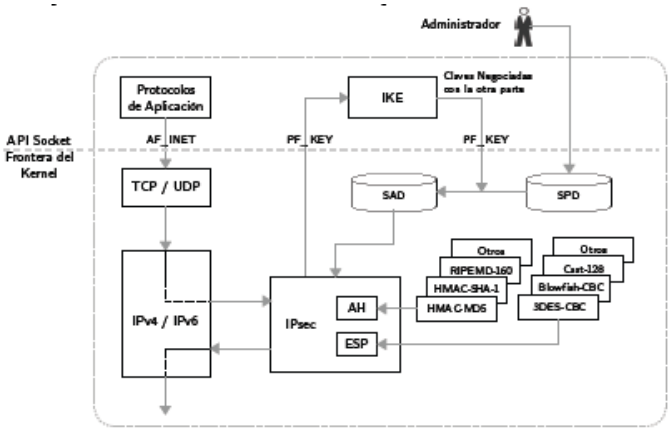


Ilustración 91. Esquema básico de componentes de Ipsec.

[87] Antiguamente la criptografía se definía como el arte de la escritura secreta, tal y como su etimología indica (Del griego krypto, "secreto", y grapho, "escritura"). En la actualidad una de las definiciones mas esmeradas de este termino es la siguiente: la criptografía es la ciencia que estudia las técnicas matemáticas relacionadas con los diferentes aspectos de la seguridad de la información. La cristología es la ciencia que engloba la criptografía y el criptoanálisis. El criptoanálisis es el estudio de las técnicas que permiten romper los criptosistemas por la criptografía. Ahora dado que uno de los posibles ataques pueden darse en un criptosistema es el de intentar probar todas las claves(ataques de fuerza bruta), por ejemplo se hace normalmente referencia a la longitud de la clave en bits; es así que una clave de 40 bits de longitud indica que son necesarias 2^{40} = 1.099.511.627.776 pruebas para encontrarla por fuerza bruta.

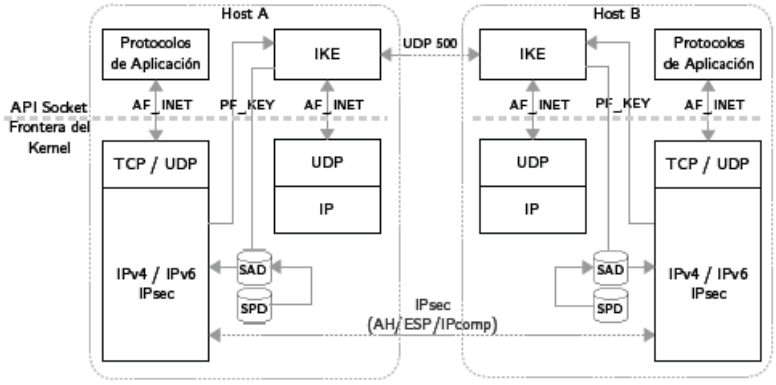


Ilustración 92. Esquema básico de interacción[88].

El protocolo IPSec ha sido diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Han sido definidos, sin embargo, ciertos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet.

Dichos Algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHA-1, como funciones de *hash.* Además es perfectamente posible usar otros algoritmos que se consideren más seguros o más adecuados para un entorno específico: por ejemplo, Como algoritmo de cifrado de clave simétrica IDEA, Blowfish o el más reciente AES que se espera sea el más utilizado en un futuro próximo.

Dentro de IPSec se distinguen los siguientes componentes:

- Dos protocolos de seguridad: IP Authentication Header **(AH)** e IP Encapsulating Security Payload **(ESP)** que proporcionan mecanismos de seguridad para proteger tráfico IP.
- Un protocolo de gestión de claves Internet Key Exchange **(IKE)** que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

[88] Rolando Chaparro Fox, "Alternativa de infraestructura de Seguridad Basada en Ipsec y DNSec", Universidad Nacional de Asunción, Facultad de Ingeniería, Centro Nacional de Computación, http://lacnic.net/documentos/lacnicviii/flip-6-rolando-chaparro-fox.pdf

A continuación presentamos sus principales características:

-Confidencialidad: Es necesario asegurarse de que los datos enviados sean difíciles de comprender para todos excepto para el receptor. Por ejemplo, hay que estar seguro de que las contraseñas que se usan al ingresar en una máquina remota a través de Internet se mantienen en secreto.

-Integridad: Hay que garantizar que los datos no puedan ser cambiados durante el trayecto. Si alguien se encuentra en una línea que lleve datos sobre facturación, querrá estar seguro de que las cantidades y cifras de contabilidad son las correctas, y que no han podido ser alteradas durante el tránsito.

-Autenticidad: Los datos deben firmarse para que otros puedan verificar quién es realmente quien los ha enviado. Es importante saber que los documentos no son falsos.

-Protección a la réplica: Necesitamos modos para asegurarnos que unos datos enviados se procesan una sola vez, al margen del número de veces que se reciban. O sea, que un atacante no pueda registrar una transacción (como por ejemplo una transacción bancaria) y más tarde replicarla al pie de la letra de modo que la otra parte de la conexión piense que se ha recibido un nuevo mensaje (una nueva transacción).

IPsec provee servicios similares a SSL (Secure Sockets Layer), pero al nivel de redes, de un modo que es completamente transparente al nivel de sus aplicaciones porque sus aplicaciones no necesitan tener ningún conocimiento de IPsec para poder usarlo. IPSec provee un mecanismo estándar, robusto y con posibilidades de expansión, para proveer seguridad al protocolo IP y protocolos de capas superiores. Se puede usar cualquier protocolo IP sobre IPsec. Se pueden crear túneles cifrados (VPN), o simple cifrado entre computadoras. Debido a que dispone de tantas opciones, IPsec es más bien complejo (¡mucho más que SSL!).

2.10.2 Arquitectura de IPsec

La arquitectura de IPSec define la granularidad con la que el usuario puede especificar su política de seguridad. Permite que cierto tráfico sea identificado para recibir el nivel de protección deseado.

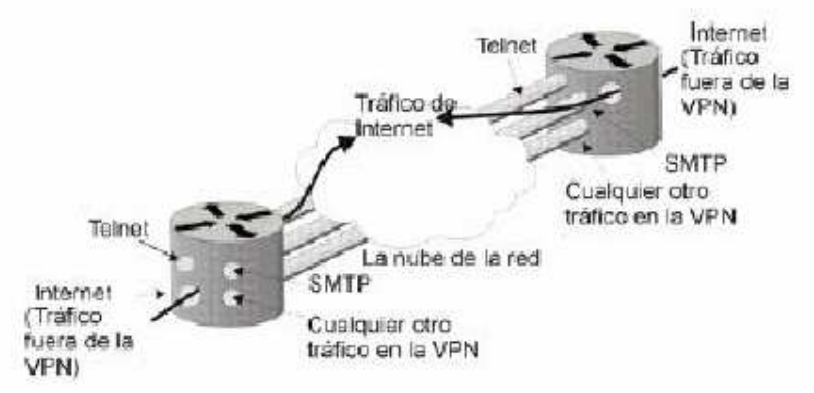


Ilustración 93. Túneles de comunicación Protegidos por IPSec entre redes separadas.

IPSec está diseñado para proveer seguridad interoperable de alta calidad basada en criptografía[89], tanto para IPv4 como para IPv6 [RFC2401, 1998]. Está compuesto por dos protocolos de seguridad de tráfico, el Authentication Header (AH) y el Encapsulating curity Payload (ESP), además de protocolos y procedimientos para el manejo de llaves encriptadas. AH provee la prueba de los datos de origen en los paquetes recibidos, la integridad de los datos, y la protección contra-respuesta, dicho de otra manera, AH provee autenticación, integridad, y protección a la réplica (pero no confidencialidad).

La diferencia principal entre las funcionalidades de autenticación de AH y ESP es que AH siempre autentica partes de la cabecera IP del paquete (como las direcciones de origen/destino). ESP sólo autentica la carga útil (*Payload*) del paquete.

ESP puede proveer autenticación, integridad, protección a la réplica, y confidencialidad de los datos (asegura todo lo que sigue a la cabecera

[89] La criptografía, según el diccionario de la Real Academia de la Lengua Española, es el arte de escribir con clave secreta o de una forma enigmática. Pos su parte, el diccionario entiende por cifrar transcribir en guarismos, letras o símbolos, de acuerdo con un clave, un mensaje cuyo conocimiento se pretende oculta.

en el paquete). La protección a la réplica requiere autenticación e integridad (estas dos van siempre juntas). La confidencialidad (cifrado) se puede usar con o sin autenticación y/o integridad. Del mismo modo, se puede usar la autenticación y/o la integridad con o sin la confidencialidad. ESP provee lo mismo que AH adicionando confidencialidad de datos y de flujo de tráfico limitado. En la práctica, se recomienda que se use ESP para la mayoría de aplicaciones. Se aprecia la arquitectura de IPSec. Al utilizar el mecanismo de AH se aplican algoritmos de autenticación, con la aplicación del mecanismo ESP, además de autenticación, también algoritmos de encriptación. El esquema de interoperabilidad se maneja a través de Asociaciones de Seguridad (SA), almacenadas en una base de datos. Los parámetros que se negocian para establecer los canales seguros se denominan Dominio de Interpretación IPSec (Domain of Interpretation, DOI), bajo políticas pre-establecidas dentro de un esquema de funcionamiento estático con valores fijos y previamente establecidos, o bien, en un esquema de funcionamiento dinámico utilizando un protocolo de manejo de llaves, Intenet Key Exchange (IKE).

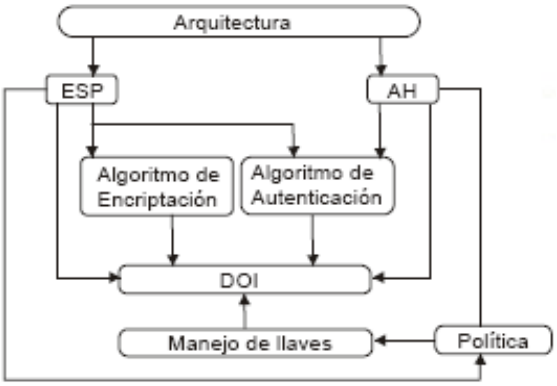


Ilustración 94. Arquitectura de Ipsec.

2.10.3 Asociaciones de seguridad

Una asociación de seguridad (SA) es la forma básica de IPSec, es el contrato entre dos entidades que desean comunicarse en forma segura. Las SA determinan los protocolos a utilizar, las

transformaciones, las llaves y la duración de validez de dichas llaves. Las SA son almacenadas en una base de datos (SADB), son de un solo sentido, es decir, cada entidad con IPSec tiene una SA para el tráfico que entra, y otra SA para el tráfico que sale. Además de ser unidireccionales, también son específicas al protocolo, hay SA separadas para AH y para ESP.

2.10.4 Modos de funcionamiento

El diseño de IPSec plantea dos modos de funcionamiento para sus protocolos:

a) Transporte.

b) Túnel.

La diferencia radica en la unidad que se esté protegiendo, en modo transporte se protege la carga útil IP (capa de transporte), en modo túnel se protege los paquetes IP (capa de red).

Se pueden implementar tres combinaciones:

- AH en modo transporte.
- ESP en modo transporte.
- ESP en modo túnel (AH en modo túnel tiene el mismo efecto que en modo transporte).

El modo transporte se aplica a nivel de Hosts. AH y ESP en este modo interceptarán los paquetes procedentes de la capa de transporte a la capa de red y aplicarán la seguridad que haya sido configurada. Se aprecia un esquema de IPSec en modo transporte, si la política de seguridad define que los paquetes deben ser encriptados, se utiliza ESP en modo transporte, en caso que solo haya sido requerida autenticación, se utiliza AH en modo transporte.

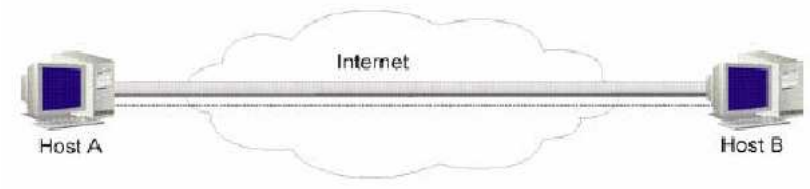


Ilustración 95. Hosts A y B implementando ESP en modo transporte.

Los paquetes de la capa de transporte como TCP y UDP pasan a la capa de red, que agrega el encabezado IP y pasa a las capas inferiores; cuando se habilita IPSec en modo transporte, los paquetes de la capa de transporte pasan al componente de IPSec (que es implementado como parte de la capa de red, en el caso de sistemas operativos), el componente de IPSec agrega los encabezados AH y/o ESP, y la capa de red agrega su encabezado IP. En el caso que se apliquen ambos protocolos, primero debe aplicarse la cabecera de ESP y después de AH, para que la integridad de datos se aplique a la carga útil de ESP que contiene la carga útil de la capa de transporte.

Encabezado IP	Encabezado AH	Encabezado ESP	Carga útil TCP

Ilustración 96. Formato del paquete con AH y ESP.

El modo túnel se utiliza cuando la seguridad es aplicada por un dispositivo diferente al generador de los paquetes, como el caso de las VPN, o bien, cuando el paquete necesita ser asegurado hacia un punto seguro como destino y es diferente al destino final, como se ilustra en la figura, el flujo de tráfico es entre A y B, e IPSec puede aplicarse con una asociación de seguridad entre RA y RB, o bien, una asociación de seguridad entre A y RB.

Ilustración 97. Aplicación de IPSec en modo túnel.

IPSec en modo túnel, tiene dos encabezados IP, interior y exterior. El encabezado interior es creado por el host y el encabezado exterior es agregado por el dispositivo que está proporcionando los servicios de seguridad. IPSec encapsula el paquete IP con los encabezados de IPSec y agrega un encabezado exterior de IP como se ilustra en la figura.

Encabezado IP	ESP	Encabezado IP	Carga útil de la red

Ilustración 98. Formato del paquete aplicando IPSec en modo túnel.

IPSec también soporta túneles anidados, aunque no son recomendados por lo complicado de su construcción, mantenimiento y consumo de recursos de red. La ilustración muestra dos túneles. A envía un paquete a B, la política indica que debe ser autenticado con el enrutador RB, además existe una VPN entre RA y RB, de tal forma que el paquete que ve RB es el que se muestra en la ilustración, el encabezado exterior es un paquete ESP tunelizado y contiene un paquete AH tunelizado, el paquete AH contiene el paquete IP para el host B generado por el host A.

Ilustración 99. Ejemplo de túneles anidados.

Encabezado IP	ESP	Encabezado IP	AH	Encabezado IP	Datos

Ilustración 100. Formato del paquete del túnel anidado.

2.10.5 Encapsulamiento de seguridad de la carga

La cabecera del protocolo (IPv4, IPv6, o de Extensión) inmediatamente antes de la cabecera de ESP contendrá el valor 50

en su Protocolo (IPv4) o en el campo Siguiente Cabecera (de IPv6, o de Extensión).

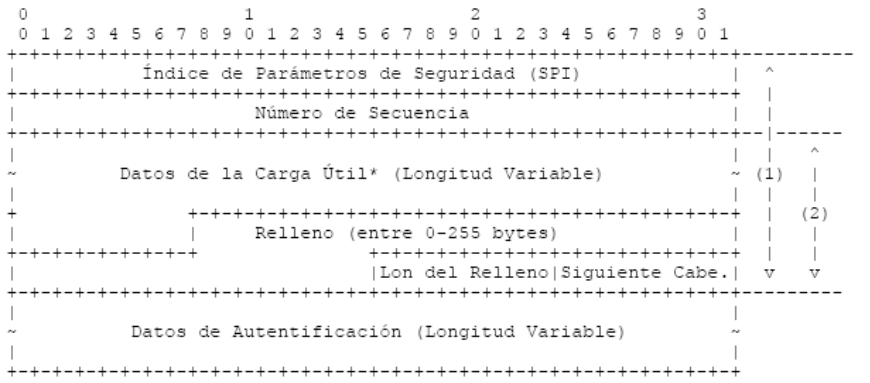


Ilustración 101. Formato del paquete de carga de seguridad encapsulada[90].

2.10.6 Gestión de claves

El uso de implementaciones IPsec en general requiere de un estándar para Internet, escalable, automatizado y con protocolos para la administración de SAs. Este soporte es requerido para facilitar el uso de las características anti-replay de AH y ESP y para una adecuada creación de SA bajo demanda, por ejemplo, para el uso de claves orientadas a usuarios o a sesiones. (Un "recambio de claves" en una SA actual implica la creación de una nueva SA con un nuevo SPI, un proceso que generalmente implica el uso automatizado de protocolos de gestión de claves/SA). El protocolo de gestión de claves automáticas por defecto que usa IPsec es IKE bajo el Domino de Interpretación (DOI) de IPsec, a través de ISAKMP. Se PUEDEN emplear otros protocolos para el manejo automatizado de SA. Cuando los protocolos de gestión de claves/SA se emplean, la salida de estos protocolos pueden ser

[90] (1) Alcance de la Autentificación
(2) Alcance de la Confidencialidad
* Si se incluye en el campo Carga útil los datos de sincronización criptográfica, (por ejemplo, un Vector de Inicialización (IV), ver Sección 2.3) usualmente estos no estarán encriptados, aunque a menudo se lo hace referencia como parte del texto cifrado.

empleados para crear múltiples claves, por ejemplo, para una SA ESP. Esto puede originarse debido a:

- Los algoritmos de encriptación usan múltiples claves (por ejemplo, Triple DES).
- Los algoritmos de autentificación usan múltiples claves.
- Se emplean tanto el algoritmo de encriptación como el algoritmo de autentificación.

El Sistema de Gestión de Claves puede proporcionar una cadena separada de bits para cada clave o puede generar una cadena de bits de la cual se extraigan todas las claves. Si una sola cadena de bits es proporcionada, hay que tener en cuenta que las partes del sistema que asignen la cadena de bit a las claves requeridas lo hagan en la misma forma en ambos extremos de la SA. Para garantizar que las implementaciones IPsec en cada extremo de la SA usan los mismos bits para las mismas claves, independientemente de que parte del sistema divide la cadena de bits entre las claves individuales, la clave o claves encriptadas DEBEN ser extraídas de los primeros bits (los de más a la izquierda, de orden superior) y la clave de autentificación DEBE ser tomada de los bits restantes. El número de bit para cada clave especifica los algoritmos requeridos para AH y ESP. En el caso de claves de encriptación múltiple o claves de autentificación múltiple, la especificación del algoritmo debe especificar el orden en el cual beben ser seleccionados de una cadena de bits provistos para el algoritmo.

2.10.7 Políticas de seguridad Ipsec

La política es uno de los componentes más importantes de la arquitectura de IPSec, determina los servicios de seguridad que serán aplicados a un paquete. Las políticas de seguridad son también almacenadas en una base de datos (Security Policy Database, SPD) indexada por seleccionadores.

La SPD es consultada tanto para el procesamiento de salida como el de entrada, se propone un administrador de la SPD para agregar, borrar y modificar. No hay un estándar que lo defina, pero se propone que los seleccionadores contengan los siguientes campos:

Dirección fuente: Puede ser indistinta, un rango de direcciones, un prefijo de red, o una dirección IP específica. Indistinta en el caso de que sea la misma política para todos los paquetes con un mismo host de origen, el rango de direcciones y prefijo de red, para los gateways de seguridad y para VPNs, la dirección específica para un host con varias direcciones, o en un gateway cuando los requerimientos de algún host sean específicos.

Dirección destino: Puede ser indistinta, un rango de direcciones, un prefijo de red,

o una dirección IP específica (homologada o no). Los tres primeros para gateways de seguridad, la dirección específica como índice para la SPD.

Nombre: Nombre de un usuario o sistema sobre el cual se aplique la política de forma específica.

Protocolo: El protocolo de transporte.

Puertos de capas superiores: Los puertos del fuente y destino sobre los que se aplica la política.

2.10.8 IP Encapsulating Security Payload (ESP).

ESP es un encabezado de protocolo insertado en el datagrama IP para proveer servicios de confidencialidad, autenticación del origen de los datos, *antireplay* e integridad de datos a IP. Es un estándar definido en el RFC 2406. El encabezado ESP se inserta después del encabezado IP y antes del encabezado del protocolo de capa superior (modo transporte) o antes del encabezado IP encapsulado (modo túnel) [RFC2406, 1998]. El encabezado de protocolo (IPv4, IPv6 o extens ión) que inmediatamente precede al encabezado ESP contendrá el valor 50 en su campo de protocolo (IPv4), o siguiente

cabecera (IPv6) [RFC1700, 1994]. El formato de los paquetes ESP para una SA dada es fijo durante la duración de la SA. El encabezado ESP tiene la forma definida en la ilustración, el SPI y número de secuencia ya fueron definidos, la carga útil de datos son los datos protegidos, el relleno (de hasta 255 bytes) se utiliza en ESP por varias circunstancias: algunos algoritmos criptográficos requieren que el elemento de entrada sea un múltiplo del tamaño de su bloque, si no se especifica confidencialidad en la SA, se utiliza el relleno para justificar los campos *Longitud de relleno* y *Siguiente cabecera* del encabezado ESP, para esconder el tamaño real de la carga útil; el contenido del relleno es dependiente del algoritmo de criptografía, el algoritmo puede definir un valor de relleno que debe ser verificado por el receptor para el proceso de desencriptado. El campo de longitud de relleno define cuánto relleno se agregó, el campo de siguiente cabecera indica el tipo de dato contenido en la carga útil de acuerdo al conjunto de Números de Protocolo IP definidos por IANA (Internet Assigned Numbers Authority) [RFC1700, 1994]. El campo de datos de autenticación contiene el valor de verificación de integridad calculado sobre el paquete ESP menos los datos de autenticación.

ESP aplicado en modo transporte solo se utiliza en implementaciones del tipo host y provee protección a los protocolos de capas superiores, pero no al encabezado IP.

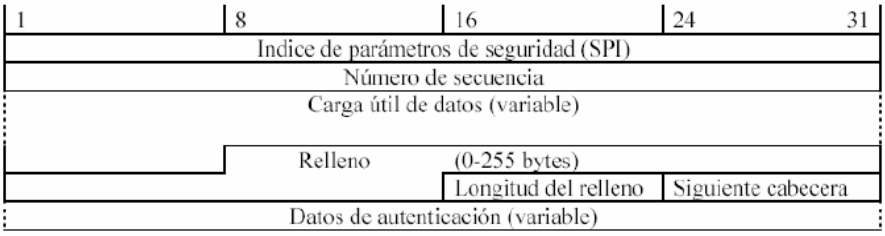


Ilustración 102. El encabezado ESP.

El encabezado ESP se inserta después del encabezado IP y antes del protocolo superior (TCP, UDP, ICMP, etc.) o antes de cualquier encabezado IP que haya sido previamente insertado. En la figura se

ilustra la transformación del paquete IP al aplicar ESP en modo transporte para IPv4; en la ilustración se muestra el caso para IPv6.

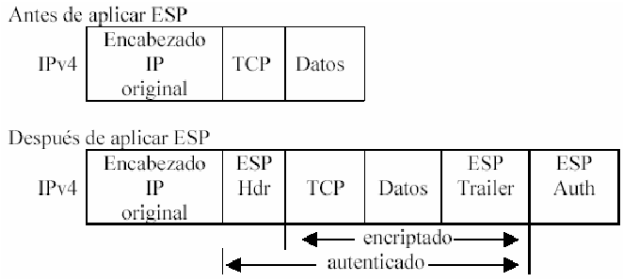


Ilustración 103. Transformación del paquete IPv4 al aplicar ESP en modo transporte.

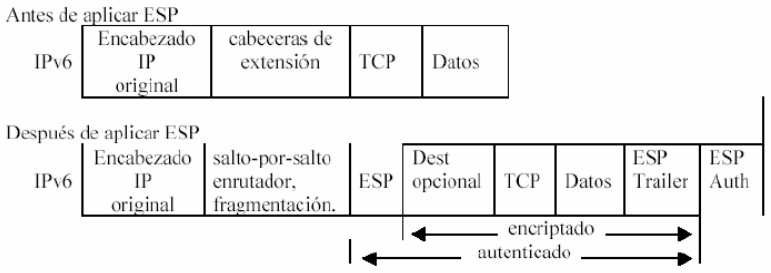


Ilustración 104. Transformación del paquete IPv6 al aplicar ESP en modo transporte.

En modo túnel, ESP puede ser empleado en hosts o en gateways. El encabezado IP interior contiene las direcciones del destino y origen del paquete, y el encabezado exterior puede contener direcciones diferentes, comúnmente direcciones de gateways de seguridad en el camino entre el origen y destino. La posición de los encabezados ESP en modo túnel con respecto a los encabezados IP exteriores es igual que en modo transporte. En la ilustración 15 se muestran los encabezados ESP para IPv4 e IPv6.

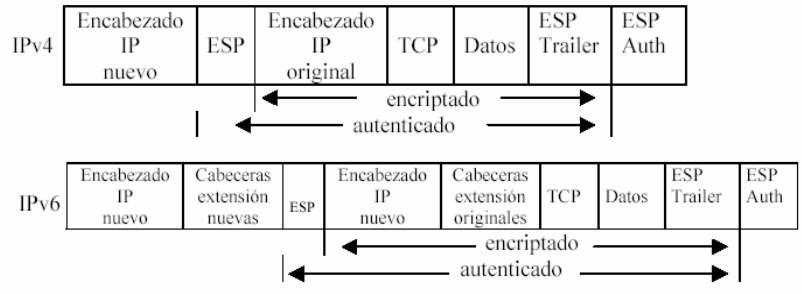


Ilustración 105. Transformación del paquete

IP al aplicar ESP en modo túnel.

En caso de no haberse indicado la confidencialidad en la SA, el algoritmo de criptografía es Nulo, en caso de aplicar confidencialidad a un paquete que se envía, el proceso aplicado en general es el siguiente:

- Encapsular en el campo de carga útil de ESP:
  - o Para modo transporte, solo la información original del protocolo de capa superior.
  - o Para modo túnel, el datagrama IP original completo.
- Agregar el relleno necesario.
- Encriptar el resultado (carga útil de datos, relleno, longitud del relleno y la siguiente cabecera) usando la llave, el algoritmo de criptografía, el modo indicado en la SA y si existe, datos de sincronización criptográfica.

En la parte del receptor se sigue en general el siguiente procedimiento para desencriptar los paquetes recibidos:

- Desencriptar la carga útil de ESP, relleno, longitud del relleno, y siguiente cabecera, utilizando la llave, el algoritmo de criptografía, el modo y en su caso, los datos de sincronización criptográfica, indicados en la SA.
- Procesar el relleno según haya sido especificado por el algoritmo utilizado.
- Reconstruir el datagrama IP original:
  i. Para modo transporte, el encabezado IP original más la información del protocolo de capa superior original en el campo de carga útil de ESP.
  ii. Para modo túnel, el encabezado IP entunelado, más el datagrama IP completo en el campo de carga útil de ESP.

Es importante mencionar que el encriptamiento no debe ser sustituto por la autenticación, la autenticación es el servicio básico de una comunicación segura, reforzada con el encriptamiento de datos.

2.10.9 Authentication Header (AH).

AH es el protocolo IPSec utilizado para proveer servicios de integridad de datos, autenticación del origen de los datos, y *antireplay* para IP. Es un estándar definido en el RFC 2402 [RFC2402, 1998]. La principal diferencia entre la autenticación provista entre ESP y AH tiene que ver con la cobertura, ESP no protege los campos del encabezado IP, a menos que sean encapsulados por ESP (modo túnel). El encabezado de protocolo (IPv4, IPv6 o extensión) que inmediatamente precede al encabezado AH contendrá el valor 51 en su campo de protocolo (IPv4), o siguiente cabecera (IPv6) [RFC1700, 1994]. La ilustración muestra el encabezado AH, todos los campos son obligatorios, tienen funciones similares a las explicadas en ESP, el campo reservado no se utiliza y su valor debe ser cero.

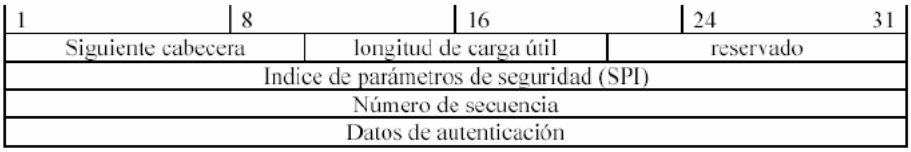


Ilustración 106. El encabezado AH.

Al igual que ESP, AH puede aplicarse tanto en modo túnel como transporte. Las ilustraciones posteriores, muestran la ubicación de AH al aplicar IPSec en modo transporte en los paquetes IP.

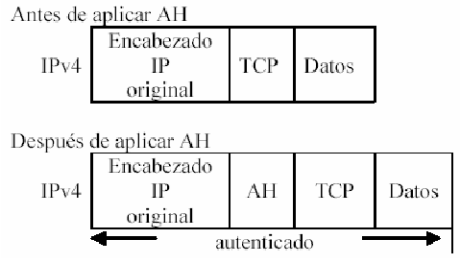


Ilustración 107. Transformación del paquete IPv4 al aplicar AH en modo transporte.

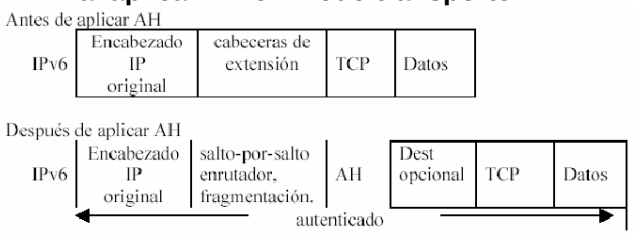


Ilustración 108. Transformación del paquete IPv6 al aplicar AH en modo transporte.

La aplicación de AH en modo túnel, tiene una ubicación similar a la de ESP, en la ilustración se muestra la transformación de los paquetes IP al aplicar AH en modo túnel.

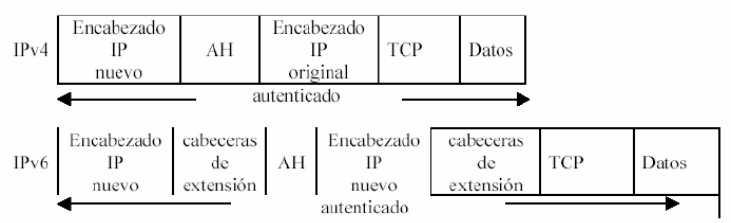


Ilustración 109. Transformación del paquete IP al aplicar AH en modo túnel.

El proceso de cálculo del valor de verificación de integridad (Integrity Check Value, ICV) que utiliza AH, llena con ceros los campos vulnerables a cambios en tránsito (TOS, Flags, Fragment, TTL, Header checksum en un encabezado IPv4) y se calcula sobre lo siguiente:

• Los campos del encabezado IP que sean inmunes a cambios en tránsito o pueda predecirse su valor (Version, longitud de carga útil, longitud total, identificación, dirección de fuente y destino en un encabezado IPv4).

• El encabezado AH (siguiente cabecera, longitud de relleno, reservado, SPI, número de secuencia y datos de autenticación (que es puesta a cero para este cálculo), y bytes de relleno en caso que existan.

• Los datos del protocolo de capa superior, que se asume son inmunes a cambios en tránsito.

Adicionalmente en el libro “IPsec en Ambiente IPv4 e IPv6” de Hugo Adrián Francisconi, se describe detalladamente los protocolos intervinientes en la arquitectura del Ipsec como son el Protocolo de gestión de claves y asociaciones de seguridad (ISAKMP), el DOI de Seguridad IP en Internet para ISAKMP, protocolo OAKLEY y el protocolo de intercambio de claves en Internet.

2.11 Criptografía

Considerando algunas definiciones previas[91]; criptografía según el Diccionario de la Real Academia, la palabra Criptografía proviene de dos palabras griegas una que significa oculto, y la otra que significa escritura, y su definición es: "Arte de escribir con clave secreta o de un modo enigmático". Obviamente la criptografía hace años que dejó de ser un arte para convertirse en una técnica, o más bien un conglomerado de técnicas, que tratan sobre la protección (ocultamiento frente a observadores no autorizados) de la información. Finalmente, el término criptología, aunque no está reconocido aún en el diccionario, se emplea habitualmente para agrupar tanto la criptografía como al criptoanálisis.

Donde los fundamentos Teóricos de la Criptografía son:

- Aritmética Modular: La aritmética modular maneja un conjunto finito de números enteros. Mucha gente la conoce como la aritmética del reloj, debido a su parecido con la forma que tenemos de contar el tiempo. Por ejemplo, si son las 19:13:59 y pasa un segundo, decimos que son las 19:14:00, y no las 19:13:60. Como vemos, los segundos (al igual que los minutos), se expresan empleando sesenta valores cíclicos, de forma que tras el 59 viene de nuevo el 0. Desde

[91] **1.- Cifrado.** Proceso de camuflar un mensaje o datos de forma que se oculte su contenido. Método para formar un mensaje oculto. El cifrado se utiliza para transformar un mensaje legible, denominado texto plano (también denominado texto no cifrado o texto sin formato) en un mensaje ilegible, codificado u oculto, denominado texto cifrado. Solamente aquel usuario con una clave de descodificación puede convertir dicho texto en el texto original.
2.- Criptosistema. Definiremos un criptosistema como una quíntupla (M, C, K, E, D), donde:
- M, representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto claro, o plaintext) que pueden ser enviados.
- C, representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- K, representa el conjunto de claves que se pueden emplear en el criptosistema.
- E, es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente E_K para cada valor posible de la clave k.
- D, es el conjunto de transformaciones de descifrado, análogo a E. Todo criptosistema ha de cumplir la siguiente condición: $D_K(E_K(m)) = m$

  Es decir, que si tenemos un mensaje m, lo ciframos empleando la clave K y luego lo desciframos empleando la misma clave, obtenemos de nuevo el mensaje original m.

3.- Criptoanálisis. El criptoanálisis consiste en comprometer la seguridad de un criptosistema.
4.- Criptografía Fuerte. Este tipo de criptografía es muy segura y es prácticamente imposible desencriptar mensajes encriptados con este tipo de criptografía.
5.- Firma Digital. Es una secuencia de caracteres calculados a partir del documento original mediante funciones de resumen (digest) o Hash que acompaña a un documento (o fichero), acreditando quién es su autor ("autenticación") y que no ha existido ninguna manipulación posterior de los datos ("integridad"). Para firmar un documento digital, su autor utiliza su propia clave secreta, cualquier persona puede verificar la validez de una firma si dispone de la clave pública del autor.
6.- Clave (Key). Llave que permite cifrar o descifrar la información recibida de forma correcta.
7.- Clave Privada. Mitad secreta de una pareja de claves criptográficas que se utiliza con un algoritmo de clave pública. Las claves privadas se usan, normalmente, para descifrar una clave de sesión simétrica, firmar datos digitalmente o descifrar datos que han sido cifrados con la clave pública correspondiente.
8.- Clave Pública. Mitad no secreta de una pareja de claves criptográficas que se utiliza con un algoritmo de clave pública. Las claves públicas se utilizan normalmente para cifrar una clave de sesión o comprobar una firma digital, etc.

el punto de vista matemático diríamos que los segundos se expresan en *módulo* de 60. Empleemos ahora un punto de vista más formal y riguroso:

Dados tres números a, b, n, que pertenezca a N decimos que a es congruente con b módulo n, y se escribe:

$a \equiv b \pmod{n}$ si se cumple: $a=b+kn$, para algún k pertenezca a Z

Por ejemplo si tenemos n=5 tendremos:

0	1	2	3	4	5	6	7	8	En Z
0	1	2	3	4	0	1	2	3	En Z

$5 \equiv 0 \pmod 5$, esto es porque 5/5 me da de resto de la división 0.
$6 \equiv 1 \pmod 5$, esto es porque 6/5 me da de resto de la división 1.
$7 \equiv 2 \pmod 5$, esto es porque 7/5 me da de resto de la división 2.

Para expresar cualquier elemento de Z como un elemento de Z_5 bastará con dividirlo por n y quedarnos con su resto. Diremos que dos elementos de Z son *equivalentes* en Z_n siempre y cuando tengan el mismo resto al dividir por n. Para nuestro ejemplo lo son -11, –6, 6, 11... Por razones de simplicidad, representamos cada clase de equivalencia por un número comprendido entre 0 y n-1. De esta forma, en nuestro ejemplo (módulo 5) tendremos el conjunto de clases de equivalencia {0, 1, 2, 3, 4, 5}, al que denominaremos Z_5. Llamaremos orden de un "grupo" *G* y lo denotaremos como (mod *G*) al número de elementos que posee el grupo en nuestro caso posee 5 elementos por ende el orden del grupo es de 5.

- Función Unidireccional o de un Solo Sentido. Supongamos que *f(x)* es una función de un sentido (o unidireccional), entonces:

1. Es fácil el cálculo $y=f(x)$, conociendo x.
2. Conocido y es computacionalmente imposible el cálculo de $x=f^{-1}(y)$.

Un ejemplo típico de una función de este tipo es: $y \equiv g^x \pmod p$
donde g y x son números reales y p es un número primo con más de 200 dígitos. Esta función es conocida como "exponenciación modular". Su función inversa será: $x \equiv \log_g y \pmod p$
Cuando p tiene un tamaño como el que se ha dicho antes es prácticamente imposible el cálculo de esta función. Esta función se conoce como "logaritmo discreto" y es de gran importancia en la criptografía asimétrica.

- El Problema de los Logaritmos Discretos. El problema inverso de la exponenciación es el cálculo de logaritmos discretos. Dados dos números a, b y el módulo n, se define el logaritmo discreto de a en base b módulo n como:

$$c = \log_b (a) \pmod n \iff a \equiv b^c \pmod n$$

En la actualidad no existen algoritmos eficientes que sean capaces de calcular en tiempo razonable logaritmos de esta naturaleza, y muchos esquemas criptográficos basan su resistencia en esta circunstancia. El problema de los logaritmos discretos está íntimamente relacionado con el de la factorización, de hecho está demostrado que si se puede calcular un logaritmo, entonces se puede factorizar fácilmente (el recíproco no se ha podido demostrar).

- El Problema de Diffie-Hellman. Antes de enunciarlo definiremos el término **generador**. Dado el conjunto Z_p^*, con p primo, diremos que α pertenezca a Z_p^* y es un generador de Z_p^*, si se cumple con:
Cualquiera sea b que pertenezca a Z_p^*, existiera un i tal que α

El enunciado del problema es el siguiente: dado un número primo p, un α^a y α^b, encontrar α^{ab} número α que sea un generador de Z_p^*, y los elementos α (mod p).

Note que nosotros conocemos α^a y α^b, pero no el valor de a ni el de b. De hecho, si pudiéramos efectuar de forma eficiente logaritmos discretos, sería suficiente con calcular a y luego $(\alpha^b)^a = \alpha^{ab}$.

Tabla 57. Fundamentos teóricos de la criptografía.

2.11.1 Criptografía Simétrica o Privada

Un intercambio de claves proporciona simetría si cualquier parte puede iniciar el intercambio, y los mensajes intercambiados pueden cruzarse en la trayectoria sin afectar la clave generada ISAKMP. En este tipo de criptografía tanto el emisor como el receptor del mensaje

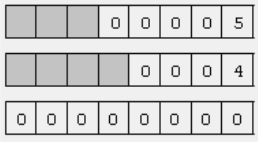
han de conocer la clave y esta clave sirve tanto para encriptar como para desencriptar los mensajes.

VENTAJAS
• Presentan una longitud de clave considerablemente menor que los algoritmos asimétricos (exceptuando los basados en curvas elípticas). • Requieren menos recursos computacionales que los algoritmos asimétricos. • Usa una clave única que sirve tanto para desencriptar como para encriptar. • El cálculo de la clave no requiere que cada parte sepa quien inició el intercambio ISAKMP. • Requiere menos recursos de ancho de banda que los algoritmos asimétricos. Sus principales desventajas son: • La simetría en el protocolo de administración de claves puede proporcionar vulnerabilidad a los ataques de reflexión (reflection attacks)ISAKMP. • La clave es generada en uno de los extremos de la comunicación, por ende si no se confía en él, este método no serviría. • Para ser empleados en comunicaciones la clave debe estar tanto en el emisor como en el receptor, lo cual nos lleva a preguntarnos cómo transmitir la clave de forma segura si tenemos un canal inseguro como Internet. Una solución puede ser: Emplear un algoritmo asimétrico (como por ejemplo, el algoritmo Diffie-Hellman) para encriptar la clave simétrica (denominada comúnmente clave de sesión). Este ultimo de los algoritmos es utilizado por ESP para encriptar la información. La ilustración inferior, muestra un esquema conceptual de un sistema simétrico. $C_K(m)$ = Cifrar el mensaje con la clave K. $D_K(m)$ = Descifrar el mensaje con la clave K. **Emisor** $C_K(m)$ canal inseguro ➔ **Receptor** $K(m)$ $D_K(C_K(mensaje)) = mensaje$

Tabla 58. Ventajas de la criptografía simétrica.

Los sistemas de claves simétricos los podemos clasificar en cifrado por Bloque o por Flujo.

a) El cifrado en bloque modo ECB, CBC y CFB. La gran mayoría de los algoritmos de cifrado simétricos se apoyan en los conceptos de confusión (consiste en tratar de ocultar la relación que existe entre el texto claro, el texto cifrado y la clave) y difusión (trata de repartir la influencia de cada bit del mensaje original lo más posible entre el mensaje cifrado) que se combinan para dar lugar a los denominados *cifrados de producto*. Estas técnicas consisten básicamente en trocear el mensaje en bloques de tamaño fijo, y aplicar la función de cifrado a cada uno de ellos. Por ende hemos de tener en cuenta lo que ocurre cuando la longitud de la cadena que queremos cifrar no es un múltiplo exacto del tamaño de bloque. Entonces tenemos que añadir información al final para que sí lo sea. El mecanismo más sencillo consiste en rellenar con ceros (o con algún otro patrón) el último bloque que se codifica. El problema ahora consiste en saber cuando se descifra por dónde hay que cortar. Lo que se suele hacer es añadir como último byte del último bloque el número de bytes que se han añadido. Esto tiene el inconveniente de que si el tamaño original es múltiplo del bloque, hay que alargarlo con otro bloque entero. Por ejemplo, si el tamaño de bloque fuera 64 bits, y nos sobraran cinco bytes al final, añadiríamos dos ceros y un tres, para completar los ocho bytes necesarios en el último bloque. Si por el contrario no sobrara nada, tendríamos que añadir siete ceros y un ocho. Se muestra el Relleno(padding) de los bytes del último bloque al emplear un algoritmo de cifrado por bloques.



Es interesante que un algoritmo criptográfico por bloque carezca de *estructura de grupo*, ya que si ciframos un mensaje primero con la clave k_1 y el resultado con la clave k_2, es como si hubiéramos empleado una clave de longitud doble, aumentando la seguridad del sistema. Si, por el contrario, la transformación criptográfica presentara estructura de grupo, esto hubiera sido equivalente a cifrar el mensaje una única vez con una tercera clave, con lo que no habríamos ganado nada. Los Modos principales de operación para algoritmos de cifrado por

bloques son: ECB, CBC, CFB.

a.1) Modo ECB. El modo ECB (Bloque de Código Electrónico) simplemente subdivide la cadena que se quiere codificar en bloques de tamaño adecuado y se cifran todos ellos empleando la misma clave. A favor de este método podemos decir que permite codificar los bloques independientemente de su orden, lo cual es adecuado para codificar bases de datos o ficheros en los que se requiera un acceso aleatorio. También es resistente a errores, pues si uno de los bloques sufriera una alteración, el resto quedaría intacto. Por contra, si el mensaje presenta patrones repetitivos, el texto cifrado también los presentará, y eso es peligroso, sobre todo cuando se codifica información muy redundante (como ficheros de texto), o con patrones comunes al inicio y final (como el correo electrónico). Un atacante puede en estos casos efectuar un ataque estadístico y extraer bastante información. Otro riesgo bastante importante que presenta el modo ECB es el de la sustitución de bloques. El atacante puede cambiar un bloque sin mayores problemas, y alterar los mensajes incluso desconociendo la clave y el algoritmo empleado. Simplemente se escucha una comunicación de la que se conozca el contenido, como por ejemplo una transacción bancaria a nuestra cuenta corriente. Luego se escuchan otras comunicaciones y se sustituyen los bloques correspondientes al número de cuenta del beneficiario de la transacción por la versión codificada de nuestro número (que ni siquiera nos habremos molestado en descifrar, "En cuestión de horas nos habremos hecho ricos").

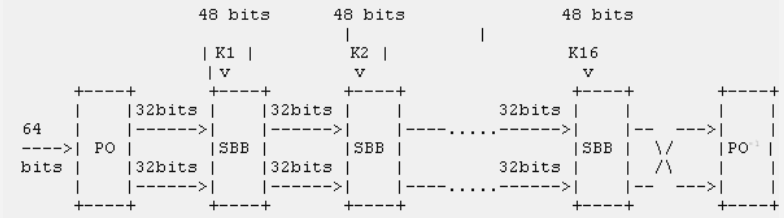
a.2) Modo CBC. El modo CBC (Cipher Book Chiang - Concatenación de Bloques Cifrados) incorpora un mecanismo de retroalimentación en el cifrado por bloques. Esto significa que la codificación de bloques anteriores condiciona la codificación del bloque actual, por lo que será imposible sustituir un bloque individual en el mensaje cifrado. Esto se consigue efectuando una operación XOR entre el bloque del mensaje que queremos codificar y el último criptograma obtenido. En cualquier caso, dos mensajes idénticos se codificarán de la misma forma usando el modo CBC. Más aún, dos mensajes que empiecen igual se codificarán igual hasta llegar a la primera diferencia entre ellos. Para evitar esto se emplea un *Vector de Inicialización*, que puede ser un bloque aleatorio, como bloque inicial de la transmisión. Este vector será descartado en destino, pero garantiza que siempre los mensajes se codifiquen de manera diferente, aunque tengan partes comunes.

a.3) Modo CFB. El modo CBC no empieza a codificar (o decodificar) hasta que no se tiene que transmitir (o se ha recibido) un bloque completo de información. Esta circunstancia puede convertirse en un serio inconveniente, por ejemplo en el caso de terminales, que deberían poder transmitir cada carácter que pulsa el usuario de manera individual. Una posible solución sería emplear un bloque completo para transmitir cada byte y rellenar el resto con ceros, pero esto hará que tengamos únicamente 256 mensajes diferentes en nuestra transmisión y que un atacante pueda efectuar un sencillo análisis estadístico para comprometerla. Otra opción sería rellenar el bloque con información aleatoria, aunque seguiríamos desperdiciando gran parte del ancho de banda de la transmisión. El modo de operación CFB (Cipher-Feedback Mode) permitirá codificar la información en unidades inferiores al tamaño del bloque, lo cual permite aprovechar totalmente la capacidad de transmisión del canal de comunicaciones, manteniendo además un nivel de seguridad adecuado.

b) Algoritmo Des, Triple Des, IDEA, AES, RC2 y RC5.

i) Algoritmo Des. Este algoritmo simétrico encripta bloques de 64 bits de longitud con una clave de 64 bits de longitud. Dentro de la clave el último bit de cada byte es de paridad, con lo cual tenemos que la clave en realidad es de 56 bits, esto hace que haya 2^56 posibles claves para este algoritmo. Dependiendo de la naturaleza de la aplicación DES puede operar en modo CBC, ECB, CFB y otros modos más no vistos aquí como el modo OFB. Este algoritmo utiliza un "dispositivo" denominado SBB (Standard Building Block o Constructor Estándar de Bloques), el cual requiere como entrada un bloque de 64 bits y una clave de 48 bits, produciendo una salida de 64 bits. El DES requiere 16 dispositivos SBB. Tenemos una clave original, k, de 64 bits, 56 en realidad, de ella se extraen 16 subclaves k_i de 48 bits de longitud. El algoritmo es el siguiente:

1. Se aplica una Permutación Original (PO) a cada bloque de 64 bits. Produciendo una salida de 64 bits (dos de 32 bits).
2. Pasamos la salida del PO y la subclave k_1 por el primer SBB, la salida la pasamos por el segundo SBB con la subclave k_2 y así con los 16 SBB.
3. A la salida del último SBB le aplicamos la permutación PO^{-1}. De donde obtenemos el texto encriptado.



Para desencriptar tomamos como entrada el texto encriptado y aplicamos las subclaves k_i en orden inverso, es decir en el primer SBB. Ésta es una lista de claves DES débiles y semi-débiles, las cuales deben evitar usarse. Las claves provienen de Sch96. Todas los claves se listan en hexadecimal.

Claves DES débiles	Claves DES semi-débiles	
0101 0101 0101 0101	01FE 01FE 01FE 01FE	FE01 FE01 FE01 FE01
1F1F 1F1F E0E0 E0E0	1FE0 1FE0 0EF1 0EF1	E01F E01F F10E F10E
E0E0 E0E0 1F1F 1F1F	01E0 01E0 01F1 01F1	E001 E001 F101 F101
FEFE FEFE FEFE FEFE	1FFE 1FFE 0EFE 0EFE	FE1F FE1F FE0E FE0E
	011F 011F 010E 010E	1F01 1F01 0E01 0E01
	E0FE E0FE F1FE F1FE	FEE0 FEE0 FEF1 FEF1

El uso de estas claves débiles y semi-débiles debe ser rechazado, seguido de una solicitud de reemplazo de claves o de la negociación de una nueva SA.

ii) Algoritmo Triple Des(3DES). A mediados de 1988 se demostró que un ataque por fuerza bruta contra el algoritmo DES ya era posible, gracias al avance de la informática entre otras cosas. Pero la debilidad no la tiene el algoritmo, sino que la tiene la clave debido a que no posee suficiente longitud. Si aumentamos la clave este algoritmo sigue siendo seguro. Por ende este algoritmo realiza tres veces el DES, aumentando la longitud de clave a 192 bits (64 x 3).

iii) Algoritmo IDEA. El algoritmo IDEA (International Data Encryption Algorithm) data de 1992 y para muchos constituye el mejor y más seguro algoritmo simétrico disponible en la actualidad. Trabaja con bloques de 64 bits de longitud y emplea una clave de 128 bits reales (no hay bits de paridad como en el DES). Como en el caso de DES, se usa el mismo algoritmo tanto para cifrar como para descifrar. IDEA es un algoritmo bastante seguro, y hasta ahora se ha mostrado resistente a multitud de ataques, entre ellos el criptoanálisis diferencial. No presenta claves débiles, y su longitud de clave hace imposible en la práctica un ataque por fuerza bruta.

iv) Algoritmo AES. Su interés radica en que todo el proceso de selección, revisión y estudio, se ha efectuado de forma pública y abierta, lo cual convierte a Rijndael en un algoritmo perfectamente digno de la confianza de todos. Este es un sistema de cifrado por bloques, diseñado para manejar longitudes de clave y de bloque variables, ambas comprendidas entre los 128 y los 256 bits. AES, a diferencia de algoritmos como el DES, no posee estructura de red de Feistel (para descifrar basta con aplicar el mismo algoritmo, pero con las k_i en orden inverso). En su lugar se ha definido cada ronda como una composición de cuatro funciones invertibles.

v) Algoritmo RC2. Es un algoritmo propietario de la empresa RSA que tiene un tamaño de bloque de 64 bits. Permite utilizar los modos ECB y CBC. Fue desarrollado como alternativa del DES y tiene una longitud de clave variable que va de 64 a 256 bits.

vi) Algoritmo RC5. También pertenece a la empresa RSA. Se caracteriza por permitir bloques de 32, 64 o 128 bits. Su tamaño de clave varía de 0 a 2040 bits (255 bytes).

c) El cifrado en flujo RC4 y RC4 con MAC. Supongamos que disponemos de un generador pseudoaleatorio capaz de generar secuencias criptográficamente aleatorias, de forma que la longitud de los posibles ciclos sea extremadamente grande. En tal caso podríamos, empleando semillas del generador como clave, podemos obtener cadenas de bits de usar y tirar, y emplearlas para cifrar mensajes simplemente aplicando la función XOR entre el texto en claro y la secuencia generada. Todo aquel que conozca la semilla podría reconstruir la secuencia pseudoaleatoria y de esta forma descifrar el mensaje. Dichos algoritmos no son más que la especificación de un generador pseudoaleatorio, y permiten cifrar mensajes de longitud arbitraria, sin necesidad de dividirlos en bloques para codificarlos por separado. Como cabría esperar, estos criptosistemas no proporcionan seguridad perfecta, ya que como empleamos un generador tenemos como máximo tantas secuencias distintas como posibles valores iniciales de la semilla.

c.1) RC4. Se caracteriza por utilizar la misma información de entrada que ha de cifrar para la generación de un número pseudoaleatorio que utilizará como clave, realizando un XOR entre la entrada y la clave. Esto significa que tanto el cifrado como el descifrado son operaciones idénticas. No se debe utilizar la misma clave más de una vez, ya

que al utilizar un XOR como operación básica un atacante podría fácilmente descubrirla (XOR(XOR(X)) = X). La clave varía de 8 a 2048 bits.

c.2) RC4 con MAC. Es una extensión del RC4 que busca asegurar la integridad en los datos mediante el uso de una función MAC (es una función que asegura la integridad de los datos, a partir del mensaje genera una secuencia de bits de tal forma que si es modificado, el receptor puede saberlo.

Tabla 59. Clasificación de sistemas simétricos.

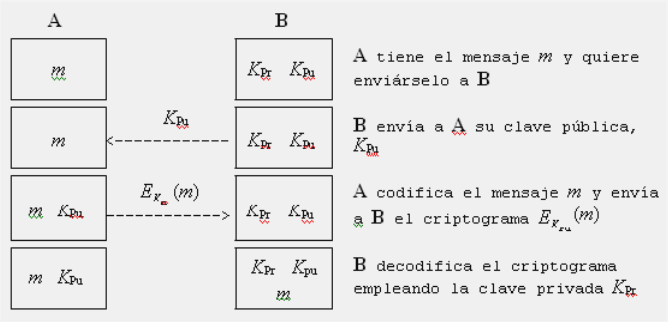
2.11.2 Criptografía Asimétrica o Pública.

Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos y difieren fundamentalmente de los algoritmos simétricos en que la claves no son únicas sino que forman pares. Por ejemplo, mientras que para algoritmos simétricos se considera segura una clave de 128 bits, para algoritmos asimétricos (si exceptuamos aquellos basados en curvas elípticas) se recomiendan claves de al menos 1024 bits. Además, la complejidad del cálculo de algoritmos asimétricos los hace considerablemente más lentos que los algoritmos de cifrado simétricos. En la práctica los métodos asimétricos se emplean únicamente para codificar la clave de sesión (simétrica) de cada mensaje o transacción particular. Por otra parte algoritmos asimétricos ofrecen un abanico superior de posibilidades, pudiendo emplearse para establecer comunicaciones seguras por canales inseguros (puesto que únicamente viaja por el canal la clave pública, que sólo sirve para cifrar), o para llevar a cabo autentificaciones. En la práctica se emplea una combinación de criptosistemas simétricos y asimétricos, puesto que los segundos presentan el inconveniente de ser computacionalmente mucho más costosos que los primeros. En el mundo real se codifican los mensajes (largos) mediante algoritmos simétricos, que suelen ser muy eficientes, y luego se hace uso de la criptografía asimétrica para codificar las claves simétricas (cortas).

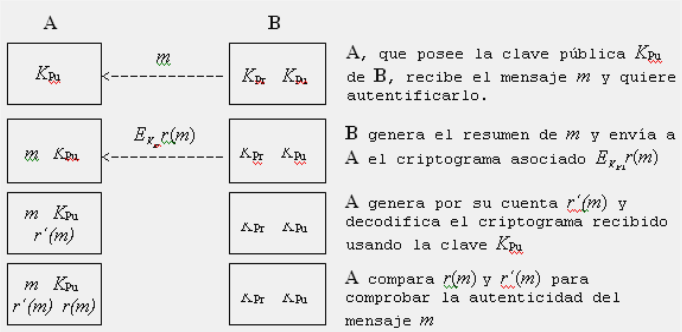
a) Aplicaciones de los Algoritmos Asimétricos. Los algoritmos asimétricos poseen dos claves diferentes en lugar de una, la clave privada K_{Pr} y la clave pública K_{Pu}, eliminando el mayor problema de los sistemas de clave privada, dar a conocer únicamente al receptor autorizado la clave usada en el sistema de cifrado/descifrado. Una de ellas se emplea para codificar, mientras que la otra se usa para decodificar. Dependiendo de la aplicación que le demos al algoritmo, la clave pública será la de cifrado o viceversa. Como se ve se introduce un nuevo problema, la autenticación del origen de los datos. Puesto que todo el mundo conoce la clave pública, se puede enviar un mensaje falseando la procedencia. En los sistemas de clave privada esto no pasaba, ya que la clave la compartían únicamente

el emisor y el receptor de la información, asegurando la confidencialidad y la procedencia de la información. Para que estos criptosistemas sean seguros también ha de cumplirse que a partir de una de las claves resulte extremadamente difícil calcular la otra. Para poder dar a conocer las claves públicas de los usuarios sin ningún riesgo, debemos asegurarnos que estas no pueden ser ni modificadas ni alteradas en ninguna forma. Con esta función se crearon las Autoridades de Certificación (Certification Authorities, CA), que son organismos encargados de distribuir las claves públicas y velar por ellas.

a.1) Protección de la Información. Una de las aplicaciones inmediatas de los algoritmos asimétricos es el cifrado de la información sin tener que transmitir la clave de decodificación, lo cual permite su uso en canales inseguros. Supongamos que **A** quiere enviar un mensaje a **B**. Para ello solicita a **B** su clave pública K_{Pu} (o la obtiene de una Autoridad de Certificación). **A** genera entonces el mensaje cifrado $E_K Pu(m)$. Una vez hecho esto únicamente quien posea la clave K_{Pr} (en nuestro ejemplo, **B**) podrá recuperar el mensaje original m. Mostrando así, la transmisión de información empleando algoritmos asimétricos, nótese que para este tipo de aplicación, la llave que se hace pública es aquella que permite codificar los mensajes, mientras que la llave privada es aquella que permite descifrarlos.



a.2) Autentificación. La segunda aplicación de los algoritmos asimétricos es la autentificación de mensajes, con ayuda de funciones resumen, que nos permiten obtener una firma digital a partir de un mensaje. Dicha firma es mucho más pequeña que el mensaje original. Supongamos que **A** recibe un mensaje m de **B** y quiere comprobar su autenticidad. Para ello **B** genera un resumen del mensaje $r(m)$ y lo codifica empleando la clave de cifrado, que en este caso será la privada.



La clave de descifrado se habrá hecho pública previamente, y debe estar en poder de **A**. **B** envía entonces a **A** el criptograma correspondiente a $r(m)$. **A** puede ahora generar su propio $r'(m)$ y compararla con $r(m)$ el cual es el valor obtenido del criptograma enviado por **B**. Si coinciden, el mensaje será auténtico, puesto que el único que posee la clave para codificar es precisamente **B**.
Nótese que en este caso la clave que se emplea para cifrar es la clave privada, justo al revés que para la simple codificación de mensajes.
En muchos de los algoritmos asimétricos ambas claves sirven tanto para cifrar como para descifrar, de manera que si empleamos una para codificar, la otra permitirá decodificar y viceversa. Esto es lo que ocurre con el algoritmo RSA, en el que un único par de claves es suficiente para codificar y autentificar.

b) Algoritmos Asimétricos

b.1) Algoritmo de Diffie-Hellman. Es un algoritmo asimétrico, basado en el problema de Diffie-Hellman, que se

emplea fundamentalmente para acordar una clave secreta común entre dos interlocutores, sin necesidad de ningún secreto preestablecido entre ellos, a través de un canal de comunicación inseguro. La ventaja de este sistema es que no son necesarias llaves públicas en el sentido estricto, sino información compartida por los dos comunicantes. Este algoritmo no proporciona ni autenticación ni cifrado, por ende no suele utilizarse para la protección de datos. Debido a que es uno de los algoritmos más utilizados con IPsec, describiré su funcionamiento:
Sean **A** y **B** los interlocutores en cuestión. En primer lugar, se calcula un número primo p y un generador α de Z_p^*, con $2 \leq \alpha \leq p-1$. Esta información es pública y conocida por ambos. El algoritmo queda como sigue:

1. **A** escoge un número aleatorio x, tal que $1 \leq x \leq p-2$ y envía a **B** el valor: $\alpha^x \ (mod\ p)$
2. **B** escoge un número aleatorio y, tal que $1 \leq y \leq p-2$ y envía a **A** el valor: $\alpha^y \ (mod\ p)$
3. **B** recoge α^x y calcula $K = (\alpha^x)^y \ (mod\ p)$
4. **A** recoge α^y y calcula $K = (\alpha^y)^x \ (mod\ p)$

Puesto que x e y no viajan por la red, al final **A** y **B** terminan compartiendo el valor de K, sin que nadie que capture los mensajes transmitidos pueda repetir el cálculo.

b.2) El Algoritmo RSA. Sus claves sirven indistintamente tanto para codificar como para autentificar. Debe su nombre a sus tres inventores: Ronald Rivest, Adi Shamir y Leonard Adleman, y estuvo bajo patente de los Laboratorios RSA hasta el 20 de septiembre de 2000, por lo que su uso comercial estuvo restringido hasta esa fecha. Nadie ha conseguido probar o rebatir su seguridad, y se lo tiene como uno de los algoritmos asimétricos más seguros. RSA se basa en la dificultad para factorizar números grandes. Las claves públicas y privadas se calculan a partir de un número que se obtiene como producto de dos primos grandes.

b.3) Criptografía de Curvas Elípticas. Para curvas elípticas existe un problema análogo al de los logaritmos discretos en grupos finitos de enteros. Esto nos va a permitir trasladar cualquier algoritmo criptográfico definido sobre enteros, y que se apoye en este problema, al ámbito de las curvas elípticas. La ventaja que se obtiene es que, con claves más pequeñas, se obtiene un nivel de seguridad equiparable. Debido a la relación existente entre ambos, muchos algoritmos que se basan en el problema de la factorización pueden ser replanteados para descansar sobre los logaritmos discretos. De hecho, existen versiones de curvas elípticas de muchos de los algoritmos asimétricos más populares.

Tabla 60. Algoritmos asimétricos.

2.12 Despliegue y experiencias del protocolo Ipv6

2.12.1 Asignación de direcciones

La responsabilidad de la administración del espacio de direcciones de Ipv6 esta distribuida globalmente de acuerdo con la estructura que se muestra a continuación:

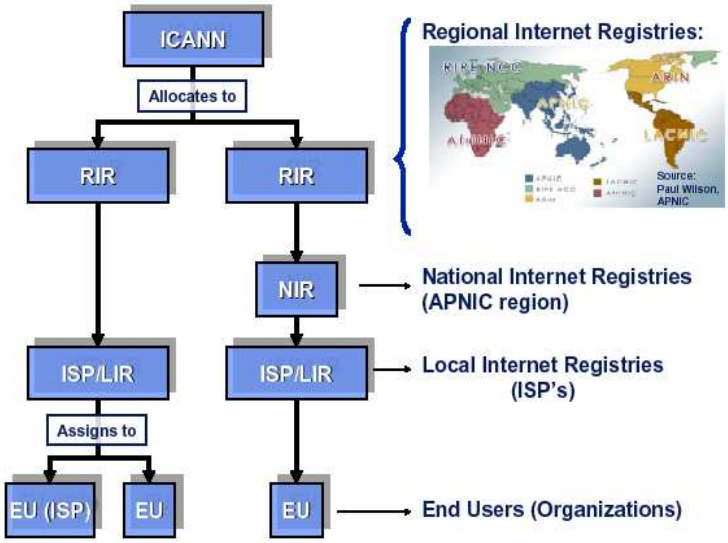


Ilustración 110. Estructura para la asignación de bloques de direcciones[92].

1) Internet Registry(IR): Es una organización responsable de la distribución de espacios de direcciones IP a sus miembros o clientes y del registro de esa distribución. Los IRs están clasificados de acuerdo a su función principal y alcance territorial dentro de la estructura jerárquica indicada. **2) Regional Internet Registry(RIR**): Son establecidos y autorizados por las comunidades regionales respectivas, y reconocidos por el IANA para servir y representar grandes regiones geográficas. El rol principal de los RIRs es administrar y distribuir el espacio de direcciones publico de Internet dentro de las respectivas regiones. **3) Nacional Internet Registry(NIR):** Adjudica principalmente espacios de direcciones a sus miembros o constituyentes, los cuales son generalmente LRs a un nivel nacional. Los NIRs existen mayormente en la región de Asia Pacifico. **4) Local Internet Registry(LIR):** Es un IR que asigna, principalmente, espacios de direcciones a los usuarios de los servicios de red que este provee. Los LIRs son generalmente ISPs, cuyos clientes son principalmente usuarios finales y posiblemente otros ISPs.[93]

Tabla 61. Descripción de la estructura de asignación de bloques.

2.12.2 Principios de la política Ipv6.

a) El espacio de direcciones no debe ser considerado propietario:

Es contrario a los objetivos del documento de las políticas de Ipv6 y no

[92] Fuente: David Fernández, "Introducción a Ipv6", Departamento de Ingeniería Sistemas Telematicos Universidad Politécnica de Madrid-2004 http://www.6sos.org/pdf/introduccion_a_ipv6_v1.pdf
ICANN(Internet Corportaion for Assigned Names and Numbers) es la organización que coordina la asignación de nombres, direcciones IP y otro identificadores utilizados en protocolos.
ICANN delega rango de direcciones a los RIR:
-APNIC(Asia-Pacific Network Information Center) –ARIN (American Resgistry for Internet Number) – LACNIC(Latin-American and Caribean IP Address registry) – RIPE NCC (Reseaux IP Europpens) - AfriNIC (Afican Regional Internet Registry)
Los RIR asignan directamente rango a ISPs o usuarios finales(Organizaciones), en el caso de APNIC se hace a través de los registros nacionales (NIR).

[93] Policitas Ipv6 LACNIC http://lacnic.net/sp/registro/ipv6.html

se encuentra entre los intereses de la comunidad de Internet en su conjunto que los espacios de direcciones sean considerados propietarios. Por que se basa en el entendimiento de que el espacio globalmente único de direcciones unicast de Ipv6 es licenciado para su uso en lugar de adueñado.[94]

b) Ruteabilidad no garantizada: no hay garantías de que la adjudicación o asignación de una dirección será ruteable globalmente. Sin embargo, los RIRs deber aplicar procedimientos que reduzcan la posibilidad de fragmentación del espacio de direcciones, lo que podría llevar a la perdida de ruteabilidad.

c) Adjudicación Mínima: Los RIRs aplicaran un tamaño mínimo para adjudicaciones de Ipv6 para facilita el filtro basado en el prefijo. El tamaño mínimo de adjudicación para un espacio de direcciones Ipv6 es 32.

d) Consideraciones de la infraestructura de Ipv4: Cuando un proveedor de servicios de Ipv4 pide espacio Ipv6 para una transición final de servicios existentes a Ipv6, el número de clientes actuales de Ipv4 podría ser usado para justificar un pedido más grande del que estaría justificado si el mismo estuviera basado solamente en la instraestructura Ipv6.

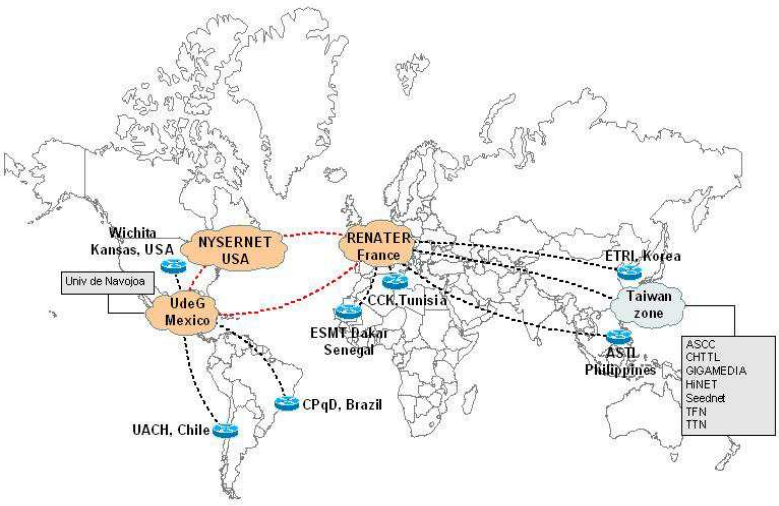
2.12.3 Estado del despliegue de Ipv6

En la actualidad se cuenta con un total de 6Bone[95] sites registrados en el mundo en 57 países.

---

[94] Específicamente las direcciones IP serán adjudicadas en base a una licencia, con licencias sujetas a renovación periódica. El otorgamiento de una licencia esta sujeta a condiciones especificas a aplicarse al comienzo como así también en cada renovación de la misma. Los RIRs generalmente renovaran las licencias automáticamente, siempre que las organizaciones solicitantes hagan un esfuerzo de buena fe para cumplir con el criterio bajo el cual calificaron o fueron otorgadas una adjudicación o asignación. Sin embargo, en aquellos casos en que una organización no esta utilizando el espacio de direcciones como se espera, o esta mostrando mala fe en regirse por las obligaciones asociadas, los RIRs se reservan el derecho de no renovar la licencia.

[95] Derivado del proyecto Ipv6 de la IETF nace 6Bone, esta es una red experimental, mundial usada para probar el protocolo Ipv6. 6Bone actualmente cuenta con 57 países participantes. La topología de esta Red esta compuesta por “Islas”, una isla es un conjunto de equipos y computadores que utilizan el protocolo Ipv6 para comunicarse entre si. Unidas por enlaces punto a punto llamadazos “túneles ipv6 sobre ipv4”, y opera según el esquema de direcciones experimental establecido en el RFC 2471: “IPV6 Testing Address Allocation”. Actualmente se hacen grandes esfuerzos para remplazar los túneles por links nativos sobre Ipv6.



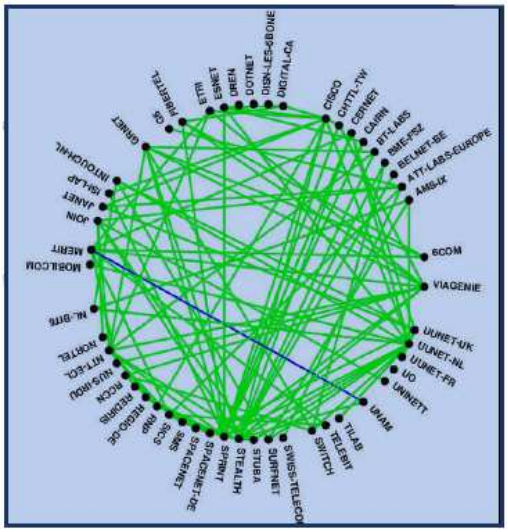


Ilustración 111. Nodos Ipv6 en el mundo[96]. **Ilustración 112. Conexiones Ipv6 en el mundo[97].**

El despliegue de Ipv6 en Latinoamérica presenta 56 sites registrados:

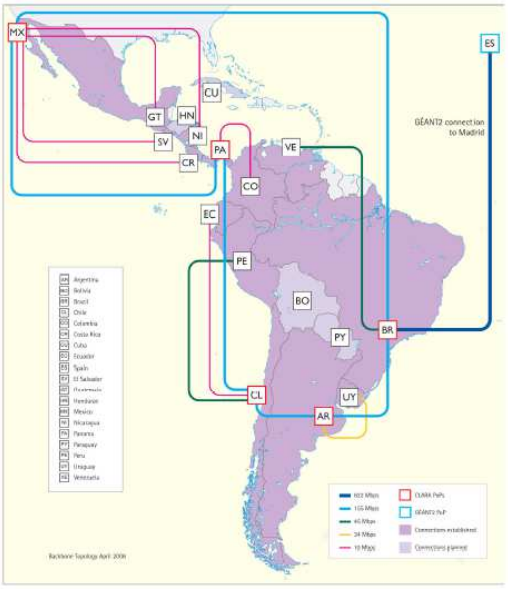


Ilustración 113. Despliegue Ipv6 [98]. **Ilustración 114. Plan de Ingeniería NEG[99].**

---

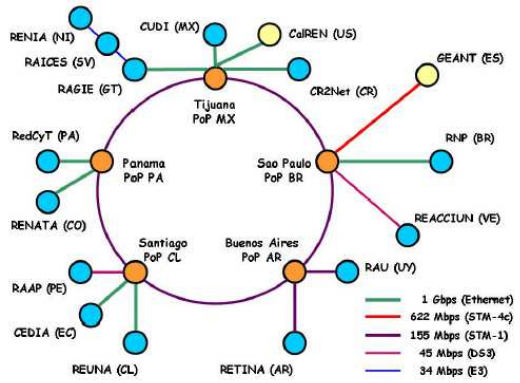
[96] Christian Lazo Ramirez Instituto de Informática Facultad de la Ingeniería Universidad Austral de Chile y Azael Fernandez Alcantara Coordinador del Proyecto IPv6 Universidad Nacional Autónoma de México, Grupo de Trabajo de Ipv6 de CUDI "IPV6, el protocolo para la nueva Internet" pag. 28 http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

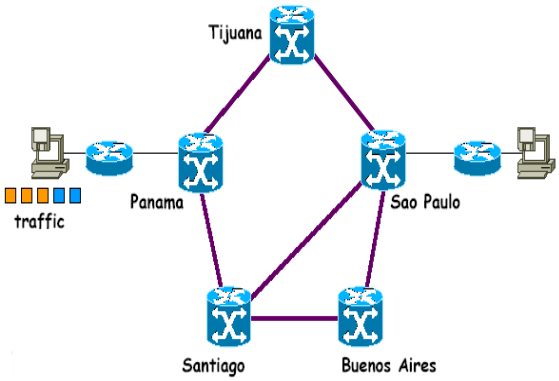
[97] Ing. Asale Fernandez Alcantara, Universidad Nacional Autónoma de México, UNAM; Grupo de Trabajo de IPv6 de la UNAN, Ipv6 Forum, Capitulo México "IPv6: Avances, mitos y perspectivas", MEXICO http://www.ipv6forum.com.mx/documentos/IPv6_AMP.pdf

País	CC	Respondio Encuesta?	Prefijo IPv6 Asignado	Master in root file?	Servidor Autoritativo responde SOA?	Registro Automatico de AAAA ?	Registro Manual de AAAA ?	Servidor Whois sobre IPv6?	Servidor WEB sobre IPv6?
Argentine	AR	Yes	No	No	2001:620::5 (*)	No	No	No	No
Belize	BZ	No	No	No	No	n/a	n/a	n/a	n/a
Bolivia	BO	No	No	No	No	n/a	n/a	n/a	n/a
Brazil	BR	Yes	2001:12ff::/32	Yes	2001:12ff::10	Yes	Yes	Yes	Yes
Chile	CL	Yes	2001:1398::/32 (**)	No	2001:4f8:0:2::13 (*) (+)	Yes	No	No	No
Colombia	CO	Yes	No	No	No	No	No	No	No
Costa Rica	CR	No	No	No	No	n/a	n/a	n/a	n/a
Cuba	CU	No	2001:1340::/32	Yes	2001:1340:1:128::136 (+)	No	Yes	Yes	Yes
Ecuador	EC	Yes	No	No	No	No	No	No	No
El Salvador	SV	No	No	No	No	n/a	n/a	n/a	n/a
French Guyana	GF	No	No	No	No	n/a	n/a	n/a	n/a
Guatemala	GT	No	No	No	2001:610:240:0:53:cc:12:92 (*)	n/a	n/a	n/a	n/a
Guyana	GY	No	No	No	2001:610:240:0:53:cc:12:95 (*)	n/a	n/a	n/a	n/a
Haiti	HT	Yes	No	No	2001:660:3006:1::1:1 (*)	No	No	No	No
Honduras (***)	HN	Yes	No	No	2001:502:d399::1 (*)	No	No	No	No
Mexico	MX	Yes	No	No	No	Yes	No	No	No
Nicaragua	NI	No	No	No	No	n/a	n/a	n/a	n/a
Panama	PA	Yes	2001:1368::/32	No	No	No	No	No	No
Paraguay	PY	Yes	2001:1320::/32 (**)	No	2001:620::5 (*)(+)	No	No	No	No
Peru	PE	Yes	No	No	2001:610:240:0:53:cc:12:173 (*)	No	No	No	No
Dominic Republic	DO	Yes	2001:13e0::/32	No	No	No	No	No	No
Suriname	SR	No	No	No	No	n/a	n/a	n/a	n/a
Uruguay	UY	Yes	2001:1328::/32	Yes	2001:1328:6::5 (+)	No	Yes	Yes	Yes
Venezuela	VE	Yes	2001:1338::/32	Yes	2001:1338::2 (+)	Yes	No	Yes	Yes

Tabla 1: Resultados de la encuesta por País.
(*) Potencialmente un servidor secundario con glue record en la zona root.
(**) Prefijo no presente en la tabla global de IPv6.
(***) Servicio a través de una compañía de terceros.
(+) Más de un servidor autoritativo contesta a SOA para el ccTLD

Tabla 62. Presencia de Ipv6 en ccTLDs (Country Code Top Level Domain) de América Latina[100].





[98] Christian Lazo Ramirez Instituto de Informática Facultad de la Ingeniería Universidad Austral de Chile y Azael Fernandez Alcantara Coordinador del Proyecto IPv6 Universidad Nacional Autónoma de México, Grupo de Trabajo de Ipv6 de CUDI "IPV6, el protocolo para la nueva Internet" pag. 63 http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

[99] Fuente: CLARA - Cooperación latino americana de redes avanzadas. "Plan de Ingeniería para el NEG, Eriko Porto, CLARA Network Engineering Group".

[100] Roque Gagliano Molla y Pablo Allietti, "Presencia de Ipv6 en ccTLDs de América Latina" Febrero 2006. Durante el 2005 32 prefijos Ipv6 han sido asignados por el Registro Regional de Internet(RIR): LACNIC(Registro de Direcciones de Internet para América Latina y el Caribe). El grafico explora si la infraestructura de DNS es esta regios esta preparada para el despliegue de Ipv6.

Ilustración 115. Topología de Red. **Ilustración 116. Ingeniería de Tráfico.**

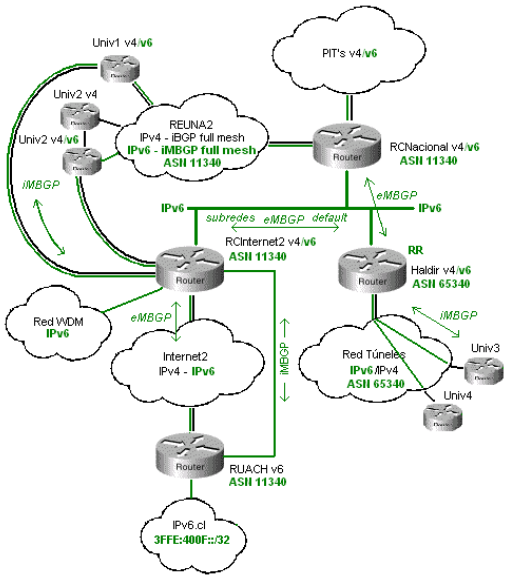


Ilustración 117. Diseño de la Red Ipv6 en Chile

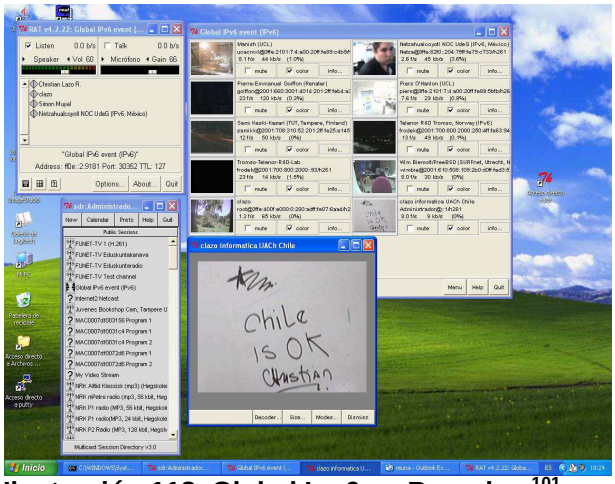


Ilustración 118. Global Ipv6 en Bruselas.[101]

2.12.4 Estado del arte de Ipv6

Por ejemplo, en Corea se estima una migración completa a Ipv6 el 2010.

[101] Cristian Lazo R. "Estado del Avance de Redes en Chile" FLIP-6 2004.

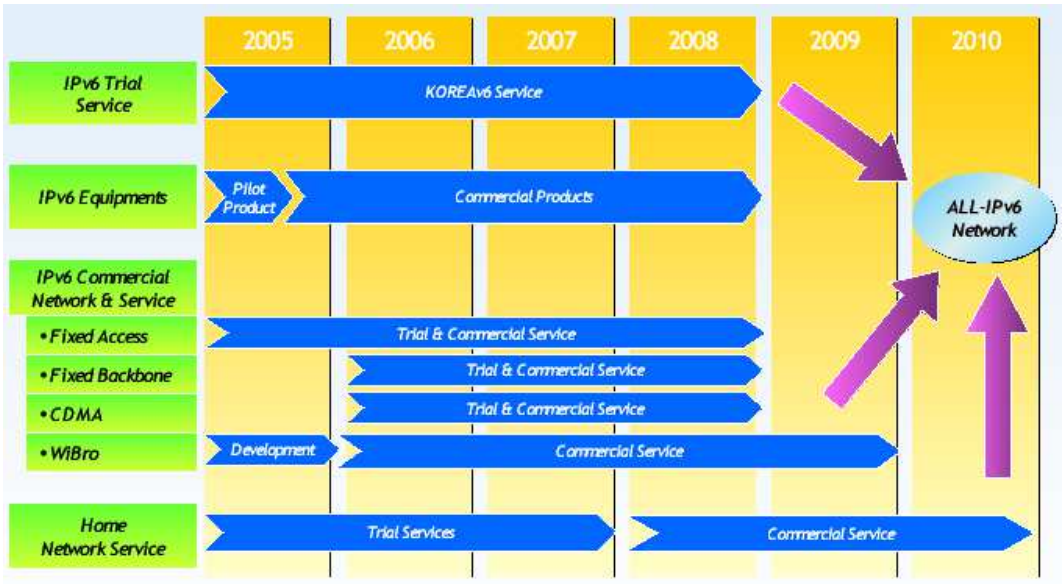


Ilustración 119. Estimación de migración de Ipv6 en Korea[102].

En materia de las aplicaciones de Ipv6 tenemos la ilustración de la izquierda que es Ipv6 Multicast: VideoLan OKINAWA EISA y en el lado derecho los Chips RFID/Ipv6 de Hitachi (a.- Chip RFID sobre un dedo humano y b.- los nuevos chips RFID al lado de un cabello humano- Conocido también como el polvo inteligente).

[102] Kwanbok Jo, "IPv6 Strategy and Deployment Status in Korea", Ubiquitous Society Strategy Office, 2006.

Ilustración 120. Ipv6 Multicast M6bone[103].

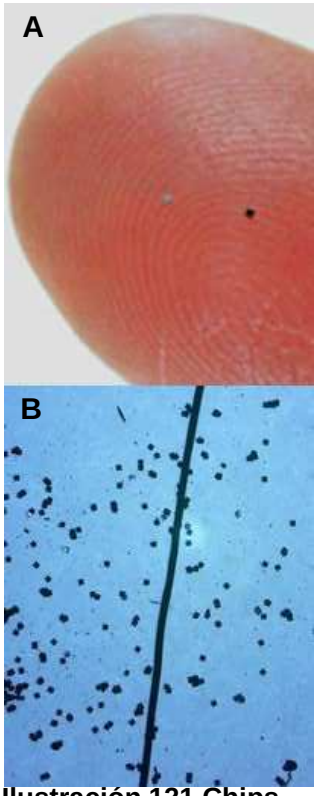


Ilustración 121.Chips RFID/Ipv6[104].

Los fabricantes de autos esperan por Ipv6, los autos podrían ser fácilmente identificados y localizados, los autos se convierten en computadoras, tele-mantenimiento y tele-monitoreo permitirán mantener funcionalidades del auto a distancia, los fabricantes de autos necesitan un gran cantidad de direcciones IP(Pantallas multi-funcionales en el tablero, Radio, GPS, joystick de información en línea como palanca de cambios, Mapas locales,Teléfono en el tablero e Identificación a través de tarjeta Ipv6-Card).

---

[103] IPv6 Multicast, Experiencia Universidad de Guadalajara, México.

[104] Lo que aparece, a pesar de parecer partículas de polvo, es algo más que polvo: son los novedosos chips RFID de Hitachi que se mostraron al mundo el pasado el 13 de febrero del 2007. Estos tienen un tamaño de 0.05 x 0.05 mm y son hasta 64 veces más pequeños que sus actuales Mu-chips de 0.4 x 0.4 mm. Los chips RFID son identificadores únicos con soporte Ipv6 que se pueden adherir a productos o seres humanos y, que tiene como particularidad, que pueden ser leídos a distancia por radiofrecuencia. Mucho se ha hablado ya sobre la posible violación de derechos a la privacidad que se puede realizar con estos chips y que se viene realizando. Espolvoreando este polvo (como lo llaman) sobre productos o personas, será fácil (o muy fácil) por parte de cualquier persona o entidad controlar hasta el último detalle de tu vida.

Ilustración 122. Electrónica de los Autos[105].

Ilustración 123. El hogar digital[106].

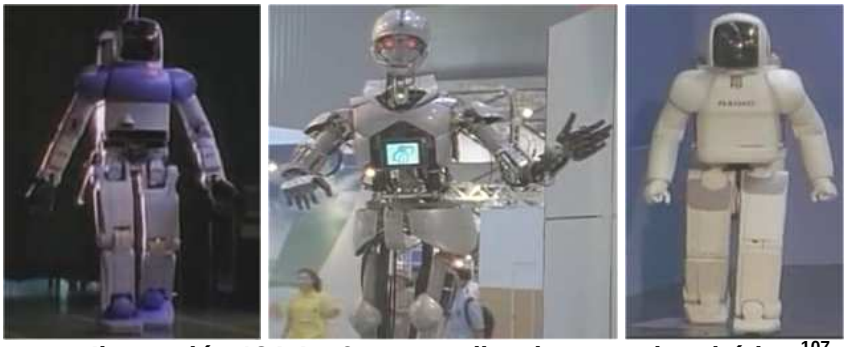


Ilustración 124. Ipv6 y sus aplicaciones en la robótica.[107]

---

[105] Rosa M. Delgado ISOC Trustee, "Escalamiento de Internet de gTLDs al Pv6", Gobierno del Internet Conferencia en el Cairo, 2005.

[106] Carlos Ralli, "Euro6IX: Red Europea de Intercambiadores IPv6", Telefónica Investigación y Desarrollo, 2004, www.euro6ix.net "Demo TID-Euro6IX, control por PDAs IPv6, Interacción Transparente v4-v6**".**

[107] En la actualidad en materia del Ipv6 aplicado a la Robótica, los robot cuentan por defecto ya con un único identificador de interfaz con el cual se permite controlar y monitorear las actividades que realizan en su entorno tanto físico con GIS(Sistemas de información geo-referencial) o virtual(A través de la trazabilidad de operaciones que este autómata solicita en las redes físicas o satelitales por la WWW, es decir de las solicitudes que generan los robots en la Web y los efectos que generara en el mundo digital al encontrarse en un foro virtual, las consultas que el robot realiza, el blogs del mismo y las respuestas que genere, por contar inmensa biblioteca de datos en sus circuitos integrados…quizá ya, en un futuro cercano ellos respondan nuestras consultas y realicen análisis de avanzada con matemática compleja; Ejm, ¿Recomiendeme el mejor libro y autor en derecho informático en el mundo?(Patron: Analsis de integridad), ¿El mejor papers publicado sobre la Ley de privacidad en Chile?(Patron: Data-Mining), ¿Deseo contratar un experto en derecho informático en Chile?(Patron: Comparación de bitácoras), etc.) como son los casos del P3 Autónomo(Izquierda), DP(Centro) y el primo de P3(Derecha) que son a hoy, las obras maestras de la ingeniería y la matemática construidas a base de cables motores y ecuaciones algorítmicas. Generando Ipv6 así un mayor escenario de control de neutralidad frente al desarrollo de estos humanos artificiales.

Ilustración 125. Servicios aplicados a Ipv6. [108]

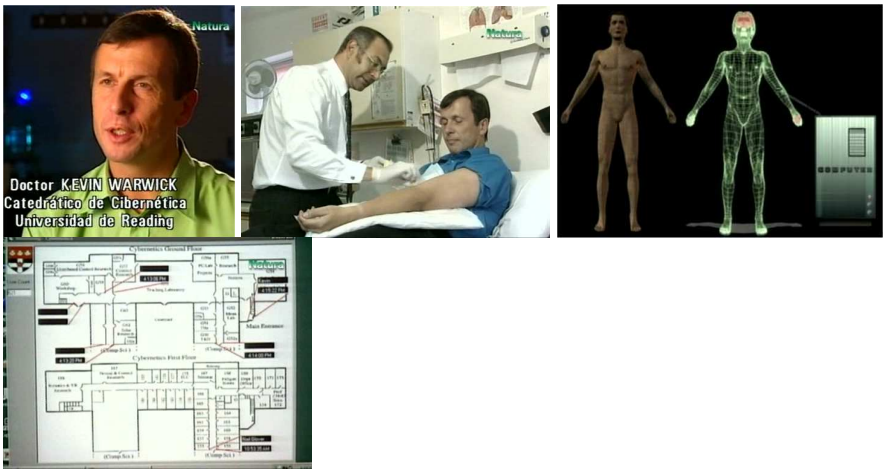


Ilustración 126. El identificador único de Ipv6 aplicado al Doctor Kevin Warwick.[109]

[108] Adriana Gomes agomes@cisco.com , Ipv6 en Ambientes Privados, y Punto de Vista en Proveedores de Servicio, Cisco Systems. (a)Higher Ed./Research: Servicios de educación, colaboración, movilidad. (b) Consumer: vides/Audio, aplicaciones, monitoreo de seguridad, juegos. (c) Manufacturing: Servicios embebidos, la industria en Internet, habilitación de componentes con Ip. (d) Trasnportation: Servicios de transito, control de tráficos. (e)Medical: Salas virtuales y atención on/line.

[109] El Doctor Kevin Warwick (Catedrático de Cibernética de la Universidad de Reading) se implanto en el brazo un chip de sílice de 25x2.5mm.un cable en espiral que funciona una señal de radio (la que da energía al cable) que envía una señal de identificación al ordenador del edificio de su Universidad de manera que este se encuentra permanentemente rastreado y monitoreado en un entorno automatizando, de manera que el profesor a su vez realiza desplazamientos controlados sin requerimientos se llaves, aparatos biométricos y cosas así; como también se sabe de la información digital que consulta por medio de su identificador único.

Ilustración 127. Identificadores de Ipv6 únicos integrados en implantes cerebrales.[110]

2.13 Apreciaciones y conclusiones referidas al capitulo segundo.

- Se presento un análisis de investigación pormenorizado de las bases tecnológicas conceptuales y los estándares internacionales, que nos servirán como instrumentos esencialmente necesarios para tener un dilucidado enfoque de comprensión con lo que respecta a la privacidad y la protección de los datos personales tratadas desde su naturaleza técnica del protocolo de Internet de próxima generación con el propósito de analizar desde una óptica tecnológica jurídica las vulnerabilidades que esta presenta, los riesgos que ofrecerá frente al carácter abierto de la red y su análisis de facilidad de uso con lo que permite realizar tratamientos invisibles que se presentan en el Internet relacionados con la interceptación de los datos o su identificación electrónica en la sociedad de la información, considerando esta última como un objeto investigación pasionaria que va mas allá de un mero esquema de análisis técnico a efectos de orientar su encuadramiento a un perfecto equilibrio de los aspectos vinculantes confirientes a la especialidad de raíz con del derecho

[110] Al tetraplegico Matiu Neguer(paralizado del cuello hacia abajo) se le inserto un implante cerebral que envía señales en los cortex motors cerebrales que se descomponen en frecuencias, creando un conmutador de interfaz denominado Brainguei una conexión directa entre su cerebro y un ordenador con un VMI(Interfaces entre cerebro y maquina); que le permite tan solo pensando controlar el computador(Navegar por Internet, jugar, procesar datos, enviar mails, chatear con su familia, … una vida virtual) a través de un microprocesador(un nodo con 100 electrodos) que se encuentra insertado en su cerebro y una interfase de computador externa haciendo de el, un hombre biónico(Una mezcla de Microchips y carne); según indica el profesor John Donoghue Co-fundador de Cyberkinetcs. En tal sentido como indica el autor de la “La bomba de calcio” y Futurólogo Douglas Mulhall “En un futuro las implicaciones tecnológicas aplicadas a la neurología serán demoledoras”.

informático[111] enfatizada a la búsqueda de perseguir un adecuado aseguramiento de la privacidad de la información y la protección de datos personales dentro del ámbito legal aplicable y que no vulnere la legislación ni los derechos y libertades que les son reconocidos a las personas. Expondremos detalladamente los elementos claves que nos servirán para establecer en los posteriores capítulos sus competencias conexas concordantes respecto a las condiciones de legalidad que IPv6 conlleva derivadas de los principales RFCs con los que en la actualidad se construyeron su ingeniería; y así lograr obtener un panorama mas amplio de las implicaciones legales que estas contraerán con el desarrollo de las nuevas tecnologías de la información, con el objetivo concreto de percibir su fuerza vinculante necesaria para tener una mayor comprensión del conglomerado de contenidos sobre el cual girara nuestro simbiótico tema de estudio.

- Concretamente se realizo un análisis de entendimiento respecto a las ventajas que ofrece el protocolo de Internet Ipv6, sus principales características, la arquitectura de su cabecera, el formato de direccionamiento, su modo de funcionamiento y sus modos de transición que servirán de base teórica para determinar la afectación que contraerá en relación con los datos personales; para luego realizar una comparación con el actual protocolo que se viene utilizando Ipv4, con el fin de realizar un paralelo detallado que nos permita determinar las directrices y factores de análisis en lo que respecta a su viabilidad del uno del otro en otorgar una mejor protección y beneficio inherente al titular de los datos; concatenado esta con el planteamiento y las definiciones de la latencia del NAT y la misma que involucra con referencia al actual protocolo, para luego continuar con el estudio de la estructura jerárquica del Internet a

[111] "Al generalizarse el procesamiento de datos, de la métrica judicial surgió, sobre todo en Europa el Derecho Informático. Este concepto lo introdujo en la enseñanza del derecho en 1970 Wilhelm Steinmuller, en la Universidad de Ratisbona en Alemania. El Derecho Informático – Rechtsinformatik – fue visto en principio como una ciencia jurídica interrelacionada con el procesamiento de datos aplicado, "applied informatics" … la inmutabilidad externa y estructura da una impresión errónea del Derecho Informático, Con el tiempo ha sufrido un cambio profundo como ciencia jurídica aun cuando la clave acoplante de la sistemática sigue siendo la Informática."" Ahti Saarempää <asaarenp@ulapland.fi> Prof. De Derecho Civil, Instituto de Informático Facultad de Derecho Universidad de Laponia finlandia, Gestión y Administración Electrónicas; enfoques del desarrollo de la sociedad jurídica de la red, clase magistral dada el 8 de agosto de 2005, con ocasión de la inauguración del Magíster en Derecho de la Informática y de las Telecomunicaciones de la Universidad de Chile.

través del modelo de referencia OSI y el protocolo TCP/IP y sus respectivos paralelos. Entrando de lleno con el protocolo de seguridad Ipsec, sus modos de funcionamiento, su arquitectura y sus políticas de seguridad confluente esta con la necesidad de adoptar especiales medidas de seguridad, como la utilización de procedimientos técnicos de cifrado y control de acceso a los archivos o informaciones que protejan los datos de carácter personal e, incluso, comprender la especial responsabilidad que tienen los agentes involucrados en los tratamientos de datos realizados a través de la red y finalmente poder demostrar y comprobar la actualísima utilización del protocolo Ipv6 aplicado a las experiencias contractuales que se presentan en tiempo en que viene siendo implantando y desplegado el protocolo mencionado.

CAPITULO TERCERO

ANALISIS DE IMPLICANCIAS DEL PROTOCOLO DE INTERNET IPV6 EN RELACION CON LA PRIVACIDAD

3.1 Aspectos preliminares en materia de Privacidad.

Antes de adentrarnos, en cualquier análisis referido al derecho a la privacidad cabe hacer una breve consideración terminológica, considerándola razonable tratarla como "Intimidad de la vida privada"[112]. Pero de todos modos, utilizaremos el termino privacidad, aunque conocemos que se trata de un anglicanismo importado del termino "privacy" utilizado de modo corriente en los Estados Unidos de América, si bien se puede desde este momento recordar que entre privacidad u "privacy" no existe la similitud que aparentemente se pueda creer[113]. Como asimismo, el termino privacidad ya figura en nuestro lenguaje corriente como sinónimo de intimidad y de intimidad de la vida privada. De ese modo, creemos que en nombre de un razonable pragmatismo y una mayor fluidez en el tratamiento del tema que se entrecruzan, la utilización del término privacidad es suficiente a los fines de la presente tesis.

---

[112] La utilización de la terminología "Intimidad de la vida privada" sirve de modo eficaz para marcar la diferencia con la vida pública. Sobre este tema ver José de Oliveira Ascensao, Dereito Civil, Teoría Geral, Vol I, Coimbra, Coimbra Editora, 1997, pags. 100-11.

[113] El contenido ético y social del termino privacidad difiere de aquel relativo a la privacy. Sobre esta diferencia ver José de Oliveira Ascensao, Teoría Geral, pag. 66.

A modo de comentario para el profesor de la Universidad de Chile, Francisco Gonzales, al consagrar la Constitución la garantía de la protección de la vida privada de las personas, "se esta refiriendo precisamente a la intimidad, en el sentido en que emplea actualmente este termino el derecho continental, esto es, incluyendo las facultades de exclusión y control"[114], en un sentido similar, el profesor Carlos Carmona indica que "el derecho a la vida privada que consagra nuestra Constitución comprende lo que la doctrina denomina derecho a la autodeterminación informativa"[115].

La intimidad en cuanto al derecho de la personalidad[116], tiene una enorme acogida en los ordenamientos jurídicos modernos. Definiendo que son aquellos que se refieren a las facultades jurídicas cuyo objeto son los diversos aspectos de la propia persona del sujeto, bien como sus emanaciones y prolongaciones[117], son todos aquellos destinados a dar contenido a la

---

[114] Agrega Gonzáles que en la doctrina comparada, aun subsiste el debate en torno a determinar si ha surgido un nuevo derecho fundamental o de la personalidad(derecho a la autodeterminación informática o libertad informática), o simplemente constatar si en la protección de la intimidad informática, no habría sino la tutela de derecho de la personalidad, tales como la intimidad, el honor, o la vida privada. Luego señala que independiente de la aceptación o no acerca de la teoría de la autodeterminación informativa, lo que importa es que de toda la discusión, el concepto de intimidad, integrado por las 2 fases; exclusión(libertad negativa) y control(libertad positiva), ha salido fortalecido y rejuvenecido.

[115] En fundamento de tal afirmación es nuevamente el concebir al derecho a la vida privada integrado por las 2 facetas; la idea de exclusión y la idea de control. Luego reafirma indicando que habría surgido un derecho implícito derivado de las libertades negativas, denominado autodeterminación informativa.

[116] Es un conjunto de idiosincrasias inherentes a cada ser humano en su individualidad, manteniendo o no este conjunto relación con la sociedad. Diversas definiciones se van sucediendo con enorme maestría, por que muchos autores conocen la dificultad de aproximarse a los distintos conceptos de la personalidad relacionados con las ciencias del espíritu y con las ciencias jurídicas. En ese sentido, recodamos, de entre muchos, Gilberto Haddad Jabur, en la obra Liberdade de Pensamiento e Directo a Vida Privada, Editora Revista dos Tribunais, Sao Paolo, 2000, cuando observa la diferencia entre las clasificaciones científicas al afirma que "… personalidad extrajuridica(psicológica, metafísica, sociológica y valorativa) es producto del ambiente, del carácter, o de la conducta. Eso lleva su formación posterior de la existencia del propio ser, lo cual no puede aceptarse para los derecho aquí vistos(Derechos de la personalidad clasificados por Hubmann como derecho a la individualidad) pues coexisten con el ser humano a partir de su primer instante…" Tambien Hegel(GWF Hegel, Principios da filosofía do directo, Martins Fontes, Rio de Janeiro, 2000, pag. 40), disponía sobre la diferenciación entre conceptos científicos de la personalidad, al afirmar que: "… la personalidad solo comienza cuando el sujeto tiene conciencia de si mismo, no como de un yo simplemente concreto y de cualquier manera determinado, sino un yo puramente abstracto y en el cual toda delimitacion y valor concreto son negados e invalidados. Es de ese modo que en la personalidad existe el conocimiento de si mismo como de un objeto exterior, elevado por el pensamiento al infinito simple y, por lo tanto , puramente idéntico a ella. Los individuos y los pueblo es no tiene personalidad en cuanto no alcance ese pensamiento y ese puro saber de si mismo…". Evidentemente tal constatación se encuentra bien alejada de una confluencia entre la definición de la personalidad en cuanto institución jurídica y demás ciencias del espíritu. La problemática referida a la definición de los derechos de la personalidad es tal que prácticamente cada autor posee su propia sistematización. Algunos merecen consideración. Recordemos la definición de Rubens Limongi Franca en su Manual de Dereito Civil, #ea edcion, Sau Paulo, editora revista dos tribunais, 1975, pag. 253, que nos parece exhaustiva, pero también muy prolija y de una subdivisión desnecesaria. Aquella que nos propone Heinrich Hubmann parece la mas eficiente, hasta el presente momento. Es preciso recordar, asimismo, el extenso estudio denominado "O directo geral de personalidade", defendido por Capelo de Souza en su tesis doctoral en la Universidad de Coimbra y que posee un cierto numero de adeptos en esa escuela. Sin embargo, creemos, como lo dicho, que la mejor clasificación es la de Hubmann.

[117] Rubens Limongi Franca, Manual de Directo Civil, 3ra edicion, Sao Paulo: Editora Revista dos Tribunais, 1975, pag. 404.

personalidad[118], son manifestaciones parciales de la personalidad humana[119], son condiciones esenciales a su ser y devenir[120], son aquellos que atienden a manifestaciones de las personalidades en si mismas[121 - 122]. Es preciso poner el acento en la grave dificultad en todo y cualquier tipo de estudio concerniente a los derechos de la personalidad[123].

Se considera en todo caso que existen 3 sustratos iusfilosóficos que se constituyen como paradigmas relacionados con la comprensión de esta categoría de derechos. En primer lugar, la diferenciada "visión de mundo"(cosmovisión)[124] inherente a cada ser humano, ya que gran parte de los bienes jurídicos tutelados por los derechos de la personalidad son bienes que requieren una interpretación subjetiva[125]: el honor, la privacidad, la imagen en cuanto atributo. El individuo estará necesariamente sometido a la historia. El nunca es alguien aislado del mundo que lo rodea. En segundo lugar se reputa relevante la cuestión de los conflictos entre derecho de la personalidad, como por ejemplo el derecho a la información (Especialmente el derecho de informar)[126] y el derecho a la privacidad. Y finalmente el tercero es la actualísima discusión acerca de conflictos éticos[127].

No hay nada más individualmente determinable que los aspectos inherentes a la privacidad de una persona, a su intimidad. Un alejamiento confortable del mundo exterior por parte del titular del derecho a la privacidad, solo puede darse o desearse, por el mismo. Y esto ocurre en cualesquiera modalidades,

---

[118] Adriano de Cupis, I Diritti della Personalitta, Milan, Giuffre Editor, 1958, pag. 19.
[119] Rabindranath Capelo de Souza, O Directo Civil. Teoria general, pag. 67.
[120] Orlando de Carvalho, os Directos do Homem no Directo Civil Portugues, Coimbra: Coimbra Editora 1973, pag. 25.
[121] José de Oliveira Ascensao em Directo Civil. Teoría General, pag. 67.
[122] Podríamos conjugar nuestra definición de personalidad con el objeto de la tutela del derecho. De ese modo, tendríamos como definición de los derechos de la personalidad una suma de derechos que tutelan un conjunto de cualidades inherentes a cada ser humano en su individualidad, manteniendo o no este conjunto relación con la sociedad.
[123]Es preciso destacar que los derechos de la personalidad abarcan un espectro de enorme magnitud y suscitan una enorme complejidad clasificadora.
[124] Weltasschung.
[125] Humann como derecho a la individualidad. Apud Oliveira Ascensao em Directo Civil, Teoria peral, p. 97.
[126]Aunque algunos autores no consideran el derecho a la información como un verdadero derecho de la personalidad, este acaba siendo un conflicto siempre presente en esta materia.
[127]Desde ya se puede poner de manifiesto algunos conflictos: la posibilidad de acceder a correos electrónicos, la determinación del uso de las bases de datos, el control de información sensible,… y el rastreo del comportamiento de las personas, por parte de gobiernos o grandes corporaciones y sin fin de terceras partes con diferentes intencionalidades.

sean referidas al mundo real o no[128]. De ahí la importancia del derecho a la privacidad, ya que el derecho debe tutelar el alejamiento exigido por el titular del derecho a la privacidad[129].

El protocolo de Ipv6 en la comunicación en la red de redes trae consigo un grave problema en lo que se refiere a la privacidad como por ejemplo en los nuevos escenarios con la telefonía IP consecuente con el intercambio de datagramas en la red, ya que se presentaran distintas situaciones de análisis en los encuadramientos e interpretaciones legales en materia de las nuevas tecnologías, como es el caso de las herramientas de criptofonía a saber, que son "procedimientos de cifrado que pueden ser aplicadas a muchas cosas, como en las comunicaciones de telefonía IP por voz o fax que pueden también ser objeto de espionaje"[130], incorporándose así, también como buenas candidatas a su regulación, en materia de la privacidad de datos. Afectando de esta manera la tenue línea divisoria entre el ámbito de lo público y lo privado consiguientemente, encontrándonos de frente con la dificultad de definir cuando cada una de estas realidades estará presente. Surgiendo en la actualidad elementos de confrontación social antes inimaginables. Basta percibir que hace tiempo siquiera se podría suponer el intercambio de mensajes electrónicos o sus grupos de discusión hoy están presentes en el ámbito de la red de Internet o también específicamente en las comunicaciones a través de las redes de académicas de avanzada como "Ca*Net4(la red Canadiense de investigaciones), ALICE(La red de América Latina Interconectada Con Europa), GEANT(La red Multi-Gigabit Europea con Euro-Tap, PVNs y servicios para investigadores y experimentos complejos), Internet2, redClara, APAN(la red avanzada del Pacifico Asiático para la investigación y el desarrollo de aplicaciones y servicios de redes avanzadas en la región del Pacífico Asiático con un sistema de hub Internacional y ligas backbone conectadas al sistema de hub internacional)"[131] como planteo el

[128]Aunque se refiera a la red de redes, también en este universo solamente podrá ejercer el alejamiento y el mantenimiento del universo privado el titular del Derecho que, son dudas, es el único autor de esa elección.
[129]Sin el extremismo propuesto por el "Right of privacy".
[130] José Antonio Millán, http://ingenieria.uchile.cl/boletin/noticia.php?id=7093
[131] Florencio I, Utreras <utreras@redclara.net> , en el marco del Magíster en Derecho Informático y de las Telecomunicaciones realizado por el CEDI de la Universidad de Chile, con el tema "Internet, una Urgencia País en su Adopción", 2005.

Prof. Florencio I. Utreras y en la actualidad la GEANT2 (Sucesora de la GEANT que es la red mas rápida del mundo, con cable de fibra óptica oscura, que utiliza luz pulsada (fotones) en vez de electrones para la transmisión de datos. La fibra oscura permite a la principal red de investigación y educación del mundo alcanzar velocidades de transferencia de hasta 320 gigabits al segundo, lo que supone que unos tres millones de usuarios en 34 países podrán disfrutar de esta potencia informática sin precedentes), que se encuentran en la actualidad diseñadas con doble infraestructura, es decir con soporte Ipv4 e Ipv6 nativo, como así mismo con sus dualidades hibridas Ipv4-Ipv6/Ipv6-Ipv4 pensado en un despliegue mas optimo; traendo así, a colación connotaciones de regulación aun mas delicadas en materia de privacidad, ya que la transferencia de información en estas redes académicas es de carácter mas sensible al convencional y de un trafico de información con características potencialmente masivas en tamaño.

Ahora de otro lado, desde el contexto de la percepción del Prof. Manuel Sánchez de Diego[132] como nos indica, “se debe prestar el debido énfasis en el impacto de los medios de comunicación en el Internet” con respecto a la penetración de la sociedad de la información y de la multitud en el universo privado que puede estar siendo en la actualidad, efectivamente, más incisiva o incluso más violenta; como es el polémico informe a Google en el tratamiento de la privacidad de los usuarios presentado en 06/07, donde el buscador más popular del mundo, está con los enfrentamientos con la organización independiente de activistas Privacy International a raíz del informe de privacidad, elaborado por dicho grupo[133]; o las actuales

[132] Acentuado en la connotación, respecto a las responsabilidades de los proveedores de acceso, los proveedores de servicios y los proveedores de contenidos concernientes al análisis de su tratamiento jurídico. Manuel Sánchez de Diego, en el marco del Magíster en Derecho Informático y de las telecomunicaciones, realizado por el CEDI de la Universidad de Chile, con el tema “Medios de comunicación en Internet” 14 de diciembre del 2005.

[133] El estudio, denominado 'A Race to the Bottom-Privacy Ranking of Internet Service Companies', situaba al buscador en última posición en una lista de una veintena de grandes compañías de Internet, y calificaba el comportamiento de la compañía de "hostil" con respecto al mantenimiento de la privacidad de sus usuarios. De hecho, prácticamente todas las empresas estudiadas, como Amazon, apple, BBC, eBay, Microsoft o Yahoo!, tienen una política de privacidad que hacen poco por proteger a sus usuarios, de acuerdo con el informe. Pero Google aparece como la peor de todas, según se han echo eco diversas publicaciones (http://news.bbc.co.uk/2/hi/technology/6740075.stm) a lo largo del día. La respuesta del buscador no se hizo esperar, alegó que el informe había malinterpretado los servicios y que la compañía trabaja duro para preservar la privacidad de sus usuarios. "Estamos decepcionados con el informe, que está basado en numerosas imprecisiones y malintepretaciones de los servicios", comentó Nicole Wong, consejera de Google. Conscientes de que colocar a Google al final de la lista iba a ser controvertida, Privacy International justifica la decisión por la enorme cantidad de

herramientas tecnológicas denominadas “motores de búsqueda” como es el caso del conocido buscador de datos personales que extrae información de las redes sociales del Internet Wink (www.wink.com)[134] que identifica ya más de 200 millones de personas, o el reciente “motor de busca personas” creado por el investigador de seguridad Sudafricano Roelof Temmingh llamado Evolution[135] que aplica técnicas sofisticadas de “datamining” para la toma de decisiones y la selección de información personal del banco de datos encontrado[136], y finalmente el futuro motor de búsqueda de personas denominado « Spock »[137] que no solo indexara los datos personales de manera automatizada sino también que prevén en futuro utilizar a personas para corregir datos o ampliar perfiles que el sistema automático no permite procesar adecuadamente. Siendo estos sistemas computacionales de búsqueda instrumentos potencialmente tecnológicos usados para rastrear información con mayor precisión, de manera mas agresiva ya que implícitamente también afectan a nuestra privacidad.

Es decir, comportamientos inherentes a la red de redes que en muchas ocasiones originan un distanciamiento social ficticio, visto que la intangibilidad trae consigo una cierta insensibilidad en cuanto a la observación del otro. Tal hecho ocurre como consecuencia del escudo protector erigido por la pantalla

---

datos que recopila el buscador de cada usuario, porque su política de privacidad es incompleta y por la escasez de las respuestas frente a las quejas. Por si fuera poco, el grupo activista acusó a Google de haber tratado de ejercer presión sobre determinados periodistas antes de la publicación del informe, con quienes contactaron para 'asegurar' que Privacy International "tiene un conflicto de intereses respecto a Microsoft". En una carta abierta al presidente de Google, Eric Schmidt, Privacy International defiende su independencia (www.privacyinternational.org/article.shtml).

[134] Wink es un buscador que integra resultados etiquetados desde distintas fuentes. Así para una búsqueda determinada, además de los resultados convencionales de un buscador (proporcionados por Google), añade los proporcionados por la red social de usuarios: aquellos etiquetados (Wink permite tanto etiquetar directamente como sincronizar con la cuenta) y puntuados, ordenados según la popularidad entre los usuarios. Además ofrece conceptos relacionados para cada término y destaca los resultados ofrecidos por la Wikipedia, aunque propone un wiki propio complementario. En cada búsqueda distingue los resultados "by google" de los "by Wink".

[135] Roelof Temmingh**,** creó una nueva herramienta de búsqueda llamada “Evolution” que busca y recolecta datos personales a través de sitios Web, motores de búsqueda, y sitios de redes sociales. Tipeando una dirección de correo personal, por ejemplo, puede dar con una dirección IP o el número de teléfono del hogar del implicado a través de la búsqueda en sitios de registros de dominio o sitios de redes sociales 06/2007, publicada en las noticias de CLCERT Chile http://www.clcert.cl/show.php?xml=xml/noticias.xml&xsl=xsl/lista_extend.xsl

[136] http://www.linux.com/feature/118798

[137] El nuevo enemigo del Web acaba Spock.com hecho en efecto, pretende ser un motor especializado en la búsqueda de personas, lo que se entiende una reunión de datos más o menos privadas a escala mundial. Una empresa sorprendente, mientras que Google, Microsoft o AOL han visto repetidamente apuntan del dedo por haber utilizado los datos privadas. Pero el concepto es diferente. *Spock es el líder en la búsqueda personal en línea, ayudando a los usuarios de encontrar y descubrir la gente. Con más de 100 millones de personas ya indexadas, y varios millones añadieron cada día, spock está elaborando el más grande y poderoso Motor de búsqueda especializado sobre la persona*, http://kontrib.com/get_translation.php?story_id=6075&lang_id=3&frame=main

del ordenador. Es decir, la sensación de invisibilidad derivada del referido escudo protector se proyecta sobre las sensaciones reales de determinados usuarios, y estos tienen la sensación de que no pueden ser observados por otros usuarios o actores. Realmente no pueden ser visualmente encontrados, pero pueden ser rastreados[138]. Y hallados. Como la actual propuesta de discusión "Operational Point Of Contact (OPOC, Punto de contacto Operacional)"[139]que se encuentra en la mesa directiva del ICANN donde WHOIS pretende mostrar la información de terceros en vez de la suya. En consecuencia en esta problemática de rastreo, parece existir una cierta confusión entre el mundo real y el mundo virtual, bien como entre las sensaciones inherentes a cada uno de ellos, en una especie de esquizofrenia cibernética[140]. Este aspecto adquiere extremada importancia en lo que concierne a la privacidad en la red de redes, pues encela que muchas actuaciones, en las que determinados agentes tal vez no busquen efecto en el mundo real, lo hacen posible por el simple hecho de que esos mismos agentes se encuentran detrás del citado escudo protector en el que se ha transformado la pantalla del ordenador.

---

[138]Algunos técnicos afirman que los hackers, los crackers u otros delincuentes informáticos en general pueden, si así lo desean, no dejan ningún rastro. Otros afirman que hay una imposibilidad total de no dejar rastros, hecho que haría imposible el crimen perfecto en Internet. El hecho es que podemos observar, con frecuencia, la busca de entidades gubernamentales y grandes empresas por la contratación de jóvenes y adolescentes lo cuales, ellos mismos, acabarían por ser responsables del derribo de la seguridad de sus posibles futuros empleadores.

[139] El grupo de trabajo de WHOIS envió recientemente su informe final sobre una propuesta para permitir a los que registran nombres de dominio mostrar información de contacto de terceros en vez de la propia. Algunos dueños de nombres de dominio usan un servicio de proxy que les permite mostrar la información del proxy en vez de su información. La propuesta, conocida como Operational Point Of Contact (OPOC, Punto de contacto Operacional), ha sido resistida por fiscales y abogados de comerciales y de propiedad intelectual. El consejo del Generic Names Supporting Organization (GNSO) está discutiendo si recomendar o no la propuesta. http://www.clcert.cl/show.php?xml=xml/noticias.xml&xsl=xsl/lista_extend.xsl

[140]Cibernética es la ciencia que se ocupa de los sistemas de control y de comunicación en las personas y en las máquinas, estudiando y aprovechando todos sus aspectos y mecanismos comunes. El nacimiento de la cibernética se estableció en el año 1942, en la época de un congreso sobre la inhibición cerebral celebrado en Nueva York, del cual surgió la idea de la fecundidad de un intercambio de conocimiento entre fisiólogos y técnicos en mecanismos de control. Cinco años más tarde, Norbert Wiener uno de los principales fundadores de esta ciencia, propuso el nombre de cibernética, derivado de una palabra griega que puede traducirse como piloto, timonel o regulador. Por tanto la palabra cibernética podría significar ciencia de los mandos. Estos mandos son estructuras con elementos especialmente electrónicos y en correlación con los mecanismos que regulan la psicología de los seres vivientes y los sistemas sociales humanos, y a la vez que permiten la organización de máquinas capaces de reaccionar y operar con más precisión y rapidez que los seres vivos, ofrecen posibilidades nuevas para penetrar más exactamente las leyes que regulan la vida general y especialmente la del hombre en sus aspectos psicológicos, económicos, sociales etc. Giovanny Guillén Bustamante, Cibernética, Conceptos y definiciones, Caracas-Venezuela, giovanni.guillen@Eniac.com

Existen 4 principales modalidades de manifestación de comunicaciones en la red o aplicaciones de Internet susceptibles de revelar datos de carácter personal visibles[141], a saber:

1. Los sitios Web: Que son direcciones de localización en la world wide web que contienen documentos de páginas web organizadas jerárquicamente.
2. Grupos de discusión: Son aplicaciones web que dan soporte a discusiones u opiniones en línea. Son los descendientes modernos de los sistema de noticias BBS(Bulletin Board System) y Usenet, muy populares en los años 1980 y 1990. Por lo general los foros en Internet existen como un complemento a un sitio web invitando a los usuarios a discutir o compartir información relevante a la temática del sitio, en discusión libre e informal, con lo cual se llega a formar una comunidad en torno a un interés común. Las discusiones suelen ser moderadas por un coordinador o dinamizador quien generalmente introduce el tema, formula la primera pregunta, estimula y guía, sin presionar, otorga la palabra, pide fundamentaciones y explicaciones y sintetiza lo expuesto antes de cerrar la discusión. Se presenta plataformas como phpBB, vBulletin, Invision power board, MyBB, SMF, YaBB, Ikonboard, UBB, JavaBB, Accurate Monitor for S&E BBPress, Eboard Red Fox Edition, InvisionFree y otros. Algunos CMS (*Content Management System* / Sistemas de administración de contenido) como Drupal, Superblogging, Joomla, RC DotNetNuke, Mambo, PostNuke, Typo3, XOOPS (eXtensible Object Oriented Portal System), etc. que son las que incluyen sus propios grupos de discusión o integran foros de otros sistemas.

3. Envío-Recepción de mensajes electrónicos: Que son correos electrónicos en inglés “electronic email” o e-mail, que son métodos para crear, enviar y

[141] Cuando se habla de aplicaciones de Internet nos estamos refiriendo a todas aquellas herramientas de Internet en las que se recoge información del usuario, con o sin su consentimiento y, debemos distinguir entre los tratamientos visibles(herramientas de Internet en las que se recoge información de los usuarios con su consentimiento, esto es aquellos elementos donde se recoge información sobre los usuarios claramente en la red) y, los tratamientos invisibles(tratamiento de datos personales sin consentimiento por parte del usuario, ya que va mas allá de los datos nominativos que circulan en la red).

recibir mensajes a través de sistemas de comunicación electrónica, citando por ejemplo Gmail2, Adolix, Outlook Express, Automatic Email Autoresponder, Mailbox Digger, AnnoyMail, JDVoiceMail, HandyBits Voice Mail, IncrediMail Xe, OpenP2M, Durie, Mail Them, Atomic Mail Sender, FoxMail, El Cartero, NetMail, E-milio, Mail PassView, MiListaCorreo, etc. con una lista inagotable.

4. Grupos de conversación: Salas de Chats o plataformas IRC(Internet Relay Chat) es un protocolo de comunicación en tiempo real basado en texto, que permite conversar con personas en forma de texto dentro de canales de salas en grupo o de forma privada, donde los mas usados son: Microsoft NetMeeting, mIRC, IRcap, ircN 7.08t, Orbital Script, ICQ, ICQBack, ICQBackup, ICQ Plus, Microsoft Comic Chat, Chat Character Pack para Comic Chat 2.0, MSN Messenger Service, Active Worlds, Cu-SeeMe, VDOPhone, WebCam32, Pirch 98, … entre otros.

A través de cada una de estas manifestaciones se observa la posibilidad de lesiones a la privacidad. Por consiguiente, para determinar la naturaleza pública o privada de una comunicación por las redes, es necesario el análisis de algunos criterios como:

1) La identificación del destinatario del mensaje.
2) El conocimiento de la cantidad de personas involucradas en comunicación.
3) El conocimiento de la relación de intimidad entre las personas participes en la comunicación.

De esta forma, la violación de la privacidad en la Internet tiene lugar por lo tanto:

1) Cuando hay un desplazamiento de dato(s) o información(es) de un ambiente de comunicación privada a un ambiente de comunicación publica.

2) Cuando hay un desplazamiento de datos o informaciones de un ambiente de comunicación privada para un ambiente de comunicación privada del cual el titular de los datos o informaciones no forme parte.

En este momento, nos parece que los planteamientos sobre la violación de la privacidad siguen un modelo general, lo cual facilita el análisis de la casuística. A pesar de la obviedad, no se puede olvidar que la autorización por parte del titular de los datos o informaciones para efectuar un desplazamiento de estos, no permitirá configurar una violación. Este deberá ser el modelo general. Y desde ya podemos analizar algunos casos, a saber: (1) mensaje de correo electrónico puestas a disposición en un sitio web sin autorización, fueron desplazadas de un ambiente privado a uno publico, podrían violar la privacidad del remitente y, posiblemente, la del destinatario; (2) mensajes enviados para un grupo de conversación privada entre dos amigos que son puestas a disposición del grupo de conversación abierta, cuyos participantes no poseen entre ellos una misma relación de intimidad podrán llevar a la violación de la privacidad. Estos son tan solo algunos de los incontables ejemplos posibles y como poseemos un modelo general, dependemos del desarrollo tecnológico para solucionar todas las posibilidades. En este momento, estamos enclaustrados y a disposición de la casuística.

Pasando de otro lado, un punto particularmente interesante es la confrontación y encuadramiento entre las posiciones adoptadas por EEUU y la Unión Europea en tal temática, bien como el tratamiento diferenciado del control efectivo en contra de actos de violación de la privacidad. Por así decir, mientras que EEUU pretende, por diversos motivos, un tratamiento legislativo menos exigente y una mayor autorregulación; por su parte, la Unión Europea se presenta más incisiva en la protección de la privacidad, en especial en lo que se refiere a los datos personales.

a) **Unión Europea(Sistema de Heterocontrol)[142].** Con respecto a la protección constitucional a los temas de privacidad y los datos personales. Creemos que la protección constitucional, además de todo peso y valor que aporta a los temas que ampara, colabora en la disminución de la discrepancia entre la tutela de aspectos relacionados con la tecnología y su respectiva tutela jurídica. En el ámbito Europeo, naturalmente más conservador que los EEUU parece existir una mayor protección de la privacidad, especialmente en lo referido a los datos personales. Parece también que la Unión Europea practica una protección más efectiva que otros países. En este momento, es necesario recordar que la tutela jurídica de temas relacionados con la tecnología, sea en los EEUU o en la Unión Europea o cualquier otro ámbito, acaba por no acompañar la velocidad del propio desarrollo tecnológico; pero esta es una situación de hecho que forma parte del cruce entre Derecho y Tecnología, y que necesita ser interpretada, con vistas a no permitir esa deficiencia en el estudio, aunque no siempre seamos capaces de hacerlo. Todavía en lo tocante a la discrepancia entre la urgencia de la tutela de temas tecnológicos y el retraso de las ciencias jurídicas, cabe recordar que el universo comunitario Europeo trae un nuevo obstáculo, cual es la necesidad de implementación del tenor de las Directivas comunitarias y el plazo que corresponde a países miembro para que lleven a cabo dicha transposición. De todas formas, lo que nos parece ser de mayor valía es el hecho de que hay textos constitucionales que tutelan la privacidad desde un amplio espectro incluido en la privacidad en las comunicaciones y, por fin, la privacidad en los que se refiere a los datos personales.[143]

---

[142] El sistema de protección fomentado por la Unión Europea-plasmado en el Convenio 108 y, especialmente, en la Directiva 95/46/CE además de prever mecanismos de autocontrol, la normativa interna de los Estados contempla entidades y procedimientos a través de los cuales se verifica el cumplimiento de la legislación sobre tratamiento de datos personales, un control radicado en seda administrativa por la denominada "autoridad de control", ante la cual formular reclamación, a fin de que esta abogue por el cumplimiento de la normativa, sea interviniendo como mediadora entre las partes, o bien ejerciendo facultades fiscalizadoras y aun sancionatorios, en su caso.

[143] Es forzoso recordar que, de hecho, la protección de los datos personales no es una especie del genero derecho a la privacidad, aunque por otro lado, son temas que se correlacionan de tal modo que la tenue división entre las materias acaba por no estar debidamente establecida lo cual dificulta de sobremanera cualquier estudio concerniente a los temas aludidos. Así se hace prudente afirmar que diversas constituciones, como se podrá observar en seguida, prevén el derecho a la privacidad(pura), otra la privacidad en los medios de comunicación y algunas, con una concepción mas amplia acaban por constitucionalizar la protección de datos personales.

En lo concerniente a la protección de los datos personales en el ordenamiento jurídico Europeo, observamos la presencia de una doble vía de protección(Vía normativa[144] y vía administrativa[145]). Entendemos que esta doble vía es necesaria, visto que corresponde a la actuación de los órganos gubernamentales responsables de la protección de los datos personales, bien como a la protección legislativa, impuesta por la necesidad de transposición interna del tenor de la Directiva 95/46/CE.

b) EEUU(Sistema de Autorregulación o Autocontrol)[146]. Las razones por las que parten los EEUU sobre la privacidad son absolutamente actuales y especialmente problemáticas. Ello se debe al hecho de que EEUU es el país de mayor presencia en Internet. Esta posición en el ranking es valida para el número de usuarios y para el número de empresas actuantes en el mercado on-line. Visto que nos colocamos en la posición Europea, las divergencias con el modelo americano pueden ser observadas desde varios ángulos. Mientras en la Unión Europea la tutela del derecho a la privacidad en Internet se viene presentando como una tutela mas rígida, desde la protección constitucional hasta las leyes nacionales, pasando por las disposiciones comunitarias; en EEUU se basa en el control de la privacidad y del tratamiento de los datos personales a través de la denominada autorregulación o auto vigilancia(self surveillance), siendo

[144] La vía Normativa es aquella establecida por los ordenamientos jurídicos desde el primer caso de la Ley Sueca de 11 de mayo de 1973, denominada datalagen. Desde entonces los países europeos vienen buscando el establecimiento de vías normativas con relación a la protección de datos personales. Así siguiendo el modelo Sueco, Alemania(1977), Francia(1978), Noruega(1978), Dinamarca(1978), Austria(1978), Luxemburgo(1978), Islandia(1979), y Portugal(1991). Así vía normativa es la que pretende el control a través de la aplicación de principios previstos en el ordenamiento legal.

[145] La vía Administrativa, es aquella ejercida por los órganos responsables del control del tratamiento de datos personales. Que se encuentra prácticamente en todo el territorio europeo, debido a los principios del desarrollo de la Unión Europea. Y ello porque no se puede olvidar que los movimientos Transfronterizos tal vez sean el principal componente en lo que se refiere a la problemática del tratamiento de los datos personales, preocupación ciertamente presente en los países de Europa que procuran también evitar el aparecimiento de los denominado paraísos de datos. Los objetivos de los órganos gubernamentales es, en la medida de lo posible, armonizar el control del tratamiento de los datos personales, en gran medida consecuencia de la actual facilidad de transportar enormes ficheros por la red de Internet, hecho que puede traer consecuencias de enorme gravedad par los ofendidos.

[146] El Sistema de control diseñado por la “Privacy Act” y un farragoso entramado de normas que regulan el tratamiento de datos personales descansa en la filosofía de entregar el resguardo del cumplimiento de la normativa a los propios sujetos que intervienen en el, ya sea mediante el control individual ejercido por el titular de los daos(a través del ejercicio de los derechos de información, acceso y rectificación, previo al accionar ante tribunales de Justicia) o bien des responsable en su tratamiento, mediante la adopción de código de conducta y demás medidas conducentes a cerciorarse de que en el tratamiento realizado al interior del banco se respeta la normativa por si o mediante funcionarios subalternos.

una vía de control mas permisiva que la Europea. En los EEUU, el derecho a la privacidad esta construido sobre la base de políticas de privacidad definidas entre las empresas y los consumidores a través de garantías proporcionadas por los sitios Web de que informaciones relacionadas con los usuarios no serán puestas a disposición de terceros. Debido a esta relación directa entre usuario y sitio Web, las garantías son proporcionadas incluso a través de empresas emisoras de certificados de seguridad sobre la privacidad de los usuarios. Un ejemplo es la empresa e-Trust[147].(Vale aclarar que el término Trust es una voz inglesa que significa "confianza", donde la primera combinación que adoptó esta forma fue en la Standard Oil Trust, fundada en 1882. Y en 1890 en el Acta Sherman se declaró ilegales a los *trusts* en los Estados Unidos de América). Eventualmente nos parece que en aquel país, por consolidar una tradición de oferta de todo y cualquier tipo de servicio o producto, se permite que la circulación de datos e información generalizadas sobre las personas están siempre activa. Este hecho no deja de causarnos cierto asombro, visto que EEUU es el padre del Right of privacy, el ya denominado derecho de los egoísmos privados[148].

c) Confrontación entre posiciones Norteamericana y Europea. Se deduce que la directiva Europea cuida del tratamiento de los datos

[147] www.etrust.com El sitio web de la empresa e-trust afirma, sobre el sello de privacidad TRUSTe's… cuando se ve el sello de privacidad TRUSTe's se puede tener la seguridad de que tendrá el control sobre los usos de sus informaciones personales con el fin de proteger su privacidad.

[148] De todos modos se sabe que en EEUU se compra y se vende todo, y para un mercado consumidor con estos, paradigmas, es necesario que haya ofertas constantes de nuevos productos y servicios. Tal ves el aspecto tan destacadamente consumista de la sociedad americana lleve a la necesidad de una atribución directa de responsabilidades entre las partes involucradas en la relación comercial. Así, el vendedor se relaciona directamente con el comprador, con un mínimo de interferencia externa posible. O sea, las políticas de privacidad entre las partes tienen un efecto que es verdaderamente regulador del mercado bajo un lógico orden jurídico. En todo caso, en el tratamiento del tema de la privacidad, especialmente en Internet, el sistema basado en políticas de privacidad, a pesar de ser extremadamente criticado, es el que viene siendo mas utilizado. Como cualquier sistema abarca errores y aciertos. El hecho es que nos parece que los errores referidos a este tipo de construcción técnica jurídica parece no permitir una segunda oportunidad y, en ese sentido desde ya nos preocupa un punto: El tráfico indiscriminado de los datos personales, así como la indistinta comercialización de ficheros. Es de todos conocido que el comercio agresivo tiene una presencia constante en EEUU, de modo que no nos sorprende que no hubiese una comercialización a lo largo de un largo espacio de tiempo de nuestros datos. Ejemplos de tales (1)e-tour vendía informaciones personales de los usuarios a Ask-Jeeves. (2)Amazon.com recogía datos de los usuarios invertidamente de manera deliberada. (3) Toy-Mart al entrar a quiebra rompe sus políticas de privacidad y comercializa sus bases de datos por considerar tal información patrimonio de la empresa.

personales, el Art. 6 de la directiva define los principios relativos a los datos personales, siendo que los que nos interesan quedan definidos en el inciso 1,a, b y e. este articulo determina que los Estados miembros deberían establecer que los datos personales posean determinadas cualidades en su tratamiento, tales como: que sean objeto de un tratamiento leal y licito(letra a), que sean recogidos para actividades determinadas, explicitas y legitimas, y que no vengan a ser posteriormente tratados de forma incompatible con esas finalidades(letra b), así como que sean conservados de forma a permitir la identificación de las personas en causa a penas durante el periodo necesario para la persecución de las finalidades para lo que fueron recogidos o para lo que serán tratados posteriormente(letra e). Por lo que se refiere al tenor de la letra b podemos concluir por el tratamiento, en este caso la recogida, sin atención al principio de efectuarla para actividades determinadas, explicitas o legitimas. No nos parece una actuación legitima que una empresa recabe datos personales para después comercializar con otra(En cuestión de las cookies)[149]. Por consiguiente se percibe que la determinación de la directiva no permitirá el tratamiento de datos personales en el esquema de los casos titulares de los datos tratados. Como se hizo evidente, también la privacidad acaba por ser violada en el tratamiento de la materia en EEUU, a través de la política de privacidad. Como recordamos que el principal destinatario de este tema son los EEUU, cabe decir que en ese país la materia se trata a través de la modalidad de autorregulación, no creemos que este país pueda ofrecer una protección adecuada de acuerdo con las exigencias europeas. Ahora bien, la propia directiva acaba por exigir, en el siguiente número del mismo artículo, la apreciación:

… de todas las circunstancias que rodean la transferencia o el conjunto de transferencias de datos…

[149] El hecho de no comunicar esta situación a los clientes ya seria también suficiente para suscitar la inexistencia de una declaración explicita. Y si al hacerlo tenia como objetivo formar su propio fichero, la comercialización con terceros no parece ser una actividad previamente determinada, incluso porque creemos que en este caso es posible que los usuarios recusasen proporcionar los datos necesarios a los bancos de datos. Y, además de no ser una actividad determinada, permitiría la identificación de las personas cuyos datos fueron recabados para mas allá del periodo de tiempo necesario para la consecución de las actividades para las que fueron recogidos(Previsto en la letra e).

Preguntamos si un país en el cual 64 sitios oficiales[150] utilizan cookies[151](Son los ficheros de datos guardado en un directorio especifico del ordenador del usuario. Se crean por los servidores web con el objeto de ser enviados a los programas navegadores del usuario, y así recoger la información que dicho fichero ha reunido[152]) para obtener acceso a informaciones relacionadas con sus ciudadanos puede pretender que este comportamiento presente un nivel de protección adecuado. Tratándose de la transferencia de datos que tienen por base Internet, nos parece que, si no se tienen en cuenta por parte de los europeos los planteamientos norteamericanos y se hace un esfuerzo para aceptar algunos aspectos del tratamiento de la materia que estos hacen, los problemas continuaran por mucho tiempo. Ahora bien, hecho este planteamiento, cabe recordar algunas diferencias que fortalecen la disparidad del tratamiento del tema entre EEUU y la Unión Europea. En los EEUU, el Right of privacy parece imperar sobre cualquier derecho. En Europa existen un mayor equilibrio entre los llamados derecho de personalidad. En los EEUU existe una política de libertad y de des-responsabilización de los proveedores de servicios para Internet. En Europa, por lo general, la tendencia es la contraria. También es preciso poner atención en que mas allá de todas las divergencias, es preciso comprender que además de los sistemas jurídicos las políticas así como todo el espectro social son diferentes. Aun así, parece que tanto los EEUU como la Unión Europea tienen interés en preservar la privacidad de sus ciudadanos, aunque orienten sus esfuerzos en sentidos eventualmente contrarios.

d) Chile. En Chile se dice que la privacidad y el anonimato digital se encuentran también débiles en general por que al navegar por Internet revelamos el tipo de Browser que utilizamos, el sistema operativo de nuestra computadora, el idioma por defecto, el último sitio visitado, la dirección IP dinámica de su equipo en ese momento, el dominio de su

[150] En una encuesta reciente divulgada en www.groups.yahoo.com/group/dereito-einternet/message/292
[151] La palabra cookie significa, literalmente, “galleta”, y se trata de una tipica jerga informatica anglosajona.
[152] Ramos Suarez, Fernando. “¿Es legal el uso de cookies?”, www.iec.csic.es/criptonomicon/articulos/expertos21.html

proveedor, la resolución de su monitor y la cantidad de colores. Luego, gracias a las tecnologías de tratamientos de datos invisibles como las Cookie's, web bugs, archivos LOG[153], revelamos las preferencias de nuestras navegaciones y finalmente cuando solicitamos un producto o servicio entregamos nuestra identidad, haciéndonos totalmente identificables para las empresas, con nuestros gustos, preferencias, etc. En la actualidad, incluso nos encontramos con la existencia de herramientas tecnológicas destinadas a vulnerar nuestra privacidad, ejemplos como CommView 5.3 build 523(Que es un programa para el monitoreo de las actividades de Internet y de una Red de Área Local (LAN), capaz de capturar y analizar paquetes de red. Recopilando información acerca de los datos que pasan por tu Ethernet, Ethernet Inalámbrico o adaptador de dial-up y decodifica los datos analizados. Pudiendo así, ver la lista de conexiones de red, estadísticas vitales de IP y examinar los paquetes individuales), Nico Network Traffic Monitor 1.03 (Que permite saber que procesos generan tráfico de red (TCP/IP) y en que puertos es generado el tráfico. El programa muestra información detallada para cada proceso, incluyendo la ruta del ejecutable de proceso, la dirección IP remota y el nombre de dicha dirección IP; colocando un icono animado en la barra de sistema, que muestra cuando se genera tráfico. También entregando una revisión histórica del tráfico), Analyzer 3.0(Que es un analizador de redes, totalmente configurable, que muestra por gráficos la información sobre paquetes de datos capturados en la red. El programa es capaz de capturar paquetes en todas las plataformas (y tecnologías de capas de enlace) soportadas por WinPcap. Su interfaz es agradable y fácil de usar), Magic NetTrace 2.8.1(Con esta utilidad se combina, en una agradable interfaz, el envío de ping, búsqueda de direcciones IP y funciones de dominios Whois. Pudiendo detectar problemas de conectividad en Internet, el origen de los correos basura,

[153] Que son los datos de conexión, se trata de la posibilidad de que el proveedor de acceso a Internet haga un uso no deseado de los “archivos log”(que muestran los siguientes datos: dirección IP del emisor; dirección IP del destinatario; fecha, hora y duración del servicio; tipo de servicio). Los “archivos log” en posesión del proveedor de acceso constituyen, por tanto, un yacimiento de datos indirectamente nominativos que genera importantes problemas, en la medida en que Internet permite pasar de la prospección en masa a la prospección orientada llamada “one to one”, es decir, directamente adaptada al perfil del comportamiento de una persona.

encontrar la localización geográfica de un servidor web, detectar los problemas con e-mail y más. Siendo muy rápido y compatible totalmente con Internet Explorer, además de contar con otras muchas características) entre otros, que sostienen el peligro latente.

Las tecnologías sofisticadas no pueden estar sobre los Derechos de la persona humana, la norma de rango Constitucional de 1980 establece en el Art. 19 No 4 "El respecto y protección de la vida privada y pública y a la honra de la persona y de su familia", garantía a partir de la cual la jurisprudencia y doctrina nacionales han esbozado la protección de las personas y Art. 19 No 5 "La inviolabilidad del hogar de TODA FORMA de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinadas por la ley". (Ejm. de violación de la privacidad. La C.S. El 19-1 1988 falla en el sentido de considerar que se viola la privacidad de una persona al fallar las instituciones bancarias a la obligación de secreto sobre los movimientos en cuentas corrientes o cuando la C S. El 12-9-1988 Resuelve que el secreto bancario comprende los movimientos de la cuenta corriente y los saldos respecto de terceros, etc). A nivel legal, el Código Penal, y la legislación especial prevé algunas normas que tipifican ilícitos asociados a la lesión de la vida privada y a ciertos ámbitos en los cuales esta se entiende desenvolver, conjunto que, en cualquier caso, reviste un carácter fragmentario, insuficiente para brindar amparo a tal derecho frente a la diversidad de ataques a que se encuentra expuesto, y las que, en caso alguno, contemplaban previsiones relativas al tratamiento de datos personales.

No dejando de lado, además la necesidad de considerar ponderable en este caso cómo indica el Prof. Eduardo Rodríguez S. “orientar a dar también un mayor grado de cumplimiento técnico al conjunto de controles de seguridad de la ISO *17799 en* su homologación en la Norma Chilena Oficial NCh2777 – ISO/IEC 17799: 2000 sobre las Tecnologías de la

información con el Código de Practica para la Gestión de Seguridad de la Información"[154] tanto para los organismos privados como para la administración publica del estado Chileno, con el tratamiento de nuestros datos personales.

En la actualidad se cuenta con la Ley 19.628, sobre protección de la vida privada en lo concerniente a datos personales que es considerada como una norma de rango legal muy débil como indica Alberto Cerda en su tesis[155] indicando que "los vacíos e inconsistencias legales le han hecho merecedora de severas criticas que han llegado al extremo de afirmar que mas bien regula el trafico comercial de los datos personales, antes que la protección de la vida privada frente al tratamiento de aquellos, siendo una de las criticas centrales, que la ley al procurar evitar el procesamiento de datos personales sin el consentimiento de su titular, con las salvedades que ella misma prevé, y brindar protección frente a la lesión de los derechos de los titulares de tales datos, esto es, de las personas a quienes ellos conciernen, a fin de evitar su uso atentatorio contra la intimidad y la eventual exposición a discriminaciones, dejo su cumplimiento entregado a la "buena voluntad" de los destinatarios de sus normas. A las criticas relativas al nivel de intervención estatal en la materia, debe adicionarse que buena parte de las disposiciones legales han caído en terreno infértil, a raíz de la escasa conciencia de la ciudadanía sobre los riesgos que importa el tratamiento de los datos que le conciernen y los derechos de que disponen para precaverse, así como del escaso conocimiento que de sus disposiciones existe entre los propios operadores jurídicos."…"la legislación vigente en el país no salvaguarda los derechos y libertades publicas, desde que no pone a disposición de las personales mecanismos suficientes para gozar de una tutela efectiva frente a los embates que el desarrollo de las nuevas tecnologías genera

[154] Eduardo Rodrigues S. <edorodriguez@yahoo.com> , en el Curso del "Diploma de Postitulo en derecho de las comunicaciones electrónicas" realizado por el CEDI en el marco del Magíster en Derecho Informático y de las telecomunicaciones, marzo 2006 con el tema "Estándares".
[155] Alberto Cerda Silva, "La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales", Centro de Estudios en Derecho Informático, Universidad de Chile, Pag. 4-5.

con ocasión del tratamiento de los datos personales." Sustentada su investigación sobre el supuesto de que gran parte de las falencias del régimen jurídico de Chile tienen lugar por la carencia de una entidad encargada de promover e informar sobre la legislación en cuestión, fiscalizar su cumplimiento y sancionar su infracción, o bien instar por la sanción al infractor, en su caso. De la extracción del mismo análisis[156] plantea "Una experiencia legislativa que innova en nuestro medio no puede estar exenta de reparos y la Ley 19.628 no rehuye tal juicio; el somero análisis que ha precedido deja ya de manifiesto algunas de ellas. La extensión de sus hipótesis de excepción, ciertas ambigüedades de su texto, un deficitario sistema registral, una insuficiente asociación de resguardos asociados a categorías de datos, y la carencia de disposición alguna que prevea mecanismo de control ante el tratamiento ilegitimo de datos personales, entre otras falencias, permite afirmar que mas que una normativa que tiene por objeto velar por los derecho de los afectados por el tratamiento de datos constituye el marco jurídico al cual se afecta tal tratamiento, lo cual queda por lo demás, avalado, en la cual se consigna el afán de resguardar la actividad desplegada por los prestadores de servicios de información y entidades tratantes de datos en general"; o el planteamiento de Washington Jaña en su tesis[157] indica que: "nuestra ley, presenta ciertamente un escenario de riesgo para los derechos fundamentales de las personas, dentro de los cuales la intimidad ocupa sin duda un lugar de preocupación constante" situación por la cual su hipótesis parte de "explorar mas allá de nuestras fronteras un ámbito que presenta gran interés en la actualidad, cual es la protección de los derechos de las personas ante el tratamiento automatizado de información personal" y finalmente el análisis de Jessica Matus&Alenjandro Montecinos en su tesis[158] indicando que: "en cuanto a que la ley es débil se ven amenazadas ante posibles practicas ilegales o ilegitimas, o

[156] Alberto Cerda Silva, "La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales", Centro de Estudios en Derecho Informático, Universidad de Chile, Pag. 120.
[157] Washington Alejandro Jaña Tapia; Análisis Legal Comparativo de la Protección de Datos Personales A Nivel Latinoamérica, Universidad de Chile / Facultad de Derecho – Santiago, Chile 2003, Pag 4.
[158] Jessica Mattus Arenas y Alejandro Montecinos Garcia; El deber de Información y el consentimiento para la transmisión de los datos personales, Universidad de Chile / Facultad de Derecho – Santiago, Chile 2004. pag. 6.

simplemente deshonestas, que en este ámbito pueden existir …" orientando sus postulados al "análisis de la legislación destinada a proteger la vida privada en el ámbito de las nuevas tecnologías encardinadas a una buena posibilidad dogmática en el desarrollo del tema de las garantías y su protección en el ámbito jurídico desde una perspectiva practico-normativa constitucional…y que por cierto estima un esfuerzo desplegado para delimitar la protección debida coherente con el desarrollo de las nuevas tecnologías, dado a los altos riesgos de vulnerabilidad a que se ven expuestas".

Hoy en Chile la privacidad de los usuarios se encuentra en riesgo, no sólo cuando realizan operaciones de comercio electrónico, sino que, por el simple hecho de utilizar la red ofrecen factores de riesgo para la privacidad en Internet(Interacción con la web, Entrega voluntaria de datos, Cookie's, Web bugs, uso personal del e-mail, E-mail marketing, Mensajería instantánea, Yahoo Messenger, MSN Messenger, Firetalk, tecnologías de servicio al cliente a través del web(Tecnología de seguimiento del usuario de mi sitio, lo puedo seguir y conectarme on-line con él en tiempo real por chat); de hecho en junio del 2007 la empresa Ipswitch lanzo al mercado su potente software WhatsUp Gold v11[159]). La inseguridad del destino de los datos entregados se presenta tanto en lo sitios de empresas privadas como en organismos públicos. Respecto al usuario podemos señalar que existe un conflicto de intereses natural entre la necesidad de saber y compartir datos y la necesidad de ocultar. Los derechos del usuario según la ex-acuicertifica.org(Asociación Chilena de Usuarios de Internet) indico que debían de ser informado sobre el tratamiento de la información del sitio web accedido y conocer la manera en que su sitio web recolecta información, saber detalladamente qué datos serán recolectados por el sitio y cuál será su destino, acceder a los datos almacenados, modificar o

[159] WhatsUp Gold, en sus ediciones Premium y Standard, es una potente herramienta que controla la red por monitoreo que convierte los datos de red en información procesable para los negocios, las mejoras en el software incluyen una nueva aplicación de web, workspaces con mas de 100 informes personalizados y una mejora en el monitoreo de Ipv6; diseñado para un rápido desarrollo, escalabilidad robusta, facilidad de uso y simplicidad de recolección de información de redes.

borrar su información (Opt-in y Opt-out), conocer las medidas de seguridad adoptadas por el sitio(cortafuegos) en todo caso al momento se debería de establecer vías de comunicación eficientes con el usuario, incorporar nuevas Tecnologías de protección de la privacidad mas eficientes, por que en medida que estas avanzan con la creación de nuevas formas de comunicación, también existirán paralelamente nuevos modos de interceptar las comunicaciones privadas. Ej. P3P[160] (Plataform for Privacy Preferentes que son las Plataformas de Preferencias de Privacidad, http://www.w3.org) y los sellos de certificación. Como es el caso en la actualidad de la Comisión de la Unión Europea que ha encargado a un consorcio de ocho organizaciones y empresas europeas encabezadas por el Centro Independiente para la Protección de la Privacidad Schleswig-Holstein (ICPP/ULD) la recopilación de los requisitos para la obtención de un Sello Europeo de Privacidad y para poner a prueba su ejemplaridad. El proyecto del "Sello de Privacidad Europeo"(Europrise) ha sido iniciado en fecha 19/07/2007 por Dietrich Austermann, Ministro de Economía de Schleswig-Holstein, en la Cámara de Industria y de Comercio de Schleswig-Holstein (JHK), el Dr. Thilo Weichert, director de ICPP/ULD, afirma que: "Hemos observado que existe una demanda internacional y una necesidad de disponer de productos que garanticen la privacidad. A la vista de la opacidad del tratamiento de los datos, los consumidores necesitan análisis exhaustivos realizados por instituciones independientes fiables y competentes según estándares reconocidos. El Sello de la Privacidad permite dichos análisis.".

A continuación presentamos un ejemplo de textos constitucionales de Protección a la privacidad:

ESPAÑA
Privacidad. Art. 18. Honor, Privacidad, Domicilio, Secreto de las comunicaciones…

[160] Especificaciones del P3P: Un esquema estándar para los datos que un sitio web puede recopilar, un conjunto estándar de divulgaciones de la privacidad, un medio de asociar directivas de privacidad a las páginas web y las cookies, un formato XML para expresar las directivas de privacidad y un mecanismo para transportar las directivas de P3P sobre http.
Objetivos de P3P: Permitir que los sitios web presenten sus prácticas de recopilación de datos de un modo normalizado, legible en formato electrónico y fácil de localizar y permitir que los usuarios de Internet sepan qué datos se obtendrán en cada sitio, cómo se utilizarán y qué datos y usos pueden ser opcionales u obligatorios.
Directivas de P3P: Un sitio Web compatible con P3P codifica sus prácticas de uso y recopilación de datos en un formato XML legible en formato electrónico que se conoce como directiva de P3P.

4. La ley limitara el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.
Privacidad en las comunicaciones Art. 18. Honor, privacidad , Domicilio, Secreto de las comunicaciones… 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. Art. 20.1. d) a comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulara el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades. Art. 20.5: Solo podrá acordarse el secuestro de publicaciones, grabaciones y otros medios de información en virtud de resolución judicial.
RUSIA
Privacidad: Art.23 Privacidad 1. Todo ciudadano tiene derecho a la inviolabilidad persona, secreto personal y familiar ,a defender su honor y su buen nombre.
Privacidad en las comunicaciones Art.23.2. Todo ciudadano tiene derecho a correspondía secreta, conversaciones telefónicas y comunicación por telégrafo secretas, entre otras. Este derecho puede ser limitado solo por una sentencia judicial.
Protección de datos personales Art.24protecion de datos personales 1. Esta prohibido reunir, guardar, utilizar y difundir contra la voluntad del individuo información sobre su vida privada. 2. Los órganos de poder estatal y de auto gobierno local y sus funcionarios deben garantizar a cada individuo la posibilidad se conocer los documentos que atañan directamente sus derechos y libertades, si la ley no prevé otra cosa.
SUIZA
Privacidad Art.13 Protección de la Privacidad 1.Toda persona tiene derecho al respeto de su vida familiar y privada, de su domicilio, de su correspondía, así como de sus relaciones postales y de sus telecomunicaciones
Privacidad en las comunicaciones Art.13 Protección de la Privacidad 1. Toda persona tiene derecho al respeto de su vida familiar y privada, de su domicilio, de su correspondía, así como de sus relaciones postales y de sus telecomunicaciones.
Protección de datos personales Art.13 Protección de la Privacidad 2. Toda persona tiene derecho a ser protegida contra el empleo abusivo de sus datos personales.
ITALIA
Privacidad
Privacidad en las comunicaciones Art.15 Libertada de correspondencía La libertada y el secreto de la correspondencia y cualquier otra forma de comunicación serán inviolables. Su limitación solamente puede tener lugar por resolución motivada de la autoridad judicial con las garantías establecidas por la ley.
ALEMANIA
Privacidad
Privacidad en las comunicaciones Art.10.Privacidad de la correspondencia ,mensajes y telecomunicaciones 1. Será inviolable el secreto de la correspondencia, así como el del correo y de las telecomunicaciones.
GRECIA
Privacidad
Privacidad en las comunicaciones Art.19 secreto de correspondencia Será absolutamente inviolable el secreto de las cartas, así como el de cualquier medio de libre correspondencia o comunicación. La ley fijara las garantías bajo las cuales no estará obligada la autoridad judicial a respetar el secreto por razones de seguridad nacional o para las necesidades de la instrucción sobre delitos de especial gravedad.
PORTUGAL
Privacidad Art.26 Otros Derechos Personales. 1. Se reconoce a todos el derecho a la identidad, al desarrollo de la personalidad, a la capacidad civil, a la ciudadanía, al buen nombre y reputación, a la imagen, a la palabra, a la reserva de la intimidad de la vida privada y familiar y a la protección legal contra cualquiera forma de discriminación.

Privacidad en las comunicaciones Art.34.Inviolabilidad del domicilio y de la correspondencia 1. El domicilio y el secreto de la correspondencia y de otros medios de comunicación privada son inviolables. 4. Se prohíbe toda injerencia de las autoridades publicas en la correspondencia, en las telecomunicaciones y en los demás medios de comunicación, salvo en los casos previstos en la ley en materia de procedimiento penal.
Protección de datos personales Art.35.Utilización de la Informática 1. Todos los ciudadanos tienen derecho a acceder a los datos informatizados que les conciernan, pudiendo exigir su rectificación y actualización, así como el derecho a conocer la finalidad a que se destinan, en los términos que establezca la ley. 2. La ley define el concepto de datos personales, así como las condiciones aplicables a su tratamiento automatizado, conexión transmisión y utilización y garantiza su protección, especialmente a través de una entidad administrativa independiente. 3. La informática no puede ser utilizada para el tratamiento de datos relativos a convicciones filosóficas o políticas, afiliación a partidos o sindicatos, confesión religiosa, vida privada y origen étnico, salvo con el consentimiento expreso del titular, autorización prevista por la ley con garantías de no discriminación o para procesamiento de datos estadísticos no identificables individualmente. 4. Se prohíbe el acceso a datos personales de terceros, salvo en caso excepcionales previstos por la ley. 5. Se prohíbe la atribución a los ciudadanos de un número nacional único. 6. Se garantiza a todos el libre acceso a las redes informáticas de uso publicó, determinando la ley el régimen aplicable a los flujos de datos Transfronterizos y a las formas adecuadas de protección de datos personales y de otros cuya salvaguardia se justifique por razones de interés nacional 7. Los datos personales que consten en ficheros manuales gozan de protección idéntica a lo previsto en los apartados anteriores, en los términos que establezco la ley.
HUNGRIA
Privacidad Art.59 Honor ,Privacidad 1. En la republica Húngara toda persona tiene derecho al honor, a la inviolabilidad del domicilio, además de la protección del secreto privado y de los datos personales.
Privacidad en las comunicaciones Art.59 Honor ,Privacidad 1. En la republica Húngara toda persona tiene derecho al honor, a la inviolabilidad del domicilio, además de la protección del secreto privado y de los datos personales.
Protección de datos personales Art.59 Honor ,Privacidad 1. En la republica Húngara toda persona tiene derecho al honor, a la inviolabilidad del domicilio, además de la protección del secreto privado y de los datos personales.
ESLOVENIA
Privacidad Art.35 Privacidad y derechos personales La integridad física y mental debe ser garantizada, como la privacidad y otros derechos personales.
Privacidad en las comunicaciones Art.37 Privacidad de la correspondencia y otros medios de comunicación. 1. Privacidad de la correspondía y de otros medios de comunicación debe ser garantizada. 2. De acuerdo con la determinación legal .el órgano jurisdiccional pueden automatizar acciones que vulneren la privacidad de la de la correspondía u otros medios de comunicación ,o aun la inviolabilidad de la privacidad individual, desde que esta acciones sean consideradas necesarias para el inicio o continuación de procedimientos penales por razones de seguridad nacional.
HOLANDA
Art.10 Privacidad Art.10 Todos tiene derecho, salvo las limitaciones que se establezcan por o en virtud de la ley, al respecto de su intimidad personal y familiar.
Privacidad en las comunicaciones Art.13 1. Se reconoce la inviolabilidad de la correspondencia, excepto, en los casos previstos por la ley ,en virtud del auto judicial,2. Se reconoce el secreto de las comunicaciones telefónicas u telegráficas, salvo en los casos previstos por la ley, por o con la autorización de quienes hayan sido designados a tal efecto por la ley. 2. La ley establecerá normas para proteger la intimidad personal y familiar en relaciones con el registro y el suministro de datos personales.
Protección de datos personales + Aunque sin una referencia directa, la constitución holandesa dispone sobre la naturaleza de las leyes sobre datos personales.

Tabla 85. Textos constitucionales de protección a la privacidad.

Un ejemplo de textos constitucionales que ignoran la Protección a la privacidad y a la libertad de expresión.

País	Texto constitucional
Irán	Art. 25. La inspección de cartas y los fallos en su entrega, la grabación y la revelación de comunicaciones telegráficas o por telefax. La censura o el fallo deliberado en su transmisión, las formas de investigación secretas son prohibidas, **excepto las permitidas por la ley.**
China	Art. 40. Correspondencia. La libertad y la privacidad de la correspondencia de los ciudadanos en la Republica Popular China son protegidos por la ley, Ninguna organización o persona física puede, en ningún nivel, atentar contra la libertad y la privacidad de la correspondencia de los ciudadanos, **excepto en casos en los que, con el fin de alcanzarlas seguridad del Estado debido a la investigación criminal, la Seguridad publica y los órganos fiscales puedan censurar correspondencia de acuerdo con los procedimientos prescritos en la ley.**
Libia	Art. 13. La libertad de opinión esta garantizada **en los límites del interés público y en los límites de la Revolución.**

Organizaciones no Gubernamentales relacionadas con la protección de la privacidad:

Privacy Internacional www.privacyinternational.org	The Progress and freedom Fundation www.pff.org
American for computer Privacy www.computerprivacy.org	Foundation for information Policy Research www.fipr.org
Stand.org www.stand.org.uk	Electronic Privacy Information Center www.epic.org
American Civil LibertiesUnion www.aclu.org	TRUSTe Privacy Policy Certification Program www.truste.org
Free Expresion Network www.freexpression.org	Digital Future Coalition www.dfc.org
Global Internet Liberty Campaign www.gilc.org	Internet free Expresión Alliance www.ifea.net
Digital Freedom Network www.ifea.net	Electronic Frontiers Network www.efa.org.au
Electronic FrontiersCanada www.efc.ca	Fronteira Electronica www.fronteira-electrónica.org
Fundacao Vanzolini www.privacidade-vanzolini.org.br	

3.2 Mecanismos de control no jurídicos[161].

Que son aquellos que no se concretan a través de un juicio, sino mediante procedimientos administrativos. La circunstancia de que los mecanismos de control no jurídicos soslayan las formalidades propias del quehacer judicial confiere a estos de mayor eficacia. Además siempre a diferencia del control radicado en sede judicial, suele presentar un carácter continuo, que prescinde del impulso de los afectados y aun queda facultado para proceder de oficio. Esto asegura que, en nuestro caso, las operaciones de tratamiento de datos queden permanentemente expuestas a la actividad de control, sea que se haya suscitado una reclamación al respecto o no. Igualmente, mientras el control jurisdiccional supone el requerimiento de los afectados por el acto u

[161] Extracto del análisis de la tesis de Alberto Cerda Silva, "La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales", Centro de Estudios en Derecho Informático, Universidad de Chile, Pág. 210-260

omisión que lesiona, menoscaba o perturba el ejercicio de sus derecho, con lo cual habitualmente opera expost, la continuidad del control no jurisdiccional permite anticiparse a la ocurrencia de hechos que signifiquen infracción a las disposiciones legales o reglamentarias vigentes, vale decir, verifica un control preventivo.

a) Códigos deontológicos[162]. Constituyen normas de conducta adoptadas por los propios destinatarios de sus previsiones. En rigor, más que constituir mecanismo de control constituyen una expresión de autorregulación. Los códigos deontológicos, al decir de Orti Vallejo, constituyen normas de conducta relativas al manejo del banco y tratamiento de datos adoptadas por determinados sectores empresariales, asociaciones gremiales o profesionales. Por consiguiente, son una expresión de autorregulación, por la cual los propios agentes fijan normas para el desempeño de sus actividades, si bien ello no excluye la participación de la autoridad publica durante el proceso de elaboración, ya sea fomentando su elaboración, verificando su legalidad o simplemente registrando su existencia…

b) Agente de control interno. Constituye un mecanismo de control interno, desde que normalmente opera y es designado a instancias del propio responsable de tratamiento, admitiéndose inclusive sea un empleado mismo. Sin embargo, ello no excluye que en el desempeño de su cometido el agente de control interno establezca una relación bastante estrecha con la autoridad de control desde que esta le brinda asistencia y le fiscaliza, mientras aquel esta obligado a denunciar las infracciones cuando los defectos observados no son subsanados por el responsable de tratamiento y, adicionalmente, goce de plena independencia en las labores de control que le corresponden…

c) Los contrato acuerdo. No constituye propiamente mecanismo de control en materia de tratamiento de datos personales, sino que, a lo sumo, entre sus diversas previsiones se contienen formulas de control. Sin embargo, nos ha parecido pertinente incluirlos en este acápite, en cuanto a través de ellos se puede alentar el cumplimiento de las normas relativo al tratamiento de datos personales, aun cuando su ámbito de aplicación sea circunscrito a las transferencias internacionales de estos…

d) La autoridad de control Esto es, un organismo público de control encargado de promover e informar a la comunidad sobre la legislación aplicable al tratamiento de datos personales, fiscalizar el cumplimiento de la normativa y sanciona en su infracción, o bien instar por la sanción del infracto, en su caso…

e) Las tecnologías de protección de la privacidad. Constituyen un elemento clave dentro del contexto a la tesis, las cuales son consideradas como aplicaciones mediante las cuales se procura promover y aun fomentar el tratamiento de datos de conformidad con la normativa vigente.
Las tecnologías de protección de la privacidad tienen por propósito instaurar sistemas y tecnologías de información y comunicación, minimar la recolección y el empleo de datos personales y dificultar las posibilidades de tratamiento ilícito. Se trata de mecanismo de control sobre el tratamiento que recae respecto de los datos personales que coadyuvan a aquello otros previstos en el ordenamiento. La Comisión de las Comunidades Europeas ha distinguido 3 tipos de productos según la tecnología empleada en su elaboración; aquellos que respetan la privacidad, los que son diseñados cumpliendo cabalmente con las disposiciones legales vigentes; aquellos que facilitan la protección de la privacidad, cuales introducen además determinados elementos que facilitan el acceso de los usuarios a aspectos relacionados con la misma, tales como proporcionar al usuario medios simples para hacer ejercicio de sus derecho; los productos que fomentan la protección de la privacidad, esto es, aquellos creados con el fin de hacer un uso lo mas amplio posible de datos verdaderamente anónimos, para lo cual recurre a **procedimientos de disociación de los datos**. Aplicaciones que responden a las características enunciadas son actualmente alentadas en la Unión Europea, particularmente en relación con el tratamiento de datos personales que supone el funcionamiento de la administración pública electrónica. Sin embargo, las mismas presentan un serio percance, cual es la dificultad para reconocer aquellos productos que responden a los estándares normativos de protección de la privacidad, mas aun, desde que se ha constatado que algunas aplicaciones que se presentan como tales no satisfacen los requisitos.

Tabla 86. Clasificación de algunos mecanismos de control no jurídicos.

[162] Una reseña sobre los código de conducta, en cuanto protección de los datos derivada de la practica desarrollada, puede encontrarse en Estadella Yuste, Olga, "La protección de la intimidad frente a la transmisión internacional de datos personales", editorial tecnos Madrid, 1995, pp.43-48

3.3 Perspectivas del tratamiento tecnológico de la privacidad.

En la sociedad de la información o como indica el Prof. Roberto Godoy Fuentes "sociedad de la información en los entornos tecnológicos, consecuente con la globalización de las comunicaciones, gasificación del uso de la TV, la radio y creciente y explosivamente de Internet, incorporación de Internet a los negocios(e-commerce), la brecha digital y finalmente la incorporación de las TICs al Gobierno(e-gov) con sus respectivos impactos en Chile"[163], los usuarios probablemente definirán y manejarán sus identidades y funciones digitales de un modo similar al real, y afirmarán y reforzarán su derecho a la privacidad. En el Internet se plantea un desafío real: las tendencias tecnológicas, como la difusión de aparatos personales (móviles 3g[164]), el acceso y la informática ubicuos, junto con la transformación electrónica del comercio(e-commerce), el gobierno(e-goverment) y los procesos laborales, suscitan problemas de uso, seguridad y tratamiento, a los que a menudo se hace frente (aunque no necesariamente) aumentando el grado de interrelación y centralización de la información. En el actual internet, no existe sólo la posibilidad de crear nuevas identidades para uno mismo, sino que cada usuario deja "rastros de datos" cuando utiliza aplicaciones o servicios digitales. Las personas, en su mayoría, no son conscientes de cuánto dicen sobre ellas los datos que dejan, y no tienen medio alguno para

---

[163] "Referido al estado del arte, se sabe que Chile lidera en América Latina en desarrollo de las TICs, pero también hoy esta lejos de Corea, Singapur, Malasia, taiwán, Hong Kong. En 1970 estaba arriba de todos ellos, la agenda del crecimiento y de productividad debería ser integral (modernización del estado +Educación+ Competencia + Innovación + Tecnología); de hecho la brecha digital debería estar ya orientada a la mejora de sus indicadores como el Socioeconómico (Acceso a Internet, sector ABC1 y C2(26% de la pob.)tienen el 68% del acceso a Internet), Geográfica(57% de las conexiones en Santiago), Generacional(84% son menores de 34 años) y educacional(65% de los usuarios tienen estudios post-secundarios)" Roberto Godoy Fuentes, en el marco del Magíster en Derecho Informático y de las Telecomunicaciones realizado por el CEDI de la Universidad de Chile, con el tema "Agenda Publica y desarrollo de la sociedad de la información", Noviembre del 2005.

[164] Connect One Ltd., un fabricante de chips incorporados, ha introducido un procesador estándar que permite a las empresas añadir rápidamente conexión a Internet a dispositivos móviles y remotos que previamente carecían de ella. El nuevo chippermite establecer comunicaciones bidireccionales en tiempo real con dispositivos como máquinas expendedoras, contadores de servicios o incluso consolas de videojuegos sin tener que rediseñar su hardware. Alan Singer, vicepresidente de Connect One, dice que el chip es un complementopost-venta que establece una conexión en serie entre el dispositivo y el procesadordel *host*, permitiendo la conexión de Red a través de cualquier ISP. Es más, Singerdice que el chip se está vendiendo sobre todo a clientes de los campos médico eindustrial, pero que la compañía está en trato también con empresas de electrónicacon el fin de incorporar el chip en dispositivos como reproductores de DVD y MP3y teléfonos inalámbricos.
Dr. George Kocur , , tema 20 "Fundamentos de las Telecomunicaciones", Curso de Tecnología de bases de datos Cod. ESD.264J, Internet e integración de sistemas, Área Ingeniería de Sistemas, MIT.

controlar eficazmente este "escape" de datos. Por otra parte, no hay garantías de que los datos de las redes digitales sean auténticos. En particular, se pueden crear falsas identidades, e incluso se pueden "usurpar" identidades de personas reales, al tiempo que el robo de identidad es un problema cada vez más importante (http://identitytheft.org). Así pues, el Internet de hoy carece al tiempo de privacidad y de autenticidad. En el internet, las personas, en su mayoría, no son conscientes de cuánto dicen sobre ellas los datos que dejan y no tienen medio alguno para controlar eficazmente este "escape" de datos.

En la futura Internet, los **sistemas de tratamiento de la identidad**(IMS-Identity Management Systems) que refuerzan la privacidad nos permitirán desempeñar nuestras funciones, utilizar nuestras identidades y mantener nuestra privacidad en la sociedad, del mismo modo al que hemos estado habituados hasta ahora. Nuestro entorno y nuestros aparatos personales, más que ser sólo enormes depósitos de datos de nuestros actos en línea, contraseñas, etc., nos ayudarán también a mantener el registro y proteger la privacidad de nuestras identidades digitales, incluyendo sus derechos y obligaciones; y a elegir cuándo y a quién proporcionar información personal. Las redes de comunicaciones nos permiten ocultar nuestras "coordenadas", como localización física, direcciones de red o de correo electrónico, y protegerlas del uso indebido, al tiempo que permiten a los administradores de las redes gestionarlas con seguridad. Podemos utilizar los equivalentes electrónicos de objetos cotidianos, como las tarjetas de la biblioteca, la guía de teléfonos o el dinero, sin dejar huellas excesivas de nuestro comportamiento en los distintos sectores de nuestra vida.

Los sistemas de tratamiento de la identidad(IMS) que refuerzan la privacidad, combinan ésta con la autenticidad. Ello exige tecnologías que permitan a los usuarios controlar el suministro de información personal, así como la relación entre las apariciones de esta información en diferentes contextos.

Los IMS que refuerzan la privacidad combinan ésta con la autenticidad. Ello exige tecnologías de avanzada que permitan a los usuarios controlar el suministro de información personal, así como la relación entre las apariciones

de esta información en diferentes contextos[165], actuando bajo seudónimo o anónimamente. Se puede conseguir la autenticidad en combinación con diversos grados de anonimato[166].

Según Sebastian Clauß y Andreas Pfitzmann, Universidad Tecnológica de Dresde, Marit Hansen, Centro Independiente para la Protección de la Privacidad, Schleswig-Holstein y Els Van Herreweghen, Laboratorios de Investigación de IBM, Zurich plantean lo siguiente:

> Actualmente, hay una amplia gama de sistemas que abordan distintos aspectos del tratamiento de la identidad. Sólo unos pocos tienen objetivos principalmente orientados a la privacidad, mientras que la mayoría se centra en la capacidad de uso y en la comodidad, como, por ejemplo, disponer de una firma única. Así, diversos clientes de correo electrónico o navegadores de la web ofrecen la opción de utilizar diferentes perfiles de usuarios. Las direcciones de correo electrónico se pueden asociar con distintas firmas y claves criptográficas digitales, por ejemplo con PGP (Pretty Good Privacy, http://www.pgpi.org). Algunos instrumentos de privacidad ofrecen funcionalidades de seguridad o privacidad configurables por el usuario, por ejemplo para controlar el comportamiento de los *cookies*, a fin de limitar la posibilidad de obtener perfiles de los usuarios, bloquear la información sobre identificación frente a los *chatters*, o utilizar programas de codificación criptográfica. La norma P3P W3C (Platform for Privacy Preferences, http://www.w.3.org/P3P/) proporciona un formato para especificar las políticas de privacidad de los servidores de la web; los navegadores P3P permiten a los usuarios especificar sus preferencias en cuanto a privacidad, que se cotejan con la política de privacidad del servidor web. La W3C ha venido especificando el lenguaje APPEL (A P3P Preference Exchange Language, http://www.w3.org/TR/P3P-preferences/) que permite el uso de distintos personajes en el fichero de preferencias del usuario.
>
> Algunos servicios de la web realizan también tratamiento de datos personales; la mayoría (por ejemplo, Microsoft.NET Passport [http://www.passport.com], Novell digitalme [http://www.digitalme.com], PrivaSeek Persona [http://www.privaseek.com] e iPrivacy [http://www.iprivacy.com]) procesa los datos personales del usuario en el servidor del proveedor; unos pocos almacenan la información localmente, en el ordenador del usuario (por ejemplo, v-GO de Passlogix [http://www.passlogix.com], Freedom Security and Privacy Suite [http://freedom.net]). La tecnología TrueSign de Privador Inc. (http://www.privador.com) se puede integrar en las infraestructuras de clave pública existentes y permite a los usuarios manejar diferentes certificados (seudónimos).
>
> La necesidad de tratar las identidades en línea ha llevado a la creación del Liberty Alliance Project (http://www.projectliberty.org), una alianza comercial formada para proporcionar una solución al tratamiento de las identidades en Internet, que permite una firma única con autenticación descentralizada y autorización abierta de muchos proveedores, y que ofrece una norma abierta para tratamiento de identidades en la red. Todavía no se han hecho públicos los resultados.
>
> También algunos proyectos académicos se refieren al tratamiento de la identidad. Un prototipo de "accesibilidad personal y gestión de la seguridad" permite el uso de diferentes seudónimos en la comunicación personal[167]. Estos seudónimos pueden contener claves públicas para codificar o firmar las comunicaciones; y pueden ser emitidos por una autoridad de certificación (CA) o creados por los propios usuarios. Otro proyecto, el ATUS (A Toolkit for Usable Security) de la Universidad de Friburgo, Alemania, están diseñando e implementando un módulo de "gestor de identidad"[168]. Actúa como una especie de cortafuegos sobre el sistema del usuario y le ayuda a manejar diferentes

[165] Pfitzmann, A. y Köhntopp, M., Anonymity, Unobservability, and Pseudonymity. A Proposal for Terminology; Draft v0.12, 2001-06-17, http://www.koehntopp.de/marit/pub/anon/ V0.8. En: H. Federrath (Ed.), Designing Privacy Enhancing Technologies. Proc. Workshop on Design Issues in Anonymity and Unobservability. LNCS 2009. Springer Verlag, 2001. 1-9.

[166] Turkle, S. *Life on the Screen. Identity in the Age of the Internet*. Simon & Schuster, Nueva York 1995.

[167] Damker, H., Ulrich Pordesch, y Martin Reichenbach. *Personal Reachability and Security Management. Negotiation of Multilateral Security*. En: G. Müller, K. Rannenberg (Eds.), Multilateral Security in Communications, vol. 3, Addison Wesley.

[168] Jendricke, U. y Gerd tom Markotten, D., *Usability meets Security. The Identity-Manager as your Personal Security Assistant for the Internet*. En Proc. 16th Annual Computer Security Applications Conference (ACSAC 2000), Nueva Orleans, EE.UU., 11-15 diciembre, 2000.

perfiles, implementados como visiones de un conjunto de datos personales que consta de los atributos típicos, como nombre, dirección postal y dirección de correo electrónico. Los perfiles se pueden vincular con URL concretos, permitiendo la elección automática del perfil al contactar con determinados servidores web. El gestor de identidad ATUS conecta automáticamente, por defecto, con cualquier servicio Internet (utilizando actualmente la tecnología AN.ON/JAP[169] de la Universidad de Dresde). Sirve para rellenar formularios y alerta al usuario de cuándo está revelando cierta información adicional predefinida, por ejemplo suministrada manualmente en un formulario. Principalmente se centra en controlar la cantidad de datos personales en una transacción determinada, y no da apoyo a transacciones seguras bajo perfiles diferentes.

Tabla 87. Tendencias tecnológicas en materia de protección de datos.

3.3.1 La privacidad en los sistemas de tratamiento de la identidad("identity management", IM)

Los sistemas de tratamiento de identidad(IM) difieren principalmente en cuanto al lugar donde se almacenan y procesan los perfiles de los usuarios (sólo en el usuario; en el usuario y en el servidor; sólo en el servidor) y en cuanto a la provisión de mecanismos de autenticación y funcionalidades adicionales de seguridad y privacidad. Teniendo en cuenta el diseño de un IMS exhaustivo, que refuerce la privacidad, se pueden enumerar varios inconvenientes de los sistemas actuales:

- **Falta de apoyo a la soberanía del usuario:** En la mayoría de los casos, el usuario no puede elegir dónde y cómo se tratan sus datos personales: tiene que confiar en los proveedores de IM que tienen pleno acceso a sus datos.
- **Funciones de privacidad limitadas:** Pocos sistemas contribuyen a afirmar el derecho a la privacidad del usuario.
- **Falta de autenticación de los seudónimos:** El estado actual de los sistemas de seudónimos o de credenciales anónimas[170] permite la implementación, probablemente segura, de transacciones anónimas autenticadas y la emisión de atributos certificados, controlados por el usuario. En particular, permite que cada usuario utilice una credencial con múltiples seudónimos, sin que dichos seudónimos puedan ser relacionados entre sí. Mediante la revocación (o la inversión) opcional del anonimato por terceras

[169] Berthold, O., Federrath, H., y Köhntopp, M. *Anonymity and Unobservability in the Internet*, Workshop on Freedom and Privacy by Design. En: Actas de la Décima Conferencia sobre Ordenadores, Libertad y Privacidad, CFP 2000: Challenging the Assumptions, Toronto/Canada

[170] Camenisch, J. y Lysyanskaya, A. Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. En: B. Pfitzmann (Ed.), Advances in Cryptology EUROCRYPT 2001.

partes de confianza, estos sistemas apoyan la responsabilidad y, por tanto, las medidas para el cumplimiento de las leyes, a pesar del uso de seudónimos. Tales sistemas no están siendo explotados, hasta ahora, por los IMS existentes.

- **Limitación a aplicaciones específicas:** Los sistemas existentes no se pueden utilizar con carácter universal, sino que están específicamente diseñados para utilizarlos con una determinada aplicación o conjunto de aplicaciones. Todavía no existen normas abiertas para interfaces IMS que se puedan implementar en todo tipo de comunicaciones informatizadas.

La falta de privacidad en los sistemas actuales subraya la necesidad de nuevas soluciones tecnológicas que refuercen la privacidad, teniendo en cuenta los sistemas legales existentes y los posibles modelos comerciales.

Las medidas legales u organizativas solas no son suficientes para ayudar a los usuarios de los IMS. La falta de privacidad en los sistemas existentes subraya la necesidad de nuevas soluciones tecnológicas que refuercen la privacidad, teniendo en cuenta los sistemas legales existentes y los posibles modelos comerciales. También se necesitan acciones para educar y entrenar a los usuarios sobre privacidad e IMS. Además, los IMS que refuerzan la privacidad exigen nuevas tecnologías y servicios de terceros, como parte de la infraestructura de IM. Por tanto, se necesita un enfoque exhaustivo del IM[171], que ninguno de los sistemas existentes, antes mencionados, ofrece.

[171] **Diseño de la arquitectura de un Sistema de tratamiento de identidad (IMS).**
Un IMS que refuerza la privacidad conciencia al usuario sobre la circulación de sus datos personales y le proporciona el control sobre la misma. Para mostrar al usuario este flujo de datos, el IMS debe proporcionarle una historia coherente y representaciones contextuales. La información histórica incluye la extensión, naturaleza y relaciones de los datos facilitados en el pasado; la información contextual puede incluir otra información adicional, por ejemplo etiquetas concretas que expresen cuándo se han de relacionar las acciones o qué propiedades debe tener un nuevo seudónimo, y que pueden ser proporcionadas por las contrapartes en la comunicación, por terceras partes tales como servicios de información sobre privacidad, o incluso por la comunidad de Internet.

Para que el usuario posea el control sobre la circulación de sus datos personales, el IMS apoya a cada usuario en la decisión sobre qué datos personales identificables o seudónimos facilita. Permite al usuario disminuir al mínimo la difusión de datos personales y determinar el grado de relación de estos datos, eligiendo qué seudónimos se han de utilizar con qué propiedades, y si se deben reutilizar los seudónimos o generar otros nuevos. Proporciona a los usuarios los mecanismos e interfaces para implementar su derecho a la privacidad, por ejemplo, obtener información de un servidor sobre qué datos personales posee sobre ellos, acceder a tales datos, corregirlos o eliminarlos, o conceder o revocar el consentimiento.

La capacidad de uso y una buena interfaz de usuario son esenciales y pueden incluir el apoyo de servicios de información sobre privacidad en línea, que proporcionen información sobre los riesgos para la seguridad y la privacidad, con respecto al IMS en cuestión.

El usuario debe poder acceder a su IMS desde una variedad de aparatos (por ejemplo, un teléfono móvil o PDA) y lugares. También, los instrumentos menos potentes deben proporcionar una interfaz utilizable y, al menos, una funcionalidad mínima.

Idealmente, el IMS del usuario está situado en un entorno en el que éste confía. Por diversas razones (por ejemplo, accesibilidad del sistema cuando se usan distintos aparatos, cómoda duplicación, o servicios de apoyo), los usuarios pueden desear subcontratar su IMS, en todo o en parte, con un proveedor. El usuario debe poder elegir tal proveedor.

La gestión de la privacidad y de la identidad no debe obstaculizar el cumplimiento de las medidas de seguridad o la eficacia de los sistemas de detección de intrusos. En muchos casos, no tiene por qué haber una contradicción entre los requisitos de cumplimiento de la ley y la privacidad plena.

La gestión de la privacidad y de la identidad no debe obstaculizar el cumplimiento de las medidas de seguridad o la eficacia de los sistemas de detección de intrusos. En muchos casos, no tiene por qué haber una contradicción entre los requisitos de cumplimiento de la ley y la privacidad plena. El diseño adecuado de las aplicaciones puede evitar el uso indebido, de modo que el anonimato del usuario no tiene que ser reversible. Al diseñar un IMS y ejecutar transacciones anónimas y no relacionables, los sistemas e instrumentos para garantizar la seguridad pueden necesitar reconfigurarse o adaptarse, a fin de abordar los distintos grados de anonimato o las propiedades de los seudónimos, por ejemplo limitando a los usuarios a un número fijo de seudónimos por tema, capacidad de transferencia a otros temas, posibilidad y frecuencia del cambio de seudónimo, limitación del número de usos, validez (límite de tiempo, restricción a una aplicación determinada), posibilidad de revocación o bloqueo, o participación de los usuarios y otras partes en la formación de los seudónimos.

Cuando los usuarios actúan bajo seudónimo o anónimamente, el cumplimiento de la ley y las consideraciones de seguridad pueden exigir que el anonimato apoyado por los IMS sea reversible, o que un seudónimo pueda ser identificado con un usuario concreto

Cuando los usuarios actúan bajo seudónimo o anónimamente, el cumplimiento de la ley y las consideraciones de seguridad pueden exigir que el anonimato apoyado por los IMS sea reversible,o que un seudónimo pueda ser identificado con un usuario concreto. La tarea de invertir el anonimato se asigna generalmente a terceras partes de confianza, como gestores de identidad o autoridades que certifican credenciales anónimas. Es de suma importancia que los usuarios puedan confiar en las terceras partes (y, si es posible, elegirlas) que pueden revelar sus identidades o relacionar sus actos. Además, hay que tomar medidas para garantizar el control público y la responsabilidad de las acciones de estas terceras partes.

En la infraestructura de IM, los usuarios deben estar apoyados (y compartir información) no sólo por los proveedores de IMS y las autoridades de certificación, sino también por otras muchas terceras partes. Para todos estos servicios, el sistema debe apoyar la confianza y la separación de conocimiento y poder (por ejemplo, un usuario puede confiar en un tercero o en un proveedor para que conozca información personal seleccionada, pero no para que actúe en su nombre). Esto significa que el usuario debe poder decidir en qué tercero o proveedor confiar y hasta qué punto.

Técnicas básicas para conseguir la imposibilidad de relación y el anonimato

Si el usuario lo desea, el IMS ofrece la imposibilidad de relacionar distintas acciones de un mismo usuario, de modo que quienes participan en dichas acciones diferentes de ese usuario no puedan combinar los datos personales que se difunden en estas acciones con el fin de construir el perfil del usuario. Mantener la imposibilidad de relacionar datos autenticados sólo es posible si los usuarios pueden actuar bajo diferentes seudónimos (no relacionables), que tengan propiedades o atributos determinados.

Si el usuario lo desea, el IMS ofrece la imposibilidad de relacionar distintas acciones de un mismo usuario, de modo que quienes participan en dichas acciones diferentes de ese usuario no puedan combinar los datos personales que se difunden en esas acciones con el fin de construir el perfil del usuario

La mayoría de los actos exigen la comunicación segura y la autenticación de algunas de las propiedades o atributos de las partes que se comunican. Si los usuarios actúan bajo seudónimo, los proveedores de servicios pueden garantizar la seguridad y la autenticidad sólo si aceptan seudónimos o credenciales anónimas. Los sistemas de credenciales anónimas como tales (Camenisch, J. y Lysyanskaya, A. Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. En: B. Pfitzmann (Ed.), Advances in Cryptology EUROCRYPT) permiten la responsabilidad y obligan a cumplir la ley, a pesar del uso de seudónimos. En muchos casos se puede prevenir el uso indebido (más que detectarlo) incorporando una seguridad adecuada en la aplicación.

Un requisito para conseguir la imposibilidad de relacionar las acciones, a nivel de aplicación, es el apoyo del anonimato por parte de la red.

3.3.2 Perspectivas de los ISM en la privacidad.

Los IMS que refuerzan la privacidad son necesarios para preservar y actualizar el concepto de privacidad en la sociedad de la información.

Descripción de la arquitectura

Un IMS completo que refuerce la privacidad debe incluir los siguientes elementos(Clauss, S. y Köhntopp, M. Identity Management and Its Support of Multilateral Security. En: Computer Networks 37 (2001). Número especial sobre sistemas de comercio electrónico. Elsevier, North-Holland 2001, 205-219. http://www.elsevier.com/gej-ng/10/15/22/67/33/34/article.pdf):

- Un Gestor de Identidad (IDM), del lado del usuario.
- Apoyo al IDM en las aplicaciones (por ejemplo, en los proveedores de contenidos, tiendas web, etc.).
- Distintos servicios de terceros.

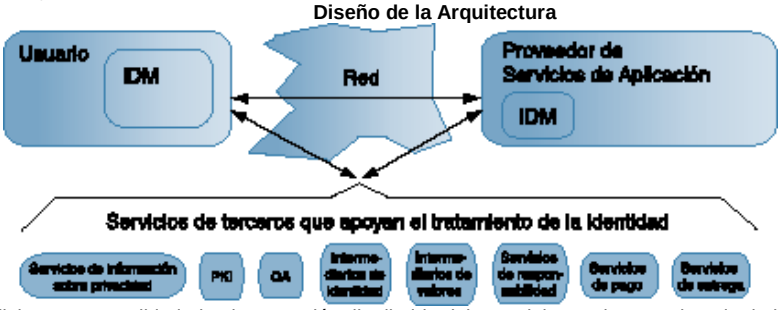
Un IMS completo que refuerce la privacidad debe incluir un gestor de identidad IDM, apoyo al mismo en las aplicaciones y distintos servicios de terceros

Algunas terceras partes ofrecen servicios de certificación, necesarios para la autenticación segura de los usuarios. Pueden soportar diversos grados de minimización de datos, por ejemplo permitiendo la autenticación de seudónimos (pero con responsabilidad). Los terceros pueden ofrecer distintos servicios de mediación: los intermediarios de identidad, por ejemplo, revelan la identidad que se oculta bajo un seudónimo en ciertas circunstancias concretas. Los servicios de responsabilidad saldan una deuda o resuelven una reclamación, en nombre de quien posee un seudónimo. Un intermediario de valores puede realizar una compraventa sin revelar datos personales adicionales. La imposibilidad de relacionar "quién (compra)" con "qué (se compra)" en una compra parcialmente en línea, puede conseguirse aplicando la "separación del conocimiento" entre el pago y la entrega (es decir, ni quien realiza el pago ni quien realiza la entrega posee los detalles completos del usuario). Asimismo, la infraestructura de comunicación tiene que soportar una seguridad y una privacidad básicas (por ejemplo, autenticación en la red, confidencialidad y posiblemente anonimato), así como la fiabilidad. Los principios de distribución de confianza y separación entre conocimiento y poder deben aplicarse en el diseño de los servicios de terceros, a fin de limitar la amenaza de que se comparta información entre terceros. Igualmente, los usuarios deben poder ejercer sus preferencias en cuanto a confianza.

El IDM del usuario actúa como pasarela central de todas las comunicaciones entre distintas aplicaciones, como navegar por la web, comprar en tiendas de Internet o realizar trámites administrativos con autoridades gubernamentales

El IDM del usuario actúa como pasarela central de todas las comunicaciones entre distintas aplicaciones, como navegar por la web, comprar en tiendas de Internet o realizar trámites administrativos con autoridades gubernamentales. Actuando como pasarela central, permite que el usuario sea consciente de la circulación de sus datos personales, y controle su suministro de acuerdo con sus necesidades concretas.

Diseño de la Arquitectura



Como se ha dicho ya, es posible la implementación distribuida del IDM del usuario. Por ejemplo, la interfaz gráfica de usuario (GUI) se puede implementar en aparatos móviles (menos potentes), mientras que otros módulos se sitúan en una estación fija más potente, utilizando una comunicación segura con la GUI externa. También, una parte del IDM del usuario puede situarse en un proveedor de IDM.

Los IDM en los servicios de aplicación se necesitan principalmente para manejar peticiones anónimas o bajo seudónimo, y especialmente la autenticación de los usuarios bajo seudónimo. También proporcionan al usuario información contextual sobre la transacción, por ejemplo, información sobre las propiedades que necesita el seudónimo.

Para conseguir una interoperabilidad máxima, se han de definir normas comunes para los protocolos e interfaces, de modo que sea posible una combinación con los sistemas existentes para reforzar su funcionalidad con respecto a la privacidad.

Nuestra visión de un IMS que refuerce la privacidad sólo puede alcanzarse plenamente si diseñamos las aplicaciones, los instrumentos y las infraestructuras de comunicación de modo que soporten la arquitectura IM y las tecnologías propuestas. Desde luego, su implementación tendrá lugar siguiendo un ciclo evolutivo, ya que las tecnologías que los apoyan se introducirán gradualmente y coexistirán con los sistemas actuales.

Los IMS que refuerzan la privacidad son necesarios para preservar y actualizar el concepto de privacidad en la sociedad de la información.

Con los sistemas de tratamiento de la identidad (IMS), las personas pueden dejar que los ordenadores manejen explícitamente sus identidades (por ejemplo, sus funciones); esto lo han hecho los seres humanos de modo, sobre todo, implícito, durante siglos. Puede haber aquí una oportunidad de nueva concienciación, e incluso de la aparición de nuevas propiedades del yo, que son invisibles sin un medio adecuado[172]. Esto significa que los IMS deben abordar tanto los aspectos interpersonales como los intrapersonales del tratamiento de la identidad. Pero, para mucha gente, puede ser también difícil captar la imposibilidad de manejar de forma puramente implícita las identidades, así como la opción de afirmar directamente el propio derecho a la privacidad. Para evitar la aparición de una brecha entre los que gozan de privacidad y los que no la tienen, la implementación de los IMS ha de ir acompañada por un proceso de educación de los usuarios. Los usuarios deben ser formados en los conceptos digitales relacionados con la privacidad, así como en utilizar IMS reales. Es necesario aprender las limitaciones del tratamiento digital de la identidad, por ejemplo, que los IMS no pueden garantizar la privacidad, ni pueden dar a los usuarios una información completa, porque no son

[172] Turkle, S. Life on the Screen. Identity in the Age of the Internet. Simon & Schuster, Nueva York.

conscientes de todo el conjunto de operaciones realizadas con unos datos determinados (la infraestructura de comunicaciones añade información sobre direccionamiento; los participantes en la comunicación obtienen, venden y fusionan datos...). Cuando se considera el complejo mundo digital y los derechos de privacidad, es un verdadero desafío diseñar GUI adecuados para distintos aparatos, dado también que pueden tener que adaptarse específicamente a un contexto cultural o a un marco legal. La fiabilidad del sistema es muy importante, pero incluso los usuarios experimentados no son normalmente capaces de evaluar la seguridad de su gestor de identidad o de otras partes del sistema de tratamiento de la identidad. Necesitan apoyos tales como una evaluación profesional del sistema de acuerdo con criterios de seguridad y privacidad, auditorías por consultores de privacidad, o la ayuda de servicios de información sobre privacidad. La concentración de datos personales delicados en un IMS convierte a éste en un objetivo atractivo para las terceras partes. Obviamente, hay que desarrollar tecnologías que garanticen su seguridad.

3.3.3 Perspectivas de las normas legales en la privacidad.

Los IMS permiten actualizar la tecnología sobre privacidad, de modo que cumpla con la legislación sobre dicho tema. Las normas existentes que autorizan y regulan el tratamiento de los datos personales pueden haberse redactado sin conocer estas nuevas tecnologías y cómo pueden reforzar la privacidad sin comprometer la seguridad. De hecho, estas normas deben reevaluarse para permitir el uso de transacciones anónimas o bajo seudónimo.

No todas las invasiones de la privacidad dependen de datos personales identificables. Aunque se utilicen seudónimos, es posible

discriminar o perjudicar a un individuo, y los IMS no pueden evitarlo por completo. Este tipo de invasiones de la privacidad no está plenamente cubierto por el actual derecho a la "autodeterminación informativa"[173]. Al actualizar las leyes tales como la Directiva de la UE sobre Protección de Datos, se podría considerar la posibilidad de adoptar un punto de vista más amplio sobre la privacidad.

Es necesarios frecuentes análisis interdisciplinarios sobre el futuro de la identidad y de la privacidad[174] que debe mostrar el camino hacia IMS completos, que refuercen la privacidad. Para esta discusión, son necesarios los conocimientos tecnológicos: el mundo digital funciona de modo diferente al mundo real. Puede amenazar la privacidad, pero también proporciona medios para hacer frente a estas amenazas, o incluso ofrece oportunidades para una mejor protección de la privacidad de lo que ha sido posible hasta ahora.

3.3.4 La plataforma P3P y la privacidad de los datos.

P3P, Plataforma de Preferencias de Privacidad (Platform for Privacy Preferences), que nace ante la necesidad de garantizar la privacidad en una Web cada vez más extensa. P3P es un lenguaje estándar que ofrece a los usuarios una forma sencilla y automatizada de controlar en mayor medida el uso que se hace de su información personal en los sitios Web que visitan. P3P permite a los sitios Web trasladar sus prácticas de privacidad a un formato estandarizado y procesable por dispositivos (basado en XML) que puede ser recuperado de forma automática y que además puede ser interpretado fácilmente por los navegadores de los usuarios. Una vez completada una simple configuración del servidor, el sitio Web informará automáticamente a los visitantes de la página que ese sitio Web es compatible con P3P. En el lado del usuario, P3P

---

[173] Tribunal Constitucional Aleman, sentencia de 15 de diciembre de 1983, publicada en BJC boletín de Jurisprudencia constitucional, numero 33, Enero 1984, Publicaciones de las Cortes Generales, Madrid. Trad. Manuel Daranas. Pp. 126-170.

[174] Bogdanowicz, M., y Beslay, L., Ciberseguridad y futuro de la identidad. The IPTS Report, nº. 57, JRC Sevilla, septiembre 2001. http://www.jrc.es/pages/ICT4E576.htm

automáticamente busca y lee las políticas de privacidad del sitio Web. Un navegador equipado para utilizar P3P puede comprobar una política de privacidad de un sitio Web e informar al usuario sobre las prácticas de información de ese sitio. El navegador puede entonces comparar automáticamente la declaración con las preferencias de privacidad del usuario, pautas reguladoras u otra variedad de estándares legales desde todo el mundo.

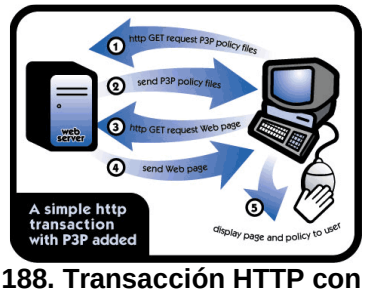


Ilustración 188. Transacción HTTP con P3P.

El siguiente ejemplo muestra un caso hipotético de uso de P3P.

Claudia, un usuario que desea realizar la compra de un libro por Internet, decide echar un vistazo a una tienda llamada EjemploCatalogo, cuya dirección es http://www.catalogo.ejemplo.com/. Supongamos que EjemploCatalogo tiene instalada una política P3P en todas sus páginas y que Claudia utiliza un navegador con P3P. Claudia escribe la dirección de EjemploCatalogo en su navegador, el cual identifica automáticamente la política P3P de esa página. La política indica que los únicos datos que el sitio Web recoge en su página principal son los datos encontrados en registros de acceso HTTP estándares. Lo siguiente que hace el navegador de Claudia es comparar esta política con las preferencias que Claudia ha introducido. ¿Acepta Claudia esta directiva? o ¿debería ser avisada? Supongamos que Claudia le ha indicado a su navegador que acepta esa directiva. En ese caso, la página principal se muestra normal, sin la aparición de mensajes de aviso. Quizá su navegador muestre un pequeño icono en algún lateral de la ventana del navegador que indica que el sitio Web tiene una política de privacidad que concuerda con sus preferencias. Después, Claudia, a través de un vínculo en la página, accede al catálogo que está en el sitio Web. El catálogo utiliza cookies para la opción de "cesta de la compra". En esta parte del sitio Web la política P3P es diferente al tratar de obtener más información. De nuevo, supongamos que las preferencias de Claudia coinciden con la política de esta parte del sitio Web por lo que no aparecerán mensajes de aviso. Claudia continúa y selecciona unos cuantos libros que desea comprar. El siguiente paso que realiza Claudia es verificar la página. La página de verificación de EjemploCatalogo necesita más información adicional: Nombre y apellidos de Claudia, dirección, número de tarjeta de crédito, número de teléfono, etc. Otra política P3P aparece para esta parte del sitio Web que especifica los datos que se van a recoger en esta sección y el uso que se va a hacer de ellos, en este caso sería finalizar la transacción requerida por Claudia, es decir, finalizar la orden de compra. El navegador de Claudia examina esta política P3P. Imaginemos que Claudia le ha indicado a su navegador que le avise siempre que un sitio Web quiera obtener su número de teléfono. En este caso, se mostrará un mensaje de aviso, que indicará que ese sitio Web quiere saber su número de teléfono, y el contenido de la política P3P. Claudia puede entonces decidir si lo acepta o no. Si lo acepta, podrá continuar con su pedido. Si no lo acepta cancelará la operación. Por otro lado, Claudia podría haber indicado a su navegador que deseaba ser avisada sólo cuando un sitio Web tratase de obtener su número de teléfono para dárselo a terceras partes o para acciones diferentes a la realización de la compra. En este caso, como EjemploCatalogo quiere esos datos para realizar únicamente la compra, Claudia no recibiría avisos de su navegador y podría continuar con la compra.

Tabla 88. Caso de ejemplo de un P3P.

P3P permite a los sitios Web mostrar sus prácticas de privacidad de una forma estándar para que puedan ser identificadas de forma sencilla y automática por los agentes de usuario. Los agentes de usuario P3P permiten a los usuarios estar informados de las acciones que realizará el sitio Web y automatizar, de esta forma, decisiones basadas en esas prácticas cuando sea necesario. El siguiente ejemplo muestra los mensajes que un usuario, como por ejemplo Claudia, obtendría al visitar la página de EjemploCatalogo.

En EjemploCatalogo, nos importa su privacidad. Cuando usted visita nuestro sitio Web para buscar un producto, utilizamos esta información sólo para mejorar nuestro sitio Web y no guardarla de una forma en la que sea posible identificarla. EjemploCatalogo, S.L, forma parte del programa SelloPrivacidadEjemplo. Este programa asegura su privacidad al mantener licencias de sitios Web en un alto nivel de privacidad y al confirmar que estas prácticas en relación a la información obtenida van a seguirse. Las preguntas en relación a esta declaración deben dirigirse a: EjemploCatalogo Paseo del Prado, 30 Madrid, España Correo-e: catalogo@ejemplo.com Teléfono (91 0000000) Si no respondemos a sus dudas, o no se ha hecho de forma satisfactoria, puede ponerse en contacto con: SelloPrivacidadEjemplo en http://www.selloprivacidad.ejemplo.org. EjemploCatalogo, corregirá todos los errores que puedan surgir en relación con la política de privacidad. ¿Qué información recogemos y por qué motivo?: Cuando visita nuestra página recogemos: información básica sobre su equipo y la conexión, para estar seguros de que se le va a ofrecer la información adecuada, y también por razones de seguridad. información sobre las páginas Web visitadas por los usuarios para mejorar nuestro sitio Web. Retención de datos: Eliminamos la información obtenida después de un mes.

Tabla 89. Detalle del ejemplo de aplicación P3P.

El código de la declaración P3P anterior podría ser el siguiente:

```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
 <POLICY name="navegadores" xml:lang="es"
  discuri="http://www.catalogo.ejemplo.com/PrivacidadNavegar.html">
  <ENTITY>
   <DATA-GROUP>
    <DATA ref="#business.name">
     EjemploCatalogo</DATA>
    <DATA ref="#business.contact-info.postal.calle">
     Murillo, 30</DATA>
    <DATA ref="#business.contact-info.postal.ciudad">
     Madrid</DATA>
    <DATA ref="#business.contact-info.postal.pais">
     España</DATA>
    <DATA ref="#business.contact-info.online.email">
     catalogo@ejemplo.com</DATA>
    <DATA ref="#business.contact-info.telecom.telefono.codigo">
     91</DATA>
    <DATA ref="#business.contact-info.telecom.telefono.numero">
     + 34 91 0000000</DATA>
   </DATA-GROUP>
  </ENTITY>
  <ACCESS><nonident/></ACCESS>
```

```
 <DISPUTES-GROUP>
  <DISPUTES resolution-type="independent"
    service="http://www.SelloPrivacidad.ejemplo.org"
    short-description="SelloPrivacidad.ejemplo.org">
   <IMG src="http://www.SelloPrivacidad.ejemplo.org/Logo.png"
     alt="Sello de Privacidad"/>
   <REMEDIES><correct/></REMEDIES>
  </DISPUTES>
 </DISPUTES-GROUP>
 <STATEMENT>
  <PURPOSE><admin/><develop/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><business-practice /></RETENTION>
  <!- Nota: la política de privacidad del sitio debe mencionar
      que se eliminan los datos cada dos semanas, o por lo menos,
      proporcionar un vínculo a esa información. -->
  <DATA-GROUP>
   <DATA ref="#dynamic.clickstream"/>
   <DATA ref="#dynamic.http"/>
  </DATA-GROUP>
 </STATEMENT>
</POLICY>
</POLICIES>
```

Tabla 90. Código del ejemplo de aplicación P3P

3.4 Aspectos convergentes entre privacidad y el protocolo de Internet Ipv6

En la actualidad el buen desarrollo de IPv6 depende en gran medida de que los usuarios tengan confianza en dicho Protocolo y conozcan sus ventajas: autoconfiguración, más direcciones IP, movilidad optimizada, extensibilidad, posibilidad de mejora de calidad y seguridad, entre otras que se indicaron anteriormente en el marco conceptual. Por ello, si IPv6 comienza a generar dudas acerca del peligro que supondría la posibilidad de realizar un seguimiento de la navegación de los usuarios y la consecuente vulneración de su privacidad, la propagación de noticias sobre este tema a través de cualquier medio, podría perjudicar gravemente el desarrollo de este Protocolo. De hecho, ya en los últimos años, comenzaron a aparecer los primeros titulares acerca de las consecuencias que IPv6 tendría en temas de privacidad, como consecuencia del uso de “Identificadores únicos” en las direcciones IP configuradas en base a IPv6. En concreto, la preocupación entonces se basaba en la posibilidad de monitorizar a los individuos mediante el seguimiento de las actividades realizadas por Internet o contenidas en cada paquete de información transmitida. Este debate cruzó el Atlántico y tanto el Consejo de Europa como el Grupo del Artículo 29 de la Comisión Europea

reconocieron que es necesario tener en cuenta los aspectos relativos al derecho a la privacidad en el desarrollo e implantación de IPv6. El objeto del presente capítulo es analizar estas consideraciones, cómo éstas se encuentran o no reguladas, si estas consideraciones se encuentran justificadas y, en su caso, qué pasos se deben llevar a cabo.

IPv6 ha sido llamado el Nuevo Internet o el Internet de la Nueva Generación. El principal problema que ha tenido la anterior versión del protocolo IP ha sido que Internet ha crecido tan rápido a lo largo de los últimos años que se preveía el próximo agotamiento de las direcciones IP existentes. Las comunicaciones a través de Internet son posibles gracias a un sistema denominado IP(Internet Protocol) el cual requiere que cada ordenador, dispositivo o nodo conectado a la Red tenga una dirección, denominada dirección IP. La actual versión de este Protocolo de Internet es IP en versión 4 (IPv4), la cual sigue siendo usada. Adicionalmente, la distribución de direcciones IP en IPv4 estaba descompensada ya que un tercio del número de direcciones a distribuir a nivel mundial estaban reservadas, inicialmente, para Estados Unidos, de hecho, dos universidades estadounidenses disponían de más direcciones IP que la propia China. De hecho por ejemplo en la actualidad Google posee bajo su tutela una gigantesca cantidad de direcciones IPv6. ¿ Para que las quiere ?. En concreto, y según pude leer en un artículo publicado por ZDNet, Google posee 7,9 x 10^{28} o 2^{96} direcciones IPv6. Según podemos comprobar en el Whois de Arin, estas direcciones abarcan desde la: 2001:4860:0000:0000:0000:0000:0000:0000 hasta la 2001:4860:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. En principio Arin tan solo asigna tal gigantesca cantidad de IPs a menos que tenga pensado transformarse en un proveedor de servicios, planee proporcionar conectividad IPv6 a organizaciones o se transforme en un LIR (Local Internet Registry) Google. Ya los informáticos que crearon Internet vislumbraron este problema de insuficiencia de direcciones IP con IPv4 y comenzaron a desarrollar una versión básica de lo que hoy es IPv6. Esta nueva versión tiene la capacidad suficiente como para facilitar mil millones de direcciones IP por cada metro cuadrado de la Tierra. En términos matemáticos, este hecho se ha conseguido cambiando de una dirección IP de 32 bits con IPv4 a otra de 128 bits con IPv6, lo cual supone claramente un importante desarrollo de Internet y de las tecnologías con él relacionadas. La transición de IPv4 a IPv6 es un paso enorme que necesita una importante inversión tanto en investigación y desarrollo como en tecnología, lo cual implica que finalmente estas actividades tengan una gran presencia y requieran una importante colaboración a nivel internacional. Aparte del problema de falta de direcciones IP ya solucionado con IPv6, el desarrollo de IPv6 permitirá disponer de una arquitectura y diseño de Internet que potenciará servicios más rápidos, eficaces, de mejor calidad y más seguros. IPv6 resuelve ciertos asuntos existentes en el Internet actual y permite otros relativos a la conectividad extremo a extremo, autoconfiguración, seguridad embebida, movilidad, multidifusión y permite la transmisión de paquetes de información más grandes. Si bien, la introducción de este nuevo protocolo de Internet es cada vez más necesaria e inevitable, continúa aumentando la necesidad de analizar los riesgos que para la privacidad podrían existir como consecuencia del diseño de direcciones IP basadas en Identificadores Únicos.

Tabla 91. Breve referencia.

3.4.1 Relación existente entre intimidad y protección de datos.

Desde la promulgación de la Convención de 1950, una nueva faceta de la intimidad comenzaba a desarrollarse, directamente vinculada con los avances tecnológicos que estaban ocurriendo y, en concreto, con el importante aumento de tratamientos automatizados de información. Esta nueva faceta de la intimidad vino a denominarse “protección de datos”, convirtiéndose este concepto en el arma para proteger la intimidad frente a la nueva Era tecnológica.

En este sentido, si bien la Carta de los Derechos Fundamentales recogía el derecho a la intimidad ya contemplado en la Convención de 1950, introducía un concepto novedoso: el derecho a la protección de datos. Su artículo 8 establece lo siguiente:

1.- Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2.- Estos datos se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3.- El respeto de estas normas quedará sujeto al control de una autoridad independiente.

En este sentido, basta con apuntar que la implantación de IPv6 conlleva asimismo implicaciones en materia de protección de datos, algunas de las cuales serán tratadas brevemente en el presente Capítulo. No obstante, la principal problemática existente sobre este tema será abordada con mayor detenimiento en el Capítulo siguiente de la presente tesis.

3.4.2 La regulación de la protección de datos.

Si bien, esta normativa será analizada con más profundidad en el siguiente Capítulo, es conveniente adelantar que la primera legislación en materia de protección de datos puede remontarse a la Ley aprobada por el Estado de Hesse en Alemania en el año 1970. Posteriormente, se promulgaron otras legislaciones tales como la de Suecia (1973), los Estados Unidos (1974), Alemania (1977) y Francia (1978).

La primera legislación importante en esta materia a nivel europeo fue el Convenio del Consejo de Europa de protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981, a través del cual se fijaron principios específicos a tener en cuenta

en el tratamiento de datos personales. A través de estos principios, se establece la protección necesaria a tener en cuenta en cada paso del tratamiento de datos desde su obtención, hasta su almacenamiento y difusión.

El Convenio de 1981 creó las bases para el nuevo derecho de protección de datos y estableció el nexo de unión entre este derecho y el derecho a la intimidad, basando la protección de los datos personales en la protección al derecho a la intimidad.

El objetivo de este Convenio fue fortalecer el derecho a la protección de datos, es decir, conferir una protección legal a los tratamientos automatizados de datos personales que se efectuaran. En este sentido, pretendía crear una serie de reglas que orientasen respecto a cómo debía ser tratada la información personal y cómo cada titular de los datos debería poder tener el control sobre tales tratamientos.

Posteriormente, los principios básicos del Convenio de 1981 fueron tenidos en cuenta en las tres principales directivas promulgadas en la Comunidad Europea sobre la materia:

- La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- La Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
- La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

La primera Directiva creó el primer marco regulatorio que permitía el libre movimiento de datos pero garantizando el respeto del derecho a la

intimidad. En este sentido, reconocía que los avances continuos de carácter tecnológico desarrollados en los últimos tiempos habían generado nuevas formas de obtener, transmitir, manipular, grabar y almacenar datos personales. Por este motivo, fue redactada de una forma flexible con el fin de que pudiera ser fácilmente adaptada a los nuevos avances tecnológicos por suceder.

La definición legal de "datos personales" se extendió hasta hacer referencia a "cualquier información relativa a una persona física identificada o identificable (titular de los datos); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social". La relevancia de esta definición respecto al fenómeno IPv6 estriba principalmente en la referencia que realiza a un número como elemento de identificación.

La Directiva estableció reglas generales para el tratamiento de datos personales tales como el principio de calidad de los datos, los criterios para efectuar un tratamiento legítimo de datos, el deber de informar al titular de los datos; el derecho del titular de los datos a acceder a su información personal, su derecho de oposición, la confidencialidad y seguridad de los datos, notificaciones, el régimen sancionador, las transferencias internacionales de datos, los códigos de conducta y las autoridades de control.

Asimismo, el artículo 29 de la Directiva 95/46 creó un grupo independiente (Grupo del Artículo 29) cuya principal función es examinar, opinar, aconsejar y emitir recomendaciones relativas a cómo el tratamiento de datos personales podría impactar en los derechos y libertades de las personas.

Por otro lado, la Directiva 97/66 pretendió extender los principios consagrados en la Directiva 95/46 y aplicarlos al sector de las telecomunicaciones, como consecuencia del pronunciamiento de la Comisión por el cual establecía que en la actualidad **"están apareciendo nuevas redes digitales públicas avanzadas de telecomunicación que crean necesidades específicas en materia de protección de datos personales y de la intimidad de los usuarios, estando el desarrollo de la sociedad de la información caracterizado por la introducción de nuevos servicios de telecomunicaciones"**.

La utilización de nuevas redes de telecomunicaciones como es el caso de la red SURFTnet6[175] entre otras, crean un conjunto de nuevos tipos de datos, los cuales no tienen por qué quedar claramente ubicados en los conceptos de "Datos personales" existentes hasta aquel momento. Por ello, esta Directiva se entendió como un medio para adecuar estas nuevas situaciones basadas en los novedosos avances tecnológicos a esta legislación vigente.

Sin embargo, esta Directiva rápidamente necesitó adaptarse a los nuevos cambios producidos en relación con el mercado y las tecnologías derivadas de los servicios de comunicaciones electrónicas, con el fin de aportar un nivel de protección en materia de protección de datos personales e intimidad equiparable al que existía para el sector de las comunicaciones electrónicas.

En este sentido, la Directiva 2002/58/CE fue promulgada como una respuesta a las nuevas tecnologías introducidas (por ejemplo redes digitales móviles), las cuales abrían un amplio abanico de posibilidades para los usuarios pero también importantes riesgos para su intimidad y

[175] Como por ejemplo las nuevas redes de telecomunicaciones de SURFnet6 que son redes inteligentes y configurables de alta densidad de Nortel que a la actualidad soporta la mayor red de investigación del mundo; cuenta con una plataforma de última generación para los investigadores que trabajan con aplicaciones que demandan de tecnología de banda ancha, como la física de ingeniería superior y las investigaciones medicas. Que es una red de infraestructura hibrida de alta velocidad y con conexión empaquetada que dispone de capacidad nativa Ipv4, Ipv6 y Lightpath. Siendo esta infraestructura de transmisión construida utilizando los productos de próxima generación de la gama óptica y de Metro Ethernet de Nortel, que incluyen: Common Photonic Layer(CPL), una gama de productos Optical Multiservice Edge 1000 y 6500, Optical Metro 5000 y Metro Routing Switch(MERS) 8600.

privacidad. Esta Directiva pretendió aportar seguridad a los usuarios garantizando que su intimidad no se vería puesta en riesgo como consecuencia de estos nuevos avances.

A pesar de ello, la Directiva 2002/58 no introdujo demasiados cambios respecto a la regulación de la anterior Directiva 97/66. Por el contrario, se dedicó a adaptarla y actualizarla a los nuevos desarrollos surgidos en el sector de las comunicaciones electrónicas. Por ello, esta nueva regulación pretendía unificar las telecomunicaciones, los medios y la tecnología de la comunicación y extenderse a toda la infraestructura de comunicaciones existente y a los servicios asociados con ésta siempre bajo la premisa de neutralidad tecnológica. La filosofía perseguida era la siguiente: el mismo servicio es regulado de la misma forma, independientemente de cómo es prestado o llevado a cabo.

El Considerando 6 de la Directiva 2002/58 establecía lo siguiente: *"Internet está revolucionando las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas.*

Los servicios de comunicaciones electrónicas disponibles al público a través de Internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad."

En conclusión, las tres mencionadas Directivas pretendían asegurar la existencia de protección suficiente en lo que a tratamientos automatizados de datos se refiere, fuera la tecnología que fuera a través de la cual se realizaran dichos tratamientos. Internet y, por lo tanto, IPv6, quedaron sometidos a las reglas y principios recogidos en estas Directivas.

La adecuación de estas tres directivas al fenómeno de IPv6 será tratado con mayor detenimiento en el siguiente capitulo. No obstante, es importante adelantar que los principios fundamentales existentes en materia de protección de datos personales son los siguientes:

- Obtención legal y legítima de los datos personales.

- Uso de los datos únicamente para las finalidades de tratamiento identificadas inicialmente.
- Datos adecuados, pertinentes y no excesivos.
- Datos actualizados, reales y exactos.
- Datos accesibles para su titular.
- Mantenimiento de los datos en condiciones seguras.
- Datos borrados o cancelados una vez que dejen de ser necesarios.

Por lo tanto, aquellas entidades involucradas en el diseño y desarrollo de IPv6 deberán tener en cuenta estos principios para asegurar que, desde el inicio, se garantiza su respeto, el cual debe continuar durante el funcionamiento de este Protocolo.

3.5 Peligros con relación al protocolo de Internet de próxima generación.

Para conocer cuáles son los principales peligros para la privacidad en relación con Internet y con IPv6, es necesario indicar que Internet es una gran red de ordenadores comunicados los unos con los otros a través del Protocolo TCP/IP. A través del Protocolo IP, los ordenadores son capaces de comunicarse entre sí, estando cada uno de ellos identificado por una única dirección IP(en IPv4 esta dirección estaba compuesta por 32 bits y en IPv6 por 128) según las especificaciones conceptuales que se dio en el anterior capítulo. Ahora, el hecho que convierte IPv6 en un posible problema para la privacidad y la protección de datos parte de la necesidad de conocer si una dirección IP puede ser un dato personal, lo cual será analizado en el capítulo siguiente. En concreto, si una dirección IP es considerada como un dato personal en sí, entonces el tratamiento de estos datos personales estará protegido por las normas que regulan el derecho a la privacidad y la protección de datos.

Existen numerosos participantes en Internet, entre los cuales se pueden destacar los siguientes:

- Las industrias de software, ordenadores y telecomunicaciones que diseñan las redes de servicios disponibles.
- Los operadores de telecomunicaciones que proporcionan la red para la transferencia de datos.
- Los proveedores de acceso a Internet responsables del sistema de transporte de Internet.
- Los Proveedores de servicios de Internet, que proporcionan servicios como HTTP(a menudo como el ISP).
- Los usuarios.

Cada uno de estos participantes tiene su propia responsabilidad con respecto a la protección de datos y respeto a la privacidad y debe observar sus competencias así como el servicio que proporciona para asegurarse de que sus acciones cumplen con la normativa vigente aplicable.
Un informe publicado por el Grupo Internacional de Protección de Datos en Telecomunicaciones("Budapest - Berlin Memorandum on Data Protection and Privacy on the Internet") de 1996, proporciona una visión general de la Privacidad en Internet que afecta a Internet en general.
Dicho documento explica que el vasto crecimiento de Internet había creado lo que había sido denominado como el primer nivel de la emergente Infraestructura Global de Información (IGI) que potencialmente causaba numerosos problemas en relación con la privacidad. Existen varios participantes en Internet y cada uno cuenta con diversas tareas, intereses y oportunidades y los principios de privacidad y de protección de datos deben ser observados en todos esos diferentes estadios.

"Considerando que Internet no está bajo un solo órgano regulador que supervise todos los aspectos de la privacidad y la protección de datos a una escala global, el usuario está obligado a confiar en la seguridad de toda la red, que es cada componente de la misma, con independencia de donde se encuentre localizado o por quien esté dirigido".

El documento establece que hay ciertas entidades (internacionales, regionales o nacionales) que dirigen varias funciones en la Red y considerando el hecho de que no existe un órgano de gobierno para Internet, el papel de estas entidades es importante, en particular **cuando se desarrollan los protocolos y los estándares para Internet, se fijan reglas para la identificación de los servidores conectados y eventualmente para la identificación de los usuarios.** Esto es directamente aplicable al contexto de IPv6.

"Debe encontrarse un equilibrio entre la persona que no quiere dejar sus huellas en la Red y el hecho de que los proveedores necesiten su identificación y autenticación para ayudar con las tareas de marketing y de tarificación".

El mencionado Grupo de Protección de Datos en las Telecomunicaciones publicó un plan de 10 puntos con una visión general de los principios que deben tenerse en cuenta en estas materias.

El plan de 10 puntos establece:

> **"No puede haber duda de que la protección legal y técnica de la privacidad de los usuarios en Internet es actualmente insuficiente".**

Por una parte, el derecho de cada individuo para usar la información en Internet sin ser observado ni identificado debe estar garantizado. Por otra parte, debe haber límites (barreras) con respecto al uso de los datos personales por terceras personas en la Red.

Una solución al dilema básico debería ser fundada en los siguientes niveles:

1) Los proveedores de servicios deberían informar inequívocamente a cada potencial usuario sobre los riesgos para la privacidad existentes

en la Red. El usuario debe hacer balance de los riesgos frente a los posibles beneficios.

2) En muchas circunstancias, la decisión de entrar en Internet y decidir cómo usarla, está sujeta a la regulación legal establecida para la protección de datos por cada Estado.
3) Deben ser apoyadas las iniciativas para una mayor cooperación internacional, incluyendo una convención internacional que regule la protección de datos en el contexto de las redes internacionales y servicios.
4) Debe establecerse un mecanismo internacional de supervisión que debe ser construido sobre la base de las estructuras ya existentes tales como la Sociedad de Internet y otras entidades. La responsabilidad por la protección de la privacidad debe ser institucionalizada en cierta forma.
5) El derecho internacional y nacional debe establecer inequívocamente que el proceso de comunicación (vía correo electrónico) se encuentra protegido por el secreto de las telecomunicaciones.
6) Además es necesario desarrollar medios técnicos para mejorar la privacidad de los usuarios en la Red. Es obligatorio desarrollar principios para la información y las comunicaciones tecnológicas y multimedia, hardware y software, que habiliten al usuario para controlar el tratamiento de sus datos personales.
7) **Los medios técnicos deben también ser usados para proteger la confidencialidad. El uso de los métodos de codificación deben constituirse y permanecer como una opción legítima para cada uno de los usuarios de Internet. El Grupo de Trabajo apoya los nuevos progresos del Protocolo de Internet(IPv6), que proporciona medios para mejorar la confidencialidad de la codificación, la clasificación de mensajes y una mejor autenticación de los procesos. Los productores de software deberían implementar los estándares de seguridad del nuevo**

Protocolo de Internet en sus productos y deberían proporcionar el uso de estos productos lo más rápido posible.

8) El Grupo de Trabajo aprobaría un estudio de la viabilidad para establecer un nuevo procedimiento de certificación que expida "sellos de calidad" para los proveedores y los productos, del tipo de un certificado de aprobación de la privacidad.
9) El anonimato es un valor adicional esencial para la protección de la privacidad en Internet. Las limitaciones al principio de anonimato deberían estar restringidas a lo que es estrictamente necesario en una sociedad democrática sin cuestionar tal principio.
10) Finalmente será decisivo descubrir como la "auto-regulación" a través de una "Netiqueta"[176] y la tecnología protectora de la privacidad podrían mejorar la implementación de una normativa internacional y nacional de protección de la privacidad.

No será suficiente con confiar en cada una de estas vías de acción: éstas deben estar combinadas de forma efectiva para alcanzar la Infraestructura Global de Información que respeta el derecho humano a la privacidad y a las comunicaciones inadvertidas.

El Grupo de Trabajo del Artículo 29, observando los aspectos fundamentales con respecto a Internet, estableció unas directrices generales. En dicho artículo se determinaba que:

- **"Internet fue concebido como una red abierta a nivel de trabajo (www) a través de la cual la información podía ser compartida. Sin embargo, es necesario encontrar un equilibrio entre la "naturaleza**

[176] Es la etiqueta que se utiliza para comunicarse en la Red o sea, la etiqueta del Ciberespacio. Y etiqueta significa "las normas requeridas por la buena educación o prescritas por una autoridad para ser tenidas en cuenta en la vida social o la oficial". En otras palabras, la "Netiqueta" encierra una serie de reglas para comportarse adecuadamente en línea. Se presentan algunas reglas básicas de las Netiquetas: 1) Recuerde lo humano**,** 2) Siga en la Red los mismos estándares de comportamiento que utiliza en la vida real, 3) Sepa en que lugar del ciberespacio está. *La "Netiqueta" varía de un dominio al otro.* 4) Respete el tiempo y el ancho de banda de los demás, 5) Ponga de su parte, véase muy bien en línea *Aproveche las ventajas del anonimato,* 6) Comparta el conocimiento de los expertos, 7) Ayude a que las controversias se mantengan bajo control, 8) Respeto por la privacidad de los demás, 9) No abuse de las ventajas que pueda usted tener, 10) Excuse los errores de otros.

abierta" de Internet y la protección de los datos personales de los usuarios de Internet (proporcionalidad).

- **Una gran cantidad de datos personales de los usuarios de Internet son recopilados a través de las páginas de Internet pero, sin embargo, a menudo los usuarios no son conscientes de este hecho. Esta falta de transparencia hacia los usuarios necesita ser redirigida para alcanzar un óptimo nivel de protección de los usuarios.**
- **Los protocolos son medios técnicos a través de los cuales se establece cómo los datos deben ser recogidos y procesados. Los programas software y navegadores web juegan también un papel importante ya que, en algunos casos, incluyen un identificador que hace posible relacionar un usuario de Internet con las actividades que ha realizado en la Red. Por lo tanto, es responsabilidad de aquellos que se encuentran involucrados en el diseño y el desarrollo de estos productos, el ofrecer a estos usuarios las soluciones que permitan cumplir con la normativa de protección de la privacidad de los usuarios".**

La cuestión del anonimato ha sido específicamente tratada en la Recomendación 3/97 sobre Anonimato en Internet de 3 de diciembre de 1997, en la cual se establece que:

"A lo largo de los últimos 25 años, se ha ido haciendo patente que una de las mayores amenazas que pesan sobre el derecho fundamental a la intimidad es la capacidad que tienen algunas organizaciones de acumular gran cantidad de información sobre los particulares, en forma digital, que permite su manipulación, alteración y transmisión a terceros con enorme rapidez (y actualmente a un coste muy bajo). La inquietud que suscita esta evolución y la posibilidad de que se haga uso indebido de tales datos personales ha llevado a todos los Estados miembros de la UE (y ahora a la Comunidad, con la Directiva 95/46/CE) a adoptar disposiciones específicas sobre protección de datos en las que se establece un marco normativo que regula el tratamiento de la información de carácter personal".

Una característica de las redes de telecomunicaciones, y de Internet en particular, es su capacidad de generar una ingente cantidad de datos transaccionales (datos generados a fin de asegurar conexiones correctas). La posibilidad de utilizar las redes de modo interactivo (característica específica de numerosos servicios de Internet) hace aumentar aún más la cantidad de datos transaccionales.

A medida que evolucionen los servicios en línea, aumentando su complejidad y su popularidad, irá adquiriendo más importancia el problema de los datos transaccionales.

Sea cual sea el lugar al que se acceda en Internet, se deja un rastro digital, de manera que, al ser cada vez mayor el número de actividades de nuestro que hacer cotidiano que se realizan en línea, irá aumentando la información que sobre nuestras ocupaciones, gustos y preferencias quede registrada.

Los datos transaccionales sólo suponen una amenaza a la intimidad de las personas si se refieren a alguien identificado o identificable. Es evidente, por tanto, que una manera de conjurar esta amenaza consistiría en cerciorarse de que, siempre que sea viable, los rastros creados al utilizar Internet no permitan identificar al usuario. De garantizarse el anonimato, cualquiera podrá participar en la revolución de Internet sin temor a que queden registrados todos sus movimientos y a que se acumule información sobre su persona que pueda utilizarse más adelante con fines contrarios a su voluntad."

Sin embargo, el principio de anonimato debe estar equilibrado con el "principio de proporcionalidad". La Recomendación se refiere al punto fundamental del anonimato, considerando que debe aplicarse la misma regla de comportamiento que fuera de la Red, a las actividades realizadas a través de la misma.

Finalmente la Recomendación concluye que:

"La posibilidad de mantener el anonimato es fundamental para que la intimidad de las personas goce de la misma protección en línea que fuera de línea". Sin embargo, esto debería estar siempre equilibrado, teniendo en cuenta otras consideraciones como la prevención de delitos. Además, en

relación con los Protocolos de Internet y, por lo tanto, con IPv6, la Recomendación establece que:

"El acceso de los usuarios y las actividades desarrolladas en Internet son raramente anónimas (…), la configuración técnica de los Protocolos de Internet no hace posible en realidad el anonimato (…)".

Internet plantea un problema porque "el uso de la infraestructura está a menudo directamente basado en el tratamiento de los datos personales, del tipo de ciertas direcciones IP".

3.6 IPSec - El elemento de seguridad del Protocolo IPv6.

IPSec es un estándar que tiene como finalidad proporcionar servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP. En cuanto a la utilidad que tiene IPSec, principalmente desde el punto de vista del análisis efectuado anteriormente, es necesario destacar que IPSec, en resumen, autentifica los equipos involucrados en una transmisión de informaciones, y, en función de la configuración que se establezca, puede llegar a cifrar dicha información para su transmisión entre hosts ubicados en una red (Internet, intranet, extranet, etc.), incluidas las comunicaciones que se establezcan entre un servidor y un terminal, cliente o estación de trabajo y entre servidores.

El trabajo de seguridad a nivel de capa IP proporcionado por IPSec tiene como fin principal proveer de protección a los paquetes IP. El Protocolo IPSec está basado es un modelo de seguridad end-to-end, de tal modo que únicamente los puntos de la red emisor y receptor deben ser compatibles con el Protocolo y aceptar la protección de la información transmitida.

El Protocolo IPSec viene siendo utilizado (por ejemplo, en la creación de Redes Privadas Virtuales o RPV) con la versión 4 del Protocolo IP (IPv4), pero como adicional o añadido al mismo. Sin embargo, en el caso de IPv6, el Protocolo IPSec se ha establecido como elemento intrínseco u obligatorio en el desarrollo e implementación del mismo, con lo que se provee del mayor grado de optimización a la vertiente de seguridad de la versión 6 del Protocolo.

Asimismo, el Protocolo IPSec, diseñado para funcionar de modo transparente en redes existentes, cuenta, entre una de sus ventajas fundamentales, el haber sido desarrollado sobre el apoyo de estándares del Internet Engineering Task Force (IETF), grupo internacional de expertos vinculados a la evolución de la arquitectura de Internet y su óptimo funcionamiento. Los resultados de las actividades de los diferentes equipos de expertos se reflejan, entre otras vías, a través de los denominados Request for Comments (RFC). Respecto a Ipsec tenemos:

- Como ya se ha dicho, se incluye por defecto en el Protocolo IPv6, a diferencia del Protocolo IPv4, donde la integración en el mismo era una mera posibilidad. La obligatoriedad de implementación de IPSec en todos los nodos IPv6, permite que, al establecer una sesión IPv6, siempre sea posible disponer de una conexión segura end-to-end.
- Proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones.
- Es independiente de la tecnología física empleada.
- Es compatible con infraestructuras de clave públicas (PKIs).
- Se implementa de forma transparente en la infraestructura de red.
- Es un estándar abierto del sector para proporcionar comunicaciones privadas y seguras. Por tanto, es también un estándar tendente a lograr privacidad, integridad y autenticación. La autenticación y el cifrado de los datos para protegerlos de otros terminales, posibilita la realización de transacciones seguras sobre IPv6. Así, por ejemplo, se podría utilizar el Protocolo IPSec como herramienta que sirviera no sólo para identificar los destinatarios de una transmisión de contenidos amparados por DPI, sino que, además, mediante el cifrado, se estaría evitando la interceptación de los contenidos por terceras partes e, incluso, su posterior reenvío por los destinatarios autorizados a terceros no legitimados.
- Permite asumir el incremento de dispositivos “nómadas”, es decir, aquellos dispositivos que reúnen características de movilidad y posibilidad de conexión a diferentes tipos de redes.

En referencia a la arquitectura de los componentes del protocolo IPsec, interpretaremos, los aspectos técnicos más relevantes de IPSec, con el fin de facilitar la comprensión de las posibilidades que su adopción conllevaría desde la perspectiva de la protección de los datos personales.

IPSec, como primera expresión de su carácter abierto y del esfuerzo de independencia frente a concretos algoritmos de cifrado, es, realmente, un conjunto de estándares para integrar en IP funciones de seguridades basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnología de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de hash (MD5, SHA-1) y certificados digitales X.509 v.3.

La tendencia hacia la neutralidad respecto de los algoritmos utilizados ha llevado a que IPSec se haya diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. No obstante, los problemas de interoperabilidad que podían surgir en Internet, han llevado a la definición de ciertos algoritmos estándar que deberán soportar todas las implementaciones que se realicen.

De esta manera, los algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHA-1, como funciones de hash. Incluso, es posible usar otros algoritmos que se consideren más seguros o adecuados para un entorno específico.

Dentro de IPSec se distinguen los siguientes componentes fundamentales:

- Dos Protocolos de seguridad: IP Authentication Header (AH) e IP Encapsulating Payload (ESP), que proporcionan mecanismos de seguridad para proteger tráfico IP.
- Un Protocolo de gestión de claves: Internet Key Exchange (IKE), que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

El Protocolo AH se utiliza con el fin de garantizar la integridad y autenticación de los datagramas IP. Con más detalle, proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados en su tránsito.

No obstante, entre sus características no se encuentra ninguna dirigida a proporcionar confidencialidad sobre los datos transmitidos. En definitiva, el Protocolo AH es una cabecera de autenticación que se inserta entre la cabecera IP estándar (tanto IPv4 como IPv6) y los datos transportados.

El funcionamiento de AH se basa en un algoritmo HMAC (Hashed Message Authentication Code), es decir, un código de autenticación de mensajes. Este algoritmo consiste en aplicar una función hash a la combinación de datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres denominada "extracto". Dicho extracto tiene la propiedad de ser como una huella personal asociada a los datos y a la persona que lo ha generado, puesto que es la única que conoce la clave.

Por su parte, el Protocolo ESP tiene como fin fundamental proporcionar confidencialidad.

A tal fin, especifica el modo de cifrar la información que se desea enviar y cómo este contenido cifrado se incluye en un datagrama IP. En combinación con un mecanismo similar al del Protocolo AH, el Protocolo ESP logra ofrecer los servicios de integridad y autenticación del origen de los datos.

La función de cifrado dentro del Protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica. De esta manera, el emisor toma el mensaje original, lo cifra, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP.

Durante el tránsito hasta su destino, si el paquete es interceptado por un tercero sólo obtendrá un conjunto de bits ininteligibles. En el destino, el receptor aplicará de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales. Como es fácil apreciar, la seguridad de este Protocolo reside en la robustez del algoritmo de cifrado, es decir, que un atacante no puede descifrar los datos sin conocer la clave, así como en que la clave ESP únicamente la conocen el emisor y el receptor.

A los efectos de determinar una utilidad concreta respecto de los procedimientos técnicos analizados en el presente Capítulo, se podría tener en cuenta un supuesto hipotético que podría ser, por ejemplo, el caso de una compañía discográfica que pretenda emitir contenidos de su catálogo musical por Internet. A través de estos procedimientos, podría llegar a asegurarse de que dichos contenidos musicales protegidos, son recibidos únicamente por los usuarios que, previamente, los hubieran solicitado y hubieran abonado una determinada cantidad de dinero. De este modo, la compañía discográfica conseguiría:

- Confidencialidad del contenido transmitido mediante su cifrado.
- Elección precisa de los destinatarios que van a recibir los contenidos.
- Aportación de garantías, al destinatario, de que los contenidos provienen del emisor correspondiente, que está autorizado para la difusión de los mismos.
- Garantía de integridad de los contenidos protegibles, evitando su modificación por terceros.

No obstante, siguiendo con el ejemplo planteado, independientemente de que la compañía discográfica pueda lograr, al menos, las finalidades señaladas haciendo uso de los protocolos utilizados por IPSec, no es menos cierto que estas ventajas no irían más allá de la concreta transmisión de contenidos a que se refieren, en este caso, la de los archivos musicales.

IPSec se convertiría en un medio de prueba de gran valor en muchos de los casos de violación de las medidas realizadas en Internet, si se piensa en cada una de las transmisiones telemáticas en que se vulneren esos derechos.

Volviendo a la descripción de los Protocolos utilizados por IPSec, es evidente que la distribución de claves de forma segura es, por consiguiente, un requisito esencial para el funcionamiento de los Protocolos ESP y AH, como hemos visto anteriormente. Asimismo, es fundamental que el emisor y el receptor estén de acuerdo tanto en el algoritmo de cifrado o de hash como en el resto de parámetros comunes que utilizan. Esta labor de puesta en contacto y negociación es realizada por un Protocolo de control, denominado IKE, sobre el cual se recogerán sus notas fundamentales más adelante, ya que en este punto del Capítulo cabe hacer una breve referencia a los dos modos de funcionamiento que permite el Protocolo IPSec:

- **Modo transporte.** En este modo, el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte. En consecuencia, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el Protocolo IPSec.
- **Modo túnel.** En éste el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP. Posteriormente, se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

Una vez establecida la cita de los modos de funcionamiento del Protocolo IPSec, se ha de traer a colación un concepto esencial en IPSec cual es el de Asociación de Seguridad (SA, Security Association). Este concepto hace referencia a un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SAs, una por cada sentido de la comunicación. Hasta el momento, se ha supuesto que ambos extremos de una SA deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir datagramas AH o ESP. Tal como se ha indicado anteriormente, es necesario que ambos nodos estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún Protocolo de control que se encargue de la negociación automática de los parámetros necesarios, denominándose esta operación como negociación de SAs. El IETF ha definido el Protocolo IKE (Internet Key Exchange) para realizar tanto esta función de gestión automática de claves como el establecimiento de las SAs correspondientes. Una característica importante de IKE es que es un Protocolo estándar de gestión de claves.
En este sentido, IKE es un Protocolo híbrido que ha resultado de la integración de dos Protocolos complementarios: ISAKMP y Oakley. ISAKMP (Internet Security Association and Key Management Protocol) define de forma genérica el Protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, mientras que Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.
El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec.
Las fases de la negociación son 2:

1. La fase en la que ambos nodos establecen un canal seguro y autenticado. Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra que se obtiene mediante un algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad de los nodos, para ello es necesario un paso adicional de autenticación.
   Existen varios métodos de autenticación, aunque los dos más usuales son los siguientes:
   - Autenticación basada en el conocimiento de un secreto compartido. Mediante el uso de funciones hash, cada extremo demuestra al otro que conoce el secreto sin revelar su valor.
   - Autenticación basada en la utilización de certificados digitales X.509 v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados requiere, lógicamente, el previo establecimiento de una Public Key Infrastructure (PKI).
2. En la segunda fase, el canal seguro IKE es usado para negociar los parámetros de seguridad especificados, asociados a un Protocolo determinado, en nuestro caso IPSec.
   Durante esta fase, se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha información.
   Como último contenido, cabe hacer un somero análisis de las características de los servicios de seguridad que ofrece IPSec. Dichos servicios son:

- Integridad y autenticación del origen de los datos. El Protocolo AH parece el más adecuado si no se requiere cifrado.
- Confidencialidad. El servicio de confidencialidad se obtiene mediante la función de cifrado incluida en el Protocolo ESP. Incluso, el Protocolo ESP también tiene herramientas para ocultar el tipo de comunicación que se está realizando.
- Detección de repeticiones. Los Protocolos ESP y AH incorporan un procedimiento para detectar paquetes repetidos. Esta secuencia no podrá ser modificada por el atacante, debido a que se encuentra protegida por medio de la opción de integridad para cual quiera de los dos Protocolos (AH y ESP) y cualquier modificación en este número provocaría un error en la comprobación de la integridad del paquete.
- Control de acceso: autenticación y autorización. Dado que el uso de ESP y AH requiere el conocimiento de claves, y dichas claves son distribuidas de modo seguro mediante una sesión IKE en la que ambos nodos se autentican mutuamente, existe la garantía de que sólo los equipos deseados participan en la comunicación. La autenticación válida no implica un acceso total a los recursos, ya que IPSec proporciona también funciones de autorización. Durante la negociación IKE se especifica el flujo de tráfico IP que circulará a través de la conexión IPSec.
- No repudio. El servicio de no repudio es técnicamente posible en IPSec, si se usa IKE con autenticación mediante certificados digitales. En este caso, el procedimiento de autenticación se basa en la firma digital de un mensaje que contiene, entre otros datos, la identidad del participante. Dicha firma, gracias al vínculo entre la clave pública y la identidad que garantiza el certificado digital, es una prueba inequívoca de que se ha establecido una conexión IPSec con un equipo determinado, de modo que éste no podrá negarlo. En la práctica, sin embargo, esta prueba es más compleja, ya que requeriría almacenar los mensajes de negociación IKE y, además, no está definido un procedimiento para referenciar este evento a una fecha concreta.

Tabla 92. Arquitectura de los componentes del protocolo IPSec.

3.7 La afectación del protocolo IPv6 con referencia a la privacidad.

Como se ha mencionado anteriormente, a finales de los 90, surgieron comentarios acerca de la preocupación sobre los aspectos fundamentales de la privacidad en relación con IPv6 en los Estados Unidos y estas preocupaciones fueron trasladadas a las autoridades europeas. El primer documento oficial fue emitido cuando la Comisión Europea publicaba la Comunicación 96 (COM, 2002), de 21 de febrero 2002. Esta publicación era una comunicación de la Comisión al Consejo y al Parlamento Europeo titulada "Next Generation Internet – priorities for action in migrating to the new Internet protocol IPv6". La finalidad de este documento fue definir los puntos de vista y las inquietudes de la Comisión Europea referentes al desarrollo de IPv6 en Europa y uno de sus principales aspectos era el tema de la privacidad. El pensamiento de la Comisión Europea queda claramente recogido en el siguiente párrafo:

"Sin embargo, para que la nueva versión de Internet habilite servicios que puedan ser realizados de forma oportuna, es fundamental estructurar, consolidar e integrar los esfuerzos europeos en IPv6, y notablemente desarrollar los medios humanos cualificados para armonizar completamente,

cuando sea necesario, los enfoques en las políticas, para mantener los desarrollos alcanzados, promover los estándares y las especificaciones de trabajo y asegurar que todos los sectores de la nueva economía probablemente afectada por IPv6 sean totalmente conscientes de los potenciales beneficios que pueden derivarse de su adopción."

Asimismo, la Comisión propone una serie de acciones para asegurar que la Unión Europea mantenga la iniciativa y el liderazgo en estos progresos globales. Estas acciones requieren una acción concertada encaminada a la estructuración, consolidación e integración de los esfuerzos europeos en IPv6, notablemente a través de:

- Un apoyo cada vez mayor de IPv6 a través de las redes y servicios.
- El establecimiento y lanzamiento de programas educacionales de IPv6.
- La estimulación continua del establecimiento de Internet a través de Europa.
- La adopción de IPv6 a través de la concienciación promovida por campañas.
- Un apoyo cada vez mayor de las actividades de IPv6, en el sexto Programa Marco.
- La consolidación del apoyo para permitir redes de investigación a nivel nacional y europeo.
- Una contribución activa para la promoción de los estándares de trabajo de IPv6.
- La integración de IPv6 en todos los planes estratégicos concernientes al uso de los nuevos servicios de Internet.

Habiendo sentado las bases, la Comunicación específicamente trata los aspectos fundamentales de la privacidad en relación con IPv6.

"Debido al hecho de que desde sus inicios, Internet ha sido considerado como una red abierta, hay muchas características de sus protocolos de

comunicación que, más por accidente que por diseño, pueden conducir a una invasión de la privacidad de los usuarios de Internet. El derecho fundamental a la privacidad y a la protección de los datos personales es recogido en la Carta de Derechos Fundamentales de la UE y desarrollado en detalle en las Directivas 95/46/CE y 97/66/CE sobre protección de datos personales, las cuales son aplicables al tratamiento de los datos personales en Internet. En su Comunicación sobre la organización y la dirección de los sistemas de dominios en Internet de abril de 2000, la Comisión ya establecía que la dirección IP puede ser un dato personal. Así el Grupo del Artículo 29, el cuerpo asesor independiente de la UE para la protección de datos personales y la privacidad, establecía que la Directiva 95/46/CE llama la atención en numerosas ocasiones a aspectos derivados de la privacidad por el uso de Internet. El Grupo del Artículo 29 así como el Grupo de Trabajo Internacional para la protección de los datos personales en las telecomunicaciones (El "Grupo de Berlín") trabajan especialmente en IPv6. Por lo tanto, es indispensable que la Comisión Europea y la Unión Europea como una sola entidad consideren los aspectos fundamentales relacionados con la privacidad en el desarrollo de Internet. Mientras que los aspectos fundamentales de la privacidad están siendo considerados en el desarrollo de IPv6, es esencial que la confianza de los usuarios de Internet en todo el sistema, incluyendo el respeto de sus derechos fundamentales, esté siendo asegurada".

En sus conclusiones, la Comisión Europea pidió a las partes:

"Estudiar el impacto de una mayor evolución de Internet incluyendo la nueva generación del Protocolo IPv6, sobre los derechos fundamentales de la privacidad y de la protección de datos personales, para conseguir asegurar que los estándares y las especificaciones necesarias tengan en cuenta estos aspectos en su totalidad".

Habiendo hecho una llamada para el estudio general sobre estos aspectos, pocos meses después, en mayo de 2002, el Grupo del Artículo 29 publicaba un documento llamado "Opinion 2/2002 on the use of unique identifiers in telecommunications terminal equipment: The example of IPv6."

Este documento remarca el peligro que supone para la privacidad “la posibilidad de la integración de un único número identificador en la dirección IP diseñado de acuerdo al nuevo protocolo”. La idea central de este documento es que la dirección IP atribuida a los usuarios de Internet podría ser considerada como un dato personal y, por lo tanto, estaría sujeta a las Directivas establecidas por la Unión Europea.

3.8 Aspectos fundamentales de preocupación sobre la privacidad.

Las preocupaciones acerca de la privacidad están fundadas en el formato de creación de direcciones IPv6, aprobado por el Internet Engineering Task Force (IETF). Este es el cuerpo técnico que asesora acerca de cómo Internet debe ser desarrollado y establece los estándares para Internet a través de la publicación de varios estándares técnicos conocidos como RFCs.

Los RFC son una serie de documentos generados en base a un conjunto de notas técnicas y organizativas acerca de Internet. En ellos se discutían varios aspectos de la red de ordenadores, incluyendo protocolos, procedimientos, programas y conceptos. Estos específicos documentos no oficiales del protocolo de Internet consiguieron una importancia creciente y fueron recogidos y publicados como los estándares RFCs. Este hecho desencadenó la consideración de los RFC’s como estándares no oficiales a través de los cuales se determinaba cómo Internet debía ser desarrollado. En este sentido, la publicación de RFC’s se convirtió en un paso fundamental para el proceso de creación de estándares definitivos y reconocidos. En concreto, los RFC’s deben publicarse previamente como borradores con el fin de que los expertos en las áreas involucradas tengan la posibilidad de formular los comentarios que consideren oportunos, con carácter previo a que se llegue a un consenso y el RFC se convierta en un estándar. En este sentido, el proceso es el siguiente: la especificación en concreto entra en un periodo de desarrollo y creación tras el cual queda sometida a la revisión por los expertos correspondientes hasta que finalmente pasa a considerarse un estándar. Por lo tanto, es posible destacar 3 niveles distintos en un RFC: • Propuesta de estándar • Borrador de estándar • Estándar

Tabla 93. Lineamientos sobre los estándares RFCs.

3.8.1 Los Identificadores Únicos las direcciones basadas en IPv6.

Existen numerosos tipos de direcciones IP basadas en IPv6 pero la posible colisión con la privacidad e intimidad se encuentra en los supuestos de autoconfiguración de las direcciones sin estado. Los aspectos técnicos sobre esta materia se encuentran especificados en los siguientes documentos: RFC2373 (arquitectura de direccionamiento IPv6), RFC2462 (autoconfiguración de direcciones IPv6 sin estado) y

RFC2374 (formato agregable de direcciones IPv6 globales de unidifusión), así como en posterior documentación existente sobre esta materia (draftietf-ipv6-unicast-aggr-v2-02.txt). El principal objetivo de la autoconfiguración de direcciones sin estado (Stateless Address Autoconfiguration) es generar una dirección global única sin la necesidad de un DHCP (Dynamic Host Configuration Protocol). DHCP es el protocolo que permite a un administrador de redes supervisar, gestionar y asignar las direcciones IP. A los efectos de conocer cómo se organiza una dirección basada en IPv6, se pone un ejemplo a continuación. Utilizando la analogía del correo postal, lo normal es poner el nombre del destinatario, seguido de la dirección, ciudad, estado, código postal y el país. Este estándar se encuentra actualmente aceptado y utilizado en el envío de correspondencia postal tradicional. En este sentido, existe un estándar parecido a seguir para las direcciones IPv6 con el fin de distribuir los 128 bits.

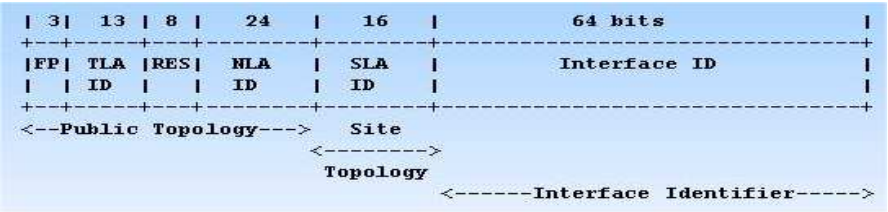


Ilustración 189. RFC2374 - Formato agregable de Direcciones IPv6 globales de unidifusión[177].

FP: Prefijo de Formato. Su valor es 001.
TLA ID: Top Level Aggregation Identifiers, se encuentra en el nivel superior de la jerarquía de encaminado. La topología del encaminado a todos los niveles debe ser diseñada para minimizar el número de rutas en la tabla de encaminado. Cada organización a la que le es asignado un TLA ID recibe 24 bits de espacio NLA ID. Este espacio puede ser delegado aproximadamente a tantas organizaciones como en el actual Internet IPv4. Las organizaciones a las que se ha asignado un TLA IP pueden proveer servicios a organizaciones que proporcionan servicios de tránsito público y a organizaciones que no lo proporcionan. Las organizaciones que reciben un NLA ID pueden incluso optar por delegar su espacio a otro NLA ID.
RES Espacio reservado para el futuro y debe dejarse en cero.
NLA ID Next Level Aggregation Identifier es utilizado en organizaciones con TLA ID para crear una jerarquía de direccionamiento y para identificar sitios. La organización puede asignar la parte superior del NLA ID para crear una jerarquía de direccionamiento apropiada para la red en cuestión.
SLA ID Site-Level Aggregation Identifier. El campo SLA ID es usado por una organización individual para crear su propia jerarquía de direcciones local y para identificar subredes. Es un campo de 16 bits y soporta 65.535

[177] Guido Wessendorft <wessend@uni-muenster.de> / Jurgen Rauschenbach <jrau@dfn.de>, "Aktuelles zu Ipv6", 1999, Berlin, http://www.join.uni-muenster.de/Dokumente/Folien/wessend/bt30/sld003.html

subredes. La selección realizada para estructurar un campo SLA ID es responsabilidad de cada organización individual.
Interface ID Los identificadores de interfaz son números de serie únicos o direcciones que están vinculadas al enlace y, por lo tanto, son utilizados para identificar interfaces en un enlace. Estos identificadores deben ser únicos para el enlace en cuestión. Esta es la parte de las direcciones que podría causar problemas de privacidad. En concreto, un interfaz es definido como un vínculo de un nodo a un enlace. Los identificadores de interfaz son números de serie únicos o direcciones vinculados al enlace. Un identificador para un interfaz es único para cada enlace (al menos).

Tabla 94. Descripción de los campos.

Esta explicación puede simplificarse a través de la siguiente figura:

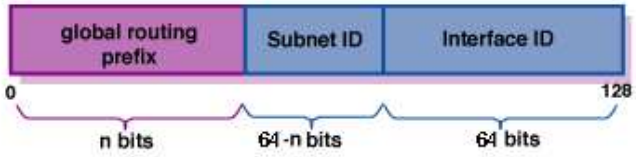


Ilustración 190. RFC2374 - Actualización del formato agregable de direcciones IPv6 globales de unidifusión[178].

IPv6 utiliza los 128 bits para generar el direccionamiento, encaminado y la información de identificación en el interfaz de un ordenador o en una tarjeta de red. Algunos sistemas basados en IPv6, usan los 64 bits de la parte derecha del gráfico para almacenar un identificador global IEEE (EUI64). Este identificador se compone de unos valores ID de entidad asignados a un fabricante por la Autoridad de Registro IEEE. Los 64 bits que conforman un identificador son una concatenación de la identificación de la entidad de 24 bits y del identificador de extensión de 40 bits asignado por la organización con la entidad de asignación de identidades. La dirección MAC de 48 bits de un interfaz de una tarjeta de red podrá también ser usada para generar el EUI64.

Los problemas relacionados con la privacidad nacieron en base a estos Identificadores de Interfaz (Interface ID), los cuales están basados en el ID del interfaz del hardware, tal y como se ha descrito anteriormente, de manera que podrían identificar individualmente a

[178] HP TCP/IP Services for OpenVMS Guide to IPv6, http://h71000.www7.hp.com/doc/732final/6645/6645pro.html <**openvmsdoc@hp.com**>

cada máquina. Por lo tanto, cada vez que se accede a Internet para enviar o recibir paquetes de información, este hecho deja una huella siempre, la cual podrá ser rastreada hasta conocer el usuario de una maquina.

3.8.2 La RFC2462 - Configuración automática de la dirección IPv6.

El RFC2462 explica como la autoconfiguración de direcciones sin estado combina un identificador de interfaz con un prefijo para formar una dirección.

El RFC establece lo siguiente: “Este documento especifica los pasos a seguir por un servidor para decidir cómo autoconfigurar sus interfaces a través de la versión 6 del protocolo IP. El proceso de autoconfiguración incluye la creación de una dirección de enlace local y la verificación del carácter único para ese enlace, determinando qué información debería ser autoconfigurada (direcciones, otra información o ambos), y en el caso de direcciones, si éstas son obtenidas a través de un mecanismo sin estado, a través de un mecanismo con estado o por ambos. Este documento determina el proceso para generar esta dirección de enlace local, el proceso para generar las direcciones globales a través de una autoconfiguración de direcciones sin estado y el procedimiento de detección de direcciones duplicadas (DAD, Duplicate Address Detection).”

“Uno de los principales objetivos de la autoconfiguración sin estado es la siguiente:

No sería necesaria la configuración manual de máquinas de forma individual con carácter previo a conectarlas a la red. En consecuencia, se necesitará algún mecanismo que permita a una máquina obtener o crear direcciones únicas para cada uno de sus interfaces. La autoconfiguración de direcciones conlleva que cada interfaz puede

generar un identificador único para dicho interfaz (un “identificador de interfaz”).
En el supuesto más sencillo, un identificador de interfaz hace referencia a la capa de enlace de la dirección del interfaz. Un identificador de interfaz puede combinarse con un prefijo para generar una dirección.”
En resumen, este RFC subraya cómo este tipo de direcciones basadas en IPv6 son generadas por ellas mismas en lugar de ser asignadas y se encuentran basadas en identificadores únicos en el hardware.

A continuación se presenta el análisis de interpretación y modelamiento de flujos del estándar de la RFC 2462:

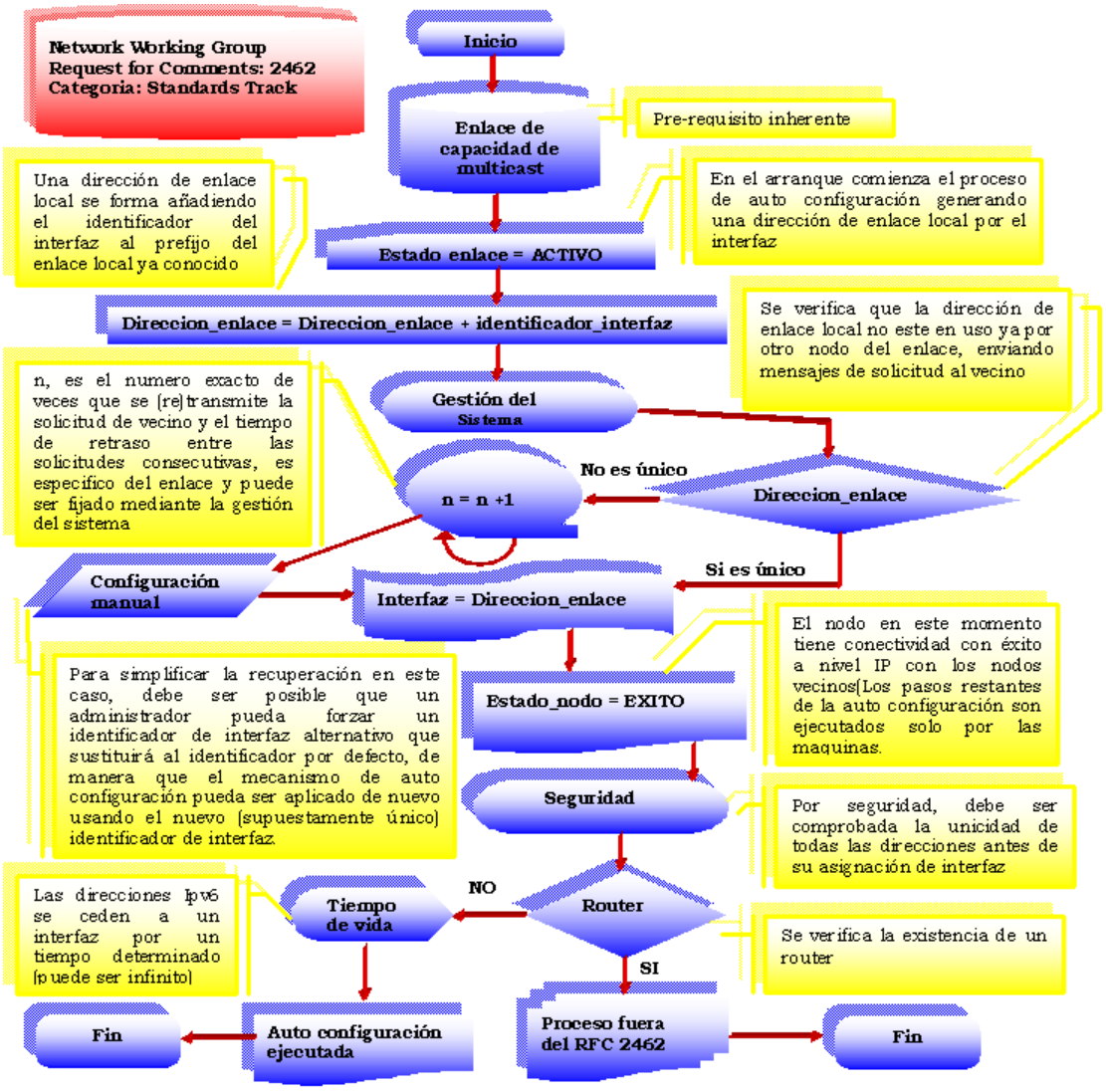


Ilustración 191. Interpretación de flujo de la RFC 2462 por Rubén Cañihua.

Luego de realizar el análisis e interpretación contractual del estándar de la RFC 2462 por los autores Susan Thomson set@thumper.bellcore.com y Thomas Narten narten@raleigh.ibm.com se observo que la construcción y la implementación en su arquitectura se encuentran excepcionalmente funcionales(No obstante se

encontraron ciertas ambigüedades[179] en su traducción que deberán ser modificadas e incorporadas en el punto 10 del apéndice B). Cave destacar que en materia de las consideraciones de seguridad la configuración de direcciones sin estado permite a una máquina conectarse a una red, configurar una dirección y comenzar a comunicarse con otros nodos sin autenticarse o registrarse siquiera con la instalación local. Aunque esto permite a usuarios no autorizados conectarse y usar la red, la amenaza es inherente a la arquitectura de Internet. Cualquier nodo con una conexión física a una red puede generar una dirección (usando distintas técnicas ex profeso) que de conectividad. El uso de la Detección de Direcciones Duplicadas abre la posibilidad de ataques de denegación de servicio. Un nodo puede responder las Solicitudes de Vecino de direcciones tentativas, causando que el otro nodo rechace la dirección por duplicada. Este ataque es similar a otros ataques incluyendo el falseo de mensajes de Descubrimiento de Vecino y puede ser evitado requiriendo que los paquetes de Descubrimiento de Vecino sean autenticados [RFC2402].

3.8.3 La problemática con la autoconfiguración de direcciones sin estado.

El potencial problema de cara a la privacidad que podría surgir con este tipo de direcciones se encuentra claramente especificado en el RFC3041. Este documento pone de manifiesto que cualquier sistema de comunicación que se base o utilice una dirección fija o un identificador tanto para recibir como para enviar información, conlleva problemas potenciales en materia de privacidad.

"La autoconfiguración de direcciones sin estado define cómo un nodo basado en IPv6 genera direcciones sin necesitar un servidor DHCP. Algunos tipos de interfaces de red tienen un identificador IEEE embebido

[179] "1<eemplo>::2<desapureba>::3<onectarlas>::4<genrando>::5<indentificador>::6<testido>::7<a>::8<embaroog>::9<toas>::10<retraser>::11<una>::12<iválida>::13<pro>::14<onjuntamente>::15<direcioes>::16<ocmo>::17<camiba>::18<máquine>".

(una dirección MAC, en la capa de enlace). En estos casos, la autoconfiguración de direcciones sin estado usa el identificador IEEE para generar un identificador de interfaz de 64 bits. Por diseño, el identificador de interfaz es único cuando se genera de esta forma. El identificador de interfaz se une a un prefijo para componer una dirección IPv6 de 128 bits.

Todos los nodos combinan identificadores de interfaz (ya sean generados a través de un identificador IEEE o través de cualquier otra técnica) con el prefijo link-local reservado para generar direcciones link-local para sus interfaces vinculados. En consecuencia, las direcciones adicionales, incluyendo las direcciones de ámbito local, son creadas mediante la combinación de prefijos señalados en los anuncios de rutas (Router Advertisements) a través del descubrimiento de vecindario (Neighbour Discovery) con el identificador de interfaz.

Sin embargo, no todos los nodos e interfaces contienen identificadores IEEE. En estos casos, los identificadores se generan a través de otros medios (por ejemplo, aleatoriamente), y el identificador resultante no es único de forma global y podrá cambiar con el tiempo.

El propósito de este documento (RFC3041) está basado en las direcciones generadas con identificadores IEEE, ya que sólo se da la problemática en materia de privacidad cuando existen identificadores únicos que, además, no cambian con el tiempo".

El propio RFC3041 pone de manifiesto el potencial problema en materia de la privacidad, derivado del uso de identificadores únicos como partes constantes de las direcciones.

El uso de identificadores de interfaz no cambiantes para componer direcciones es un caso específico fuera de los casos más generales donde el identificador es reutilizado a lo largo de un determinado periodo de tiempo y en actividades múltiples y distintas. En los casos en los que el mismo identificador es utilizado en múltiples contextos, nace la posibilidad de que dicho identificador sea utilizado para relacionar otras actividades no vinculadas hasta ese momento. Por ejemplo, un sniffer

colocado estratégicamente en un lugar por donde pasa el tráfico tanto de entrada como de salida hacia un nodo o servidor, podrá mantener un seguimiento acerca de los destinos con los que un nodo está comunicándose y sobre el momento en el que se produce esa comunicación. Esta información podrá ser interesante y ser utilizada para otros propósitos, por ejemplo, conocer las horas en las que un empleado se encuentra trabajando, las horas durante las que una persona estuvo en su casa, etc.

Los navegadores web y los servidores frecuentemente se intercambian entre sí “cookies” que pueden permitir a los servidores web relacionar una actividad que se está llevando a cabo con otra anterior. En este sentido, una de las actividades más comunes que se está realizando es enviar publicidad a un usuario utilizando la cookie del navegador web para identificar qué consultas o actividades se solicitaron con anterioridad. En este caso, tomando como referencia la información aportada por las cookies, resulta mucho más sencillo enviar publicidad que se adapte con mayor precisión a los gustos y preferencias del usuario en cuestión.

El uso de un identificador constante en una dirección es especialmente importante porque las direcciones son un elemento fundamental para que exista la comunicación y no es fácil mantenerlas escondidas o preservadas de rastreadores o terceros. Incluso en los supuestos en los que las capas superiores codifiquen sus informaciones, las direcciones en los encabezados del paquete siguen apareciendo en claro. En consecuencia, si un dispositivo móvil (como un ordenador portátil) accede a la red desde distintos puntos, cualquier rastreador será capaz de seguir sus movimientos de un lugar a otro, incluso en el supuesto de que las informaciones de las capas superiores de la dirección se encuentren codificadas.

3.8.4 Aspectos relevantes relacionados con las direcciones IPv6

La división de las direcciones de IPv6 en distintas topologías e identificadores podría suponer que una porción fija de una dirección de IPv6 (un identificador de interfaz) podría contener un identificador que permanezca constante incluso cuando la topología de la dirección cambie (como en el caso resultante de conectarse desde otro punto de Internet). Por el contrario, con IPv4, cuando parte de una dirección cambiaba, conllevaba el cambio de la dirección completa (incluyendo la parte local de la dirección).

En este sentido, si las direcciones fueran generadas en base a un identificador de interfaz, la dirección utilizada por un usuario desde su casa contendría un identificador único, el cual se mantendría igual en una sesión que en otra, a pesar de que se modificara el resto de la dirección. Sin embargo, un supuesto más problemático es el de los dispositivos móviles (portátiles, PDAs, etc.) los cuales pueden moverse y conectarse desde distintos puntos a Internet. En cada supuesto en el que estos dispositivos se mueven (y en los casos en los que no dispongan de tecnología basada en movilidad IP), estos dispositivos crearían sus propias direcciones en base a su punto de enganche actual.

Mientras que la dirección del dispositivo cambia cuando éste se mueve, en todo caso, el identificador único existente en la dirección se mantiene igual. En este caso, el identificador podrá ser utilizado para rastrear el movimiento y el uso de una máquina o dispositivo concreto. Por ejemplo, un servidor que almacena el uso de la información así como la dirección de origen también estará almacenando el identificador único ya que éste estará incluido en la dirección. En consecuencia, cualquier actividad de data-mining a través de la cual se puedan relacionar actividades efectuadas con las direcciones a través de las cuales se llevaron a cabo, también serán de aplicación en los supuestos en los que existan identificadores únicos en las direcciones.

3.9 RFC3041 respecto a la problemática relacionada con la privacidad en la Autoconfiguración de direcciones sin estado.

El RFC3041 “Privacy Extensions for Stateless Address Autoconfiguration in IPv6” es un estándar técnico que se considera, en la actualidad, como una posible solución de naturaleza técnica a los posibles riesgos que, respecto a la privacidad y la protección de datos de los usuarios, podrían existir como consecuencia del uso del nuevo Protocolo IPv6.

Este RFC establece un sistema de dos direcciones: una dirección que es la utilizada para recibir comunicaciones, de manera que la interfaz del terminal es siempre localizable a través de la dirección permanente y otra dirección generada aleatoriamente utilizada por el Terminal para las comunicaciones salientes. De esta manera, a través del RFC3041, en líneas generales, cuando las comunicaciones son generadas por el usuario, su dirección IP no sería rastreable por terceros.

3.10 Apreciaciones y conclusiones referidas al capitulo tercero.

- Realizamos un análisis de rigor contractual e inferencia en materia de la privacidad de la información considerando su conglomerado definiciones pragmáticas clásicas, sus sustratos iusfilosóficos, las modalidades de actuación en la red y sus formas de lesión, desde una óptica del derecho comparado de los ordenamientos jurídicos modernos, vinculado esta en general al estudio de la legislación Europea y sus perspectivas, con una mirada descriptiva a la legislación Chilena 19.628, para luego adentrarnos a determinar orientar el estudio de un mecanismo de control no jurídico efectivo que permita establecer las garantías de la privacidad inherentes a los usuarios del Internet con el protocolo de Ipv6 dentro de la categoría de las tecnologías de protección de la privacidad encaminada con la utilización de los mecanismos tecnológicos orientados a minimar la recolección y el empleo de datos personales y dificultar las posibilidades de tratamiento ilícito, con el diseño de procedimientos de disociación de los datos, permitida esta a anticiparnos a una regulación de la ocurrencia de

los hechos que signifiquen infracción a las disposiciones legales o reglamentarias que satisfagan los estándares normativos vigentes.

- Se estableció contextualizar una investigación de las perspectivas tecnológicas de la privacidad de avanzada que en la actualidad se utilizan, dentro de las categorías de los sistemas de tratamiento de la identidad(ISM-Identify Management Systems) a efectos de analizar los instrumentos que refuerzan la privacidad y combinan la autenticidad con diversos grados del anonimato del usuario en las redes de comunicaciones permitiendo así, ocultar nuestras "coordenadas", como localización física, direcciones de red o de correo electrónico, y protegerlas del uso indebido, al tiempo de ser administradas y gestionadas con seguridad, sin dejar huellas excesivas de nuestro comportamiento en los distintos sectores de nuestra vida, determinando así, que los propios usuarios puedan controlar el suministro de su información personal, así como la relación entre las apariciones de esta información en diferentes contextos en la sociedad de la información de nuestras identidades digitales, determinando que es necesario combinar las tecnologías(claves criptográficas y sellos de seguridad) con el propósito de asegurar el resguardo de la privacidad de nuestros datos y ultimando esta a que el proyecto ATUS(A Toolkit for Usable Security) de la Universidad de Friburgo, Alemania, está diseñando e implementando una solución alternativa pero solo a nivel de la capa de aplicación de la OSI; que consiste de la construcción de un módulo de "gestor de identidad" con P3P-W3C(Plataform for Privacy) codificadas en lenguaje APPEL(A P3P), que actuara como una especie de cortafuegos sobre el sistema del usuario que le ayudara a manejar diferentes perfiles, implementados como visiones de un conjunto de datos personales, conectados automáticamente, por defecto, con cualquier servicio de Internet (utilizando actualmente la tecnología AN.ON/JAP de la Universidad de Dresde) que servirá de manera efectiva para navegar con privacidad por la world wide web con la correspondiente garantía de privacidad, por que le alertara al usuario de cuándo este revelando cierta información

adicional predefinida, permitiendo asi, a los usuarios afirmar su derecho a la autodeterminación informativa, mucho mejor que antes, siendo necesarios en todas las comunicaciones informatizadas, y aún más con la llegada de las nuevas tecnologías, como los UMTS (Universal Mobile Telecommunications System) que son lo sistemas de telecomunicaciones móviles 3G o la penetración de la informática ubicua.

- En referencia a las implicaciones en materia de privacidad con el protocolo de Internet Ipv6 se plantea que es necesario, a la celeridad con la que se suscita el rápido desarrollo del IPv6 y éste potencia su despliegue, es ponderable enfatizar la importancia de no olvidar que debe de efectuarse y preverse las salvaguardas correspondientes a los principios esenciales indicados por la Unión Europea. Además de que se ve imperioso considerar un desarrollo tecnológico concordante que ofrezca las garantías al derecho a la privacidad y que sean analizadas desde las perspectivas de las experiencias de las legislaciones internacionales para luego en lo posteriore ser aplicadas a la legislación Chilena vigente, siendo considerando prevaleciente su respeto y cumplimiento como una obligación esencial inherente al equilibrio tecnológico. Resaltando la coherente interpretación que se realizo del estándar RFC 2462 en su línea de flujos, a efectos de analizar en detalle la construcción de la arquitectura per se a determinar la afectación que esta implica en vistas a tener un único identificador que le vinculada al titular de sus datos. A vidas cuentas, que si bien la tecnología se desarrolla y avanza con gran velocidad, la legislación internacional debe pretender facilitar una serie de elementos contingentes para verificar el cumplimiento y garantizar la protección del derecho a la intimidad como es el caso de la legislación Europea investigada a lo largo de todos los pasos existentes en la implementación de cualquier nueva tecnología, ponderada esta a su vez por el derecho comparado reactivo que puede ofrecer la Legislación Chilena; en líneas medulares, a los desarrolladores de nuevas tecnologías y protocolos que deben tener en mente la obligación de respetar el derecho a la intimidad o

privacidad y los principios de protección de datos. En el sentido, que en Chile es imperioso considerar la existencia de una legislación especializada que regule la protección a la vida privada y que asuma los principios doctrinarios sustentados por el derecho comparado, como exigencia de los tiempos en que vivimos, como instrumentos eficaces de tutela de la persona y de respeto a su dignidad en los derecho fundamentales que ella contrae.

CAPITULO CUARTO

IMPLICANCIAS DEL PROTOCOLO DE INTERNET IPV6 EN RELACION A LA PROTECCION DE DATOS PERSONALES

4.1 Aspectos preliminares en materia de protección de datos[180] personales.

La creciente complejidad de la sociedad postmoderna viene exigiendo una constante revisión de las posturas y de la comprensión del mundo por parte de los juristas. En efecto, el derecho históricamente entendido como instrumento para resolver conflictos entre los individuos, ahora se depara con un enorme abanico de conflictos y situaciones que se alejan del viejo modelo; la era de las nuevas tecnologías nos exige el máximo grado de prudencia con el tratamiento de nuestros datos. En ese contexto se presenta la protección de datos personales, conciente de que para una nueva mirada, debemos poner nuestra atención en lo nuevo, bajo pena de transformar el nuevo en viejo. Sabiendo que en una sociedad en permanente transformación, en la cual el espacio privado se reduce de forma evidente, la discusión sobre el problema de la privacidad y de la protección de datos asume un papel destacado. Desde el panóptico de Foulcault hasta el Big Brither orweliano, el derecho se encuentra en una encrucijada en la que los caminos se multiplican y se entrecruzan. El avance de la tecnología arrolla a los juristas, que preparados para la resolución de conflictos previsibles, no se dan cuenta de la sociedad de riesgos que se avecina. Derechos de cuarta generación no pueden ser analizados bajo el mismo paradigma[181] que orientaba los conflictos entre derechos de primera, segunda y tercera generación.

El eje central del análisis es el derecho a la protección de datos, que se presenta el estado de la cuestión, tratando de alcanzar vuelos más allá de la problemática meramente jurídica.

Información es poder, es manipulación, es ideología. A fin de cuentas, Internet es la gran red de ordenadores a la que tienen acceso grandes corporaciones, gobiernos, instituciones y usuarios, haciendo que día a día las distancias en el mundo sean menores. Hoy el mundo es interpretado en sus 4 rincones, a

---

[180] Es posible que la expresión "Protección de datos" no responda por si misma al amplio contenido y alta consideración que pretende abarcar; sin embargo, se trata de una expresión sobradamente aceptada y que tiene un desarrollo uniforme en los países de lo que podíamos llamar nuestro entorno socio-cultural.

[181] Podemos observar un cambio de paradigma tiene origen en dos factores: Velocidad y Exactitud. Pero es una situación traicionera. La posibilidad de acceso a las informaciones supera la inicial situación de superioridad y se puede transformar en una posición de manipulación de situaciones y voluntades. Manipulaciones en un grado nunca antes concebido. **Las innovaciones que trae consigo Ipseg son, sin duda, extremadamente valiosas para el ciudadano común, y mas aun para quien las observa desde una posición superior.**

partir de las informaciones que circulan en la “Gran red”. Internet es de ese modo el intérprete virtual de la cotidianeidad postmoderna.[182] A saber, por ejemplo para el profesor Shaarempää <asaarenp@ulapland.fi> el tratamiento y la protección de datos constituyen un extraordinario problema legal por 4 razones, como son; las exigencias de la democracia, la sociedad de la red, la búsqueda de la eficiencia y el complejo curso vital de la información.

1.- Las exigencias de la democracia: Concernida, la cuestión de relación entre lo público y lo privado. Nosotros disponemos de nuestro derecho a la autodeterminación. Nosotros concedemos a la sociedad, a los medios de comunicación y al mercado autorización en la medida necesaria para supervisar y monitorearnos y usar nuestros datos personales. Formalmente, en la democracia burocrática, los ciudadanos existen para la maquina, los medios y la organización 2.- La sociedad de la red: Que se encuentra añadiendo nuevas dimensiones a nuestras vidas. Trabajamos mas y mas con redes de información. El e-goverment esta convirtiéndose en una central y visible forma de gobierno. Observamos el surgimiento de caber-comunidades que trabajan virtualmente sobre redes de información. En una sociedad tal, quienes quizás han progresado mas en Europa han sido precisamente los países nórdicos, en los cuales el procesamiento de datos personales en las redes de información es parte de la rutina diaria. 3.- La búsqueda de la eficiencia: Ahora, estamos entrando en la era de los sistemas documentales, pero solo se trata de los primeros pasos. Una proporción significativa de la producción de documentos por las diferentes organizaciones es realizada electrónicamente, pero mediante el convencional procesamiento de textos. Ha sido y continúa siendo difícil obtener que las organizaciones que producen documentos en la sociedad de la información planifiquen desde un comienzo tal proceso respetando al ser humano y sus datos personales. En otras palabras, los datos personales deben ser tratados desde el principio como información que se procesa de una forma diferente. Esto es costoso, pero sus costes son menores que remover los datos personales incluidos en los documentos después de concluidos. Disponer del código correcto en el momento y lugar adecuado es una cosa increíblemente importante. Si esto es descuidado posteriormente la protección de de los datos personales llega a ser una propuesta muy costosa. 4.- El complejo curso vital de la información: La forma y ubicación de la información, así como el modo en que es procesada pueden cambiar totalmente con rapidez. El legislador debe ser capaz de regular un fenómeno dinámico. Y esto no es sencillo de lograr.

Tabla 95. Apreciación del Profesor Shaarempää.[183]

Que a su vez, de lo mencionado líneas atrás, se interpreta que uno de los problemas mas visibles de la protección de los datos ha sido y continua siéndolo, es el desarrollo e identificación de los principios legales que informan la protección de datos personales; por que desde que la información cambia de formas, muchas veces durante su curso vital, la ley sobre protección de datos debería permanecer en un nivel **comparativamente abstracto** (Las leyes deberían ser genuinamente interpretadas) por ello estimados considerable, recoger las 4 soluciones en mente que plantea el mismo frente a este problema Europeo, a saber: “a) la información suministrada al publico por las autoridades de protección de datos: debe ser

[182] Victor Drummond, Internet, Privacidad y datos personales, Editorial Reus Madrid-España 2004. pag. 18.
[183] A. Shaarempää, “Europa y la protección de los datos personales”, Revista Chilena de Derecho Informático. ISSN:0717-9162; Nº 3 Diciembre 2003 www.derechoinformatico.uchile.cl

cuidadosa la elaboración y difusión de las orientaciones emitidas por las autoridades sobre la protección de datos suministradas al publico como lo hace en este caso de las Autoridades de la Inspección de Protección de Datos de Suecia que mantienen al publico permanentemente informado", en esta línea por ejemplo la Comisión Europea tiene un eurobarómetro[184] sobre protección de datos en la Unión Europea, "b) los códigos de conducta: Deberían ser usado mas frecuentemente como instrumentos legislativos con una actitud menos esceptica, c) la aplicación de mayor rigor de los principios legales de la protección de datos(Derecho fundamental y principio de consentimiento) y d) las leyes especiales para contextos específicos".

Antes de entrar en materia, debemos hacer algunas observaciones: El análisis que proponemos no puede ser analizado a partir de un material legislativo aislado, representativo de una determinada jurisdicción. Y ello ocurre por cualquier tema relacionado con Internet y con las nuevas tecnologías de telecomunicaciones ya sea por "cable o satélite"[185] según la categoría establecida por el Prof. Rodrigo León, con el propósito de orientar estas, a su perspectiva de la universalidad o su contemporaneidad, debiendo ser tratadas siempre a través de análisis comparados. De esta forma consideramos de cierto modo innovador el hecho de que el estudio de la protección de datos ya nace como un tema del derecho comparado. Por ello, no habrá ningún texto legislativo que nos sirva de modelo exclusivo, aunque de todos modos, algunos serán utilizados como punto de partida para el citado análisis de derecho comparado. Lawerence Lessig[186], a través de una de sus obras mas conocidas en la literatura internacional, Code and Other Laws of Cyberspace, traza un perfil de la gran red y de sus consecuencias, y trae a colación una discusión fundamental que concierne, al mismo tiempo a los datos personales y al estado de privacidad. Afirma "Cuando digo identidad quiero decir algo

[184] Centrado en la visión que los ciudadanos europeos que tienen en relación con el tratamiento de sus datos personales por organizaciones públicas y privadas. Informática y Derecho, X Congreso Iberoamericano de derecho e informática, Alfonso Ortega Jiménez, "El derecho a la protección de datos de carácter personal en Internet", pag. 225.
[185] Rodrigo León, en el marco del Magíster en Derecho Informático y de las Telecomunicaciones realizado por el CEDI de la Universidad de Chile, con el tema "La ordenación Internacional de las Telecomunicaciones", el rol de los organismo supranacionales y de las entidades no gubernamentales, Mayo 2006.
[186] Lawerence Lessin "Code and Other Laws of Cyberspace" Basic Books, 1999.

mas que simplemente quien eres. Puedo referirme a hechos sobre ti que son verdaderos. Tu identidad, en ese sentido, incluye tu nombre, tu sexo, donde vives, tu grado de escolarización, el numero de tu carne de conducir, tu numero de seguro social, tus compras en el Amazon.com y también si eres abogado, etc." Inmediatamente nos trasladamos a una de las cuestiones fundamentales de Internet. ¿Cuál es el nivel de información que terceros pueden tener acerca de nosotros?¿En que momento se da una violación?. Para determinados análisis, es fundamental conocer algunos conceptos determinantes, de entre estos se encuentran los conceptos de **datos personales y de información**. Un dato es una información, es una dimensión mas reducida, una única información aislada[187], una información singular[188].

¿Y que pueden contener estos datos, estas informaciones destacadas? Aisladamente tal vez no importen demasiado.¿De que sirve saber el nombre de alguien si no hay forma de aprovecharse de ese hecho? El problema empieza en el momento en que los datos no permanecen aislados. Y esta es una preocupación de los legisladores cuando impiden el tratamiento[189] de algunas de las cualidades de los datos, o su tratamiento sin autorización previa. El peligro se hace evidente en el siguiente paso. La confluencia de datos, aunque sin demasiada importancia, si genera un banco que los reúna, desde que tratamos con competencia, puede llegar a trazar el perfil de personas, por más ingenuos que puedan ser los datos respecto de ellas. Lo que parece de suma importancia en lo que se refiere a la relación intima que poseen el tema de la privacidad y los datos personales es que, de hecho, lo que se tutela no son los datos en si mismo, visto que estos acaban por poseer

[187] Pues estará excluida de todo y cualquier contexto interpretativo que le pueda atribuir algún valor. Será, por tanto, inocua. En cuanto información aislada, un dato(puesto que esta fuera de contexto) no significa nada. Acaba por ser un elemento único de información inoperante, no siendo suficiente, por lo tanto, para permitir cualquier identificación relevante. En el momento de la contextualizacion, con todo un dato puede en cuanto tal, adquirir alguna relevancia. Cabe hacer referencia a lo que denominamos contextualizacion primaria, entendida como la apreciación de la importancia de hasta la minima información contenida en un dato personal, para hacerla relevante.

[188] Será una información singulares, pues tendrá, como único valor su propio valor informativo intrínseco.

[189] Tratamiento, en la definición del art.2, letra b, de la Directiva 95/46/CE, es "cualquier operación o conjunto de operaciones efectuadas sobre datos personales, con o sin medios automatizados, tales como la recogida, registro, organización, conservación, adaptación o alteración, recuperación, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de colocación a disposición, con comparación o interconexión, bien como el bloque, borrado o destrucción…"

una significación vacía[190]. Aunque se diga que hay informaciones valiosas o importantes, estas no son tuteladas en si mismas, sino el valor intrínseco que ellas representan en lo concerniente a la privacidad del individuo. En ese sentido, una información o un dato divulgado públicamente no perjudican la vida de ninguna persona, pero el valor intrínseco[191] que de ello se extrae puede ser devastador. En ese sentido, deber ser desatacada la categorización de datos personales y la atribución de una gradación valorativa de estos. Ello significara que existe una diferenciación de los datos y una variación cuantitativa que estará directamente relacionada con la intimidad de sus titulares y los efectos que su tratamiento pueden acarrear.

En lo que se refiere a la interconexión entre archivos y datos la llegada de Internet trae, en general, la misma problemática que los medios informáticos en general ya acarreaban, o sea, el desarrollo tecnológico posibilitan el análisis, la recogida y, más genéricamente, el tratamiento de los datos personales con más velocidad, eficiencia y menor margen de error.

El aspecto innovador en lo que respecta a los medios informáticos concierne, en los márgenes de nuestro estudio, a la posibilidad de acceso a datos personales en un ambiente propicio a su captación por ejemplo a través de cookies, o el control del información establecido por los programas norteamericanos Carnivore[192](Antecesores de Etherpeek / Omnivore /

---

[190] Y ello ocurría aunque tratemos del cruce de datos que transmita muchas informaciones sobre los ciudadanos. En esta posición coincido con Olga Estalleda Yuste, en La Protección de la Intimidad frente a la transmisión internacional de datos personales, Tecno Madrid, 1995, pag.24…. La noción de protección de datos puede conducir a falsas apariencias respecto de su contenido, ya que no se destina a proteger a los datos en si mismos, sino una parte del derecho a la intimidad personal, es decir, aquella que se refiere a la información individual.

[191] La exposición del valor intrínseco puede suscitar críticas, juicios de valor o percepciones distintas sobre los hechos que podrían ser narrado. En este caso la privacidad si correo un elevado peligro. Y esta es, obviamente, una problemática que no escapa a las innovaciones relacionadas con Internet; por el contrario, trae a la luz una aportación analítica mas turbadora, pues la gran red disminuye las distancias, aumenta la velocidad y facilita el acceso a informaciones diversas, incluyéndose ahí los datos personales.

[192] Carnivore, según la Wikipedia, se instalaba en el proveedor de acceso (ISP) de la persona a espiar, previa orden judicial, y era capaz de discriminar la interceptación de sólo los datos autorizados por el juez, que copiaba al vuelo y mandaba a un ordenador central. El sistema Carnivore provocó muchas controversias por sus fallos, como espiar a la persona equivocada, y porque se usó sin permiso judicial, según los grupos de libertades civiles. La ley *USA Patriot* acabó con la discusión, al decretar que el FBI podía monitorizar redes sin orden de un juez ni sospechas fundadas, mientras sólo captase la información del tráfico y no su contenido. A partir de entonces, se habló menos de Carnivore. Por una parte, los ISP monitorizaban sus redes y mandaban los datos al Gobierno. Y por otra parte, floreció el mercado de sistemas comerciales más evolucionados, que sustituyeron a Carnivore. Su existencia se conoció en el año 2000, por una disputa legal con un ISP que se negaba a instalarlo, y desencadenó las protestas de grupos de libertades civiles de todo el mundo. Se hizo tan popular que hubo quien realizó obras de arte basadas en Carnivore, rebautizado después por el FBI como DCS-1000.

Carnivore era la tercera generación de los sistemas de espionaje de redes del FBI. El primero fue Etherpeek, actualmente un programa comercial. El segundo, Omnivore, usado entre 1997 y 1999 y sustituido por DragonWare

DragonWare / Packeteer / Coolminer), Echelon[193] y AST(Analizador Semántico de Tráfico de la empresa Narus, supuestamente usado por la Agencia Nacional de Seguridad (NSA))[194] o el actual Carnivore Europeo OSEMINTI(Que es un paso más en los sistemas inteligentes de espionaje telemático), donde como plantea Shaarempää "nos encontramos retornando a la sociedad desnuda*(naked society)* donde las autoridades recopilan una ascendente cantidad de datos sobre nosotros"[195], complementado también, con los intereses de otras terceras partes, que realizan tal, procesamiento de datos, tanto dentro de nuestro país o a través de movimientos transfronterizos[196].

En Chile, el marco jurídico para el tratamiento de los datos personales, por organismos públicos y particulares, se contiene en la Ley 19.628 Sobre Protección de la Vida Privada, la cual tuvo su origen en una moción parlamentaria presentado ante el senado con fecha 5 de enero de 1993, cuyo propósito era llenar un vacío manifiesto en el ordenamiento jurídico nacional mediante el otorgamiento de una adecuada protección al derecho de la vida privada de las personas, en el ámbito del derecho civil, ante eventuales intromisiones ilegitimas[197]…

La doctrina, utiliza la expresión Protección de Datos, refiriéndose a la protección jurídica en lo concerniente al tratamiento automatizado de sus datos personales, por tal entendemos que es al amparo o tutela otorgada por el derecho a los ciudadanos, con el objetivo de evitar la utilización por terceros extraños y no consentida por el titular, resumiendo se trata de 3 ideas: protección jurídica ante la potencial agresividad de la informática(Por lo tanto datos susceptibles de tratamiento), el resultado del procesamiento informático(debe dar la posibilidad de identificar al titular de los datos) y el manejo de la información debe efectuarse sin el consentimiento del titular o para un fin distinto de aquel que el titular autorizo.

Ahora en lo que referencia a un **análisis de términos** de la protección de los datos personales, derecho a la

---

y constaba de tres partes: Carnivore, que capturaba la información; Packeteer, que convertía los paquetes interceptados en textos coherentes, y Coolminer, que los analizaba.

[193] No hay que negar la evidente percepción de ofensas éticas y violaciones a la privacidad del ciudadano en las situaciones anteriormente propuestas. La interconexión de archivos y de datos en general parece alcanzar el ápice de su ofensa ética cuando el tratamiento de datos tiene por objetivo esbozar la personalidad de sus titulares. En ese momento, incluso los datos mas irrelevantes pasan a tener una destacada importancia. Este hecho puede volverse extremadamente peligroso y puede dar lugar a situaciones problemáticas de difícil resolución(En el ámbito mas general que concierne a Internet se puede decir, a titulo de ilustración, que el conocimiento del mapeo genético de un titula por parte de terceros puede destruir atingentes aspectos)

[194] Se instala en diferentes puntos de una red y puede examinar cantidades ingentes de tráfico en tiempo real, identificando los paquetes interesantes, procedentes de correos, mensajería instantánea, vídeos o telefonía IP, aunque viajen a más de 10 Gbps.

[195] Paradójicamente, sin embargo, tales acciones incrementan los riesgos de una eficaz y destructiva información de guerra. La proliferación de registros de datos personales y las telecomunicaciones asociadas a ellos ofrece la impresión –deseable- de construir objetivos en tal conflicto. A. Shaarempää, "Europa y la protección de los datos personales, Cinco generaciones de protección de datos personales en Europa, Revista Chilena de Derecho Informático. ISSN:0717-9162; Nº 3 Diciembre 2003 www.derechoinformatico.uchile.cl

[196] El movimiento transfronterizo está a la orden del día entre los temas relacionados con el Internet, la privacidad y la protección de datos personales. En las negociaciones entre la Unión Europea y los Estados Unidos destaca principalmente, exigencia de que la transferencia de datos personales a países terceros tan sólo puede efectuarse "cuando, sin perjuicio del cumplimiento las disposiciones de la presente directiva, el país tercero de que se trata garantice nivel de protección adecuado". No es ningún secreto que las disposiciones relacionadas con países terceros referidas en la directiva 95-46-CE tiene un destinatario principal y cierto: los Estados Unidos de América, país que ofrece una grande protección mucho menor que los países europeos, y cuyo numero de empresas presente s en el mercado europeo es enorme.

[197] DSS, Sesion 20(Anexo de documentos), pp. 3079-3089. La macion contemplaba disposiciones que determinaban la extensión de la vida privada, excluia las intromisiones ilegitimas a su respecto, brindaba instrumentos procesales para su proteccion frente a estasy aun de compensación para el evento de haberse producido.

autodeterminación informativa, libertad informática y habeas data es una cuestión que no se puede responder simplemente, pues no existe unanimidad en el parecer de la doctrina para referirse a estos termina. Con todo, cabe señalar que esas expresiones tienen en general como un denominador, el querer significar el reconocimiento de un nuevo derecho, cuyo núcleo esencial esta dado por un poder de control de cada persona sobre la propia información y su calidad. Para algunos autores, el termino correcto a utilizar para significar este nuevo derecho seria derecho a la protección de datos personales(Puccinelli) o protección de datos(Estadella Yuste). Otros autores utilizan términos mas específicos como libertad informatica(Moeykens), autodeterminación informatica(Perez-Luño y Murillo de la Cueva) e incluso el termino habeas data(Pomed Sanchez). Respecto de los termino derecho a la proteccion de datos personales o protección de datos se ha señalado que si bien el contenido o extensión de estos es un punto discutido en la doctrina, existe al menos un grado de acuerdo, el cual consiste en afirmar que en estricto rigor, el derecho a la protección de datos, no dice relación o no esta destinado a la protección del dato en si mismo o el dato per se, sino que se relaciona con la protección de diversos bienes jurídicos.

En materia de las **bases constitucionales**, el Art. 19 numeral 4 de la constitución política de la republica de Chile, asegura a todas las personas "el respeto y protección a la vida privada y publica y a la honra de la persona y de su familia". La consagración constitucional del derecho a la vida privada, responde al reconocimiento del carácter fundamental asignado por representar su protección , un punto de especial sensibilidad en el tema de las libertades y derechos de las personas dentro de un estado de derecho.

En cuanto a las **bases legales,** que dicen relación con la protección a la vida privada y, en consecuencia, a los datos de carácter personal, nos encontramos que la legislación sobre el tratamiento de datos de carácter personal comienza con el Decreto Supremo Nº 950 del Ministerio de Hacienda, publicado en el diario oficial el 28 de marzo de 1928, posteriormente se regula en su integridad con la Ley Nº 19.628, sobre Protección a la Vida Privada, publicada en el diario oficial con fecha 28 de agosto de 1999(con las etapas… proceso: a) de los proyectos de la Comisión Hajna, en abril y noviembre de 1985, 1986 con el proyecto de ley informática, b) proyecto elaborado en 1993 que seguía muy cerca la ley española de protección de datos e incorporaba la existencia de un "Servicio Nacional de Protección de Datos", c) Moción del entonces senador Eugenia Cantuarias del 5 de enero de 1993 "ley de protección de los datos de carácter personal" y d) cuando la constitución no lo señalo expresamente ciertos derechos garantizados en normas internacionales que prescribe en su Art. 5º inciso 2º "El ejercicio de la soberanía reconoce como limitación el respeto a los derecho esenciales que emanan de la naturaleza humana. Es deber de los órganos del estado respetar y promover tales derecho, garantizados por esta constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes").

Tabla 96. Síntesis Doctrinaria, bases constitucionales y legales.

4.2 Escenario de estudio de la protección de datos personales.

Una de las razones que motivan el estudio sobre protección de datos objeto de este Capítulo, se deriva del hecho de que la legislación de protección de datos, a nivel general, va consolidándose y siendo conocida tanto por las empresas, como por los organismos públicos y por los ciudadanos, los cuales se encuentran adquiriendo, a medida que pasa el tiempo, una sensibilización y un conocimiento amplio acerca de cuáles son sus derechos y obligaciones conforme a esta normativa.

Este hecho, sin duda, es otro de los principales motivos que obligan a tener en cuenta cualquier aspecto que pudiera afectar a la implantación y uso de IPv6 sobre esta materia, de forma que se potencie la consideración de este Protocolo como un elemento seguro y que aporte confianza a sus potenciales usuarios.

El objeto de este Capítulo, si bien está estrechamente unido con el derecho a la privacidad, es analizar las posibles implicaciones que IPv6 podría tener en materia de protección de datos personales, como consecuencia de la posible consideración de las direcciones IP como datos de esta naturaleza, en determinadas ocasiones, como ya ha venido apuntándose en Capítulos anteriores. En este sentido, conviene aclarar que si bien la protección de datos personales suele entenderse incluida dentro de la amplia esfera que constituye el derecho a la privacidad de las personas, es una rama específica que se centra en asegurar que los tratamientos o usos a los que se destinen los datos personales de una persona física, se efectúen conforme a la legalidad existente.

Por lo tanto, este Capítulo se centra, en primer lugar, en analizar la legislación actual existente a nivel europeo en materia de protección de datos personales, a los efectos de poder discernir si ésta contempla y regula las posibles problemáticas que pudieran surgir como consecuencia de la implantación de IPv6 o si, por el contrario, se hace necesaria su modificación o adaptación a este Protocolo.

Asimismo, será objeto de este Capítulo, identificar algunos supuestos problemáticos derivados de la implantación de IPv6, en relación con la normativa de protección de datos así como la aplicabilidad de ciertas soluciones técnicas que se han venido desarrollando al objeto de preservar la privacidad de los usuarios de este Protocolo, en concreto, los aspectos relacionados con el RFC3041.

4.3 Consideración de la Dirección IP como un dato de carácter personal.

A continuación, como ya se viene apuntando a lo largo de otros capítulos, se pretende determinar si una dirección IP puede ser considerada como un dato de carácter personal para lo cual, con carácter previo, se expondrán una serie de conceptos básicos que deberán ser tenidos en cuenta.

En este sentido, el pionero Convenio de 28 de enero de 1981 del Consejo de Europa (conocido como el Convenio 108) definía dato personal de la siguiente

forma genérica: “cualquier información relativa a una persona física identificada o identificable”.

Asimismo, la propia Directiva 95/46/CE en su artículo 2 (a) considera como dato personal “cualquier información relativa a una persona identificada o identificable como, por ejemplo, los datos de carácter numérico o cualquier información característica de su identidad física, psíquica, económica, cultural o social”.

En consecuencia, a través de esta definición, pueden extraerse dos elementos esenciales que deben existir para poder considerar cierta información como un dato de carácter personal:

• El titular del dato debe ser siempre una persona física, no una persona jurídica.

• Posibilidad de asociar esta información de cualquier naturaleza, con esa persona física, bien directa o indirectamente.

Dicho esto, cabe deducirse que siempre que cualquier información sea posible relacionarla con una persona física que ya se encuentre identificada o que pueda serlo en el futuro (a través de medios razonablemente posibles), se entenderá que dicha información es un dato personal y, por lo tanto, su tratamiento deberá efectuarse conforme a las exigencias determinadas por la legislación vigente en la materia.

El Considerando 26 de dicha Directiva establece que para determinar si una persona es identificable, hay que tener en cuenta el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona.

Asimismo, otro de los conceptos esenciales a la hora de comprender esta normativa, es el concepto de tratamiento de datos personales. En este sentido, es importante resaltar que lo que realmente está regulado por esta normativa es el hecho de que se efectúe un tratamiento con los datos personales. El mero hecho de ser titular de los mismos, en principio, no confiere al sujeto ninguna obligación al respecto propiamente dicha sino, por el contrario, una serie de derechos sobre los datos de su titularidad. Sin embargo, el hecho de que un tercero trate tales datos es una actividad que sí

quedaría vinculada por esta normativa. En este sentido, la Directiva 95/46/CE define en su artículo 2 b) el concepto de "tratamiento de datos personales" como cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

Por todo ello, teniendo en cuenta estas consideraciones, podría establecerse que una dirección IP tendría la consideración de dato de carácter personal, en la medida en que es una información numérica que, la entidad o persona que se encuentra tratándola, podría relacionarla, en último término, con un determinado usuario, el cual, en última instancia, sería una persona física. Por ejemplo, una dirección IP podría ser relacionada con el usuario titular de la misma, por parte de su proveedor de acceso a Internet o por su proveedor de servicios en Internet.

El Grupo del Artículo 29 establece que *"el Considerando 26 de la Directiva 95/46 especifica que los datos son calificados como personales en tanto en cuanto se pueda establecer una conexión con la identidad del sujeto de los datos (en este caso el usuario de la dirección IP), por el responsable del tratamiento o cualquier tercero por medios razonables. En el caso de la dirección IP, el ISP es siempre capaz de establecer una conexión entre la identidad del usuario y la dirección IP y de esta forma, por ejemplo, terceras personas podrían hacer uso de ellas a través de los registros disponibles de direcciones IP establecidas o usando otros medios técnicos existentes".*

La posibilidad de asociación de un dato personal a una persona concreta se favorece, en principio, con IPv6, ya que algunas de las direcciones creadas en base a esta versión 6 del Protocolo, incluirían un identificador de usuario único (Interface ID: 64 bits) que identificaría inequívocamente a cada terminal (PC, ordenador portátil, PDA´s, etc), el cual podría incluso terminar siendo asociado a un determinado usuario a partir de distintos mecanismos (por ejemplo, guías públicas, bases de datos públicas del estilo a la base de datos Whois, etc) que

serán tratados posteriormente. Es importante resaltar que las implicaciones en materia de protección de datos que podrían existir como consecuencia de la implantación de esta nueva versión del Protocolo no surgen exclusivamente por el hecho de que la dirección IP pueda asociarse a una persona sino porque, incluso, ésta puede actuar a modo de "matrícula" de la persona respecto de los actos que realice. En este sentido, podría existir mucha información originada a partir de dicha IP y asociable a ésta, por ejemplo, compras, comportamientos, datos personales, etc.

- **IP basadas en un Identificador Único referente a datos de carácter personal:** Si bien, en líneas generales, se afirma que las direcciones IP basadas en la nueva versión 6 del Protocolo, que contienen en su configuración un Identificador Único, son datos de carácter personal, es importante resaltar que no siempre es así. Para que esta afirmación sea cierta, sería necesario poder asociar dicha IP a una determinada persona física, lo cual podría ser posible como se verá en apartados posteriores. Imaginemos un ordenador personal que se encuentra conectado a la red de Internet utilizando el protocolo IPv6. En este sentido, el usuario, a través de su terminal, accedería a la Red a través de una dirección IP única cuyo Identificador Único, que forma parte de ella, estaría identificando a su terminal de forma directa y al usuario titular, de forma indirecta. En este caso y dando por supuesto que el proveedor de servicios en Internet tuviera la posibilidad de asociar la dirección IP al usuario, titular de la misma, por ejemplo, como consecuencia de la contratación de servicios efectuada con este usuario, para el proveedor, la dirección IP del usuario sería claramente un dato de carácter personal. Por el contrario, imaginemos este mismo supuesto, pero en el cual dicho ordenador personal pertenece a un Cibercafé, de manera que el usuario que accede a través de dicha dirección IP variaría cada cierto espacio de tiempo. En este segundo supuesto, probablemente, el proveedor de servicios de Internet no podría asociar dicha dirección IP a un usuario

concreto, por lo que el dato de dirección IP no tendría una consideración clara como dato personal.

- **Direcciones IP basadas en un Identificador Único correspondientes al lugar de trabajo, datos de carácter personal:** Se han planteado dudas acerca de si una dirección IP que identifica un determinado puesto de trabajo (dispositivo, ordenador) en una compañía, podría tener la consideración de un dato personal, habida cuenta de que, en líneas generales, las actividades desarrolladas a través de la misma, no estarían incluidas en el ámbito íntimo del usuario que la utiliza.

En concreto, es frecuente que se piense que una dirección IP de carácter particular es un dato personal y, en cambio, la IP de un puesto de trabajo no lo es, por no pertenecer a la esfera íntima del usuario. En principio, podría considerarse que esta valoración no es acertada desde el punto de vista de la normativa de protección de datos ya que, el único criterio a tener en cuenta para determinar si una dirección IP es un dato personal, es que dicha dirección IP pueda relacionarse con la persona física que dirige el nodo o el terminal que está accediendo a la Red. En cuanto a las posibilidades de relacionar dicha dirección IP con una persona física concreta, será necesario tener en cuenta las consideraciones que sobre este aspecto, se recogen en apartados posteriores de esta tesis ya que, ciertos proveedores (en adelante, agentes tratantes o actores) podrán realizar esta asociación de una forma directa, mientras que otros no tendrán esta posibilidad o tendrán que acudir a medios alternativos de asociación.

4.4 Normativas de la protección de datos.

El objeto de este capitulo es realizar un breve análisis de las Directivas y Convenios europeos más importantes en materia de protección de datos, los cuales podrían ser de aplicación, inicialmente, al Protocolo IPv6.

Sin embargo, no corresponde ser objeto del mismo, el análisis de la progresión de las distintas normativas existentes sobre esta materia ni el

estudio sobre el inicio de la preocupación acerca de la protección de datos personales en los distintos Estados.

En este sentido, el objetivo principal del presente capítulo es de naturaleza triple:

- Conocer cómo se encuentra regulado, actualmente, el tratamiento de datos de carácter personal en Europa, a través del análisis de los bloques normativos principales.
- Conocer cómo los Estados Miembros han incluido en sus ordenamientos jurídicos estas obligaciones, resaltando aquellas particularidades más importantes localizadas en todas ellas.
- Discernir si IPv6 quedaría perfectamente regularizado a través de la normativa vigente en esta materia o si, por el contrario, existen otras particularidades que, necesariamente, deberán ser tenidas en cuenta por la legislación.

La doctrina extranjera ha constatado 2 niveles de protección en el tratamiento de los datos personales:
1.- El primer nivel consiste en una serie de reglas de carácter técnico-sustantivo (que no por su operatibilidad práctica dejan de involucrar una serie de garantías que pueden confundirse con los principios que protegen el tratamiento de datos).
Reglas básicas: Pablo Murillo de la Cueva, en su articulo "La construcción del derecho a la autodeterminación informativa", señala las reglas básicas del derecho de la protección de datos, que fueron positivizadas por la LORTAD y luego por la LOPD-Ley Orgánica de protección de datos- españolas e inspiradas por el Convenio 108 del Consejo de Europa:
a) las que apuntan a la relación que debe existir entre el tratamiento informático de datos personales que se pretende y el cumplimiento de una finalidad legitima. b) las que se refieren a la adecuación que debe existir entre la finalidad e información utilizada, c) la regla que impone la recogida leal de los datos. La lealtad en este contexto requiere el consentimiento informado del interesado o la cobertura de una autorización legal, d) juega también la exigencia de la calidad de la información obrante en el fichero o sometida a tratamiento, e) las cautelas a observar en los supuestos en los que se ceda esa información personal y a la necesidad de que solo tenga lugar tal cesión cuando, mediando consentimiento del afectado o autorización legal, se guarde la conexión de finalidad, asi como la proporción, que están en la recogida de estos datos personales, y f) debe tenerse presente el respecto a los derechos del interesado, que no han de padecer otras limitaciones que expresamente establecidas por la ley y aun estas, cuando concurran, han de motivarse por quien pretenda hacerlas efectivas.
Ahora desde un perspectiva de análisis son estas reglas, junto a la normativa existente, la que deben considerarse en todos los momentos o fases por los que puede pasar el tratamiento automatizado de los datos; "no es, como algunos interpretan, que se deban atender los derechos del ciudadano en el momento de recabar los datos, mediante la información acerca del tratamiento para proceder a ese tratamiento se trata de atender a los principios de la protección de datos en todas las fases por las que el tratamientos", según lo señala miguel Ángel Davara: a) "El momento de recabar los datos", bien sea directamente del intercedo o de un tercero, en el que tienen gran importancia su licitud y lealtad, con las características de conocimiento y, en su caso, consentimiento del afectado, b) "El momento del tratamiento automatizado de los datos", que pueden ser cruzados y relacionados en forma automática junto con otros datos, buscando definir un perfil determinado del afectado que incluso el mismo llega a desconocer", y c) "El momento de la utilización y, en su caso, comunicación a terceros de los resultados del tratamiento; la denominada "cesión de datos", que, al igual que en la recogida y en el tratamiento, se tendrá que considerar el conocimiento y consentimiento del titular".

2.- El segundo nivel de protección estas dado por los principios que fundamentan la garantía de juricidad en sede constitucional del tratamiento de datos. El peso específico de cada uno de ellos es una cuestión que varia dependiendo de la legislación que los trate, según el grado de compromiso que tenga con el respeto da los derechos

fundamentales de las personas. Principios del derecho, distinto de las reglas básica, pero íntimamente ligados, podemos mencionar a modo ejemplar 3 de los más importantes, a saber: a) El consentimiento del titulas de los datos. El ciudadano es el único que decide cuando, donde y como se presentas sus datos al exterior, o se dan a conocer esos datos a terceros. b) La calidad de los datos. Los datos que se recaben deber ser pertinentes y adecuados al fin que se pretenda, además de que no podrán permanecer en el fichero por el tiempo mayor al necesario y c) La información al recabar los datos. Es un principio general de la protección de datos que todo ciudadano tiene derecho a conocer la información almacenada sobre si mismo.

Tabla 97. Estándares de protección de datos personales[198].

4.4.1 Convenio de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal.

Este Convenio, también denominado Convenio 108, es la representación de uno de los primeros esfuerzos efectuados a nivel internacional para la creación y divulgación de las normativas establecidas en materia de protección de datos, tendentes a regularizar los tratamientos de los datos personales de las personas físicas. A través del mismo, los Estados firmantes adquirieron el compromiso de tomar "en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos…". Precisamente, el objetivo de este Convenio es "garantizar, en el territorio de cada Parte a cualquier persona física sean cual fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona".

4.4.2 Directiva 95/46/CE del Parlamento Europeo y del consejo del 24 de octubre, relativa protección de las personas físicas en lo que se respecto al tratamiento de datos personales y a la libre circulación de estos datos.

Transcurridos bastantes años desde la firma del Convenio 108, surge en 1995 la Directiva 95/46/CE, a través de la cual se aportan a los Estados Miembros los principios en materia de protección de datos que deber

[198] Jessica Mattus Arenas y Alejandro Montecinos Garcia; El deber de Información y el consentimiento para la transmisión de los datos personales, Universidad de Chile / Facultad de Derecho – Santiago, Chile 2004. pags. 22-26.

regir sus ordenamientos jurídicos nacionales. De esta manera, se crea un marco legislativo común y homogéneo a nivel comunitario aplicable a los Estados miembros. Tal y como se desprende de su Considerando 25, su objeto es garantizar la protección de los datos personales que vayan a ser tratados tanto por entidades publicas como privadas, de forma automatizada, En concreto, establece que "las personas, autoridades publicas, empresas, agencias u otros organismo que realicen tratamientos de datos personales tienen las obligaciones impuestas en esta directiva, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y el resto de obligaciones que incumben a la realización a las autoridades de control y el resto de obligaciones que incumben a la realización de tratamientos legítimos y, por ultimo, el respeto a los derechos de los titulares de los datos".

4.4.3 Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

Teniendo en cuenta la gran proliferación de nuevas redes digitales publicas avanzadas de telecomunicaciones y los importantes tratamientos de datos personales efectuados por las operadoras de telecomunicaciones, se publico esta Directiva, a través de la cual se definían los principios que deberían regir los tratamientos específicos de datos llevados a cabo en los servicios de telecomunicaciones.

En concreto, algunos de estos aspectos son:

- El tratamiento de datos de tráfico y facturación.
- La facturación desglosada.
- La presentación y limitación de la identificación de línea llamante y conectada.
- Las guías publicas con datos personales de los abonados, etc.

Como puede observarse, lejos de establecerse un marco general como ocurre con las directiva 95/46/CE, la Directiva 97/66 entraba a solucionar

problemas concretos de este sector, los cuales, en numerosas ocasiones, podrían servir como referente a la hora de resolver posibles problemáticas detectadas a nivel Ipv6, como por ejemplo, la regulación ofrecida respecto de la limitación de la línea llamante o respecto de las guías publicas de abonados. Sin embargo, esta Directiva se ha visto derogada por la reciente Directiva 2002/58. No obstante, si bien esta ultima amplia su regulación a todo el marco de la protección de datos en relación con las nuevas tecnologías (telecomunicaciones y comunicaciones electrónicas, en general), mantiene parte de la regulación ya esta lecifda en la Directiva 97/66.

4.4.4 Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Tal y como se determinaba anteriormente, esta Directiva procedió a la derogación de la directiva 97/66 y a través de la misma se pretende especificar y completar las disposiciones de la Directiva 95/46/CE para un sector concreto, el de las comunicaciones electrónicas. Con esta norma se pretende proteger y custodiar la intimidad de los abonados y usuarios de servicios de comunicaciones electrónicas. En concreto esta Directiva regula, principalmente, los siguientes aspectos:

- La seguridad técnica y gestión que deben adoptar los proveedores de servicios de comunicaciones electrónicas.
- La confidencialidad de las comunicaciones
- El tratamiento de datos de trafico
- La facturación desglosada
- La presentación y restricción de la línea de origen y la conectada
- El tratamiento de los datos de localización
- Las guías de abonados, etc.

4.5 Normativa de protección de datos vigente en relación con el uso del Protocolo IPv6.

Es objeto de esta parte conocer el grado de adecuación de las directivas anteriormente citadas y analizadas a la implantación del Protocolo Ipv6, a los efectos de poder determinar las mismas que prevén todos aquellos aspectos nuevos que pudieran surgir como consecuencia de esta implantación o si, por el contrario deberían verse modificadas.

En especial, el análisis se centrara en la Directiva 95/46/CE, como consecuencia de su consideración como el principal bloque normativo en protección de datos, delimitadora de los criterios básicos a tener en cuenta por las regulaciones de los distintos Estados Miembros. Asimismo, será efectuado este análisis respecto de la Directiva 2002/58/CE como consecuencia de su mayor adaptación al mundo de las comunicaciones electrónicas, dentro del cual podrían ubicarse las funcionalidades del nuevo Protocolo en su versión 6.

Se recogen unas breves consideraciones acerca de la adecuación de alguna de las normativas nacionales adoptadas por la Unión Europea en relación con esta materia.

4.5.1 La Directiva 95/46/CE.

A efectos aclarativos, el análisis de esta directiva se centrara en 3 aspectos fundamentales existentes en el tratamiento de los datos personales y, en concreto, en el tratamiento del dato de dirección IP.

En concreto, estos momentos principales son:

- La obtención del dato de dirección IP.
- El tratamiento del dato de dirección IP por los agentes tratantes cuando estos son capaces de asociar dicho datos a un terminal e incluso a un usuario.
- La cancelación y supresión de los datos de dirección IP.

A lo largo de cada uno de estos momentos principales, normalmente existentes en cualquier tratamiento de datos, la normativa sobre esta materia prevé una serie de principios y obligaciones que cualquier agente tratante deberá tener en cuenta. Pues bien, en este apartado, se analizara si respecto del tratamiento del dato de dirección IP conforme a estos momentos clave(recogida, tratamiento y cancelación), las

disposiciones de la Directiva prevén la regulación apropiada para la nueva versión 6 de este protocolo.

a) **La obtención del dato de dirección IP.** Tres son las principales obligaciones impuestas por esta normativa que deberían ser tenidas en cuenta cuando se proceda a recabar datos de carácter personales por cualquier persona, tanto física como jurídica: calidad de los datos; deber de información y obtención del debido consentimiento.
b) Respecto del principio de calidad de los datos, el articulo 6 exige que los datos recabados sean:
   - Tratados de forma leal y licita
   - Recogidos para fines determinados, explícitos y legítimos
   - No sean tratados, posteriormente , para fines no compatibles
   - Adecuados, pertinentes y no excesivos respecto de los fines que motiven su obtención
   - Exactos y actualizados
   - Conservados en una forma que permita identificar a su titular por un periodo no superior al necesario

   Las consecuencias derivadas de este articulo para Ipv6 supone que tanto el tratamiento de los datos de dirección IP, considerado como un dato personal en si mismo, como el de los datos que puedan ser asociados a un IP, deben regirse por estos parámetros.

   Respecto del deber de información, el articulo 10 establece los puntos respecto de los cuales, la persona física o jurídica que recaba los datos, deberá informar a los titulares de los mismos:
   - Identidad del responsable del tratamiento y, en su caso, de su representante
   - Fines del tratamiento
   - Destinatarios de los datos
   - Carácter obligatorio de la aportación de los datos
   - Ejercicio de los derechos de acceso y rectificación

   En consecuencia, en el momento en el que se obtenga tanto el dato de la dirección IP como los datos que potencialmente puedan asociarse a esta, deberá ser informado el interesado de estos aspectos. El principal problema es que este articulo es aplicable cuando el usuario aporta sus datos a la entidad que corresponda pero se plantea el supuesto de que, en ocasiones, el usuario estará aportado su dirección IP con su mera conexión y navegación por la Red, y por lo tanto, sin ser plenamente consciente de dicha aportación. En este caso, se plantea quienes están obligados a dar cumplimiento a esta obligación y el modo de hacerlo. Si bien, la contestación a este problema debe analizarse caso por caso, una contestación genérica supondría que toda persona física o jurídica que con motivo de la conexión y/o navegación por la Red de un usuario, conozca su IP, la trate, la almacene y pueda asociarla a la persona física titular, estará obligado por esta disposición, así como por el resto de los requerimientos de la Directiva. Por otro lado, el articulo 11 hace referencia a los supuestos en los que se debe informar aunque los datos no se hubieran obtenido directamente de los usuarios, por ejemplo, a través de la obtención del datos de dirección IP y de la información asociada a las mismas, facilitada por un proveedor de acceso a Internet a una empresa de marketing, dedicada al estudio de perfiles de usuarios. Como puede observarse, estos artículos establecen obligaciones que en ciertos casos, pueden conllevar ciertas dificultades practicas para su adaptación por cada uno de los agentes tratantes. Una dirección IP seria, en principio, asociable a su titular por parte de un proveedor de acceso a Internet. Sin embargo, podrían existir otra serie de agentes tratantes(i.e un prestador de servicios de tienda virtual) que a través de medios razonables(guías publicas, bases de datos, etc.) tuvieran la posibilidad de asociar la IP con su titular, en estos casos, se plantea la duda de decidir quien deberá proceder al cumplimiento de este deber de información el proveedor de acceso; el proveedor de los servicios de la tienda virtual o ambos.

   Obtención del consentimiento para el tratamiento de la dirección IP y de la información que pudiera asociarse a la misma, el articulo 7 de la directiva establece que solo podrán tratarse los datos cuando:
   - El interesado consienta (expresamente, en unos casos y tácitamente, en otros).
   - El tratamiento sea necesario para la ejecución de un contrato en el que el interesado sea parte.
   - Sea necesario para cumplir una obligación jurídica.
   - Sea necesario para proteger el interés vital del interesado.
   - Sea necesario para satisfacer un interés legitimo del responsable del tratamiento o de aquello a los que se le comuniquen los datos.

   En definitiva, la Directiva, en su articulo 8, establece una seria de requisitos mayores para cuando los datos tratados(en el supuesto analizado, los datos asociados a una dirección IP determinada) pertenezcan a categorías especiales(origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, salud o sexualidad). En este sentido, la Directiva prohíbe el tratamiento de estos datos a no ser que este se encuentre fundado en alguna de las excepciones que se establezcan como, por ejemplo, la obtención del

consentimiento explicito del titular de los datos, el tratamiento con el fin de salvaguardar el interés vital del tercero, o con fines de diagnostico medico, prestación sanitaria, etc.

Estas puntualizaciones son relevantes desde el punto de vista de determinados supuestos en los que un proveedor de servicios pueda tener acceso a este tipo de datos, Por ejemplo imaginemos un proveedor de contenido erótico que dispone de una pagina Web a la que pueden acceder los usuarios, Si alguno de ello accediera con una IP basada en un identificador único, este podría tener información acerca del tipo de contenidos de orientación sexual al que este accedería y , además, asociarla al terminal y potencialmente al usuario. En este sentido, estaría tratando datos de sexualidad asociados a una IP y a un usuario, con lo que dicho tratamiento quedaría vinculado por las disposiciones contenidas en este articulo

c) **El tratamiento del dato de dirección IP.** Una vez recabados los datos (la dirección IP en si misma y, en algunos casos, otra información personal que pudiera asociarse a esta), la Directiva prevé otra seria de artículos tendentes a regularizar el tratamiento que se efectué sobre los mismos. A través de estos artículos, se establece la obligación de adoptar por los agentes tratantes, una seria de medidas tanto técnicas como organizativas para asegurar la confidencialidad integridad y seguridad de los datos. La directiva no establece el tipo de medidas a implantar. Asimismo, establece como debe llevarse a cabo el tratamiento de los datos por terceros distintos de la persona física o jurídica responsable de los mismos.

d) **La cancelación o conservación del dato de dirección IP.**

La Directiva no se pronuncia de forma clara acerca de los parámetros que deben tenerse en cuenta para proceder a la cancelación o a la conservación de los datos personales. Por lo tanto a través de la Directiva no es posible conocer por cuanto tiempo deberán conservarse las direcciones IP en los sistemas de los agentes tratantes o en que supuestos deberán cancelarse. Al igual que ocurre para el resto de los datos personales, habrá que estar a lo dispuesto en las legislaciones de los Estados Miembros para poder determinar con cierta exactitud los citados plazos de conservación, atendiendo en su caso, al resto de normativa que fuere aplicable a cada supuesto de conservación de datos.

e) **¿Debe modificarse la Directiva 95/46/CE con la implantación del protocolo IPv6?**

Es indiscutible que uno de los principales debates generados como consecuencia de la futura utilización del nuevo Protocolo, se cierne en conocer si resultaría necesaria o no la modificación de esta Directiva a los efectos de adaptarla a nuevos problemas que pudieran ocasionarse como consecuencia de este Protocolo o si, por el contrario, a través de la misma se regulan los aspectos fundamentales aplicables al mismo. Tal y como se ha determinado, los artículos de la Directiva podrían considerarse, en principio, aplicables a los tratamientos de datos derivados del uso del protocolo IPV6 y, por lo tanto, puesto que las consecuencias derivadas de este no discrepan o contradicen los principios, obligaciones y derecho estipulados en la Directiva 95/46/CE y, tomando como apoyo lo establecido por esta misma a través de su Considerando 68, cabria determinar que, en principio, no resultaría necesaria la modificación de la citada Directiva. A efectos aclaratorios, el citado Considerando establece lo siguiente: "Considerando que los principios de protección de los derechos y libertades de las personas y, en particular, el respeto de la intimidad en lo que se refiere al tratamiento de los datos personales objeto de la presente Directiva podrán completarse o precisarse, sobre todo en determinados sectores, mediante normas especificas conformes a estos principios".

Asimismo, la labor de adecuación de estos principios a sectores más específicos deberá efectuarse, por ejemplo, a través de normas de desarrollo y de códigos tipo que facilitan que, de una manera dinámica y flexible, se adapten las consideraciones relativas al tratamiento de datos personales a cada sector. El propio articulo 27 de la Directiva diferencia entre Códigos de Conducta de ámbito nacional, los cuales deberán ser potenciados por los Estados Miembros y revisados por las Autoridades nacionales y los Códigos de ámbito comunitario, los cuales serán sometidos a la revisión del Grupo del Artículo 29.

Tabla 98. Apreciaciones de la Directiva 95/46/CE.

4.5.2 La directiva 2002/58/CE.

Esta Directiva se corresponde con la regulación comunitaria en materia de protección de datos que mas se ajusta al supuesto que es objeto del presente análisis, ya que a través de la misma se pretenden tratar las necesidades especificas en materia de protección de datos respecto de los nuevos servicios de comunicaciones electrónicas de la sociedad de la información. Algunos de los aspectos regulados podrían ser los

servicios de localización de terminales, el suministro de información, el tratamiento de los datos de tráfico relativos a las comunicaciones llevadas a cabo y, en general, cualquier servicio que pudiera ser prestado a través de redes publicas de comunicaciones electrónicas. Asimismo, es importante resaltar que en todo aquello que no sea tratado por esta directiva será de aplicación la Directiva 95/46/CE. Por este motivo, en este apartado solo se trataran las particularidades recogidas en esta Directiva 2002/58/CE.

a) Consideración del dato de dirección IP como un dato de tráfico. Uno de los conceptos más relevantes desde el punto de vista del Protocolo IPv6, tratados por esta Directiva es el concepto de "Datos de tráfico" el cual se encuentra definido en el apartado b) del artículo 2 de la citada Directiva. En concreto, debe entenderse por dato de tráfico, "cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma"

Por "comunicación" debe entenderse "cualquier información intercambiada o conducida entre un numero finito de interesados por medio de un servicio de comunicaciones electrónicas". En este sentido, el propio Considerando 15 de la misma aclara que "los datos de trafico pueden referirse, entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo terminal del remitente o destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión". En consecuencia, es posible considerar que el dato de dirección IP puede ser considerado como un dato de trafico en la medida en la que este posibilita la conducción de las comunicaciones a través de redes de comunicaciones electrónicas. En consecuencia, es posible considerar que el dato de dirección IP puede ser considerado como un dato de trafico en la medida en la que este posibilita la conducción de las comunicaciones a través de redes de comunicaciones electrónicas. En

este sentido, la Directiva introduce una serie de parámetros dedicados a la forma de tratar este tipo de datos.

1.- Consideraciones generales relativas a los datos de trafico
Uno de los principales puntos relativos a los datos de tráfico recogidos en el artículo 5 de la Directiva es el relativo a la exigencia de garantizar la confidencialidad, no solo de la información transmitida sino también de los datos de tráfico relacionados con esta. Únicamente podrán ser interceptadas, grabadas, almacenadas, escuchadas o vigiladas estas comunicaciones y los datos de trafico asociados a las mismas cuando:

- El usuario haya consentido.
- Las personas que desarrollan estas actuaciones estén autorizadas legalmente.

Sin embargo, como es lógico, la Directiva permite el almacenamiento técnico de la información y de los datos de tráfico, necesario para la conducción de la información. Por ello, el almacenamiento que puedan realizar los proveedores de acceso a Internet, operadores de telecomunicaciones, Etc, siempre que se realice con esta única finalidad, estaría permitido por la Directiva. Extrapolando estas consideraciones a IPv6, las direcciones IP, como datos de tráfico, deben ser confidenciales. El cumplimiento de esta obligación es más importante respecto de las IP generadas con un identificador único puesto que seria mas sencillo asociar por terceros no autorizados, el contenido de la comunicación, con la IP, con el terminal y con el usuario que la genera. Por este motivo, y siguiendo con lo establecido por este articulo, se podrán tratar estos datos para la conducción de las comunicaciones, para la facturación de los servicios y como prueba de una transacción comercial por las entidades destinadas a la prestación de los mismos. Para cualquier otro tratamiento de este tipo de datos(por ejemplo, promoción comercial o prestación de servicios de valor añadido), en principio y como regla general, se requerirá el consentimiento del titular. Por ultimo, destacar que los agentes tratantes de estos datos, en todo caso, deberán dar cumplimiento a los parámetros del deber de información y obtención del debido consentimiento, conforme se ha reflejado en el apartado anterior.

2.- ¿Cuál es el periodo de conservación de los datos de tráfico?
La directiva permite almacenar los datos de tráfico por determinados proveedores, pero conforme a una serie de criterios que garanticen que en dicho almacenamiento se efectúa por el tiempo necesario. En concreto, deben eliminarse cuando hayan dejado de ser necesarios para el cumplimiento de estas finalidades. El Considerando 27 aclara el termino "dejar de ser necesarios para la transmisión" cuando determina que, por ejemplo, "para una llamada de telefonía vocal, la transmisión finalizara en cuanto uno de los usuarios interrumpa la conexión; para el correo electrónico la transmisión finaliza en cuanto el destinatarios recoge el mensaje, en general, del servidor de su proveedor de servicios".
Asimismo, es significativo que una de las alternativas que ofrece la Directiva a la eliminación de estos datos de trafico es "hacerlos anónimos" lo cual plantea ciertas dificultades practicas para los proveedores de servicios, en el caso de IP generadas por identificador Único. Este hecho requeriría adoptar algún tipo de medida que les impida asociar la IP con el usuario contratante, titular de la misma. Si bien, estas son las consideraciones de la Directiva, es importante poner de manifiesto una nueva tendencia legislativa que se esta forjando en la UE. En concreto, a través de la nota de prensa 7555-04 (Presse 94) de la Sesión Extraordinaria del Consejo de Justicia y Asuntos de Interior, celebrada en Bruselas el 19 de marzo de 2004 como consecuencia de los atentado terroristas perpetrados en Madrid y presidida por D. Michael McDOwell, ha sido manifestada la intención de la Comisión Europea de presentar en el mes de junio, una propuesta legislativa para obligar a los operadores de Internet y a los operadores telefónico a conservar,(aproximadamente durante un periodo mínimo de 2 a 3 años), los datos de trafico de los usuarios, con el objetivo principal de combatir el uso de Internet como medio catalizador de la comisión de actos terroristas.
Esta futura regulación no seria contradictoria con lo establecido por la presente Directiva ya que en su artículo 15 se permite la limitación de los derechos de los usuarios y abonados en aras de proteger la seguridad, investigación y descubrimiento de la comisión de actos delictivos y conservarlos por más tiempo en base a estos motivos. Sin embargo, seria necesario regular las limitaciones al uso de esta información durante el tiempo en el que este permitida su conservación.

Tabla 99. Aspectos referidos a la dirección IP como un dato de tráfico.

b)¿Cuándo requiere la Directiva que se obtenga el consentimiento de los usuarios-abonados para el tratamiento de sus datos?. En

líneas generales, el espíritu de la Directiva pretende que cualquier actividad relacionada con el suministro de servicios de comunicaciones electrónicas que vayan mas allá de la transición de una comunicación o de su facturación(i.e. la presentación de servicios de valor añadido), deberá basarse en datos anónimos y, en el caso de que esto no fuera posible, obtener el consentimiento de los titulares.

c) Restricción de la identificación de la línea de origen. Otro de los principales artículos que podría ser aplicable por analogía a Ipv6 es el Articulo 8 dedicado a la presentación y restricción de la línea de origen y de la línea conectada. En este sentido, si bien este articulo podría parecer mas destinado a la regulación de los servicios de telefonía(móvil o fija), en principio, podría entenderse como aplicable para el supuesto de comunicaciones electrónicas efectuadas a través del protocolo Ipv6. A través del mismo se manifiesta la voluntad del legislador de preservar la intimidad del usuario que efectúa la llamada, obligando a los proveedores del servicio a ofrecerle la posibilidad técnica de que evite la identificación de la línea llamante, cuando exista la posibilidad de que esta pueda ser visualizada.

Asimismo, desea proteger los intereses del usuario que recibe las llamadas permitiéndole excluir la reaceptación de llamadas por parte de usuarios que hubieran impedido la identificación de su línea llamada. Siguiendo el criterio establecido en este articulo, podría determinarse que respecto de las direcciones Ip formalizadas en base de un identificador único, podría exigírsele a los proveedores la posibilidad de adoptar ciertos mecanismos que impida:

- La identificación de la dirección IP del usuario en las comunicaciones que efectué, siempre que esta identificación no fuera necesaria
- La posibilidad de evitar la recepción de comunicaciones transmitidas a través de una determinada IP, cuando el usuario que origina la llamada haya evitado el conocimiento de su IP.

No obstante, el Considerando 19 establece que en los casos particulares en los que la adopción de estas medidas sea técnicamente imposible para el proveedor o en los que se requiera un esfuerzo económico desproporcionado, la implantación de estas medidas no tendrá carácter obligatorio. En todo caso, los usuarios deberán ser informados de esta imposibilidad y los estados Miembros, notificarlo a la Comisión.

En cierto modo, en la actualidad, se están adoptando ciertas medidas técnicas encargadas de favorecer este tipo de actividades que, por analogía, parece que deberían ser aplicables respecto de las direcciones IP, algunas de ellas basadas en el estándar RFC3041.

No obstante, la Directiva enumera varios casos en los que el servicio de anulación de la identificación de la línea llamante, no deberá ser prestado por los proveedores de servicios de comunicaciones electrónicas:

- Para identificar el numero de origen de llamadas malevolentes o molestas.
- Para atender llamadas de urgencia por parte de organismos reconocidos por los estados Miembros para prestar estos servicios, policía, ambulancias, bomberos, etc.

d) Consideración del dato de dirección IP como dato de localización. Por “dato de localización” debe entenderse, conforme establece el apartado c) del articulo 2 de la Directiva “cualquier dato tratado en una red de comunicaciones electrónica que indique la posición geográfica del equipo terminal del usuario de un servicio de comunicaciones electrónicas disponible para el publico”.

Conforme al Considerando 14, los datos de localización serán aquellos referidos a “la latitud, longitud y a la altitud del equipo terminal del usuario, a la dirección de la marcha, al nivel de precisión de la información de localización ha sido registrada”. En las redes móviles digitales es posible que se traten los datos sobre localización(los cuales son considerados datos de trafico) que pueden proporcionar la posición

geográfica del equipo terminal móvil del usuario para hacer posible la trasmisión de las comunicaciones.

Este hecho adquiere mayor relevancia en los supuesto en los que un dispositivo con movilidad(PDA's, portátiles, teléfonos móviles, etc.) acceda a la Red a través de una IP, puesto que además de existir la posibilidad de rastrear su navegación, seria posible conocer su ubicación física, tanto del terminal como del propio usuario titular del mismo.

Esta posibilidad abre numerosos frentes de tratamientos de datos que deberán regularizarse conforme a la Directiva 95/46/Ce y a las legislaciones nacionales de desarrollo de la misma, por ejemplo, la posibilidad de adquirir(en la mayor parte de los casos de forma ilícita) este tipo de información por prestadores de servicios de información sobre las condiciones del trafico por carretera para ofrecer determinados servicios a un usuario, en ocasiones sin que este hubiera solicitado(por ejemplo, estado del trafico en la carretera por la que circula); el control de los tele-trabajadores o la creación de perfiles, hábitos de viaje de una determinada persona, lo cual, desde un aspecto meramente comercial, podría reportar importante ventajas económicas para aquello agentes que deseen aprovecharse de este tipo de avances tecnológicos.

Es este sentido, es fundamental resaltar que la Directiva establece que este tipo de datos, únicamente, podrán tratarse con el consentimiento informado del usuario afectado e incluso, aunque este lo hubiera prestado en un momento determinado, deben establecerse mecanismos que favorezcan la revocación de este consentimiento en cualquier momento.

Asimismo la directiva permite que únicamente trate estos datos aquellos agentes que actúen en nombre y por cuenta del proveedor de servicios de comunicaciones electrónicas adquiridos por el usuario, impidiendo su tratamiento por terceros ajenos a estos.

e) Regulación de las guías de abonados. Tal y como se vera en posteriores, uno de los medios que permitirían la asociación de una determinada IP con un determinado usuario y, por lo tanto, que

potenciaría la consideración del dato de dirección IP como un dato personal, es la adopción de guías publicas que contengan una relación de usuarios con sus respectivas direcciones IP.

Teniendo en cuenta esto, podría servir como criterio a la hora de adoptar esta práctica lo establecido en esta Directiva, en relación con las guías de abonados. A través de las mismas, el usuario puede decidir si desea públicos sus datos a terceros o no, pero, en todo caso, la inclusión de los mismo en las citadas guías requerirá que las entidades gestoras o suministradores de las mismas, informen a los titulares de los datos de las finalidades de estas guías, así como del resto de los parámetros del deber de información(cesiones de datos, posibilidad de ejercitar los derechos de acceso, rectificación, etc), por supuesto, obteniendo para ello su consentimiento. En este sentido, cualquier utilización de estas guías por parte de un agente tratante con fines distintos de aquellos para los que se obtuvo el consentimiento inicialmente del usuario, requerirá que este agente tratante lo obtenga de nuevo.

En resumen, el artículo 12 establece una serie de parámetros que deberán ser tenidos en cuento por los Estados Miembros a la hora de crear guías publicas:

- Obligación de informar a los titulares de los datos de su inclusión en la guía.
- Posibilidad de que las guías sean impresas o electrónicas
- Facultad de decidir por parte de los titulares de los datos, cuales de ellos van a figurar en las guías
- Respeto al principio de calidad de datos: inclusión de datos adecuados, pertinentes y no excesivos.
- Carácter gratuito de la no inclusión, comprobación, corrección o supresión de datos en una guía publica.

f) ¿Debe modificarse la Directiva 2002/58/CE con la implantación del protocolo Ipv6?

Actualmente, esta Directiva se corresponde con el marco regulador en materia de protección de la intimidad y de protección de datos

personales que mas se aproxima a la regulación que debería ser ofrecida para la utilización del nuevo protocolo Ipv6.

La mayor parte de los artículos recogidos en la misma regulan supuestos que, bien directamente o bien de forma más indirecta, se encuentran relacionados con Ipv6. En algunos supuestos, como ocurre con la regulación de la posibilidad de restringir la identificación de la línea de origen o la regulación de las guías de abonados, si bien parecería claro que dichos artículos pretenden regular un supuesto de hecho diferente, podrían ser aplicables de forma analógica a la utilización del protocolo en su nueva versión 6.

Por ello, cabria afirmar que a través de la misma se ofrecen los criterios generales a tener en cuenta, los cuales deberían ser adaptados por los estados miembros a la hora de regular, a través de cada una de sus legislaciones nacionales, el uso de Ipv6 y la forma de dar cumplimiento a las obligaciones impuesta en esta directiva como en la Directiva 95/46/CE.

4.6 Desarrollo normativo en materia de protección de datos.

Como consecuencia del Considerando 22 y del artículo 32 de la Directiva 95/46/CE, los Estados Miembros tendrán que adecuar su legislación a las consideraciones efectuadas por la misma. Por este motivo, los distintos Estados comunitarios han ido adoptando sus propias normativas nacionales tendentes a regular estos aspectos. A efectos meramente informativos, algunos de estos Estados que ya disponen de una normativa, más o menos restrictiva en materia de tratamiento de datos personales son Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Gran Bretaña, Grecia, Holanda, Irlanda, Italia, Luxemburgo, Portugal y Suecia. Pero cabe destacar que también se considerara a EEUU.

Tal y como podrá comprobarse, son pocas las innovaciones recogidas en estas normas, las cuales suelen ser un mero reflejo de las disposiciones de la Directiva 95/46/CE de referencia.

Existen una serie de antecedentes que son fundamentales para comprender la legislación vigente en

materia de protección de datos de carácter personal. Estos antecedentes se remontan a finales de la década de los 70, la Organización de Naciones Unidas recoge hace tiempo una serie de principios rectores aplicables a los ficheros automatizados de datos personales que han sido la base de la actual legislación. Estos principios son: principio de licitud y lealtad, principio de exactitud, principio de finalidad, principio de acceso a la personal interesada, principio de no discriminación facultad de establecer excepciones, principio de seguridad, control de sanciones, flujo transfronterizo de datos y campo de aplicación.
Además existen una serie de convenios internacionales que han influido, tales como:
-La Declaración Universal de los Derecho Humanos adoptada y proclamada por la ONU el 10 de diciembre de 1984.
-Convenio Europeo para la protección de los Derechos Humanos y Libertades Fundamentales de 4 de noviembre de 1950.
-Convenio Nº 108 de 28 de Enero de 1981, del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal. En este ámbito nos podemos remontar a las resoluciones y recomendación del Consejo de Europa: a) Resolución 721/80. Informática y protección de los derechos del Hombre, b) Recomendación 890/80. Protección de datos de carácter personal y c) Recomendación 1037/86. Protección de datos y libertad de información.

Tabla 100. Síntesis de Legislación comparada.

a) Alemania: Alemania fue un país pionero en la adopción de normas de protección de datos, ya que la primera fue la conocida como Ley de Hesse, de 7 de octubre de 1970. Seguidamente, fue aprobada la Ley Alemana Federal de Protección de Datos, de fecha 27 de enero de 1977, la cual fue modificada por la ley llamada Bundesdatenschutzgesetz (BDSG), la cual entró en vigor el 1 de junio de 1991. Actualmente la norma que se encuentra en vigor es denominada "The Federal Data Protection Act" (Bundesdatenschutzgesetz) de 18 de mayo de 2001. Asimismo, es importante destacar que existen numerosas normas adoptadas por distintas ciudades alemanas (Berlín, Brandenburgo, Essen, Saarland, etc) sobre esta materia.

Consideraciones a destacar. El propósito de la Norma es proteger el derecho a la privacidad de los individuos frente a los tratamientos de sus datos personales realizados en su perjuicio (artículo 1). Con este fin, la norma es un reflejo fiel del modelo de protección de datos personales creado por la Directiva 95/46/CE y regula principios y obligaciones como los requisitos de calidad en la obtención de los datos; necesidad de obtención del consentimiento para el tratamiento; principio de seguridad y auditoría, etc. Es relevante, dentro del texto de la Norma, que la persona que provee un medio de grabación o procesamiento de datos personales, que instala dicho medio o que modifica o pone a disposición un procedimiento para el procesamiento automático de datos personales que

funcione total o parcialmente en un medio como el citado, debe informar al interesado de ciertos aspectos, a menos que éste tuviera conocimiento de los mismos (artículo 6 c). Asimismo, en su Capítulo III, se regula el funcionamiento de la Autoridad de Control alemana (Federal Data Protection Commissioner).

b) Austria: La primera ley austriaca de protección de datos (Datenschutzgesetz) data del 18 de octubre de 1978 y fue posteriormente modificada por la decisión 609/1989 de la Corte Constitucional. Actualmente, la norma que se encuentra en vigor es el Federal Act Concerning the Protection of Personal Data (Dasenschutzgesetz 2000), la cual entró en vigor el 1 de enero del año 2000. Asimismo, distintas regiones (Länders) han adoptado su normativa a esta ley, tales como Kärnten, Salzburgo o Viena, entre otras.

Consideraciones a destacar. Alguno de los aspectos más relevantes tratados por esta Norma son los siguientes:

• El derecho a la protección de datos se considera como un derecho fundamental(artículo 1).

• Las restricciones al deber de confidencialidad solo están permitidas cuando se trate de proteger un interés superior y legítimo de un tercero (artículo 1).

• Los intervinientes en un sistema o conjunto de información (sistema de procesamiento conjunto de datos por varios responsables con acceso recíproco a los datos) deberán señalar un operador cuyo nombre y dirección sea incluido en el Registro de Procesamiento de Datos (artículo 50).

En definitiva, además de cumplir con la necesidad de trasposición de la Directiva 95/46/CE, la ley austriaca regula, sin salirse de la norma comunitaria, algunos supuestos que no aparecen en otros ordenamientos, como el citado del artículo 50.

c) Bélgica: La primera norma en materia de protección de datos adoptada en Bélgica es de 8 de diciembre de 1992. Actualmente, la normativa vigente entró en vigor el 1 de septiembre de 2001.

Consideraciones a destacar. Se señala que toda persona física tiene derecho a la protección de sus libertades y Derecho fundamentales, particularmente a la protección de la vida privada, en el tratamiento de sus datos de carácter personal (artículo 2). El ámbito de aplicación de la ley se extiende tanto a los tratamientos automatizados como a los no automatizados (artículo 3). Siguiendo esta línea inicial, la Norma viene a reflejar los requerimientos establecidos por la Directiva 95/46/CE y, por lo tanto, alguno de los principios y obligaciones contenidos en la misma son la obligación de notificar ficheros; el respeto a los derechos del titular de los datos; el especial tratamiento de los datos sensibles, etc.

d) Dinamarca: En Dinamarca, la primera legislación de protección de datos fue doble: una primera norma aplicable a ficheros de titularidad pública, la Ley 294 de 8 de junio de 1978 sobre registros públicos (posteriormente modificada en varias ocasiones) y una segunda, para ficheros de titularidad privada, la ley 293 de 8 de junio de 1978 sobre registros privados, también modificada en varias ocasiones. La legislación vigente en esta materia es "The Act on Processing of Personal Data" (Act No 429) de 31 de mayo del 2000.

Consideraciones a destacar. La Norma se aplica a los tratamientos, automatizados o no, de datos personales de personas físicas. No obstante, determinadas partes se aplican, igualmente, a los tratamientos de datos referentes a empresas (artículo 1), con lo que se introduce un cambio significativo en el ámbito de aplicación con relación al que se contiene en la Directiva 95/46/CE. Como referencia con incidencia en el ámbito de las telecomunicaciones, se indica que no cabrá que las autoridades públicas, empresas privadas, etc. registren de forma automática las llamadas realizadas o recibidas desde sus teléfonos, salvo autorización previa de la autoridad de supervisión y siempre que haya un interés, público o privado, suficiente. Esta prohibición no se aplica cuando se realice por operadores de telecomunicaciones o en la prestación de servicios de identificación de llamada entrante.

e) España: En el caso de España, la primera norma que entró en vigor fue la conocida LORTAD, Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Posteriormente, esta ley se ha visto derogada por la vigente Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, también denominada LOPD. Asimismo, es importante resaltar que como desarrollo del artículo 9 de la LOPD se aprobó el Real Decreto 994/1999 de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad. En este Reglamento se recogen las medidas de seguridad técnicas y organizativas que deberán adoptarse para proteger los ficheros con datos personales que sean tratados por cualquier entidad.

En este sentido, los datos de carácter personal se dividen en tres categorías diferentes (nivel básico, medio y alto) y dependiendo de la categoría de los datos tratados, se adoptarán un tipo de medidas de seguridad u otro.

Consideraciones a destacar. La ley tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar. En términos generales, la norma española es un fiel reflejo del régimen comunitario común establecido por la Directiva 95/46/CE. En este sentido, regula el principio de calidad de los datos; deber de información; necesidad de obtener el consentimiento para el tratamiento (salvo excepciones); especial tratamiento para los datos sensibles; condiciones de tratamiento de datos por terceros, etc. Alguno de los artículos que podrían estar relacionados con algunos de los temas a tratar en este libro es el relativo a los repertorios telefónicos que son considerados como una fuente accesible al público, en los términos previstos en su normativa específica. Las fuentes accesibles al público se definen como aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación (artículo 3). En cuanto a los datos que podrán figurar en

las guías de servicios de telecomunicaciones disponibles al público, se remite a sus normas específicas.

Vale aclarar que la Ley Organica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de carácter personal(LORTAD), adoptada en España en 1992, constituye la piedra angular sobre la cual se diseño la ley Chilena, Ley 19.628[199].

f) Finlandia: La regulación finlandesa en materia de protección de datos personales ha estado basada en tres normas fundamentales:

• Ley de 30 de abril de 1987 sobre ficheros de datos personales

• Ley de 30 de abril de 1987 sobre la Comisión y el Ombudsman de protección de datos

• Decreto de 30 de abril de 1987 sobre ficheros de datos personales

Actualmente, la legislación vigente en esta materia es "The Finnish Personal Data Act" (523/1999) de 22 de abril. No obstante, esta ley ha sufrido ciertas modificaciones a partir del Act on the amendment of the Personal Data Act (986/2000) que entró en vigor el 1 de diciembre de 2000.

Consideraciones a destacar. El artículo 1 de esta Norma establece como su objetivo, implantar en el tratamiento de datos personales, la protección a la vida privada y otros derechos fundamentales que salvaguardan el derecho a la intimidad, así como potenciar el desarrollo de una buena práctica en el trata- miento de datos personales. Algunas de las reglas generales para el tratamiento de datos personales, enumeradas en el Capítulo 2 de la Norma son: determinación de la finalidad del tratamiento; tratamiento de los datos exclusivamente conforme a dicha finalidad; calidad de los datos; deber de información; tratamiento de datos sensibles, el cual se encuentra prohibido si no median algunas circunstancias tales como la obtención del consentimiento expreso del titular; transferencias internacionales; regulación de los derechos de acceso y rectificación, etc. Una de las novedades se introduce en la Sección 13 cuando se regula el tratamiento del número personal de identidad, de forma específica,

[199] Para una revisión sobre el proceso histórico de la legislación sobre protección de datos personales en España, vid. Suñé Llinás, Emilio, "Tratado…"

requiriéndose para ello, la obtención del consentimiento inequívoco del interesado. Asimismo, la Sección 17 regula la creación de registros de consulta pública, de manera que los datos se incluirán en los mismos siempre que su titular no se hubiera negado a ello. Otra de las novedades se encuentra en la Sección 21 donde se establecen los distintos plazos de conservación de la información por los responsables de los ficheros. Por último, la Sección 38 crea la autoridad de Control en Finlandia, la cual es denominada “The Data Protection Ombudsman”.

g) Francia: La primera ley francesa sobre esta materia fue la Ley 78-17 de 6 de enero de 1978. Actualmente, se está debatiendo en el Parlamento la adopción de una serie de modificaciones a la misma.

Consideraciones a destacar. El tratamiento de datos personales no podrá ser contrario a la identidad humana, los derechos del hombre, la privacidad o las libertades individuales o públicas (artículo 1). El concepto de tratamiento automatizado de datos se refiere a cualquier serie de operaciones efectuadas por medios automáticos, incluyendo la recogida, la grabación, la preparación, la modificación, el almacenaje y la destrucción de datos personales así como cualesquiera operaciones que se relacionan con el empleo de ficheros o bases de datos, incluyendo interconexiones o comparaciones, la consulta o la comunicación de datos personales (artículo 5). Puesto que la norma francesa es sensiblemente anterior a la Directiva 95/46/CE, es necesario garantizar su evolución conforme a los criterios marcados por la norma comunitaria y, por lo tanto, estos criterios deberán ser tenidos en cuenta para la nueva normativa que se adopte en Francia.

h) Gran Bretaña: La legislación británica en materia de protección de datos comienza con la Ley de 12 de julio de 1984 (Data Protection Act), la cual entró en vigor en dos momentos distintos y por partes:

12 de septiembre de 1984 y 11 de noviembre de 1987. Asimismo, Gran Bretaña dispone de un Reglamento de 13 de octubre de 1985 dedicado al Tribunal de Protección de Datos. Posteriormente, esta legislación se ha derogado, encontrándose en vigor el “Data Protection Act” de 1998.

Consideraciones a destacar. A través de esta normativa se regulan las distintas obligaciones requeridas por la Directiva 95/46/CE. En la Parte I se recogen algunas de ellas, como el deber de información, obligación de rectificar, bloquear, borrar o destruir los datos de carácter personal o la prohibición de tratar datos personales si previamente no se ha notificado el fichero a la autoridad de control británica denominada "Data Protection Commissioner". Asimismo, se establece que cualquier tratamiento de datos que se realice con finalidades de prevención o detección de delitos, arresto o enjuiciamiento de los responsables, no estará vinculado por el deber de información. Es decir, el tratamiento del dato de dirección IP y de la información asociada a la misma para estos fines no requerirá informar al titular de la misma. El principio de obtención del consentimiento como premisa para efectuar un tratamiento o cesión de datos se recoge en la Sección 55. Por otro lado, The Data Protection Act de 1998 recoge una serie de modificaciones en su cuerpo normativo al Consumer Credit Act del año 1974. La Parte II recoge la interpretación de los principios enumerados en la norma así como de la determinación de las condiciones a tener en cuenta respecto de estos principios, para el tratamiento de todo tipo de datos y para el tratamiento de datos sensibles, así como una enumeración de los supuestos en los que cada uno de estos principios no son aplicables. Otro de los aspectos regulados son los procedimientos de inspección o la regulación de las fuentes de acceso público.

i) Grecia: La Ley de protección de datos griega es la 2472/1997 de protección de las personas con respecto al tratamiento de datos de carácter personal, aprobada el 10 de abril.

Consideraciones a destacar. El objeto de esta norma es determinar las condiciones relativas al tratamiento de datos personales y la protección de los derechos humanos, libertades fundamentales y la vida privada, según establece el artículo 1. De nuevo, siguiendo las consideraciones de la Directiva de referencia (95/46/CE) establece en su articulado el respeto a principios tales como la calidad de los datos, el deber de información, la necesidad de obtener el consentimiento para el

tratamiento, salvo las excepciones del artículo 2 y, en todo caso, será necesario el consentimiento escrito para el tratamiento de datos sensibles. Otros de los temas regulados son la cesión de datos, las cuales deberán ser comunicadas a la Autoridad de control griega y, en el caso de que se basen en datos sensibles, se deberá obtener su autorización; regulación de transferencias internacionales de datos; ejercicio de derechos de acceso y oposición o el régimen de sanciones e infracciones penales y administrativas, entre otras.

j) Holanda: La primera ley holandesa en materia de protección de datos fue la Ley de 28 de diciembre de 1988, denominada "Wet personenregistraties" y más conocida como WPR. Actualmente, se encuentra vigente Personal Data Protection Act de 6 de julio de 2000.

Consideraciones a destacar. Se establece que esta Norma se aplica tanto a los tratamientos automatizados como no automatizados de datos personales.

A través de los artículos 7 al 11 se recogen algunos de los requisitos que deben darse en todo tratamiento de datos: obtención de los datos para fines legítimos y claramente determinados; necesarios para cumplir una obligación legal o el cumplimiento de un contrato (entre otras causas); conservación de los datos por el tiempo necesario para el cumplimiento de la finalidad de tratamiento, etc.

Por otro lado, los artículos 16 al 24 regulan el tratamiento de los datos sensibles (religión, filosofía de vida, política, raza, salud, vida sexual, afiliación sindical; antecedentes criminales). En algunos casos, por ejemplo, para el tratamiento de datos de raza u origen ético, entre las causas que permiten su tratamiento, se encuentra el hecho de que el titular de los datos no se hubiera opuesto al mismo por escrito (artículo 18 3º), lo cual difiere de las regulaciones de otros Estados Miembros sobre este asunto. El artículo 25 recoge la posibilidad de adoptar Códigos de Conducta por distintas entidades, para lo cual necesitarán la aprobación de la Data Protection Commission (Autoridad de Control holandesa). El deber de información se recoge en los artículos 33 y 34 de esta Norma.

Asimismo, regula los derechos de los titulares de los datos, las transferencias internacionales y el régimen de infracciones y sanciones, entre otras obligaciones ya impuestas en la Directiva 95/46/CE.

k) Irlanda: La primera Ley de protección de datos irlandesa fue de fecha 13 de julio de 1988. Actualmente, está siendo debatido ante el Parlamento un proyecto de ley.

Consideraciones a destacar.

La Data Protection Act de 1988 es una norma bastante antigua en el tiempo.

En su artículo 1 se define como "dato personal", toda información relativa a una persona viva que pueda ser identificada bien a través de los datos, o por medio de los datos asociados con otra información que esté en posesión del responsable del fichero. A través de los artículo 4 a 6 se regulan las condiciones para ejercitar el derecho de acceso y rectificación por parte de los titulares de los datos. Su Autoridad de Control (Comisión) es creada a partir de los artículos 9 y 10. Otros aspectos regulados son la transferencia internacional de datos; condiciones específicas para la notificación de ficheros o el régimen de infracciones y sanciones.

l) Italia: La ley de protección de datos italiana es la Ley 675/96 de 31 de diciembre (Tutella delle persone e di altri soggetti rispetto al tratamento dei dati personali). Asimismo, se han aprobado un conjunto de normas en base a la misma, en particular, reales decretos tales como el nº 123 de mayo de 1997; nº 255 de julio de 1997; nº 135 de mayo de 1998 o el más reciente, el nº 282 de julio de 1999.

Consideraciones a destacar. Conforme se establece en su artículo 1, esta Norma pretende asegurar que el tratamiento de datos personales se realice respetando los derechos fundamentales y las libertades y dignidad de las personas físicas, con especial atención a su derecho a la privacidad. Asimismo, como novedad, garantiza los derechos de las personas jurídicas, en esta materia. Siguiendo los criterios de la Directiva 95/46/CE, algunos de los principios tratados son: calidad de los datos; deber de información; obtención del consentimiento y excepciones; seguridad de los

datos, principio que será desarrollado a través de real decreto; transmisiones de datos a terceros; tratamiento de datos sensibles o transferencias internacionales, entre otros. Específicamente, esta norma recoge qué debe hacerse por el responsable del fichero, una vez que finalice el tratamiento de los datos: destruirlos, transmitirlos a otro responsable o mantenerlos disociados.

m) Luxemburgo: La primera regulación existente en esta materia en Luxemburgo fue la Ley de 31 de marzo de 1979 (Act Regulating the Use of National Data in Data Processing), la cual ha sufrido varias modificaciones posteriores y el Reglamento del Gran Ducado de 2 de agosto de 1979, sobre la Comisión Consultiva prevista en el artículo 30 de la ley de 31 de marzo. Actualmente, la ley vigente es del año 2002.

Consideraciones a destacar. La Norma protege los derechos fundamentales y las libertades de personas físicas, en partiular sus vidas privadas, en cuanto al tratamiento de datos personales, y asegura el respeto de los intereses legalmente protegidos de las mismas (artículo 1). Conforme a la definición de Procesamiento de datos personales del artículo 2, la ley se aplica a los tratamientos automatizados y no automatizados de datos. Ya con estas referencias se puede observar una clara tendencia en la consecución de una fiel transposición del régimen comunitario establecido por la Directiva 95/46/CE.

n) Portugal: La primera ley de protección de datos portuguesa es de fecha de 9 de abril de 1991 (Ley 10/91). Actualmente, se encuentra en vigor la Ley 67/98 de 26 de octubre (Lei da Proteccao de Dados Pessoais).

Consideraciones a destacar. El principio general perseguido por esta Norma se recoge en su artículo 2: el tratamiento de datos personales debe realizarse de forma transparente y con estricto respeto a la vida privada, los derechos, libertades y garantías fundamentales. Esta Norma no introduce novedades respecto de los principios y obligaciones impuestas por la Directiva 95/46/CE, de manera que alguno de éstos son los siguientes: calidad de los datos; necesidad de amparar el tratamiento en el consentimiento inequívoco del titular o en alguna de las excepciones

recogidas en la Norma; tratamiento especial para los datos sensibles; regulación de las cesiones de datos; derechos de los titulares; deber de información; seguridad; tratamiento de datos por entidades subcontratadas; transferencias internacionales; códigos de conducta; etc. La autoridad de control en Portugal recibe el nombre de Comissao Nacional de Proteccao de Dados, también llamada CNPD.

o) Suecia: La primera ley sueca de protección de datos fue la Ley 1973/289 que, posteriormente, se ha visto modificada en 1989. Actualmente, la ley vigente es el Personal Data Act (1998/204).

Consideraciones a destacar. El propósito de esta Norma es proteger a las personas contra la violación de su integridad a través del tratamiento de sus datos personales. Al igual que el resto de normativas nacionales analizadas, esta protección se asegura a través de una serie de principios y obligaciones que deberán ser adoptados. A lo largo de la misma, se establecen unos requisitos esenciales para todo tratamiento de datos: legitimidad del tratamiento; determinación clara de las finalidades del tratamiento; solicitud de datos adecuados, pertinentes y puestos al día; obligación general de obtener el consentimiento del titular (salvo excepciones); especiales medidas para el tratamiento de datos sensibles; deber de información; regularización de tratamientos efectuados por terceros, etc. Como ha podido comprobarse, las principales normas aprobadas por los Estados Miembros sobre esta materia, recogen fielmente las obligaciones, derechos y principios referidos en la Directiva 95/46/CE, de manera que no es frecuente encontrar artículos "novedosos" aplicables de forma específica a IPv6. En este sentido, sería necesario conocer la legislación recogida en estos Estados, de carácter sectorial, como por ejemplo, la legislación de telecomunicaciones, comunicaciones electrónicas, etc.

A modo de comentario en **EEUU,** la primera norma sobre la materia las encontramos contenidas en la Fair Credit Reporting Act, del 26 de octubre de 1970[200], en la cual se establece

[200] La Fair Credit Reporting Act se encuentra en el United Status Code 15, seccion 1681, pag. 255. Tracuccion en español en "Informatica. Leyes de Proteccion de datos", Documentación Informatica, Nº 2(Serie

el derecho afectado a acceder al conocimiento de la información existente sobre el y la correspondiente obligación de la empresa dedicada al suministro de datos personales de comunicársela, de modo que pueda conocer la naturaleza y contenido de toda la información que posea sobre el; las fuentes de la información obtenida y los receptores de la información. El 31 de diciembre de 1974, se añade la Privacy Act. En el intertanto, en el año 1973, el departamento de Salud, Educación y Bienes elaboro y dio a conocer un estudio titulado *Records Computers and the Rights of Citizens*. En el se proponía la elaboración de un código federal de *fair information practices* encaminado a resguarda la intimidad personal. *La Privacy Act* de 1974, fue modificada varias veces en los años sucesivos materializando muchas de estas sugerencias. De este modo, se reconoció a los individuos el derecho a la reserva de la información que sobre ello posee el gobierno federal, limitando en aras de la defensa de la personalidad, la libertad de expresión e información. No obstante, el panorama norteamericano no termina con ellas, pues junto a estas normas generales existen diversas leyes sectoriales como *The Family Education of Information Act*, de 1974(sobre los expedientes académicos); *The Freedom of information Act*, de 1974(que exime al gobierno de hacer públicos sus archivos cuando esto suponga una injustificada invasión de la intimidad de las personas); The Tax Reform Act, de 1978(Sobre la obligación de confidencialidad de los datos bancarios); The Electronic Fund Transfer Act de 1978(sobre la obligación de las instituciones financieras que efectúen transferencias electrónicas u otros servicios bancarios por ese procedimiento, de informar a sus clientes del acceso de terceras personales a sus bancos de datos); *The Privacy protection Act,* de 1980(Sobre la tutela especial que se establece a favor de periodistas o informadores limitando las facultades de los agentes públicos dedicados a la persecución de los delitos en relación con el registro de sus materiales de trabajo).

Tabla 101. Consideración en EEUU.

4.7 Implicaciones practicas de la protección de datos a la implantación del Ipv6.

Una vez que ha sido analizada la legislación vigente en esta materia, a continuación, se expondrán algunos de los problemas prácticos con implicaciones en protección de datos más relevantes, tras la implantación de IPv6.

a) Nuevos tratamientos de datos como consecuencia del uso de IPv6. El dato de dirección IP podría considerarse como un dato de carácter personal habida cuenta que existe la posibilidad de relacionar dicha dirección IP (a partir del Identificador Único que forma parte de la misma) con el terminal al que identifica y, en consecuencia, podría existir la posibilidad de relacionarla con el usuario titular de dicha IP.

Verde), Legislación, 1ª. Ed., Servicio Central de Publicaciones, Presidencia del Gobierno de Madrid, 1977, pag, 105 y ss.

Este hecho, conlleva dos consecuencias y dos ámbitos que, necesariamente, deberán regularse en materia de protección de datos personales:

- Las consecuencias derivadas de la obtención y tratamiento de la dirección IP basada en un Identificador Único, como dato en sí de carácter personal.
- Los nuevos tratamientos de datos que se generarán como consecuencia de la potencialidad de asociar cierta información distinta de la propia dirección IP, que hasta ahora podría ser anónima, con una determinada persona. Por ejemplo, con las direcciones IP asignadas de forma dinámica por un Internet Access Provider y utilizadas a través del actual Protocolo, versión 4, un usuario cada vez que accedía a la Red lo hacía a través de una IP diferente. En una sesión podría acceder a una página web concreta donde se le solicitaran una serie de datos a los efectos de conocer qué tipo de usuarios acceden a dicha página, por ejemplo, su edad y sexo.

En este caso, si el usuario no aportaba su nombre y apellidos y en el caso de que el portal no tuviera mecanismos de rastreo, cookies, etc, en principio, dichos datos serían anónimos. Como mucho podrían quedar asociados a una dirección IP dinámica, la cual cambiaría para ese usuario en una próxima conexión.

Por otro lado, es importante indicar que muchos proveedores de acceso proporcionan direcciones estáticas a sus usuarios, y en general, debido a la necesidad de intercepción legal y registro de las transacciones, no hay una situación real de conexión anónima.

Pues bien, con IPv6 dichos datos podrían ser asociados a una determinada IP con Identificador Único que identificaría automáticamente a un terminal y, potencialmente, a un usuario concreto.

Por este motivo, la implantación de IPv6 conlleva que en ambos casos exista, salvo excepciones, un tratamiento de datos nuevo y, por tanto, unas nuevas obligaciones a cumplir por parte de los agentes tratantes involucrados.

Es clave recordar la importancia a este respecto del RFC3041, que como anteriormente se ha indicado, cuando se usa, proporciona un nivel de privacidad superior, no disponible con IPv4.

b) **Posibilidad de "portabilidad" en las direcciones IP con Identificador Único.** Otro de los problemas jurídicos que podrían plantearse está basado en quien o qué entidad será la encargada de otorgar este tipo de direcciones IP y, asimismo, en el caso de que fueran otorgadas por el proveedor de acceso o por la operadora de telecomunicaciones, si dichas direcciones serán las mismas para cada usuario o podrán variar si dicho usuario cambiara de proveedor de acceso o de operadora.

   El hecho de que estas direcciones no tuvieran el carácter de "propias y permanentes" para cada uno de los usuarios, conllevaría la necesidad de llevar a cabo ciertas actividades relevantes desde el punto de vista de la protección de datos, que deberían regularizarse.

   Por ejemplo, la obligaciones de actualizar las guías públicas que pudieran generarse sobre esta materia y la necesidad de que los proveedores de acceso, operadoras de telecomunicaciones y cualquier otro agente tratante comuniquen las modificaciones efectuadas sobre la titularidad de estas IP´s.

   En estos supuestos, deberían crearse disposiciones que regularan o, al menos, aportaran criterios para proceder al tratamiento de los datos conforme a la normativa vigente.

c) **Posibilidad de rastrear la navegación de los usuarios.** Uno de los principales problemas que han sido detectados con respecto a la implantación de las direcciones IP basadas en un Identificador Único, es el hecho de que es posible rastrear la navegación y actividades realizadas por el usuario conectado a la Red (lo cual ya era posible en la versión del Protocolo IP anterior a través de cookies, mecanismos espía, etc), pero la novedad se basa en el hecho de que los resultados de dicho

rastreo pueden asociarse a un terminal y, potencialmente, a su titular o persona que los ha llevado a cabo.

Si bien, una de las principales premisas de la normativa analizada es que los tratamientos de datos personales se efectúen con una serie de garantías para el titular de los mismos, esta posibilidad permitida por IPv6 abre las puertas a nuevos tipos de tratamientos que, hasta ahora, no tenían la necesidad de ser regularizados.

Por ejemplo, un rastreador con capacidad de asociar la información a su titular, podría llegar a conocer, por ejemplo, los lugares o páginas web visitadas por éste, las horas de conexión y de desconexión, los objetos o servicios adquiridos, las compras realizadas, por ejemplo, a través de las solicitudes efectuadas al supermercado por su nevera, e incluso, la localización del terminal desde el cual se estarían efectuando las comunicaciones correspondientes.

Sin embargo, analizando este supuesto desde otra perspectiva, tal vez menos alarmista, es posible darnos cuenta de que en el momento en el que un usuario obtenga una determinada dirección IP basada en un Identificador Único, comenzará a ser consciente de la posibilidad de que se efectúen este tipo de tratamientos sobre su información personal y, además, debería ser informado de ello por los distintos agentes tratantes. En consecuencia, deberá exigir a su proveedor la adopción de medidas técnicas que faciliten la preservación de su identidad (i.e. RFC3041).

En este sentido, la Posición Común respecto a la elaboración de perfiles en línea en Internet, adoptado en el 27 Encuentro del Grupo de Trabajo de Berlín, en Creta el 4/5 de Mayo de 2000, establece para los proveedores de servicios de Internet, la obligación de notificar a los usuarios, en todo caso, el tipo, propósito, lugar, duración del almacenamiento, recogida, tratamiento y uso de los datos con la finalidad de obtener perfiles del usuario. Incluso, esta obligación va más allá, al exigir a los proveedores que este deber de información deberá cumplirse aunque los datos recogidos se asociaran a un pseudónimo.

d) **¿Qué medios pueden existir para dar cumplimiento al deber de información por los agentes tratantes?**

Realmente, no se plantean, en principio, problemas distintos acerca del cumplimiento del deber de información por parte de los agentes tratantes que no existieran con versiones anteriores de este Protocolo.

En los casos en los que se efectúe una contratación con el usuario y se pretenda conservar su dirección de IP para determinadas finalidades, deberá incluirse una cláusula informativa en dicho contrato.

Si por el contrario, dicha obtención y tratamiento se efectúa a través de la navegación, por medio de cualquier tipo de dispositivo conectado a la Red, deberá introducirse la cláusula informativa correspondiente en cada una de las páginas web accedidas, cuyo titular pretenda tratar este dato personal.

En este sentido, es importante resaltar que si un determinado agente tratante hubiera informado al titular de la dirección IP de cada uno de los aspectos determinados por la Directiva, incluidas las finalidades del tratamiento de sus datos previstas, en el caso de que con posterioridad decidiera tratarlos para finalidades distintas o nuevas, deberá volver a informar de ello a los titulares de los datos, así como obtener el debido consentimiento (tácito en unas ocasiones y expreso en otras) de éstos. En definitiva, respecto del cumplimiento de esta obligación, así como de otras contenidas en la legislación vigente, no se encontrarían especialidades respecto del modo o del medio para informar. Tal vez, el principal cambio se debe a que serán más el número de agentes tratantes que deban informar, al pasar a considerarse este dato, como un dato de carácter personal.

e) **Movilidad en IPv6.** Cuando se habla de “movilidad en IPv6”, debemos entender todos aquellos dispositivos que tienen la posibilidad de conectarse a la Red a través de distintos puntos, de manera que es como si “se movieran a lo largo de la Red” (por ejemplo, ordenadores portátiles, terminales de telefonía móvil, PDA´s, etc). Es decir, se trata de cualquier

dispositivo que pueda conectarse en un punto u otro punto de la Red sin perder su dirección IP.

Pensemos en el ordenador portátil de un ejecutivo, éste puede conectarse a la Red desde su oficina, desde su casa, desde el hotel donde se aloja, etc.

Para este tipo de dispositivos, es frecuente preguntarse si sus direcciones IP, basadas en IPv6, contienen la parte de Identificador Único y, por lo tanto, si a partir de las mismas, existe la posibilidad de identificar el dispositivo y la potencialidad de conocer a su titular.

En este caso, sí es posible que este tipo de direcciones se den para dispositivos móviles, cómo es posible conocerlas si éstos se conectan a la Red desde distintos lugares físicos, teniendo en cuenta que cuando estos dispositivos se mueven por la Red, generan nuevas direcciones como consecuencia de su nuevo punto de conexión.

Sin embargo, es importante resaltar que aunque parte de su dirección se ve modificada, el Identificador Único contenido en la dirección, se mantiene igual. De este modo, es posible identificar el dispositivo.

Como es lógico, esto plantea problemas más allá de la mera identificación del usuario, como por ejemplo, la posibilidad de conocer, con bastante acierto, su localización geográfica, ya que una dirección IP puede ser un dato de localización. Además, puesto que los datos de localización son datos de tráfico, tanto los operadores de telecomunicaciones como los ISPs, tienen la obligación de proceder a su retención para la persecución de actividades contrarias a la ley. En estos casos, si bien la intimidad de los usuarios podría verse afectada, éstos deberán tener en cuenta que este tratamiento está obligado por ley y que su capacidad para limitarlo se encuentra claramente reducida.

En este sentido, la Directiva 2002/58/CE permite que los Estados miembros determinen las medidas para llevar a cabo dicha retención de datos de tráfico. Así, su artículo 15 establece que “los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 (Confidencialidad de

las comunicaciones) y 6 (Datos de tráfico), en los apartados 1 a 5 del artículo 8 (Presentación y restricción de la identificación de la línea de origen y de la línea conectada) y en el artículo 9 (Datos de localización distintos de los datos de tráfico) de la presente Directiva, cuando tal limitación constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática para (…) la prevención, investigación, descubrimiento y persecución de delitos (…). Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado".

El mismo artículo señala que la adopción de tales medidas se adecuará a lo establecido en la Directiva 95/46/CE y que, además, el Grupo del Artículo 29 velará porque dichas medidas sean conformes a la protección de los derechos y libertades fundamentales y de los intereses legítimos en el sector de las comunicaciones electrónicas.

En consecuencia, la utilización de dispositivos con movilidad que hagan uso del protocolo IPv6 requiere tener en cuenta ciertos aspectos jurídicos, en gran medida similares a los que se han de tener en cuenta actualmente cuando el protocolo utilizado es IPv4.

Así, por ejemplo, supongamos que estamos utilizando un dispositivo móvil con IPv6 que dispone, en un solo equipo, de características típicas de un ordenador personal, un teléfono móvil, una PDA y un GPS. El dispositivo es adquirido a un proveedor de telecomunicaciones que actúa también como ISP y que gestiona una plataforma de servicios propios y servicios prestados por terceras partes.

El proveedor del dispositivo deberá obtener el consentimiento informado del usuario con relación a los tratamientos de datos que vayan a realizarse como consecuencia de la utilización del dispositivo móvil, tanto datos de tráfico como cualesquiera otros que se indique.

De tal manera, el proveedor deberá haber previsto, por ejemplo, en el momento de adquisición del dispositivo y a través de un contrato, la regulación necesaria en cuanto a tratamiento de datos personales,

referida, al menos, a qué datos se van a tratar, con qué finalidad, durante cuánto tiempo, qué otras partes (además del proveedor) van a acceder a los mismos, qué fines diferentes a los de gestión de datos de tráfico podrán llevarse a cabo, qué obligaciones legales de retención de datos existen, cómo podrá el usuario pedir el cese temporal de la recogida de datos o cómo podrá ejercitar sus derechos con relación a dichos datos.

El consentimiento se extenderá, únicamente, sobre los tipos de datos y tratamientos de los que expresamente se haya informado al usuario.

Otra situación, relativa al tratamiento de datos de localización distinta a los datos de tráfico, sería, por ejemplo, aquella en que se combinan las características de localización del dispositivo, a partir de la red a que se encuentre conectado, y GPS, para crear la ruta de un viaje o un desplazamiento del usuario en su vehículo.

En este caso, la Directiva 2002/58/CE establece que únicamente podrán tratarse los datos de localización del usuario distintos a los de tráfico, de manera personalizada, si se ha obtenido el consentimiento del usuario, en la medida y por el tiempo necesario para la prestación de un servicio de valor añadido (por ejemplo, incorporando información sobre los lugares por donde se está pasando, estado de la circulación de vehículos, rutas alternativas, etc.). Conforme indica la Directiva, el proveedor del servicio deberá informar a los usuarios o abonados, antes de obtener su consentimiento, del tipo de datos de localización distintos de los de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a efectos de la prestación del servicio de valor añadido. Igualmente, el usuario deberá contar con la posibilidad de retirar el consentimiento para el tratamiento de dichos datos y disponer de un método sencillo y gratuito para rechazar temporalmente el tratamiento de tales datos para cada conexión a la red correspondiente o para cada comunicación realizada.

En otro supuesto, igualmente utilizando el dispositivo móvil incorporado al vehículo del usuario, podemos plantear qué pasa si el vehículo es robado. En este caso, en primer lugar, las autoridades

competentes podrían utilizar la posibilidad de acceder a datos de tráfico relativos al dispositivo robado para lograr su localización física. Incluso, con el consentimiento informado del usuario, se podría acceder remotamente al dispositivo para, por ejemplo, a través de una cámara web incorporada al dispositivo, saber qué está pasando en el vehículo y proceder a su detención. En este supuesto, el proveedor de telecomunicaciones debería adoptar el compromiso de no atribuir al usuario, como datos personales, los generados desde el robo del dispositivo móvil hasta su recuperación y poner a disposición de las autoridades todos los datos generados por la utilización del dispositivo por quien lo robó (servicios utilizados, coste, duración, imágenes grabadas, borrado de datos grabados en el dispositivo, etc.).

Por último, cabe plantear, de manera aproximativa, qué implicaciones tiene el hecho conectar el dispositivo móvil a una red distinta a la habitual, con relación al tratamiento de datos personales. Por ejemplo, cuando se conecta a la red inalámbrica gratuita de un aeropuerto para gestionar un billete de avión. En este caso, el proveedor de la red inalámbrica deberá acordar con el usuario, mediante una cláusula de información y consentimiento, que deberá ser aceptada previamente a la utilización del servicio, todos los términos relativos a tipos de datos a tratar, finalidad, duración del tratamiento, etc., inclusive el hecho de que el dato de la IP basada en IPv6 y los datos que se generen asociados al mismo sólo se tratarán a efectos del acceso a la red inalámbrica.

Una vez esto, por ejemplo, el usuario comienza a gestionar su billete de avión, y debe realizar una videoconferencia con la compañía aérea para solucionar una incidencia. En este caso, se estaría utilizando la IP del usuario, de manera simultánea para una comunicación con telefonía móvil y un acceso a red inalámbrica. Recordemos que los tratamientos de datos han sido acordados, de manera separada y para cada servicio, con el operador de tele-comunicaciones y con el proveedor de la red inalámbrica. Lo más relevante en este caso es el compromiso, contractual y técnico, de ambos operadores de que sólo asociarán a la

concreta IP los datos relativos a su propio servicio, y no realizarán un cruce de datos por el hecho de que el usuario esté utilizando dos servicios diferentes de manera simultánea y haciendo uso de la misma IP o de dos IPs con un mismo Identificador Único.

En definitiva, podemos ver como, aunque la definición de los tratamientos personales variará en función de los servicios que establezcan, la utilización de dispositivos móviles con IPv6 genera una serie de tratamientos de dichos datos, en todo caso, que deberá adecuarse a los principios que se desarrollan a lo largo de esta Parte y cuyas fuentes principales son, actualmente, la Directiva 95/46/CE y la Directiva 2002/58/CE.

f) **IPv6 y Domótica.** Uno de los sectores donde más aplicación están teniendo los avances logrados durante estos últimos años por la Domótica es en el hogar y, en concreto, en los electrodomésticos. En este sentido, ha llegado a definirse la Domótica como "el uso simultáneo de la electricidad, la electrónica y la informática, aplicadas a la gestión técnica de las viviendas". En concreto, algunos de los objetivos perseguidos por estos avances son:

- Ahorro energético: control de temperatura, iluminación, consumos, etc.
- Seguridad: custodia y vigilancia frente a la intrusión, la inundación, el fuego, los escapes de gas, pero también la seguridad personal, etc.
- Comunicaciones: telecontrol y telemetría, acceso a Internet, comunicación interna y compartición de recursos informáticos dentro del hogar.
- Confort: programaciones horarias calefacción, escenarios luminosos, riego automático, etc. Para ello, la Domótica usa multitud de dispositivos que pueden ser distribuidos por toda la vivienda en función de las necesidades de los propietarios. Básicamente, estos dispositivos se pueden dividir en sensores y actuadores con inteligencia suficiente como para implementar "una red de área local" de control distribuido.

Respecto al presente estudio, interesa conocer qué implicaciones pueden existir en el uso del protocolo IPv6 en electrodomésticos de esta categoría.
Por ejemplo, en el caso de que los distintos aparatos o dispositivos de Domótica existentes en una casa tuvieran cada uno de ellos una IP para acceder a la Red, con Identificador Único, aquellos agentes tratantes que tuvieran la posibilidad de acceder a los resultados de dicha navegación o acceso, podrían obtener información tan valiosa como los perfiles de consumo de los titulares de la casa, sus horarios, sus gustos, etc.
Asimismo, esta posibilidad aumentaría si fuera posible que todos los dispositivos o nodos existentes en una casa tuvieran el mismo prefijo en su dirección IP, siendo un identificador constante. Sin embargo, desde el punto de vista de la protección de datos, es importante resaltar que:

- Las actividades de generación de perfiles, de forma inconsentida, es un problema que viene existiendo con las anteriores versiones del Protocolo y que, por lo tanto, no es un problema iniciado por el uso de IPv6.
- No es una actividad sencilla para un único agente tratante, acceder a estas IP´s e incluso agrupar todas aquellas que existan en una casa, para obtener perfiles.
- La obtención de perfiles es lícita si se efectúa dando cumplimiento a las disposiciones contenidas en la Directiva y en las legislaciones de cada Estado Miembro, adoptadas sobre protección de datos.
- No en todos los casos, la dirección IP que para un agente tratante tiene la consideración de dato personal, tiene que serlo para otro agente o prestador de servicios distinto.

En el supuesto de que la dirección IP pueda tener la consideración de dato personal y pensando en aquel caso que, existiendo o no un prefijo único para todos los elementos de la Domótica de un hogar, es posible conocer el usuario de una IP (por ejemplo, mediante guías públicas), los requisitos derivados del tratamiento de datos personales pueden ser diferentes en función del uso o servicio proporcionado por el elemento de la Domótica.

Podemos pensar el caso de un de un equipo terminal con una dirección IP propia y que es utilizado para la prestación de un servicio de teleasistencia sanitaria para todos los miembros de la familia, accesible a través de la identificación individualizada de los mismos mediante un dispositivo biométrico.

De manera simplificada, en la prestación del servicio intervendrían tres partes: el proveedor de las telecomunicaciones necesarias, el proveedor del servicio (que provee también el dispositivo) y los usuarios.

En cuanto al proveedor de telecomunicaciones, los datos que podría asociar a la IP basada en IPv6 del dispositivo domótico serían los necesarios para la gestión, facturación y cobro del tráfico generado en su utilización y, en su caso, aquellos otros datos que hubiera acordado con el titular del dispositivo que podrían ser recabados y tratados.

Respecto a este segundo tipo de datos, el proveedor de telecomunicaciones tendrían que haber informado al usuario sobre qué datos son, con qué fin se recaban, durante cuánto tiempo van a ser tratados, qué otras partes van acceder a los mismos y cómo podrá el usuario ejercitar sus derechos sobre los mismos. A continuación, se deberá obtener el consentimiento del usuario sobre cada uno de los extremos citados. Se podría dar cumplimiento a ambas obligaciones a través de la inclusión de las cláusulas oportunas en el contrato que regule el uso de las telecomunicaciones asociadas al uso del dispositivo de teleasistencia.

El proveedor del servicio y del dispositivo tiene también que dar cumplimiento a las obligaciones de información y consentimiento relativas a los datos personales que se deban tratar en el uso del servicio de teleasistencia. Sin embargo, normalmente, este proveedor va a tener unos requisitos adicionales.

Así, puesto que es muy probable que se efectúe un tratamiento de datos de salud de los miembros de la unidad familiar que hagan uso del servicio de teleasistencia (por ejemplo, toma de tensión o temperatura, comunicación de síntomas, comunicación de medicación, etc.) se

requeriría la obtención de un consentimiento explícito. Este consentimiento deberá obtenerse de cada uno de los miembros de la familia (salvo en el caso de hijos que se encuentren bajo la patria potestad de sus padres), mediante el contrato de teleasistencia o mediante acuerdos o cláusulas diferentes.

Como se ha señalado, uno de los temas jurídicos más repetidamente planteados con relación al uso de la Domótica es el relacionado con la creación de perfiles referidos tanto a una unidad familiar como a los miembros individuales de la misma. Por ejemplo, podemos pensar qué consideraciones jurídicas habría que tener en cuenta en la creación de ambientes personalizados en dormitorios (por ejemplo, máquinas de estado que determinen intensidad de luz, temperatura, control de persianas, programación de la televisión, etc.) y su combinación con hábitos de alimentación asociados al mes del año que corresponda. Además, podemos pensar que estos servicios están asistidos por una empresa externa que gestiona la correcta creación de ambientes, el aprovisionamiento automatizado de alimentos y la lectura de etiquetas de la ropa de los usuarios y de determinados alimentos.

Recordando lo que se ha venido señalando en cuanto a información y consentimiento, podemos centrarnos ahora en la cuestión de la creación de perfiles. Como se ha señalado, la creación de perfiles es lícita si se efectúa conforme a la Directiva 95/46/CE y, lógicamente, conforme a la normativa de cada Estado Miembro sobre datos personales.

No obstante, el usuario dispondrá siempre de sus derechos de acceso, rectificación, cancelación y oposición, reconocidos por la propia Directiva para, por ejemplo, eliminar los datos de su perfil (datos de la persona asociados a la IP basada en IPv6 y a los elementos de la Domótica de su hogar) obtenidos hasta una determinada fecha, evitar que se modifique la temperatura de un dormitorio a partir de la lectura de las etiquetas de su ropa, limitar el reaprovisionamiento automático de ciertos alimentos (por ejemplo, alimentos especiales, alimentos para dietas por tratamiento

médico, alimentos de temporada, etc.), o evitar que la programación de la televisión incluya contenidos no aptos para menores.

Existe otro aspecto importante, relativo al proveedor que está gestionando la creación de ambientes personalizados y el reaprovisionamiento automático de alimentos basado en el mes en curso. Este proveedor, normalmente, va a utilizar los servicios de otras partes para, por ejemplo, generar y entregar un pedido virtual basado en lectura de etiquetas o códigos de barras, fotografía digital de una nevera, etc.

En el caso de que estas terceras partes, para prestar su servicio, tengan acceso a los datos del usuario asociados a su IP, por ejemplo, de su nevera (porque gestionan el reaprovisionamiento de la misma), deberán regular tal circunstancia en el contrato que rija la relación entre el proveedor principal y éste proveedor que ha sido subcontratado por el mismo.

La regulación contractual deberá indicar, al menos, qué datos de IP del usuario basada en IPv6 van a ser tratados para gestionar el servicio, cómo transmitirá el proveedor principal sus órdenes al subcontratado o qué sucederá con los datos (de IP y demás datos personales asociados a la misma) una vez finalice el servicio.

En conclusión, el uso de la Domótica mediante dispositivos basados en IPv6 viene a continuar con los problemas y soluciones jurídicas que suceden con IPv4. No obstante, el desarrollo del nuevo protocolo puede ser un buen momento para plantear y regular los aspectos relativos al tratamiento de datos personales derivado del uso de tales dispositivos basados en IPv6.

g) Medidas de seguridad a implantar en el tratamiento de datos de IP.

Las Directivas de protección de datos obligan a los distintos responsables de los tratamientos a adoptar las medidas técnicas y organizativas necesarias que, además de garantizar la confidencialidad de la información y su correcto tratamiento, aporten, asimismo, seguridad.

En este sentido, no se determina en ninguna de ellas un conjunto aproximativo de medidas de seguridad a tener en cuenta por los Estados Miembros, lo cual, a efectos prácticos, produce que, en ocasiones, los Estados Miembros dispongan de mecanismos jurídicos de desarrollo de esta obligación pero con un contenido distinto entre unas normativas y otras. Respecto a la implantación de medidas de seguridad, únicamente resaltar que el nuevo Protocolo IPv6 dispone de una opción de seguridad específica denominada IPSec, a través de la cual se garantiza, entre otros asuntos:

- La autentificación en el origen de los datos y, por lo tanto, la posibilidad de no recibir comunicaciones provenientes de usuarios con una IP determinada
- La integridad de la información transmitida a partir de este Protocolo.
- La confidencialidad de la misma.

En este sentido, cabe indicar que las consideraciones acerca de este estándar de seguridad IPSec fueron objeto de análisis en el bloque anterior, habida cuenta de las implicaciones que su adopción puede conllevar en la lucha contra la piratería y en la defensa de los derechos de propiedad intelectual, copyrights, etc.

4.8 Perspectiva Europea en materia de IPv6 y el papel de la Task Force.

La Comisión Europea creó en el año 2001, el IPv6 Task Force ("EC IPv6 TF"), con el fin de ayudar al desarrollo del Protocolo IPv6 en Europa, siendo asimismo una de sus principales funciones atender las consultas o polémicas que pudieran surgir sobre IPv6. Incluso, alguno de los miembros del EC IPv6 TF son miembros del Proyecto Euro6IX, dedicados tanto a este organismo como al Proyecto de estudio del impacto de IPv6 en la intimidad.

El CE IPv6 TF entendió que la Opinión 2/2002 mencionada en otras ocasiones del Grupo del Artículo 29 potencialmente podría aportar una visión no equilibrada de los beneficios de IPv6 y, por ello, decidió convocar una reunión en el Grupo dedicado a Internet del Grupo del Artículo 29 para tratar estos

asuntos con más detalle y explicar con más detenimiento los aspectos de IPv6 incidentes en materia de privacidad e intimidad.

Varios de los partners del Proyecto Euro6IX y el IPv6 Task Force formaron parte del grupo que participó en esta reunión celebrada en Bruselas, el 25 de febrero de 2003.

Con anterioridad a la celebración de esta reunión, el EC IPv6 Task Force publicó un escrito donde se trataban los siguientes aspectos:

- El EC IPv6 Task Force reconocía que el uso de identificadores únicos en cualquier tipo de tecnología o medio de comunicación (por ejemplo Ethernet, WLAN, GSM, ID Cards, IPv4 e IPv6) podría suponer un importante riesgo para la privacidad e intimidad.
- Sin embargo, el EC IPv6 Task Force puso de manifiesto que el uso de identificadores estáticos es un hecho importante para cualquier sistema de comunicación existente.
- Cualquier tipo de comunicaciones están sujetas a problemas en materia de respeto a la privacidad e intimidad y, por lo tanto, IPv6 no es ninguna excepción.
- IPv6 dispone de un mecanismo (RFC3041) que podría ayudar a resolver parte de estos problemas, mediante la aportación de un mayor grado de protección a los usuarios con respecto al facilitado por IPv4.
- Adicionalmente, los mecanismos IP Security (IPSec) se encuentran disponibles para IPv6 (RFC2460). Si bien su uso no es obligatorio en la actualidad, introducen grandes mejoras respecto a IPv4, donde actualmente IPSec no se encuentra disponible por defecto.

Las siguientes claves que se aportan deberán ser tenidas en cuenta cuando se analicen las implicaciones existentes en materia de privacidad e intimidad en cualquier sistema de comunicación basado en el protocolo IP, es decir, tanto para IPv4 como para IPv6.

1. También existen problemas en materia de privacidad e intimidad con IPv4 en relación con las direcciones fijas, ya que éstas también podrían ser consideradas como identificadores y ser rastreadas.
2. IPv6, en determinados supuestos, podrá generar direcciones IP que permitirían la correlación de actividades donde un mismo mecanismo se encuentre conectado a diferentes redes gracias a la utilización de un identificador fijo, incluido en la propia dirección IP.
3. El RFC3041 soluciona los problemas de correlación permitiendo a una dirección IPv6, el generar un identificador aleatorio incluido en la propia dirección.
4. Muchos sistemas de Internet utilizan direcciones IP como un sistema de autenticación.

   Sin embargo, el respeto a la privacidad en ocasiones impide que dicha autenticación se lleve a cabo. Sin embargo, IPv6 incluye IPSec por defecto, permitiendo la utilización de sistemas más robustos de autenticación.
5. Los sistemas de extensión de IPv6 permiten que un puesto fijo, por ejemplo, el puesto de trabajo de una oficina, utilice diferentes direcciones IPv6 durante distintos momentos, por ejemplo, una dirección IPv6 distinta diariamente, permitiendo un mayor respeto a la privacidad tanto para los mecanismos no movibles como para los usuarios.
6. En IPv6 es una práctica habitual que los mecanismos que usan este protocolo tengan varias direcciones. En cambio, en IPv4, normalmente sólo existe una dirección. Será por tanto posible, en el futuro, que aplicaciones que utilicen IPv6 usen múltiples direcciones IPv6 dinámicas, lo cual reducirá, por ejemplo, la posibilidad de rastrear acciones en las aplicaciones peer to peer.
7. **Investigaciones posteriores podrán incluso dar paso a la generación de nuevas clases de direcciones IPv6, por ejemplo, las generadas criptográficamente. Esto sólo será posible con IPv6.**
8. El EC IPv6 TF recomendó enérgicamente que todos los proveedores y suministradores implementaran el RFC3041 por defecto en todos sus

sistemas y mecanismos. De hecho, ya puso de manifiesto que alguno de ellos estaba comenzando a hacerlo.

9. En todo caso, deberían definirse sistemas sencillos para activar o desactivar el RFC3041.

Incluso esta posibilidad podría hacerse de forma automática dependiendo del tráfico iniciado, encontrarse preconfigurado por defecto o incluido expresamente por solicitud del usuario. Por supuesto, esta proposición podría requerir de una labor de investigación posterior, pero en todo caso, estas posibilidades solo podrán darse gracias a IPv6".

El EC IPv6 Task Force determinó que "el tema de la privacidad es una pieza importante en el gran ajedrez de la seguridad, transmisión, e-business, legislación aplicable e incluso un buen gobierno. Así que cualquier recomendación formulada entre distintos gobiernos sobre esta materia, sería muy útil ya que pondría de manifiesto un emergente acercamiento interdisciplinario para el futuro".

"El EC IPv6 TF entiende que las nuevas propiedades existentes en IPv6 aportan un conjunto de herramientas para potenciar la privacidad de los usuarios de una forma que no era posible con el anterior IPv4. La combinación de IPSec junto con otras propiedades existentes en IPv6, le convierten en una herramienta muy potente para mejorar las posibilidades de protección de la privacidad de los usuarios.

El EC IPv6 TF recomienda enérgicamente la implementación del RFC3041 por todos los suministradores y proveedores relacionados con IPv6. De todas formas, es importante tener presente que en cualquier medio de comunicación hay que mantener el equilibrio entre el respeto a la privacidad y su uso".

El EC IPv6 TF solicitó al Grupo del Artículo 29 que reconsiderara sus pronunciamientos sobre la materia teniendo en cuenta los importantes avances que IPv6 aporta en comparación con IPv4 en materia de privacidad y respeto a la intimidad. Asimismo, puso de manifiesto que un pronunciamiento de este Grupo del Artículo 29 sobre la materia tendría un impacto relevante para toda la

comunidad interesada en IPv6 que tras leer su Opinión quedaron preocupados por las implicaciones de IPv6 en materia de privacidad.

Tras la publicación del documento analizado en el apartado anterior, el EC IPv6 TF asistió en Bruselas a la reunión mantenida con el Grupo de Internet del Artículo 29. El IPv6 Task Force presentó su estudio e introdujo un breve análisis del RFC3041. Pretendió dejar claro una serie de puntos que deberían ser tenidos en cuenta cuando se estuvieran tratando los aspectos relativos a la privacidad tanto en IPv4 como en IPv6: 1. También existen problemas en materia de privacidad e intimidad con IPv4 en relación con las direcciones fijas, ya que éstas también podrían ser consideradas como identificadores y ser rastreadas. 2. IPv6, en determinados supuestos, podrá generar direcciones IP que permitirían la relacionar actividades, en los casos en los que un mismo mecanismo se encontrara conectado a diferentes redes, gracias a la utilización de un identificador fijo incluido en la propia dirección IP. 3. El RFC3041 podría ser una alternativa de solución a los problemas de correlación permitiendo a una dirección IPv6, generar un identificador aleatorio incluido en la propia dirección. Finalmente fue acordado en la reunión, de forma general, el hecho de que era necesaria la colaboración conjunta entre el EC IPv6 Task Force y el Grupo del Artículo 29 sobre este tema. El Grupo del Artículo 29 manifestó su deseo de entrar en un diálogo con el EC IPv6 Task Force e incluso se ofreció a participar en el Proyecto Euro6IX. En concreto, se ofrecieron a revisar los trabajos que sobre esta materia se iban a desarrollar a lo largo del mencionado Proyecto.

Tabla 102. Consideraciones de la reunión con el Grupo del Artículo 29 en Bruselas.

4.9 Extensiones de privacidad para la configuración automática de direcciones sin estado en IPv6(RFC 3041)

Con referencia a la introducción anteriormente señalada, en relación con los identificadores únicos de las direcciones IP, IPv6 ha permitido por primera vez que los identificadores de interfaz puedan formarse de forma automática en los dispositivos, como una de las maneras existentes para crear direcciones. Por lo tanto, los asuntos relacionados con la privacidad se derivan de que éstos se encuentran de forma permanente en las direcciones, permitiendo la trazabilidad de los sujetos titulares de dichos dispositivos.

En la actualidad existen numerosos tipos de empresas destinadas a realizar estudios de mercado, sirviéndose para ello de variados tipos de técnicas (data-mining) que permiten realizar seguimientos del uso de Internet y, en los casos en las que las direcciones IP no cambien, asociar la navegación y actividades realizadas con los titulares de dichas direcciones. Este hecho es especialmente importante en relación con la proliferación de dispositivos de nueva generación conectados a Internet (por ejemplo, PDAs, teléfonos móviles, etc.) los cuales podrían llegar a ser asociados con sus titulares. En

este sentido, es importante tener en cuenta que con la proliferación de enlaces “always-on” (DSL, cable modems), aumenta la posibilidad de que los usuarios puedan ser sometidos a actividades de data-mining y al seguimiento de sus direcciones fijas.

Thomas Narten y Track Draves publicaron un procedimiento que pretendía tratar este tema y asegurar la privacidad de los usuarios de IPv6 - RFC3041 titulado “Extensiones de privacidad para la autoconfiguración de direcciones sin estado en IPv6” *(“Privacy Extensions for Stateless Address Autoconfiguration in IPv6”)*, el cual fue publicado en enero de 2001 por el IETF. Este procedimiento se basa en la existencia de un algoritmo creado por Narten y Draves, a través del cual se generan identificadores de interfaz aleatorios y direcciones temporales para una sesión de usuario en lo que respecta a comunicaciones salientes. En este sentido, estos identificadores aleatorios sustituyen el identificador único de la dirección, siendo el RFC3041 el medio para estandarizar cómo y cuándo es posible realizar esta actividad.

El principal objetivo de este documento era reducir la preocupación acerca de que IPv6 pudiera significar un peligro para la privacidad, mediante la creación de un identificador aleatorio para las comunicaciones salientes. De este modo, se dificulta la posibilidad de relacionar el nodo con su titular.

El resumen inicial de este documento establece lo siguiente:

“Los nodos utilizan la autoconfiguración de direcciones sin estado para generar direcciones sin la necesidad de utilizar un servidor Dynamic Host Configuration Protocol (DHCP). Estas direcciones son creadas a partir de la combinación de prefijos de red con un identificador de interfaz. En los interfaces que contienen Identificadores IEEE, el identificador de interfaz se deriva de éste. Sin embargo, en otro tipo de interfaces, el identificador de interfaz se genera a través de otros mecanismos, por ejemplo, a través de la generación aleatoria. Este documento hace referencia a la autoconfiguración de direcciones sin estado cuyo identificador de interfaz se deriva de un identificador IEEE. Esta situación implica que los nodos generen direcciones globales a través de identificadores de interfaz que varían, incluso en los

casos en los que el interfaz contenga identificadores IEEE. El cambio del identificador de interfaz (y de la dirección global generada a raíz de éste) dificulta claramente que los rastreadores y cualquier otro tipo de entidad o persona dedicada a recabar información, pueda identificar en qué casos direcciones diferentes usadas en transacciones distintas, se corresponden con el mismo nodo".

La autoconfiguración de direcciones sin estado es un mecanismo que genera direcciones basadas en IPv6 de 128 bits. La parte de la izquierda de la dirección está compuesto por 64 bit y se llama "prefijo" y los 64 bits de la parte derecha constituyen el identificador único o EUI-64 IID.

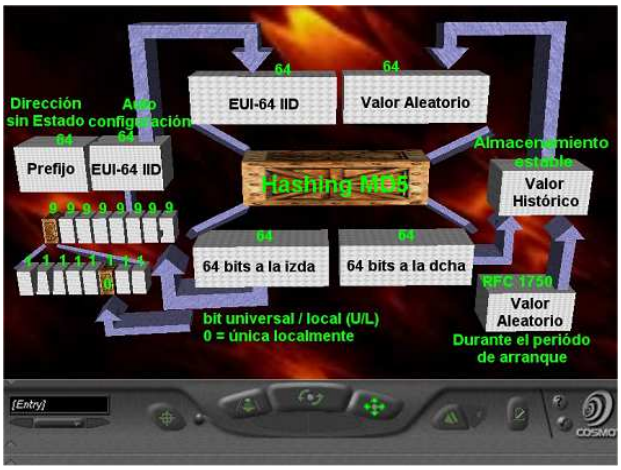


Ilustración 192. Diseño de un Identificador de Interfaz siguiendo el RFC3041.

Tal y como se aprecia en el diagrama superior, un número aleatorio reemplazará al EU1-64IID. El mecanismo vinculará un valor aleatorio de 64 bit al EUI-64 IID y un algoritmo hash tendrá lugar. Este es un algoritmo de un solo sentido por lo que no permitirá reconstruir el número original. Por el contrario, este algoritmo generará aleatoriamente un número de 128 bits. Los 64 bits de la parte izquierda de la dirección forman parte de la autoconfiguración de la dirección dinámica (la cual no estará relacionada con el dispositivo ya que el número ha sido generado aleatoriamente, no estando basado en ningún identificador único) para crear una dirección de IPv6 y el identificador de la

derecha permanece almacenado de forma fija para evitar duplicaciones. Esta dirección será utilizada para comunicaciones salientes.

Por lo tanto, se utilizarán dos direcciones: una dirección "n" generada en base a la dirección única MAC, utilizada para comunicaciones entrantes (el terminal siempre se encontrará localizable a través de esta dirección permanente), y otra dirección generada a través del RFC3041 de una forma aleatoria, la cual será utilizada para comunicaciones salientes. Por lo tanto, cuando el Terminal (y el usuario que se encuentra detrás del terminal) es responsable de la conexión efectuada, éste no podrá ser identificado a través de la dirección MAC.

En todo caso, parece deducirse que si este RFC se implementara de forma general, estaría facilitando en alguna medida una solución alternativa a los problemas en materia de privacidad descritos con anterioridad. Pero si bien la idea de innovación extremadamente valiosa del RFC 3041 es la de ofrecer una alternativa para asegurar la privacidad de los usuarios al problema de vulneración que enfrenta el RFC 2462 con el identificador único en el Internet de próxima generación, se puede plantear concretamente un esquema de extensión mas especializado con las mismas características de confidencialidad, integridad, autenticidad y protección a la replica a partir del algoritmo diseñado por Tomas Narten y Track Draves cual seria el de construir una arquitectura de protección de la privacidad de la información con 2 grados de privilegios o niveles de privacidad que se complementarían perfectamente con la tecnología PKI(*Public Key Infraestructure*) además que encuadraría adecuadamente en la regulación del escenario de la Ley de firma electrónica Nº 19.799 siendo incluso también entre otros factores, recomendada por el Prof. Raúl Arrieta Cortés[201] indicando que "en la actualidad es recomendable recurrir a mecanismos que operan sobre la base de la tecnología PKI" y que permitirían un patrón común mas estándar por razones de interoperabilidad y que también integraría algoritmos criptográficos mas robustos que puedan ser diseñados en un futuro conjuntamente con el protocolo de seguridad

[201] Raúl Arrieta Cortés. <rarrieta@subtel.cl> ,en el marco del Magíster en Derecho Informático y de las telecomunicaciones, realizado por el CEDI de la Universidad de Chile 2006 con el tema "Problemas Jurídicos de la contratación Electrónica".

Ipsec(RFC-2401), considerándose así, los siguientes niveles o modos de solución:

1.- Nivel 1 (o de grado mínimo). El primero consistiría en un algoritmo de acceso seguro y transparente de uso regular(o publico de acceso controlado) a las redes del Internet, realizando así la navegación propiamente por tal, el cual consistiría en reemplazar el algoritmo hash MD5 (RFC 1321, acrónimo de *Message-Digest Algorithm 5*, Algoritmo de Resumen del Mensaje 5, es un algoritmo de reducción criptográfico de 128 bits ampliamente usado)[202] expresando en el RFC 3041, por uno de los 2 siguientes algoritmos de cifrado: RSA[203](Rivest Shamir y Adelman) y Diffie-Hellman[204] los mismos que al contar con las características técnicas de ser en doble sentido podrán reconstituirse con ingeniería inversa el numero original del direccionamiento, cuyo objetivo vinculante seria el de contener una puerta trasera[205]-[206] de tal manera que

---

[202] A pesar de haber sido considerado criptográficamente seguro en un principio, ciertas investigaciones han revelado vulnerabilidades que hacen cuestionable el uso futuro del MD5. En agosto del 2004, Xiaoyun Wang, Dengguo Feng, Xuejia Lai y Hongbo Yu anunciaron el descubrimiento de colisiones de hash para MD5. Su ataque se consumó en una hora de cálculo con un clúster IBM P690.
Aunque dicho ataque era analítico, el tamaño del *hash* (128 bits) es lo suficientemente pequeño como para que resulte vulnerable frente a ataques de 'fuerza bruta' tipo 'cumpleaños' (Ataque de cumpleaños). El proyecto de computación distribuida *MD5CRK* arrancó en marzo del 2004 con el propósito de demostrar que MD5 es inseguro frente a uno de tales ataques, aunque acabó poco después del aviso de la publicación de la vulnerabilidad del equipo de Wang.
Debido al descubrimiento de métodos sencillos para generar colisiones de hash, muchos investigadores recomiendan su sustitución por algoritmos alternativos tales como SHA-1 o RIPEMD-160.

[203] Mediante un programa de cómputo cualquier persona puede obtener un par de números, matemáticamente relacionados, a los que se denominan llaves. Una llave es un número de gran tamaño, que usted puede conceptualizar como un mensaje digital, como un archivo binario, o como una cadena de bits o bytes. Las llaves, públicas y privadas, tienen características matemáticas, su generación se produce siempre en parejas, y se relacionan de tal forma que si dos llaves públicas son diferentes, entonces, las correspondientes llaves privadas son diferentes y viceversa. En otras palabras, si dos sujetos tienen llaves públicas diferentes, entonces sus llaves privadas son diferentes. La idea es que cada individuo genere un par de llaves: pública y privada. El individuo debe de mantener en secreto su llave privada, mientras que la llave pública la puede dar a conocer.

[204] Diffie-Hellman obtiene su nivel de seguridad de la dificultad para calcular logaritmos discretos en un campo finito. El algoritmo Diffie-Hellman puede utilizarse únicamente para el intercambio de claves (permite que dos entidades se pongan de acuerdo en un número, a través de un canal público, sin que dicho número pueda ser conocido por ningún atacante que esté monitorizando la comunicación. Es más, ambas entidades no necesitan compartir ningún secreto, por lo que puede utilizarse para comunicar de forma segura a dos entidades que nunca antes se hayan comunicado. Una vez que esas entidades acuerdan un valor, de forma segura, éste puede ser utilizado, por ejemplo, como clave de cifrado simétrico para intercambiar más información de forma confidencial).

[205] Funciones de un solo sentido, f() es una función de un solo sentido: 1) Dado cualquier y es computacionalmente imposible hallar x tal que f(x)=y.(se traduce en que descifrar resulta imposible…) 2) Existe una función h y una información secreta s tal que conocidos s e y: - es fácil de calcular h(s,y). – f(h(s,y))=y. ..si no se conoce la puerta trasera. La información se denomina puerta trasera. “Tras un criptosistema siempre hay una función de un solo sentido con puerta trasera”. “Criptografía de clave publica o asimétrica”, Escuela Técnica Superior de Ingeniería Informática, Universidad de Sevilla, http://ma1.eii.us.es/Material/RSA.pdf

[206] Fundamentos matemáticos: Las funciones de una sola dirección son aquellas en las obtener el resultado en una dirección es fácil, pero en la otra es casi imposible. Los algoritmos criptográficos de clave publica se basan en funciones de una sola dirección con puerta trasera, que son aquellos en los que el problema es resoluble en la dirección opuesta (la que antes era muy difícil) empleando una ayuda (la puerta trasera). Las funciones de una sola

pueda ser decodificada en situaciones de algún efecto contingente, Ejm: Personas que realicen trafico de información pornográfica, narcotráfico, terrorismo digital etc. relacionados con las configuraciones de delitos informáticos o figuras de delincuencia digital.

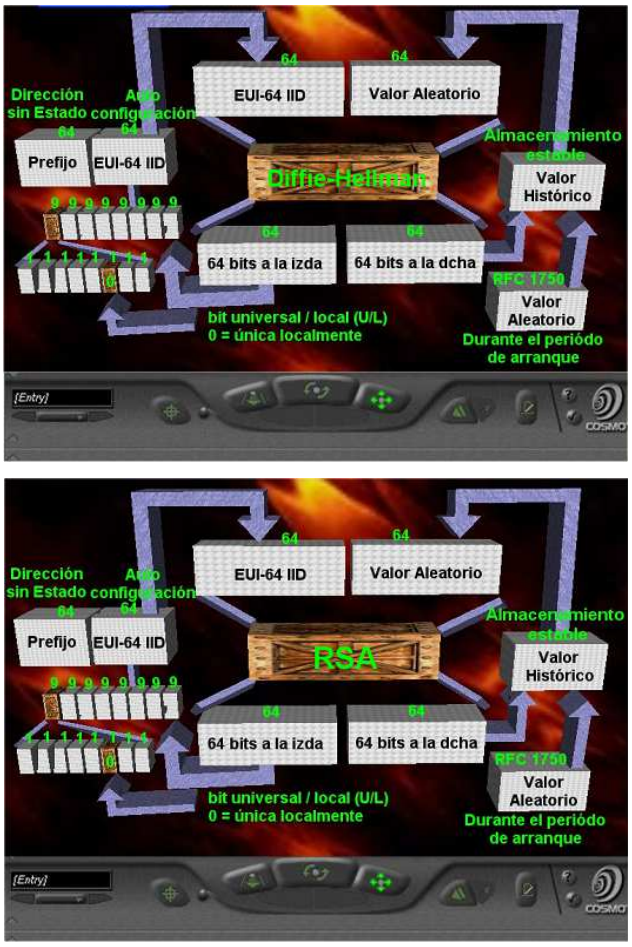


Ilustración 193. Diseño de las extensiones de privacidad para la arquitectura del RFC 3041 por R. Cañihua, modo publico.

2.- Nivel 2 (o de grado robusto). Robusteciendo favorablemente la arquitectura de privacidad del RFC 3041, el segundo consistiría en un algoritmo mas fuerte que el algoritmo hash MD5 (RFC 1321, acrónimo de

---

dirección con puerta trasera son la base de los algoritmos públicos. Sergio Talens-Oliag, stalens@inforcentre.gva.es, "Introducción a la criptografía", http://www.uv.es/~sto/articulos/BEI-2003-04/criptologia.pdf.

Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5, es un algoritmo de reducción criptográfico de 128 bits ampliamente usado)[207] el cual tendría que ser reemplazado por el SHA-2(Secure Hash Algorithm, Algoritmo de Hash Seguro)[208] por la celeridad con que decodificados y se vulnerados en la actualidad los algoritmos criptográficos en materia de criptoanálisis. Como por Ejm, es el caso del matemático Francés Antoine Joux ha descubierto una vulnerabilidad en el algoritmo de firma digital MD5 diseñado originalmente por el matemático Ron Rivest como evolución del MD4, siendo tal vulnerabilidad confirmada por 4 matemáticos Chinos(Xiaoyun Wang, Hongbo Yu /The School of Mathematics and System Science, Shandong University, Dengguo FENA/ Institute of Software, Chinese Academy of Sciences, Xuejia Lai3, /Dept. of Computer Science and Engineering, Shanghai Jiaotong University) con la consecuente y contractual publicacion de su ensayo[209] (http://eprint.iacr.org/2004/199.pdf), entre otros factores de riesgo critico que enfrenta el MD5. Por tal situación se plantea adoptar la solución del SHA-2 aplicado por ejemplo para dispositivos electrónicos que generan desplazamiento (pdas, notebooks, móviles 3g, etc) cualquier rastreador no será capaz de seguir sus movimientos de un lugar a otro o en equipos de organismos que requieran un alto grado de privacidad, entre otros; incluso en

---

[207] A pesar de haber sido considerado criptográficamente seguro en un principio, ciertas investigaciones han revelado vulnerabilidades que hacen cuestionable el uso futuro del MD5. En agosto del 2004, Xiaoyun Wang, Dengguo Feng, Xuejia Lai y Hongbo Yu anunciaron el descubrimiento de colisiones de hash para MD5. Su ataque se consumó en una hora de cálculo con un clúster IBM P690.
Aunque dicho ataque era analítico, el tamaño del *hash* (128 bits) es lo suficientemente pequeño como para que resulte vulnerable frente a ataques de 'fuerza bruta' tipo 'cumpleaños' (Ataque de cumpleaños). El proyecto de computación distribuida *MD5CRK* arrancó en marzo del 2004 con el propósito de demostrar que MD5 es inseguro frente a uno de tales ataques, aunque acabó poco después del aviso de la publicación de la vulnerabilidad del equipo de Wang.
Debido al descubrimiento de métodos sencillos para generar colisiones de hash, muchos investigadores recomiendan su sustitución por algoritmos alternativos tales como SHA-1 o RIPEMD-160.

[208] Referente a la familia SHA (Secure Hash Algorithm, Algoritmo de Hash Seguro) es un sistema e funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el Nacional Institute of Standards and Technology (NIST). El primer miembro de la familia fue publicado en 1993 es oficialmente llamado SHA. Sin embargo, hoy día, o oficialmente se le llama SHA-0 para evitar confusiones con sus sucesores. Dos años más tarde el primer sucesor de SHA fue publicado con el nombre de SHA-1. Existen cuatro variantes más que se han publicado desde entonces cuyas diferencias se basan en un diseño algo modificado y rangos de salida incrementados: SHA-224, SHA-256, SHA-384, y SHA-512 (todos ellos son referidos como SHA-2).

[209] Una aplicación de este algoritmo comúnmente utilizado es para calcular la huella digital única de un determinado conjunto de bytes, el cual es usado para corroborar el hash de un archivo cuando bajamos información del Internet, o para verificar una firma digital con PGP o SSL. Al parecer el "hash collision" o duplicación del hash que puede realizarse en más o menos 1 hora con una PC potente. Por tal situación es de saber que las repercusiones de esto podrían ser interminables ya que dichos algoritmos son ampliamente usados en un montón de programas y los hashes que producen se suponen "únicos".

el supuesto de que las informaciones de las capas superiores de la dirección se encuentren o no codificadas.

Ilustración 194. Diseño de las extensiones de privacidad para la arquitectura del RFC 3041 por R. Cañihua, modo protegido.

De tal manera que esta seria una alternativa de solución, otorgándose así 3 niveles de privacidad, uno de carácter estándar y otros 2 sub-niveles según la categoría requerida; considerados como una evolución especializada propiamente tal del protocolo Ipv6.

Aunque cabria la posibilidad que en un futuro seria conveniente incorporar una variable algorítmica criptográfica constante en una extensión especializada del RFC 3041 como una nueva generación de clases de direcciones Ipv6 generada criptograficamente, que permitiera ofrecer una flexibilidad de cambios mas robusta frente a los avances tecnológicos e innovaciones con los que se presentan el desarrollo de la criptografía o la criptografía cuántica[210], por las entidades como la Agencia de Seguridad Nacional de

[210] Según Fernando Acero, la seguridad de un sistema cuántico, se basa en la imposibilidad de que alguien escuche el mensaje, en este caso la clave de cifrado, sin que ello suponga el aumento de tasa de errores en la determinación de los parámetros cuánticos en un 50% adicional. Si el error es superior al esperado en un 50%, no hay duda, nos están espiando y debemos desechar la clave transmitida.
Lo anterior se basa en tres principios (Criptografía Cuántica M. Baig):
1. Teorema de "no clonación" que nos asegura que un estado cuántico determinado no puede ser copiado. De forma algo alegre, podemos decir que un texto cuántico no puede ser "fotocopiado", ya que no existe la "fotocopiadora" cuántica.
2. Cualquier intento de obtener toda la información cuántica de un qbit puede implicar una cierta modificación del mismo, o destrucción de la información que porta. Por lo que no se puede obtener información sin modificación de los datos transmitidos.

EEUU(NSA)[211] que cuenta con mas de 16.000 especialistas, el laboratorio de Criptografía Aplicada y Seguridad(CASLab[212]) bajo el liderazgo de los profesores Marcos Kiwi, Antonio Diaz y Eduardo Rodríguez que pretenden combinar la experiencia en informática teórica y criptología del Centro de Modelamiento Matemático(CMM), con el conocimiento de soluciones informáticas y de redes del Departamento de Ciencias de la Computación(DCC) entre otros organismos que presentan tales desarrollos en la materia; si, pero esto ya es parte de otra futura investigación que se traducirá en un papers, pero en teoría, ya que las cosas pueden torcerse en la practica, principalmente, por la fragilidad intrínseca del concepto teoría en el campo de estos algoritmos.

4.9.1 Análisis del grado de obligatoriedad del RFC3041

El RFC3041 se encuentra en la "carrera para convertirse en un estándar", estando englobado en la actualidad en la categoría de "propuesta de estándar"(PS), es decir, se encuentra en uno de los tres niveles definidos hasta obtener la categoría de estándar.

Puesto que actualmente este RFC es una propuesta de estándar, se ha llegado a cuestionar su grado de obligatoriedad y su fuerza vinculante.

Sin embargo, es necesario tener en cuenta que en relación con Internet se han hecho importantes desarrollos que se utilizan en el funcionamiento diario de Internet (PPP, POP3, IPv6, FTP y extensiones TCP, etc.) las cuales se encuentran todavía dentro de la categoría "PS",

---

3. Las medidas cuánticas son irreversibles. Después de realizar una medida, el sistema colapsa a uno de los estados propios del operador correspondiente a la magnitud que se ha medido y ese proceso es irreversible, es decir, no se puede volver el sistema manipulado al estado que tenía antes de la medición. Es decir, un espía siempre deja rastro y no lo puede camuflar.

[211] *Nacional Security Agency*(NSA), que es la Agencia de Seguridad Nacional de los EEUU, que cuenta con fondos multimillonarios (presupuesto anual estimado de 13.000 MMUS$ con mas de 16.000 especialistas, con las mejores mentes y talentos en matemáticas y criptografía.).La NSA surgió con el objetivo de proteger en forma secreta la información del gobierno de la EEUU y descifrar la información de los servicios de inteligencia extranjeros. CLCERT-EDD1-001 http://www.clcert.cl/show.php?xml=xml/editoriales/doc_01_01.xml&xsl=xsl/editoriales.xsl Levy Steven, CRYTO.

[212] CASLab es el laboratorio de Criptografía Aplicada y Seguridad www.caslab.cl de hecho ellos redactaron parte del decreto supremo Nº 93 que regulan los SPAM en Chile; estableciendo una seria de normas técnicas para minimizar la recepción de mensajes electrónicos masivos no deseados en las casillas electrónicas, que se dicto en el marco de la Política Nacional de Gobierno electrónico, para mejorar los servicios e información ofrecidos a los ciudadanos, aumentar la eficacia de la gestión publica, e incrementar sustantivamente la transparencias del sector publico y la participación de los ciudadanos.

siendo esto así como consecuencia de que el proceso de aprobación del IETF es bastante lento. Por todo ello, muchos de estos desarrollos pasan a considerarse en la práctica como estándares aunque realmente no tengan esa categoría, como consecuencia de su aceptación generalizada y a obtener "de facto" un status de estándar. En concreto, el RFC3041 ya ha sido implementado en sistemas operativos tan potentes como Microsoft Windows XP/2003[213] y Linux y su fuerza e importancia habla por sí misma. A saber por ejemplo; Juniper Networks cuenta en la actualidad con NetScreen para ScreenOS, que es un sistema operativo de seguridad compatible con Ipv6 que se presenta en la industria con capacidades de cortafuegos extremo a extremo(Incorpora una arquitectura de doble pila que proporciona la flexibilidad necesaria para soportar Ipv4 y/o Ipv6 en un único dispositivo, auto-configuración para Ipv6 y múltiples mecanismos de transición, como NAT/NAT-PT e Ipv6 Están conversiones incluyen "4ª6" y "6ª4" y traducción "4ª6"y "6ª4"), incluso soporte para redes privadas virtuales(VPN), para la demanda mundial de comunicaciones móviles, redes domesticas, juegos online, flujos de video y aplicaciones emergentes.

4.9.2 Implicaciones de su adopción desde la perspectiva de protección de datos.

Si la adopción de esta medida impidiera a ciertos agentes conocer el Identificador Único de una determinada dirección IP, en principio, podría afirmarse que dicha dirección no sería posible asociarla por el agente tratante a un determinado dispositivo y, por lo tanto, a un concreto usuario y, asimismo, tampoco le facultaría para rastrear sus movimientos a lo largo de la Red.

En consecuencia, el dato de dirección IP, para dicho agente tratante, no tendría la consideración de dato personal y, por lo tanto, éste no

[213] A pesar de que Microsoft admite que su cortafuegos no logra bloquear el trafico de Ipv6, las funciones de Internet Connection firewal y Basic Firewall solo están en condiciones de bloquear paquetes de datos Ipv4, por lo que el trafico de Ipv6 puede entrar sin restricciones; por lo cual es necesario para este caso instalar una aplicación especializada de cortafuegos para Ipv6.

quedaría obligado al cumplimiento de las obligaciones impuestas por la normativa de protección de datos personales ya que, en estas circunstancias, dicha información tendría una consideración de dato anónimo o, al menos, disociado.

Estas afirmaciones serán realmente así en el caso de que dicho agente no tuviera medios alternativos para poder identificar el dispositivo al que corresponde dicha dirección IP.

Por otro lado, a pesar de la utilización de esta medida, necesariamente otros agentes deberán seguir conociendo la dirección IP verdadera que contenga el Identificador Único, por lo que para ellos, seguirían existiendo las obligaciones impuestas en esta normativa.

4.9.3 Implantación por los fabricantes de hardware y software.

Siguiendo las recomendaciones efectuadas por el Grupo del Artículo del 29, los fabricantes deberán adoptar las medidas necesarias para la implantación de las medidas técnicas existentes en cada momento, que garanticen la privacidad de los usuarios.

Asimismo, la propia Directiva 2002/58/CE, en su Considerando 46 establece que “puede ser necesario adoptar medidas que exijan a los fabricantes de determinados equipos utilizados en los servicios de comunicaciones electrónicas que fabriquen sus productos de manera que incorporen salvaguardias para garantizar la protección de los datos personales y la intimidad del usuario y del abonado”.

En este sentido, sería recomendable que los fabricantes, tanto de software como de hardware, facilitaran a los usuarios la posibilidad de utilizar este tipo de dispositivos o acceder a la Red obviándolos. De esta manera, deberían informar a través de cláusulas informativas estandarizadas de las posibilidades conferidas por estos mecanismos y las consecuencias de su utilización.

En este sentido, al margen de las posibles dificultades de carácter técnico que pudieran existir para su implementación, cabrían varias posibilidades distintas a adoptar por estos fabricantes:

- Sistema OPT OUT: según este sistema todos los fabricantes, de forma obligada, deberían introducir en los elementos hardware o software que elaboren, dispositivos de esta naturaleza basados en el RFC3041 o en cualquier otro estándar de esta naturaleza. Si el usuario no deseara utilizar este tipo de herramienta, debería solicitar su “desactivación” al fabricante o proveedor correspondiente.
- Sistema OPT IN: por el contrario, esta nueva modalidad supondría que los fabricantes no incluirían de forma generalizada este tipo de herramientas en los elementos hardware o software que generen pero, en cambio, quedarían obligados a dar la opción a los usuarios de los mismos de adquirirlas, informándoles detenidamente del modo de uso y de las consecuencias de su utilización.
- Sistema Intermedio: a través de este sistema, los fabricantes podrán dar la posibilidad a los usuarios adquirientes de sus productos de activar o desactivar la solución técnica, según deseen que su acceso sea anónimo o no.

Esta última opción se presenta, en principio, como la más idónea ya que en determinadas ocasiones será necesario que el usuario acceda a través de una IP reconocible, a los efectos de que el prestador del servicio pueda reconocerle y proveerle aquello que el usuario solicita.

La adopción del tipo de direcciones IP generadas a partir del Identificador Único han suscitado ciertos comentarios basados en el hecho de que, al margen de las implicaciones respecto de la privacidad de los usuarios, éstas contradicen una de las principales características de Internet: su carácter anónimo.

Por este motivo, el desarrollo de medidas técnicas del estilo de las propuestas por el RFC3041 han tenido, en principio, una buena acogida por ciertos sectores. No obstante, se han planteado ciertas dudas sobre su utilización, por ejemplo, el hecho de que estas medidas

podrían llegar a entorpecer investigaciones policiales o judiciales derivadas de la comisión de actividades infractoras o delictivas.

En este sentido, sería conveniente analizar qué agentes tratantes dentro de Internet, por ejemplo, los proveedores de acceso, continuarían teniendo la posibilidad de identificar una determinada dirección IP a partir de su Identificador Único, a pesar de la utilización por el usuario de la medida técnica "protectora de su anonimato". Este punto es especialmente relevante porque convertiría a este tipo de agentes tratantes en el principal medio existente para colaborar con las autoridades pertinentes en la persecución de las actividades delictivas que correspondan.

4.10 Apreciaciones y conclusiones referidas al capitulo cuarto.

- Se realizo un análisis de investigación bibliográfica y contractual de las bases de información obtenidas de la world wide web dentro del contexto de la protección de datos personales, desde una nueva mirada de la construcción del paradigma de los derechos de cuarta[214] o quinta[215] generación en la cotidianeidad postmoderna del Internet respecto al avance de las tecnologías de la información frente a la necesidad conciente de conocer los riesgos y cambios que se avecinan en la sociedad de la información desde la perspectiva de los ordenamientos jurídicos de análisis comparados y con las peculiaridades del carácter innovador en lo que respecta al desarrollo con los que en la actualidad los medios informáticos vulneran la posibilidad de acceso a nuestros datos personales o su captación por ejemplo a través de diferentes factores como las tecnologías de los Cookie's, mecanismos de *IP Spoofing* (falseo de datagramas IP), *IP Hijacking* (interceptación de datagramas IP), *Packet Sniffing* (escucha de datagramas IP), técnicas aplicadas

[214] Drummond, Internet, Privacidad y datos personales, Editorial Reus Madrid-España 2004. pag. 18.

[215] A. Shaarempää, "Europa y la protección de los datos personales", Cinco generaciones de protección de datos en Europa, Revista Chilena de Derecho Informático. ISSN:0717-9162; Nº 3 Diciembre 2003 www.derechoinformatico.uchile.cl

datamining/datawarehouse o el control establecido por los sistemas inteligentes de espionaje telemático como Carnivore, Echelon, AST y OSEMINT.

- Se determino que uno de los principales problemas detectados con respecto a la implantación y el despliegue del protocolo de Internet IPv6 es, el de la posibilidad de rastrear la navegación de las actividades realizadas por el usuario que se encuentra conectado a la red y el de asociar tales resultados de dicho rastreo a un dispositivo electrónico y, potencialmente, a su titular o persona que realizo dichas operaciones por la world wide web. Estas actividades, en principio, no tendrían por qué ser consideradas ilícitas siempre y cuando el tratamiento de los datos se efectúe conforme a lo que se establece en este caso a la legislación vigente investigada. Por lo cual cabe señalar que tenemos que tener la debida importancia del caso respecto a la elaboración de perfiles en Internet de forma inconsentida, por que en futuro seguirá siendo un serio problema, ya que en la actualidad por ejemplo, se vienen realizando tales perfiles con el protocolo de Internet IPv4 que cotidianamente utilizamos y que, por lo tanto, no fue un problema iniciado con el uso de IPv6, por tal situación considere fundamentalmente necesario realizar la investigación de las implicancias en materia de la protección de los datos personales con Ipv6, con el propósito de que los organismos y en general los individuos de la sociedad de la información, seamos frecuentemente consientes de nuestros derechos y obligaciones con el fin de tener una plena confianza de la seguridad de la información que recorren a través de las conexiones de información por cables o satélites con el presente protocolo hacia la búsqueda del equilibrio en el adecuado tratamiento de nuestros datos personales.

- Debemos tomar la debida referencia a la protección jurídica de los datos personales en lo referente al tratamiento automatizado, con lo que respecta a que una dirección IP será un dato personal si es posible asociarla a una determinada persona física, bien de forma directa o indirectamente, consientes de que con IPv6, las direcciones IP con

Identificador Único permiten claramente asociar dicha IP al nodo o dispositivo que la utiliza. Entonces, si es posible que un tercero la asocie a su titular por algún mecanismo, con lo cual tenemos que tener la consideración de un dato personal y que su tratamiento quedará directamente vinculado. Ahora si por terceras partes no tuviera esta posibilidad de asociación a través de ningún medio, para él, esta dirección IP no sería un dato personal.

- Se estableció que la Directiva 95/46/CE es el componente normativo central en materia de protección de datos, a través de la cual se establecen los principios y obligaciones básicos aplicables a los tratamientos de datos personales y que se le puede enfocar desde una óptica tecnológica. Ahora, seria conveniente que sus disposiciones podrían considerarse aplicables directamente a los tratamientos de datos derivados del uso del protocolo IPv6 y, por lo tanto, puesto que las consecuencias derivadas éste no discrepan o contradicen los principios, obligaciones y derechos estipulados en la misma, cabría determinar también que, en principio, no resultaría necesaria la modificación de la citada Directiva. Además seria adecuado tomar importancia en la necesidad de crear, adoptar y potenciar autorregulaciones que permitan la adhesión a códigos de conducta acordes al despliegue que presentara Ipv6.

- En materia de la Directiva 2002/58/CE se considera imperioso pretender modificar y regularizar las necesidades específicas en materia de la protección de datos respecto de los nuevos servicios de comunicaciones electrónicas, considerando al dato de dirección IP como dato de tráfico(cualquier tratamiento de estos datos distinto del necesario para la conducción de las comunicaciones, la facturación o como prueba de una transacción comercial, como regla general, requerirá la obtención del consentimiento del titular), permitiendo a los usuarios que originan llamadas, solicitar la restricción de la identificación de la línea de origen así como, a los usuarios que las reciben, impedir aquellas que provengan de

líneas con identificador restringido. Por analogía, esta práctica podría ser aplicable a IPv6 ya que actualmente se lleva a cabo a través de soluciones técnicas basadas en el estándar RFC3041, como es el caso especifico de la propuesta de extensión planteada en la presente tesis con los 2 modelos de diseño, por lo que la dirección IP puede ser considerada como un dato de localización geográfica de un determinado equipo electrónico, pudiendo así, existir la posibilidad de identificar al usuario titular del sus datos.

- Si la adopción del RFC3041 con las extensiones planteadas, impidieran a ciertos agentes conocer el Identificador Único de una determinada dirección IP y asociarla al dispositivo y al titular, el dato de dirección IP, para dicho agente tratante, no tendría la consideración de dato de carácter personal y, por lo tanto, éste no quedaría obligado al cumplimiento de las obligaciones impuestas por la normativa de protección de datos personales. Sería recomendable que los fabricantes, tanto de software como de hardware, facilitaran a los usuarios la posibilidad de utilizar dispositivos basados en este estándar o acceder a la red obviándolos, informándoles, a través de cláusulas informativas estandarizadas, de las posibilidades conferidas por estos mecanismos y las consecuencias que se pueden realizar por su ocupación.

CONCLUSIONES FINALES

I. Partiendo por el punto de que todos los avances tecnológicos de los científicos en materia de programación factibles no siempre serán jurídicamente aceptables, se realizo un consecuente análisis de las implicancias que traen las sofisticadas tecnologías de información referidas estas, al protocolo de Internet Ipv6, determinando así, su estructura de sus mecanismos de funcionamiento efectivos e interpretación de su modelo de arquitectura técnica en tiempo en que se vienen implantando, llegando así a definir de raíz desde la óptica técnica de discernimiento simplista y el análisis circunscrito de las directivas internacionales, las condiciones de legalidad en materia de protección de datos personales y de la privacidad frente a la trazabilidad de datos en el world wide web atingente a los riesgos y la velocidad del cambio tecnológico que se presentan en las nuevas redes de telecomunicaciones con la **entrega de una solución concreta a los problemas de los "identificadores únicos" descritos en la RFC 2462 cual es, la modificación especializada de la RFC 3041 con el diseño de 2 nuevas arquitecturas uno de modo publico y el otro de carácter robusto** en una medida de adopción tecnológica, dentro del contexto de los mecanismos de control no jurídicos.

II. Se explico estrechamente a través de un concordante estudio de investigación las influencias sobre cual giran, los fenómenos(de la obtención legal y legítima de los datos personales, el uso de los datos únicamente para las finalidades de tratamiento identificadas, los datos adecuados, pertinentes y no excesivos, los datos actualizados reales y exactos, los datos accesibles para su titular, el mantenimiento de los datos en condiciones seguras, los datos borrados o cancelados una vez que dejen de ser necesarios) y los limites de la informática para que sean aplicadas y traducidas en un futuro cercano, a un panorama de

regulación potencialmente eficaz, genuino, flexible, con previsiones de evitar "parches o vacíos legislativos" y con capacidad de adaptarse convergentemente a un cuerpo legal robusto que permita ofrecer garantías al resguardo de nuestros derechos, acorde con nuestros tiempos, en medida que se vienen creando las nuevas formas de comunicación, no solo en beneficio de la propia individualidad del ser humano, sino de la existencia misma de la convivencia en la sociedad contemporánea en pos del correcto uso en el equilibrio del empleo de las tecnologías de información y el adecuado resguardo de los bienes jurídicos reactivos que nos son protegidos por ley , especialmente en lo que dice relación con información protegida y el nuevo que hacer contractual que la informática depara con el protocolo Ipv6 que se sigue imponiendo. Determinando así también que es **viable construir e implantar una legislación especializada acorde que se puedan incorporar en los** encuadramientos normativos de la Ley Nº 19.628, con su resguardo legal detectándose efectivamente que:

"Si existe la posibilidad de que terceros realicen un rastreo, y el mismo sea potencialmente asociado a una conexión de un dispositivo electrónico en la navegación de una persona física esta dirección IP entonces seria un dato personal; ahora en caso contrario no existiera ninguna posibilidad informática de asociación de datos tanto indirecta o directamente a una persona por parte de un identificador, la dirección IP no seria un dato personal".

III. Frente al hecho indispensable que en estos tiempos la sociedad tecnológicamente avanzada representa una serie amenaza a la vida privada se requiere no solo de un **sistema legal de protección a la vida privada en particular con el uso indebido de las nuevas tecnologías de información, si no también se considera que es necesario el uso de medidas tecnológicas** de avanzada que sean diseñadas respetando las exigencias de nuestros códigos deontológicos de ética y buenas practicas y nos otorguen garantías previsibles en cuanto al resguardo tecnológico que satisfagan con los estándares normativos vigentes, tomando como importancia la necesidad de crear y potenciar las autorregulaciones que otorguen la adhesión a códigos de conducta con respecto

al protocolo IPv6, en pos del correcto equilibrio tecnológico azumados análisis de los principios doctrinarios sustentados establecidos por el derecho comparado, frente al tratamiento de nuestros datos personales, aplicados al empleo de las nuevas clases de herramientas criptográficas con el uso del protocolo IPv6 de manera que permitan en forma efectiva velar por la seguridad jurídica de la vida privada tomando debida importancia frente a las huellas sensibles dejadas en el world wide web de forma inconsentida o ilícita; como viene ocurriendo en la actualidad para el caso de los IPs de carácter estáticos.

IV. Sabiendo que en el ámbito de la seguridad de los sistemas por de facto la informática y el derecho se entrecruzan con frecuencia se determino la consistencia y el equilibrio de que, la actual implantación del protocolo IPv6 va a suponer sin duda mejoras significativas en términos de seguridad en la innovación de las telecomunicaciones a través de Internet con la denominada Ipsec que garantiza el trafico de datos con protocolo seguro respecto a la autentificación en el origen de los datos, la integridad de la información transmitida y la confidencialidad, pero si bien ello trasunta, no podemos decir que IPv6 se encuentra maduro por completo respecto a las implicancias legales que derivara en toda su dimensión. Por ello se determino que es **potencialmente factible diseñar e implementar en la actualidad herramientas de protección de la privacidad** más robustas que permitan proteger nuestra información que transita a través de las redes del Internet de manera que conceda el resguardo y la protección de los datos personales inherentes al individuo.

TRABAJOS FUTUROS

Se considera que es imperioso realizar futuras investigaciones respecto al impacto que conllevara el despliegue del protocolo de próxima generación IPv6, como así mismo de sus modificaciones regentadas en los estándares internacionales de las RFC’s, dentro del contexto de la privacidad y la protección de datos personales

para tener un panorama claro de las implicaciones legislativas que podrían presentarse dentro del ámbito de aplicación jurídica; modificaciones como por ejemplo, el caso que se presento contractualmente sobre el Bosquejo del RFC3041- *Considered Harmful* "draft-dupont-ipv6-rfc3041harmful-04.txt"[216] realizado por el Francés Francis Dupont <francis.dupont@enst-bretagne.fr> y el Finlandes Pekka Savola <psavola@funet.fi> " propuesta que intenta, cambiar el tiempo dinámico el identificador de interfaz en las extensiones de privacidad para que las direcciones de autoconfiguración sin estado sean mas difíciles de penetrar por terceros, "espías" u otros "colectores de información" no logren identificarnos, cuando diversas direcciones usadas en diversas transacciones correspondan a un mismo nodo, estudio que plantearon como un avance tecnológico[217] mas a las nuevas generaciones de clases de direcciones Ipv6 que se vienen diseñando. Y así estar plenamente concientes de los cambios que se avecinan para determinar ámbitos de protección técnicos que se traducirán en consecuentes derivaciones de regulación legal que nos permitan resguardar nuestra vida privada en la era digital.

[216] La lista de los bosquejos actuales del Internet se pueden encontrar en www.ietf.org/ietf/1id-abstracts.txt
La lista de los directorios de los bosquejos del Internet se pueden encontrar en www.ietf.org/shadow.html

[217] Según los expertos de Laboratorios Bell de Lucent Technologies, para el 2025, el mundo entero estará envuelto en una piel de comunicaciones. "Ya estamos construyendo la primera capa de una mega-red que abarcará todo el planeta a modo de piel", dice Arun Netravali, presidente de Laboratorios Bell. "A medida que las comunicaciones se hacen más rápidas, pequeñas, baratas e inteligentes, en el próximo milenio, esta piel, alimentada por un flujo constante de información, crecerá y se hará más útil". Dicha piel estará formada por millones de dispositivos electrónicos de medición (termostatos, manómetros, detectores de contaminación, cámaras, micrófonos), que controlarán las ciudades, las carreteras y el entorno. Todos ellos transmitirán datos directamente a la red, igual que nuestra piel transmite un flujo constante de datos sensoriales a nuestros cerebros", dice Netravali. Estos sistemas se pueden utilizar para muchas cosas, entre ellas, para hacer un seguimiento constante del tráfico de una carretera local, del nivel de agua de un río, de la temperatura de una playa o de la cantidad de alimentos de una nevera. Estos sensores serán una sola fuente de una cantidad en aumento de comunicación máquina a máquina y objeto a objeto en el futuro. De hecho, para el 2010, Netravali predice que el volumen de esta comunicación entre máquinas en la red llegará a superar la comunicación entre humanos. "En casa, su lavavajillas podrá llamar directamente a su fabricante cuando detecte un mal funcionamiento y el fabricante emitirá un diagnóstico remoto", explica. "O su sistema de riego podrá consultar la página Web del Instituto Nacional de Meteorología antes de ponerse en funcionamiento, para asegurarse de que parte no indica lluvia". Los expertos de Laboratorios Bell predicen también que a medida que se desarrolle el milenio, los avances en las comunicaciones harán mucho por esperar al teléfono que, navegar por Internet y viajar por negocios resulte tan anticuado como utilizar papel de carbón hoy en día.
Dr. George Kocur**, tema 20 "Fundamentos de las Telecomunicaciones", Curso de** Tecnología de bases de datos Cod. ESD.264J, Internet e integración de sistemas, Área Ingeniería de Sistemas**, MIT.**

BIBLIOGRAFÍA

- Miguel Ángel Davara Rodrigues, Guía Práctica de Protección de Datos, Universidad Pontificia Comillas Madrid-España 1999.
- Miquel Peguera Poch, Albert Agustinoy Guilayn, Ramon Casas Valles, Agusti Cerrillo i Martinez, Ana M. Delgado Garcia, Jordi Herrera Joancomarti, Mark Jeffery, Oscar Morales Garcia, Rafael Oliver Cuello, Guillermo Ormanzabal Sanchez, Monica Vilasau Solana y Raquel Xalabarder Plantada “Derecho y nuevas tecnologías”, Editorial UOC 2005.
- Luis Angel Ballesteros Moffa, La privacidad electrónica, Editorial Tirant lo Blanch Valencia-España 2005.
- Maria de los reyes Corripio Gil-Delgado Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet, IV edición Agencia de Protección de datos Madrid.
- Victor Drummond, Internet, Privacidad y datos personales, Editorial Reus Madrid-España 2004.
- Dr. Caetan Vas, El derecho a la intimidad, Editorial Universidad S.R. Argentina.
- Cristina Almuzara Estudio práctico sobre la protección de datos de carácter personal, Editorial Lex nova 2005.

- Pablo A. Palazzi, La protección de los datos personales en la Argentina, Edicion Errepar 2004.
- Emilio Guichot, Datos personales y Administración Publica, Editorial Aranzadi 2005 España.
- Maria de los Reyes Corripio Gil-Delgado, El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones, V edición Agencia de Protección de datos Madrid.
- Informática y derecho 6-7, La protección de datos personales, Edita Universidad Nacional de Educación a Distancia Centro regional de Extremadura-Mérida 1994.
- Comision Europea, ConsulIntel, Ecija, Jordi Palet Martínez, Basar Kaisor(U. de Oxford), Francisco Javier Carballo Varques(U. de Cantabria), Alvaro Ecija Bernal(U. Autonoma de Madrid), Jennifer Gil Krokun(U. Complutense de Madrid), Antonio F. Gomez(U. de Murcia), Alberto Saiz Peña(U. de Alcala) y David G Mills(U. de Southampton) "IPv6: Aspectos Legales del Nuevo Protocolo de Internet".
- Jaime Witker, La investigación Jurídica, McGraw-Hill, México 1995.
- Manuel Castell, La galaxia Internet, Barcelona, edición Arete, 2001
- Miguel Angel Davara, Manual de derecho Informático, Aranzadi Editorial Pamplona 1997.
- Pablo Garcia Mexia, Principios de derecho en Internet, Valencia 2002.
- Antonio Lucas Marin, La nueva sociedad de la Información, una perspectiva desde Silicon Valley. Editorial trotta, Madrid 2000.
- Julio tellez. Derecho Informatico. McGraw Hill. Mexico, 1996.
- Antonio Ruiz carrillo. Los datos de carácter personal, Editorial Bosh, Madrid, 1999.
- Antonio Orti Vallejo. Derecho a la intimidad e informática, Editorial Comares, España, 1994.
- Kwanbok Jo "IPv6 Strategy and Deployment Status in Korea" MIC, Ipv6 Promotion Policies 2006.
- Hugo Adrián Francisconi, "IPsec en Ambiente IPv4 e IPv6" Edición Carril Godoy Ver 1.0, Mendoza - Argentina 2005.

- Roque Gagliano Molla, Pablo Allietti “Presencia de IPv6 en ccTLDs de América Latina” - 2006.
- Eriko Porto “Plan de Ingenieria para el NEG” Cooperación Latino Americana de Redes Avanzadas.
- Ásael Fernandez Alcantara, Experiencia de CUDI con IPv6 / Situación Actual de IPv6 en la Red Clara – 2005 en el “Seminario sobre Ipv6 y Políticas Publicas, Caracas- Venezuela” .
- Ásael Fernandez Alcantara, “Desarrollo de Proyectos con Soporte IPv6” Segundo Foro Latinoamericano de IPv6(FLIP-6), San José-Costa Rica 2004
- Luis Peralta, Universitat Jaume I “IPv6 @ UJI” – 2005.
- Jordi Palet, “IPv6 Deployment Status in Europe and the IPv6 Task Forces”, Ipv6 Forum, Education & Promotion WG Co-chair.
- Christian Lazo R. “Estado del Avance de Redes Ipv6 en Chile” FLIP-6 Montevideo 2004.
- Eva M. Castro, Jesús Gonzales, Gregorio Robles y Tomas de Miguel “Interoperabilidad de aplicaciones IPv4 e Ipv6”; Universidad Rey Juan Carlos de Madrid, Departamento de Informática, estadística y Telemática y la Universidad Politécnica de Madrid, Departamento de Ingeniería y Sistemas Telemáticos.

ORGANISMOS Y ESTANDARES

- Organización internacional para la estandarización www.iso.org
- Organización internacional para la normalización www.ietf.org
- Organización Mundial del Comercio OMC www.wto.org
- Unión Internacional de Telecomunicaciones UIT www.itu.int
- IEEE Asociación profesional mundial de la estandarización www.ieee.org
- Internet Corporation for Assigned Names and Numbers www.icann.org
- Comisión Interamericana de Telecomunicaciones CITEL www.citel.oas.org
- Agencia Española de Protección de datos www.agpd.es
- Asociación de usuarios de Internet www.aui.es
- IPv6 INternet IniTiative 6INIT www.6init.org

- Large-Scale Internacional IPv6 Pilot Network 6NET www.6net.org
- IPv6, QoS & Power Line Integration 6POWER www.6power.org
- IPv6 QoS Measurement 6QM www.6qm.org
- Management of End-to-end Quality of Service Across the Internet at Large MESCAL www.ist-mescal.org
- EU Ipv6 Task Force www.eu.ipv6tf.org
- Ipv6 Forum www.ipv6forum.org
- INTER-domain quality of service MONitoring INTERMON www.ist-intermon.org
- Next Generation Networks Initiative NGNI www.ngni.org
- TORRENT www.torrent-innovations.org
- European IPv6 Internet Exchanges Backbone Euro6IX www.euro6ix.org

TESIS DE GRADO

- Alberto Cerda Silva; La Autoridad de Control en la legislación sobre protección frente al tratamiento de datos personales, Universidad de Chile / Facultad de Derecho – Santiago, Chile 2003.
- Daniel Álvarez Valenzuela; Libertad de Expresión en Internet y el control de Contenidos Ilícitos y Nocivos, Universidad de Chile / Facultad de Derecho – Santiago, Chile 2004.
- Washington Alejandro Jaña Tapia; Análisis Legal Comparativo de la Protección de Datos Personales A Nivel Latinoamérica, Universidad de Chile / Facultad de Derecho – Santiago, Chile 2003.
- Rodrigo Alberto Álvarez Ahumada; Análisis del régimen jurídico de protección de datos de carácter personal, Universidad de Chile / Facultad de Derecho – Santiago, Chile 2002.
- Jessica Mattus Arenas y Alejandro Montecinos Garcia; El deber de Información y el consentimiento para la transmisión de los datos personales, Universidad de Chile / Facultad de Derecho – Santiago, Chile 2004.

- Darwin Lamarck Santana Yunes, “IPv6: Nueva Generación Protocolo de Internet” Universidad Nacional Pedro Henriquez Ureña / Facultad de Ciencia y Tecnología, Santo Domingo – 2004.
- Francisco Javier Valdez Barrera; Protocolo de Internet Ipv6: Desarrollo de un laboratorio de pruebas, Universidad de Chile / Departamento de Ciencias de la Computación – Santiago, Chile 1999.
- Pablo Andres Garrido Moreno; Implementación de un nodo de una red óptica y análisis de la calidad de servicio, Universidad de Chile / Departamento de Ingeniería Eléctrica – Santiago, Chile 2003.
- Heinz Waldemar Herlitz Gatica; Transversabilidad en NAT/FIREWALL, Universidad Católica de Temuco / Facultad de Ciencias, Chile 2005.
- Pedro M. Ruiz, Curso de Doctorado “Introducción y estado del arte en redes ad hoc” Universidad de Murcia, departamento de Ingeniería de la información y las comunicaciones - 2003.
- Rafael Moreno Vozmediano, Curso de redes de computadores “Interfaz de programación de sockets” Universidad Complutense de Madrid, Ingeniería electrónica.

TESIS DOCTORALES

- Marcelo Bagnulo Braun; “Herramientas para la Conectividad IPv6 con Multiples Proveedores” Universidad Carlos III de Madrid / Departamento de Ingeniería Telemática, España 2005.
- Alberto Escudero Pascual, “Privacy in the next generation Internet” Data protection in the context of European Union policy, Royal Institute of Technology - Telecommunication Systems Laboratory / Department of Microelectronics and Information Technology – 2002.
- Eva M. Castro “Contribución al estudio y definición de una metodología de transición gradual de IPv4 a IPv6” Universidad Politécnica de Madrid.

GLOSARIO

GLOSARIO OFICIAL DEL ESTANDAR DE LA RFC 791 (http://www.rfc-es.org/rfc/rfc0791-es.txt)

1822: BBN Report 1822, "Especificación de la Interconexión de un Host y un IMP". La especificación de la interfaz entre un host y ARPANET.
ARPANET leader: La información de control en un mensaje ARPANET en la interfaz host-IMP.
mensaje ARPANET: La unidad de transmisión entre un host y un IMP en ARPANET. El tamaño máximo es aproximadamente 1012 octetos (8096 bits).
paquete ARPANET: Una unidad de transmisión usada internamente entre IMPs en ARPANET. El tamaño máximo es aprox. 126 octetos (1008 bits).
Destino: La dirección de destino, un campo de la cabecera internet.
DF: El bit 'Don't Fragment' (No Fragmentar) del campo de indicadores.
Indicadores (Flags): Un campo de la cabecera internet con varios indicadores de control.
Posición del Fragmento: Posición del fragmento. Este campo de la cabecera internet indica a que lugar del datagrama internet pertenece un fragmento.
GGP: Gateway to Gateway Protocol (Protocolo Pasarela a Pasarela), el protocolo usado principalmente entre pasarelas para controlar el encaminamiento y otras funciones de pasarela.
Cabecera: Información de control al principio de un mensaje, segmento, datagrama, paquete de datos.
ICMP: Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet), implementado en el módulo internet, el ICMP es usado de pasarelas a hosts y entre hosts para informar de errores y hacer sugerencias de encaminamiento.
Identificación: Un campo de la cabecera internet que almacena el valor identificador asignado por el remitente como ayuda para ensamblar los fragmentos de un datagrama.
IHL: El campo de la cabecera internet 'Internet Header Length'(Longitud de la cabecera internet) es la longitud de la cabecera internet medida en palabras de 32 bits.
IMP: Interface Message Processor (Procesador de Mensajes de Interfaz), el intercambiador de paquetes de ARPANET.
Dirección Internet: Una dirección de origen o destino de 4 octetos (32 bits) formada por un campo de Red y un campo de Dirección Local.
Datagrama internet: La unidad de datos intercambiada entre un par de módulos (incluye la cabecera).
Fragmento internet: Una parte de los datos de un datagrama internet con una cabecera internet.
Dirección Local: La dirección de un host en una red. La relación real entre una dirección local internet con las direcciones de un host en una red es muy general, permitiéndose relaciones de muchos a uno.
MF: El indicador 'More-Fragments' (Más Fragmentos) presente en el campo indicadores de la cabecera internet.
Segmento TCP: La unidad de datos intercambiada entre dos módulos TCP(incluyendo la cabecera TCP).
TFTP: Trivial File Transfer Protocol (Protocolo de Transferencia de Archivos Trivial): Un sencillo protocolo de transferencia de archivos construido sobre UDP).
UDP: User Datagram Protocol (Protocolo de Datagrama de Usuario): Un protocolo a nivel de usuario para aplicaciones orientadas a transacciones.
Usuario: El usuario del protocolo internet. Este puede ser un módulo de protocolo de nivel superior, una aplicación, o un programa pasarela.
Versión: El campo Versión indica el formato de una cabecera internet.

ANEXO

Network Working Group S. Deering

Request for Comments: 2460

Obsoletos: 1883 R. Hinden
Categoría: Track de Estándares
Nokia

Diciembre 1998

Especificación
Protocolo Internet, Versión 6 (IPv6)

Estatus de este Memorándum

Este documento especifica un protocolo del track de estándares Internet para la comunidad Internet, y solicita debate y sugerencias para mejorías. Por favor remítase a la edición actual de los "Estándares de Protocolos Oficiales Internet" (STD 1) para el estado de estandarización y estatus de este protocolo. La distribución de este memorándum es ilimitada.

Aviso de Copyright

Resumen

Este documento especifica la versión 6 del Protocolo Internet (IPv6), algunas veces también referido como IP Siguiente Generación o IPng.

Lista de Contenidos

1. Introducción

El IP versión 6 (IPv6) es la nueva versión del Protocolo Internet, diseñado como el sucesor para el IP versión 4 (IPv4) [RFC-791]. Los cambios del IPv4 al IPv6 recaen principalmente en las siguientes categorías:

- Capacidades de Direccionamiento Extendida

  El IPv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico, un número mucho mayor de nodos direccionables, y una autoconfiguración más simple de direcciones. La escalabilidad del enrutamiento multienvío se mejora agregando un campo "ámbito" a las direcciones multienvío. Y se define un nuevo tipo de dirección llamada "dirección envío a uno de", usado para enviar un paquete a cualquiera de un grupo de nodos.

- Simplificación del Formato de Cabecera

Algunos campos de la cabecera IPv4 se han sacado o se han hecho opcional, para reducir el costo del caso común de proceso de tratamiento de paquete y para limitar el costo del ancho de banda, de la cabecera IPv6.

- Soporte Mejorado para las Extensiones y Opciones

  Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.

- Capacidad de Etiquetado de Flujo

  Una nueva capacidad se agrega para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares para lo cuál el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".

- Capacidades de Autenticación y Privacidad

  Extensiones para utilizar autenticación, integridad de los datos, y (opcional) confidencialidad de los datos, se especifican para el IPv6.

Este documento especifica la cabecera IPv6 básica y las cabeceras de extensión IPv6 y las opciones inicialmente definidas. Aborda también cuestiones de tamaño del paquete, las semánticas de las etiquetas de flujo y las clases de tráfico, y los efectos del IPv6 en protocolos de capa superior. Los formatos y semánticas de las direcciones IPv6 son especificadas separadamente en [ADDRARCH]. La versión IPv6 del ICMP, que a todas las implementaciones IPv6 se exige incluir, es especificada en [ICMPv6].

2. Terminología

nodo	- un dispositivo que implementa el IPv6.
enrutador	- un nodo que reenvía paquetes IPv6 no explícitamente destinados hacia sí mismo. [Ver Nota abajo].
host	- cualquier nodo que no es un enrutador. [Ver Nota abajo].
capa superior	- una capa de protocolo inmediatamente encima del IPv6. Ejemplos son los protocolos transporte tal como el TCP y el UDP, protocolos control tal como el ICMP, protocolos enrutamiento tal como el OSPF, y protocolos internet o de capa inferior que están siendo "tunelizados" sobre (es decir, encapsulados dentro) IPv6 tal como el IPX, el AppleTalk, o el mismo IPv6.
enlace	- una facilidad de comunicación o medio sobre el cual

los nodos pueden comunicarse en la capa de enlace,
es decir, la capa inmediatamente debajo del IPv6.
Ejemplos son las Ethernets (simples o de puentes);
enlaces PPP; X.25, Frame Relay, o redes ATM;
y "túneles" de capa internet (o superior), tal como
los túneles sobre IPv4 o sobre el mismo IPv6.

vecinos - nodos conectados al mismo enlace.

interface - lo que acopla un nodo a un enlace.

dirección - un identificador de capa IPv6 para una interface o
un conjunto de interfaces.

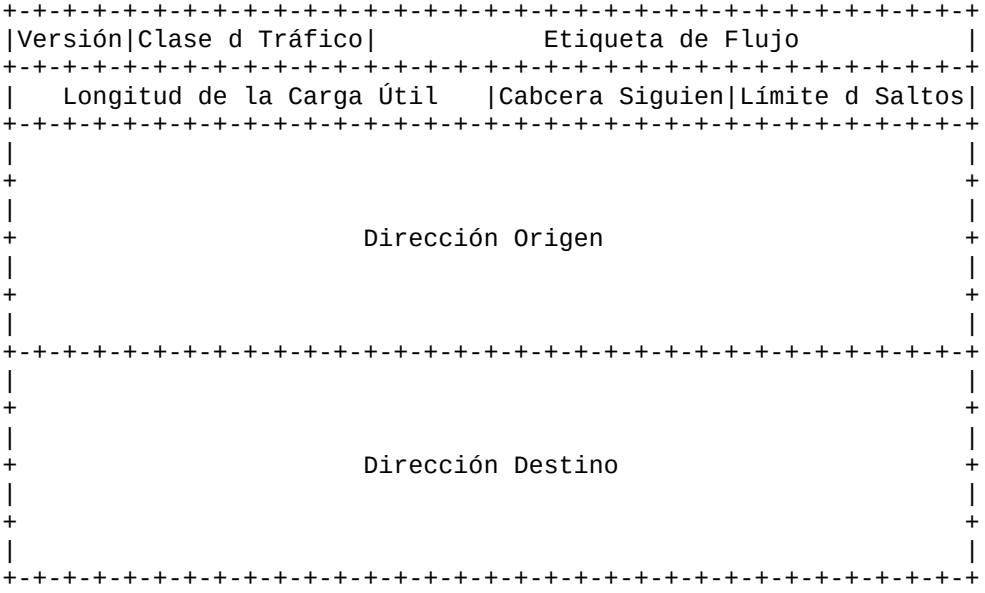
paquete - una cabecera IPv6 más carga útil.

MTU de enlace - la unidad de transmisión máxima, es decir, el tamaño del paquete máximo en octetos, que puede transportarse sobre un enlace.

MTU de ruta - la MTU de enlace mínima de todos los enlaces dentro de una ruta entre un nodo origen y un nodo destino.

Nota: es posible, aunque inusual, para un dispositivo con interfaces múltiples ser configurado para reenviar paquetes no autodestinados que llegan desde algún conjunto (menos que todas) de sus interfaces, y para descartar paquetes no autodestinados que llegan desde sus otras interfaces. Un dispositivo semejante debe cumplir con los requisitos de protocolo para enrutadores al recibir paquetes de, e interactuar con vecinos sobre, las interfaces anteriores (reenviantes). Debe cumplir con los requisitos de protocolo para hosts la recibir paquetes de, e interactuar con vecinos sobre, las interfaces posteriores (no reenviantes).

3. Formato de la Cabecera IPv6

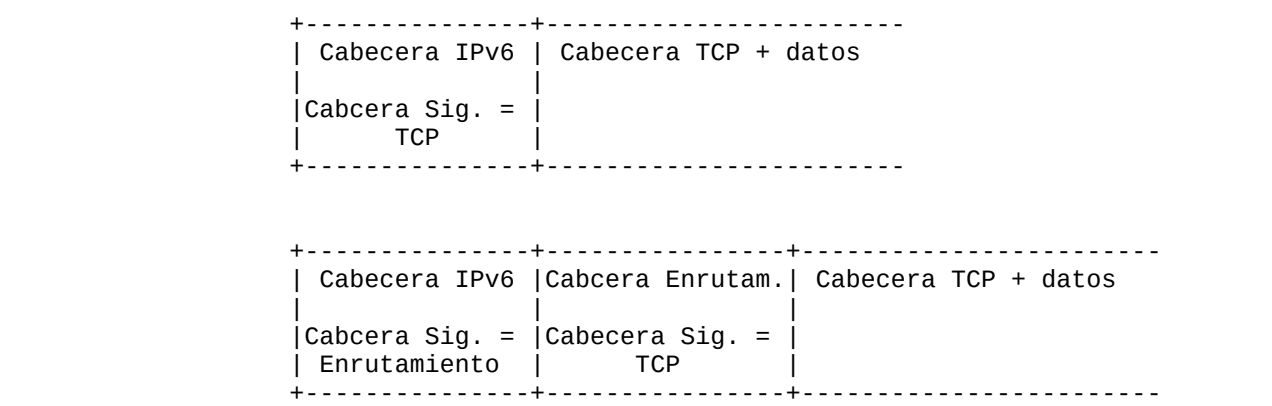


Versión	Número = 6 de versión del Protocolo Internet de 4 bits.
Clase de Tráfico	Campo clase de tráfico de 8 bits. Ver la sección 7.
Etiqueta de Flujo	Etiqueta de flujo de 20 bits. Ver la sección 6.

Longitud de la Carga Útil	Entero sin signo de 16 bits. Longitud de la carga útil IPv6, es decir, el resto del paquete que sigue a esta cabecera IPv6, en octetos. (Notar que cualesquiera de las cabeceras de extensión [sección 4] presente es considerada parte de la carga útil, es decir, incluida en el conteo de la longitud).
Cabecera Siguiente	Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC-1700 et seq.].
Límite de Saltos	Entero sin signo de 8 bits. Decrementado en 1 por cada nodo que reenvía el paquete. Se descarta el paquete si el Límite de Saltos es decrementado hasta cero.
Dirección Origen	Dirección de 128 bits del originador del paquete. Ver la [ADDRARCH].
Dirección Destino	Dirección de 128 bits del recipiente pretendido del paquete (posiblemente no el último recipiente, si está presente una cabecera Enrutamiento). Ver la [ADDRARCH] y la sección 4.4.

4. Cabeceras de Extensión IPv6

En el IPv6, la información de capa internet opcional se codifica en cabeceras separadas que se pueden colocar entre la cabecera IPv6 y la cabecera de capa superior dentro de un paquete. Hay un número pequeño de tales cabeceras de extensión, cada una identificada por un valor de Cabecera Siguiente distinto. Según lo ilustrado en estos ejemplos, un paquete IPv6 puede llevar cero, una, o más cabeceras de extensión, cada una identificada por el campo Cabecera Siguiente de la cabecera precedente:



Con una excepción, las cabeceras de extensión no son examinadas ni procesadas por ningún nodo a lo largo de la ruta de entrega de un paquete, hasta que el paquete alcance el nodo (o cada uno del

conjunto de nodos, en el caso de multienvío) identificado en el campo
Dirección Destino de la cabecera IPv6. Allí, el demultiplexaje normal
en el campo Cabecera Siguiente de la cabecera IPv6 invoca el módulo
para procesar la primera cabecera de extensión, o la cabecera de capa
superior si no hay ninguna cabecera de extensión presente. El
contenido y la semántica de cada cabecera de extensión determinan si
se procede o no a la cabecera siguiente. Por lo tanto, las cabeceras
de extensión se deben procesar estrictamente en el orden que aparecen
en el paquete; un receptor no debe, por ejemplo, examinar a través de
un paquete buscando un tipo en particular de cabecera de extensión y
procesar esa cabecera antes de procesar todas las precedentes.

La excepción mencionada en el párrafo precedente es la cabecera Opciones de Salto a Salto, la cual lleva información que debe ser examinada y procesada por cada nodo a lo largo de la ruta de entrega de un paquete, incluyendo los nodos de origen y de destino. La cabecera Opciones de Salto a Salto, cuando está presente, debe seguir inmediatamente a la cabecera IPv6. Su presencia es indicada por el valor cero en el campo Cabecera Siguiente de la cabecera IPv6.

Si, como resultado de procesar una cabecera, un nodo necesita proceder a la cabecera siguiente pero el valor Cabecera Siguiente en la cabecera actual es desconocido por el nodo, debe descartar el paquete y enviar un mensaje ICMP de Problema de Parámetro al origen del paquete, con un valor Código ICMP de 1 ("encontrado tipo de Cabecera Siguiente desconocido") y el campo Puntero ICMP conteniendo el desplazamiento del valor desconocido dentro del paquete original.
La misma acción se debería tomar si un nodo encuentra un valor Cabecera Siguiente de cero en cualquier cabecera con excepción de una cabecera IPv6.

Cada cabecera de extensión es un entero múltiplo de 8 octetos de largo, para conservar la alineación de 8 octetos para las cabeceras subsiguientes. Los campos Multiocteto dentro de cada cabecera de extensión se alinean en sus límites naturales, es decir, los campos de ancho de n octetos son colocados en un entero múltiplo de n octetos desde el inicio de la cabecera, para n = 1, 2, 4, o 8.

Una implementación completa del IPv6 comprende la implementación de las siguientes cabeceras de extensión:

- Opciones de Salto a Salto
- Enrutamiento (Tipo 0)
- Fragmento
- Opciones de Destino
- Autenticación
- Seguridad del Encapsulado de la Carga Útil

Las primeras cuatro están especificadas en este documento; las últimas dos están especificadas en la [RFC-2402] y la [RFC-2406],

respectivamente.

4.1 Orden de las Cabeceras de Extensión

Cuando más de una cabecera de extensión se usa en un mismo paquete,
se recomienda que esas cabeceras aparezcan en el siguiente orden:

- Cabecera IPv6
- Cabecera Opciones de Salto a Salto
- Cabecera Opciones de Destino (nota 1)
- Cabecera Enrutamiento
- Cabecera Fragmento

Cabecera Autenticación (nota 2)
Cabecera Seguridad del Encapsulado de la Carga Útil (nota 2)
Cabecera Opciones de Destino (nota 3)
Cabecera de Capa Superior

nota 1: para las opciones a ser procesadas por el primer destino que aparece en el campo Dirección Destino IPv6 más los destinos subsiguientes listados en la Cabecera Enrutamiento.

nota 2: recomendaciones adicionales con respecto al orden relativo de las cabeceras Autenticación y Seguridad del Encapsulado de la Carga Útil se dan en la [RFC-2406].

nota 3: para las opciones a ser procesadas solo por el destino final del paquete.

Cada cabecera de extensión debe ocurrir solamente una vez, a excepción de la cabecera Opciones de Destino la cual debe de ocurrir a lo sumo dos veces (una vez antes de una cabecera Enrutamiento y la otra vez antes de una cabecera de capa superior).

Si la cabecera de capa superior es otra cabecera IPv6 (en el caso de que el IPv6 sea tunelizado o encapsulado en el IPv6), puede ser seguida por sus propias cabeceras de extensión, las cuales están separadamente sujetas a las mismas recomendaciones de orden.

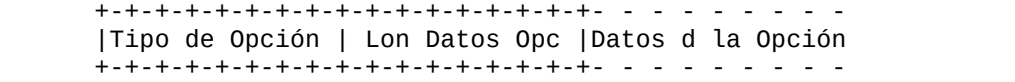
Siempre y cuando se definan otras cabeceras de extensión, sus restricciones de orden concerniente a las cabeceras arriba listadas deben ser especificadas.

Los nodos IPv6 deben aceptar e intentar procesar cabeceras de extensión en cualquier orden y cualquier número de veces que ocurran en un mismo paquete, a excepción de la cabecera Opciones de Salto a Salto la cual está restringida a aparecer sólo inmediatamente después de una cabecera IPv6. No obstante, se aconseja fuertemente que los

originadores de paquetes IPv6 se apeguen al orden recomendado arriba
hasta y a menos que especificaciones subsiguientes corrijan esa recomendación.

4.2 Opciones

Dos de las cabeceras de extensión actualmente definidas -- la cabecera Opciones de Salto a Salto y la cabecera Opciones de Destino -- llevan un número variable de "opciones" codificadas tipo-longitud-valor (TLV), de la siguiente forma:



Tipo de Opción	Identificador de 8 bits del tipo de opción.
Lon Datos Opc	Entero sin signo de 8 bits. Longitud del campo Datos de la Opción de esta opción, en octetos.
Datos de la Opción	Campo de longitud variable. Datos específicos del Tipo de Opción.

La secuencia de opciones dentro de una cabecera se deben procesar estrictamente en el orden que aparecen en la cabecera; un receptor no debe, por ejemplo, examinar a través de una cabecera buscando un tipo en particular de opción y procesar esa opción antes de procesar todas las precedentes.

Los identificadores Tipo de Opción se codifican internamente tales que sus 2 bits de más alto orden especifican la acción que se debe tomar si el nodo IPv6 en proceso no reconoce el Tipo de Opción:

00 - no tomar en cuenta esta opción y continuar procesando la cabecera.

01 - descartar el paquete.

10 - descartar el paquete y, sin tener en cuenta si o no la Dirección Destino del paquete fue una dirección multienvío,

enviar un mensaje ICMP Problema de Parámetro, Código 2, a la
Dirección Origen del paquete señalando el Tipo de Opción
desconocido.

11 - descartar el paquete y, solo si la Dirección Destino del
paquete no fue una dirección multienvío, enviar un mensaje
ICMP Problema de Parámetro, Código 2, a la Dirección Origen
del paquete señalando el Tipo de Opción desconocido.

El tercer bit de más alto orden del Tipo de Opción especifica si o no
los Datos de la Opción de esa opción pueden modificar el enrutado
hacia el destino final del paquete. Cuando una cabecera Autenticación

está presente en el paquete, para cualquier opción cuyos datos pueden modificar el enrutado, su campo entero Datos de la Opción se debe tratar como octetos de valor cero cuando se calcula o verifica el valor de autenticidad del paquete.

0 - los Datos de la Opción no modifican el enrutado.

1 - los Datos de la Opción pueden modificar el enrutado.

Los tres bits de alto orden descritos arriba están para ser tratados como parte del Tipo de Opción, no independientemente del Tipo de Opción. Es decir, una opción en particular se identifica por un Tipo de Opción de 8 bits completo, no sólo por los 5 bits de bajo orden de un Tipo de Opción.

El mismo espacio de enumeración del Tipo de Opción se usa tanto para la cabecera Opciones de Salto a Salto como para la cabecera Opciones de Destino. Sin embargo, la especificación de una opción en particular puede restringir su uso a solamente una de esas dos cabeceras.

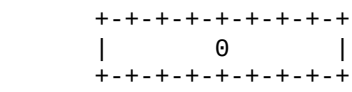
Las opciones individuales pueden tener requisitos específicos de alineación, para asegurar que los valores multiocteto dentro de los campos Datos de la Opción caigan en límites naturales. El requisito de alineación de una opción se especifica usando la notación xn+y, lo que significa que el Tipo de Opción debe aparecer en un entero múltiplo de x octetos desde el inicio de la cabecera, más y octetos. Por ejemplo:

2n	significa cualquier desplazamiento de 2 octetos a partir del comienzo de la cabecera.
8n+2	significa cualquier desplazamiento de 8 octetos a partir del comienzo de la cabecera, más 2 octetos.

Hay dos opciones de relleno las cuales se usan cuando es necesario

alinear opciones subsiguientes y rellenar la cabecera contenedora a
una longitud múltiplo de 8 octetos. Estas opciones de relleno deben
ser reconocidas por todas las implementaciones IPv6:

Opción Pad1 (requisito de alineación: ninguno)

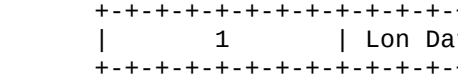


NOTA! el formato de la opción Pad1 es un caso especial -- no tiene
los campos longitud y valor.

La opción Pad1 se usa para insertar un octeto de relleno dentro
del área de Opciones de una cabecera. Si se requiere más de un

octeto de relleno, la opción PadN, descrita a continuación, se debería usar, en lugar de múltiples opciones Pad1.

Opción PadN (requisito de alineación: ninguno)

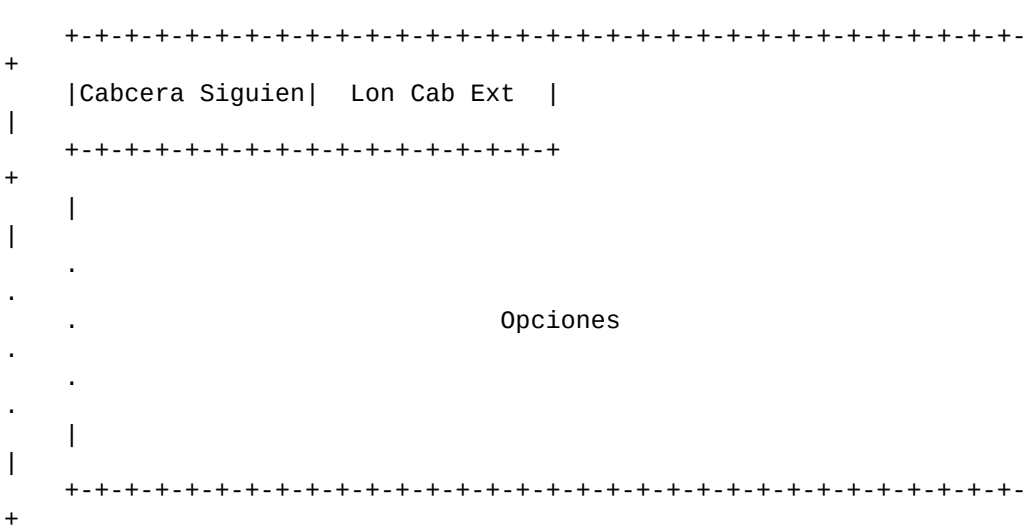


La opción PadN se usa para insertar dos o más octetos de relleno dentro del área de Opciones de una cabecera. Para N octetos de relleno, el campo Lon Datos Opc contiene el valor N-2, y el campo Datos de la Opción consiste en N-2 octetos de valor cero.

El Apéndice B contiene pautas de formateo para diseñar Opciones nuevas.

4.3 Cabecera Opciones de Salto a Salto

La cabecera Opciones de Salto a Salto se usa para llevar información opcional que debe ser examinada por cada nodo a lo largo de la ruta de entrega de un paquete. La cabecera Opciones de Salto a Salto se identifica por un valor Cabecera Siguiente de 0 en la cabecera IPv6, y tiene el siguiente formato:

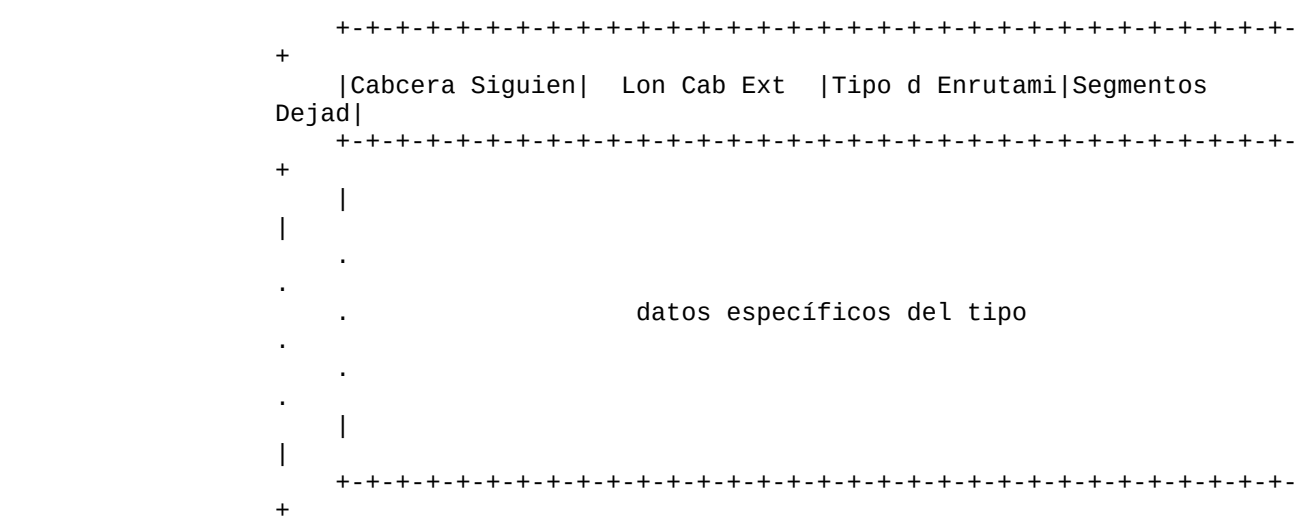


Cabecera Siguiente	Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Opciones de Salto a Salto. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC-1700 et seq.].
Lon Cab Ext	Entero sin signo de 8 bits. Longitud de la cabecera Opciones de Salto a Salto en unidades de 8 octetos, no incluye los primeros 8 octetos.
Opciones	Campo de longitud variable, de longitud tal que la cabecera Opciones de Salto a Salto completa es un entero múltiplo de 8 octetos de largo. Contiene una o más opciones codificadas TLV, como se describe en la sección 4.2.

Las únicas opciones de salto a salto definidas en este documento son las opciones Pad1 y PadN especificadas en la sección 4.2.

4.4 Cabecera Enrutamiento

La cabecera Enrutamiento es utilizada por un origen IPv6 para listar uno o más nodos intermedio a ser "visitados" en el camino hacia el destino de un paquete. Esta función es muy similar a las opciones Origen Impreciso y Registro de Ruta del IPv4. La cabecera Enrutamiento se identifica por una Cabecera Siguiente de valor 43 en la cabecera inmediatamente precedente, y tiene el siguiente formato:



Cabecera Siguiente	Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Enrutamiento. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC-1700 et seq.].
Lon Cab Ext	Entero sin signo de 8 bits. Longitud de

	la cabecera Enrutamiento en unidades de 8 octetos, no incluye los primeros 8 octetos.
Tipo de Enrutamiento	Identificador de 8 bits de una variante en particular de cabecera Enrutamiento.
Segmentos Dejados	Entero sin signo de 8 bits. Número de segmentos de ruta restantes, es decir, número de nodos intermedio explícitamente listados aún a ser visitados antes de alcanzar el destino final.
Datos específicos del tipo formato	Campo de longitud variable, de determinado por el Tipo de Enrutamiento, y de longitud tal que la cabecera Enrutamiento completa es un entero múltiplo de 8 octetos de largo.

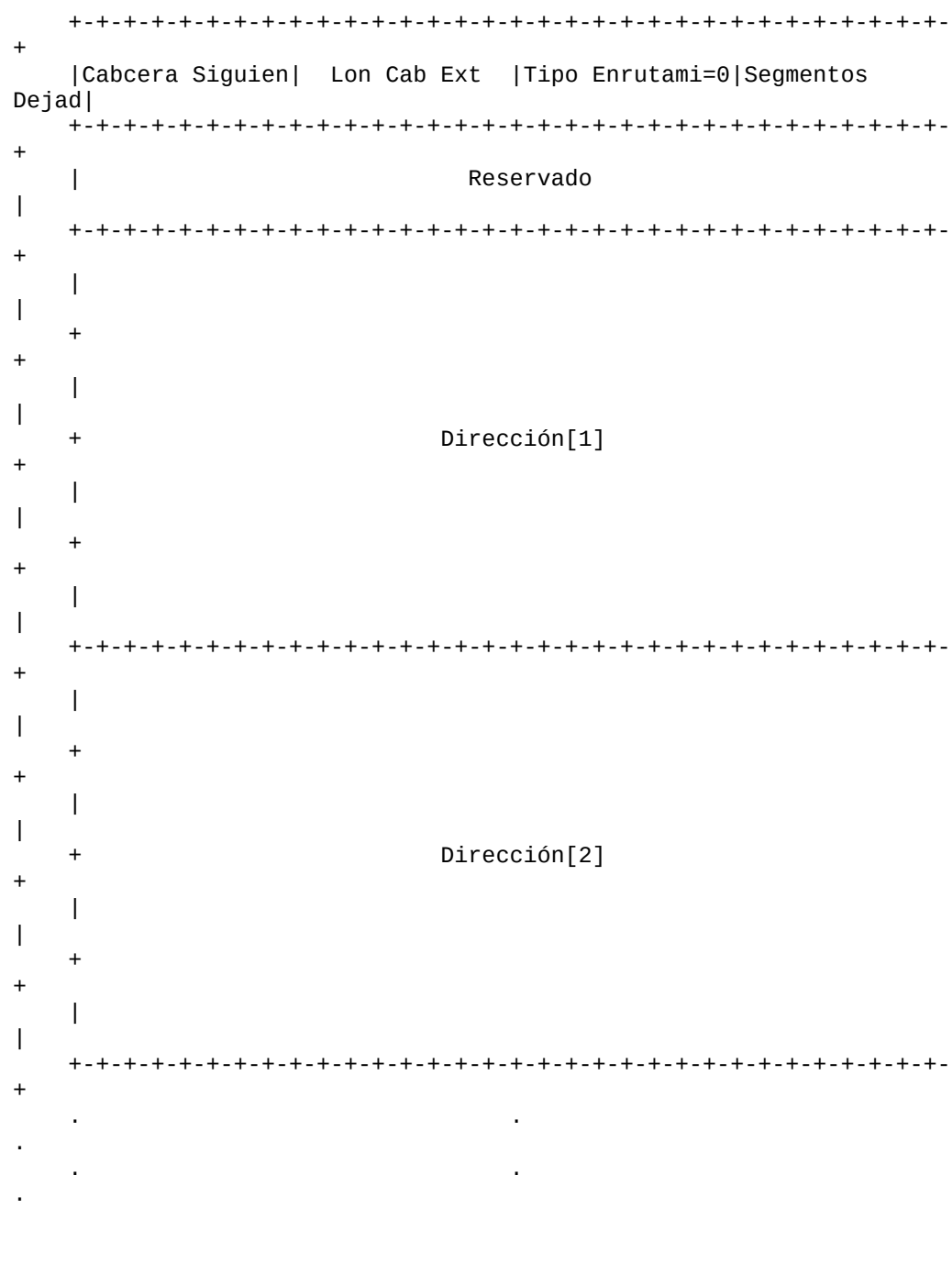
Si, al procesar un paquete recibido, un nodo encuentra una cabecera
Enrutamiento con un valor Tipo de Enrutamiento desconocido, el comportamiento requerido del nodo depende del valor del campo Segmentos Dejados, como sigue:

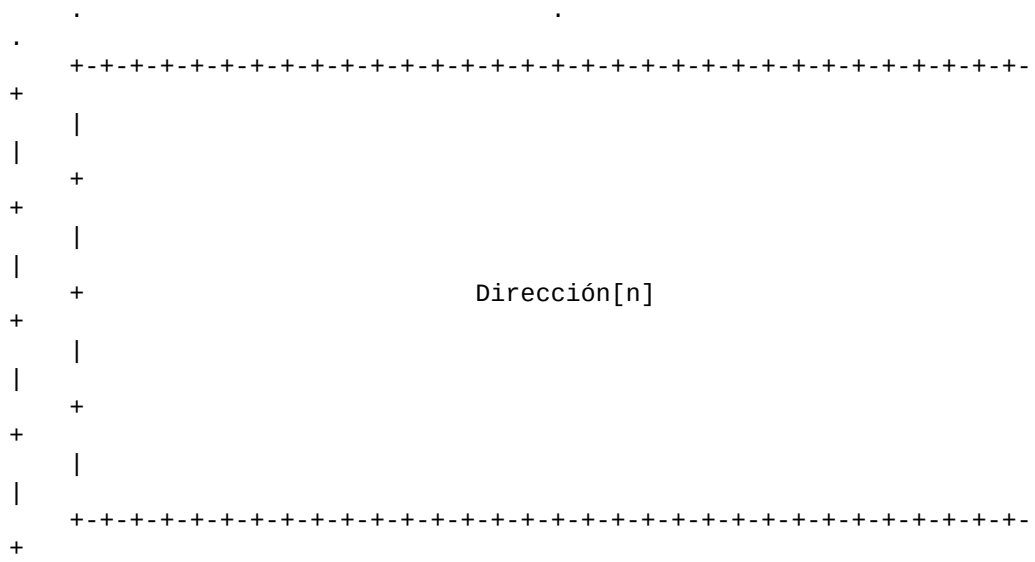
Si Segmentos Dejados es cero, el nodo debe ignorar la cabecera Enrutamiento y proceder a procesar la siguiente cabecera en el paquete, cuyo tipo se identifica por el campo Cabecera Siguiente en la cabecera Enrutamiento.

Si Segmentos Dejados no es cero, el nodo debe descartar el paquete y enviar un mensaje ICMP Problema de Parámetro, Código 0, a la Dirección Origen del paquete, apuntando al Tipo de Enrutamiento desconocido.

Si, después de procesar una cabecera Enrutamiento de un paquete recibido, un nodo intermedio determina que el paquete será remitido hacia un enlace cuya MTU de enlace es menor que el tamaño del paquete, el nodo debe descartar el paquete y enviar un mensaje ICMP Paquete Demasiado Grande a la Dirección Origen del paquete.

La cabecera Enrutamiento de Tipo 0 tiene el siguiente formato:





Cabecera Siguiente	Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Enrutamiento. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC-1700 et seq.].
Lon Cab Ext	Entero sin signo de 8 bits. Longitud de la cabecera Enrutamiento en unidades de 8 octetos, sin incluir los primeros 8 octetos. Para la cabecera Enrutamiento de Tipo 0, Lon Cab Ext es igual a dos veces el número de direcciones en la cabecera.
Tipo de Enrutamiento	0.

Segmentos Dejados	Entero sin signo de 8 bits. Número de segmentos de ruta restantes, es decir, número de nodos intermedio explícitamente listados aún a ser visitados antes de alcanzar el destino final.
Reservado	Campo reservado de 32 bits. Inicializado a cero para la transmisión; ignorado en la recepción.
Dirección[1..n]	Vector de direcciones de 128 bits, numerados desde 1 hasta n.

Las direcciones multienvío no deben aparecer en una cabecera Enrutamiento de Tipo 0, o en el campo Dirección Destino IPv6 de un paquete que lleva una cabecera Enrutamiento de Tipo 0.

Una cabecera Enrutamiento no se examina o procesa hasta que alcance el nodo identificado en el campo Dirección Destino de la cabecera IPv6. En ese nodo, al despachar el campo Cabecera Siguiente de la cabecera inmediatamente precedente ocasiona que el módulo cabecera Enrutamiento sea invocado, el cual, en el caso de Enrutamiento Tipo 0, lleva a cabo el siguiente algoritmo:

```
   si Segmentos Dejados = 0 {
      proceder a procesar la cabecera siguiente en el paquete, cuyo
tipo
      se identifica por el campo Cabecera Siguiente en la cabecera
      Enrutamiento
   }
   sino si Lon Cab Ext es impar {
         enviar un mensaje ICMP Problema de Parámetro, Código 0, a
la
         Dirección Origen, apuntando al campo Lon Cab Ext, y
descartar
         el paquete
   }
   sino {
      calcular n, el número de direcciones en la cabecera
Enrutamiento,
      al dividir Lon Cab Ext por 2

      si Segmentos Dejados es mayor que n {
         enviar un mensaje ICMP Problema de Parámetro, Código 0, a
la
         Dirección de Origen, apuntando al campo Segmentos Dejados,
y
         descartar el paquete
      }
      sino {
         decrementar Segmentos Dejados en 1;
         calcular i, el índice de la dirección siguiente a ser
visitado
         en el vector de dirección, substrayendo Segmentos Dejados
de n

         si la Dirección [i] o la Dirección Destino IPv6 es
multienvío {
            descartar el paquete
         }
         sino {
            intercambiar la Dirección Destino IPv6 y la Dirección
[i]

            si el Límite de Saltos es menor que o iguala a 1 {
               enviar un mensaje ICMP Tiempo Excedido -- Límite de
               Saltos Excedido en Transito a la Dirección Origen y
               descartar el paquete
            }
            sino {
               decrementar el Límite de Saltos en 1
```

```
                resometer el paquete al módulo IPv6 para la
transmisión
                hacia el nuevo destino
             }
          }
       }
    }
```

Como un ejemplo de los efectos del algoritmo de arriba, considerar el caso de un nodo origen S que envía un paquete al nodo de destino D, usando una cabecera Enrutamiento para causar que el paquete sea enrutado vía los nodos intermedio I1, I2, e I3. Los valores de los campos pertinentes de la cabecera IPv6 y de la cabecera Enrutamiento en cada segmento de la ruta de entrega serían como sigue:

Conforme el paquete viaja de S a I1:

Dirección de Origen = S	Lon Cab Ext = 6
Dirección de Destino = I1	Segmentos Dejados = 3
	Dirección[1] = I2
	Dirección[2] = I3
	Dirección[3] = D

Conforme el paquete viaja de I1 a I2:

Dirección de Origen = S	Lon Cab Ext = 6
Dirección de Destino = I2	Segmentos Dejados = 2
	Dirección[1] = I1
	Dirección[2] = I3
	Dirección[3] = D

Conforme el paquete viaja de I2 a I3:

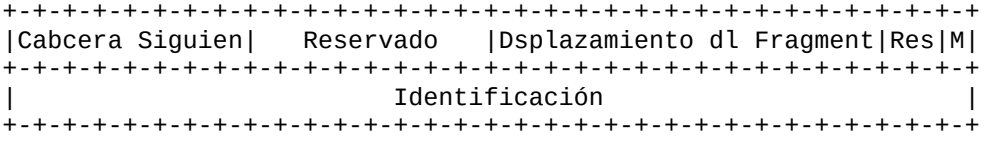
Dirección de Origen = S	Lon Cab Ext = 6
Dirección de Destino = I3	Segmentos Dejados = 1
	Dirección[1] = I1
	Dirección[2] = I2
	Dirección[3] = D

Conforme el paquete viaja de I3 a D:

Dirección de Origen = S	Lon Cab Ext = 6
Dirección de Destino = D	Segmentos Dejados = 0
	Dirección[1] = I1
	Dirección[2] = I2
	Dirección[3] = I3

4.5 Cabecera Fragmento

La cabecera Fragmento es utilizada por un origen IPv6 para enviar un paquete más grande de lo que cabría en la MTU de la ruta hacia su destino. (Nota: a diferencia del IPv4, la fragmentación en el IPv6 sólo se lleva a cabo por los nodos origen, no por los enrutadores a lo largo de la ruta de entrega de un paquete -- ver sección 5.) La cabecera Fragmento se identifica por un valor Cabecera Siguiente de 44 en la cabecera inmediatamente precedente, y tiene el siguiente formato:



Cabecera Siguiente	Selector de 8 bits. Identifica el tipo de cabecera inicial de la Parte Fragmentable del paquete original (definido abajo). Usa los mismos valores que el campo Protocolo del IPv4 [EL RFC-1700 ET SEQ.].
Reservado	Campo reservado de 8 bits. Inicializado a cero para la transmisión; ignorado en la recepción.
Desplazamiento del Fragmento	Entero sin signo de 13 bits. El desplazamiento, en unidades de 8 octetos, de los datos que siguen a esta cabecera, relativo al comienzo de la Parte Fragmentable del paquete original.
Res	Campo reservado de 2 bits. Inicializado a cero para la transmisión; ignorado en la recepción.
Bandera M	1 = más fragmentos;

	0 = último fragmento.
Identificación	32 bits. Ver descripción abajo.

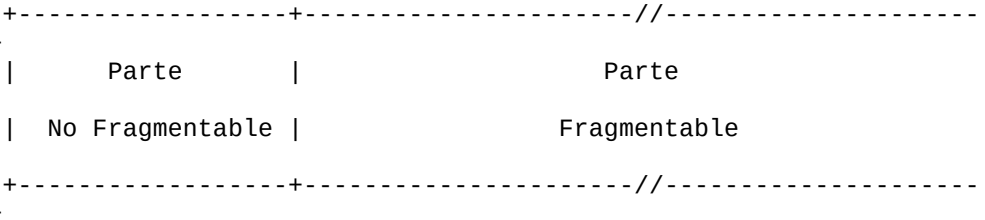
Para enviar un paquete que es demasiado grande para caber en la MTU de la ruta hacia su destino, un nodo origen puede dividir el paquete en fragmentos y enviar cada fragmento como un paquete separado, para ser reensamblado en el receptor.

Por cada paquete que será fragmentado, el nodo origen genera un valor Identificación. La Identificación debe ser diferente que el de cualquier otro paquete fragmentado enviado recientemente* con la misma Dirección Origen y Dirección Destino. Si una cabecera Enrutamiento está presente, la Dirección Destino de interés es la del destino final.

* "recientemente" significa dentro del máximo tiempo de vida probable de un paquete, incluyendo el tiempo de tránsito del origen hacia el destino y el tiempo gastado esperando el reensemblaje con otros fragmentos del mismo paquete. Sin embargo, no se requiere que un nodo origen conozca el máximo tiempo de vida de un paquete. Más bien, se asume que el requisito puede encontrarse manteniendo el valor Identificación como un simple, contador "envoltura alrededor", de 32 bits, incrementado cada vez que un paquete debe fragmentarse. Es una opción de implementación si para mantener a un solo contador para el nodo o contadores múltiples, por ejemplo, uno para cada una de las posibles direcciones origen del nodo, o uno para cada combinación (dirección origen, dirección destino) activa.

El paquete inicial, grande, no fragmentado es referido como el "paquete original", y se considera que consiste en dos partes, tal como se ilustra:

paquete original:



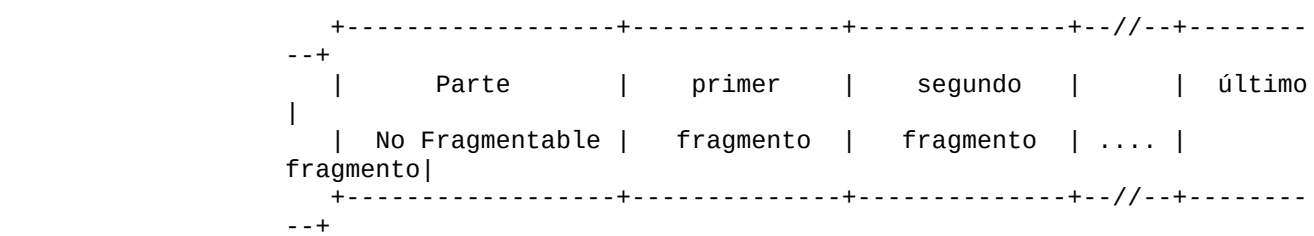
La Parte No Fragmentable consiste en la cabecera IPv6 más cualesquiera de las cabeceras de extensión que debe procesarse por nodos en camino hacia el destino, es decir, todas las cabeceras e incluso la cabecera Enrutamiento si esta presente, sino la

cabecera Opciones de Salto a Salto si esta presente, sino ninguna
de las cabeceras de extensión.

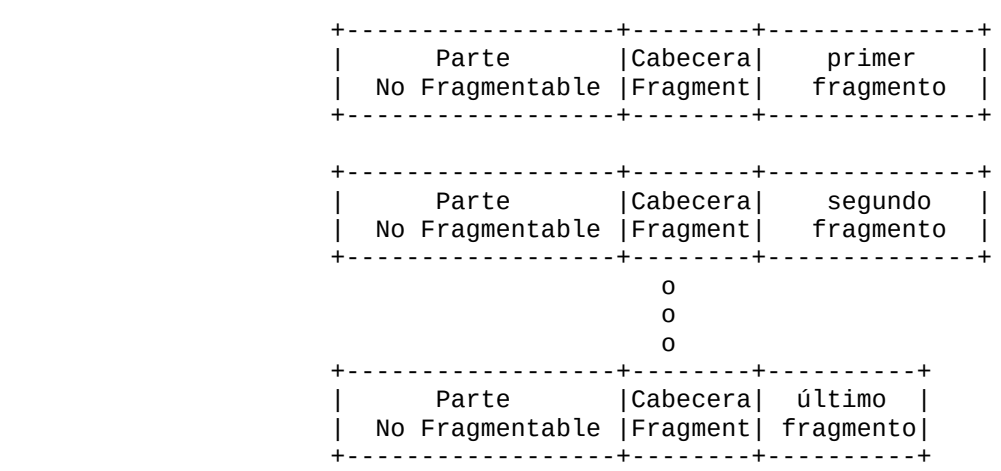
La Parte Fragmentable consiste en el resto del paquete, es decir,
cualquiera de las cabeceras de extensión que necesita que sólo se
procese por el nodo(s) destino final, más la cabecera de capa superior y los datos.

La Parte Fragmentable del paquete original es dividida en fragmentos,
cada uno, excepto posiblemente el último ("el de la extrema derecha"), siendo un entero múltiplo de 8 octetos de largo. Los fragmentos se transmiten en "paquetes fragmento" separados tal como
se ilustra:

paquete original:



paquetes fragmento:



Cada paquete fragmento está compuesto de:

(1) La Parte No Fragmentable del paquete original, con la Longitud de la Carga Útil de la cabecera IPv6 original cambiada para contener la longitud de tan sólo este paquete fragmento (excluyendo la longitud de la propia cabecera IPv6), y el campo Cabecera Siguiente de la última cabecera de la Parte No Fragmentable cambiado a 44.

(2) Una cabecera Fragmento conteniendo:

El valor Siguiente Cabecera que identifica la primera cabecera de la Parte Fragmentable del paquete original.

Un Desplazamiento del Fragmento que contiene el

desplazamiento del fragmento, en unidades de 8 octetos, relativo al comienzo de la Parte Fragmentable del paquete original. El Desplazamiento del Fragmento del primer ("el de la extrema izquierda") fragmento es 0.

Una bandera M de valor 0 si el fragmento es el último ("el de la extrema derecha"), sino una bandera M de valor 1.

El valor Identificación generado para el paquete original.

(3) El propio fragmento.

Deben escogerse las longitudes de los fragmentos tal que los paquetes fragmento resultantes quepan dentro de la MTU de la ruta hacia el(los) destino(s) del paquete.

En el destino, se reensamblan los paquetes fragmento en su forma original, no fragmentada, tal como se ilustra:

paquete original reensamblado:

Las siguientes reglas gobiernan el reensamblaje:

Un paquete original sólo se reensambla a partir de paquetes fragmento que tienen la misma Dirección Origen, Dirección Destino, e Identificación del Fragmento.

La Parte No Fragmentable del paquete reensamblado consiste en todas las cabeceras, pero sin incluir, la cabecera Fragmento del primer paquete fragmento (es decir, el paquete cuyo Desplazamiento del Fragmento es cero), con los siguiente dos cambios:

El campo Cabecera Siguiente de la última cabecera de la Parte No Fragmentable se obtiene del campo Cabecera Siguiente de la cabecera Fragmento del primer fragmento.

Se calcula la Longitud de la Carga Útil del paquete reensamblado a partir de la longitud de la Parte No Fragmentable y de la longitud y desplazamiento del último

fragmento. Por ejemplo, una fórmula para calcular la Longitud de la Carga Útil del paquete original reensamblado es:

```
  LCU.orig = LCU.inicial - LF.inicial - 8 + (8*DF.final) +
             LF.final

  donde
  LCU.orig    = campo Longitud de la Carga Útil del paquete
                reensamblado.
  LCU.inicial = campo Longitud de la Carga Útil del primer
                paquete fragmento.
  LF.inicial  = longitud del fragmento siguiente a la cabecera
                Fragmento del primer paquete fragmento.
```

DF.final = campo Desplazamiento del Fragmento de la cabecera Fragmento del último paquete fragmento.
LF.final = longitud del fragmento siguiente a la cabecera Fragmento del último paquete fragmento.

La Parte Fragmentable del paquete reensamblado se construye a partir de los fragmentos siguientes a las cabeceras Fragmento dentro de cada uno de los paquetes fragmento. La longitud de cada fragmento es calculada substrayendo de la Longitud de la Carga Útil del paquete la longitud de las cabeceras entre la cabecera IPv6 y el propio fragmento, su posición relativa en la Parte Fragmentable se calcula a partir de su valor Desplazamiento del Fragmento.

La cabecera Fragmento no está presente en el paquete reensamblado, final.

Las siguientes condiciones de error pueden originarse al reensamblar paquetes fragmentados:

Si se reciben fragmentos insuficientes para completar el reensamblaje de un paquete dentro de los 60 segundos a partir de la recepción del primer fragmento en llegar de ese paquete, el reensamblaje de ese paquete debe abandonarse y deben descartarse todos los fragmentos que se han recibido para ese paquete. Si el primer fragmento (es decir, el único con un Desplazamiento del Fragmento de cero) se ha recibido, un mensaje ICMP Tiempo Excedido -- Tiempo Excedido para el Reensamblaje del Fragmento, debe enviarse al origen de ese fragmento.

Si la longitud de un fragmento, tal como se dedujo a partir del campo Longitud de la Carga Útil del paquete fragmento, no es un múltiplo de 8 octetos y la bandera M de ese fragmento es 1, entonces ese fragmento debe descartarse y un mensaje ICMP Problema de Parámetro, Código 0, debe enviarse al origen del fragmento,

apuntando al campo Longitud de la Carga Útil del paquete fragmento.

Si la longitud y el desplazamiento de un fragmento son tales que la Longitud de la Carga Útil del paquete reensamblado de ese fragmento excedería los 65,535 octetos, entonces ese fragmento debe descartarse y un mensaje ICMP Problema de Parámetro, Código 0, debe enviarse al origen del fragmento, apuntando al campo Desplazamiento del Fragmento del paquete fragmento.

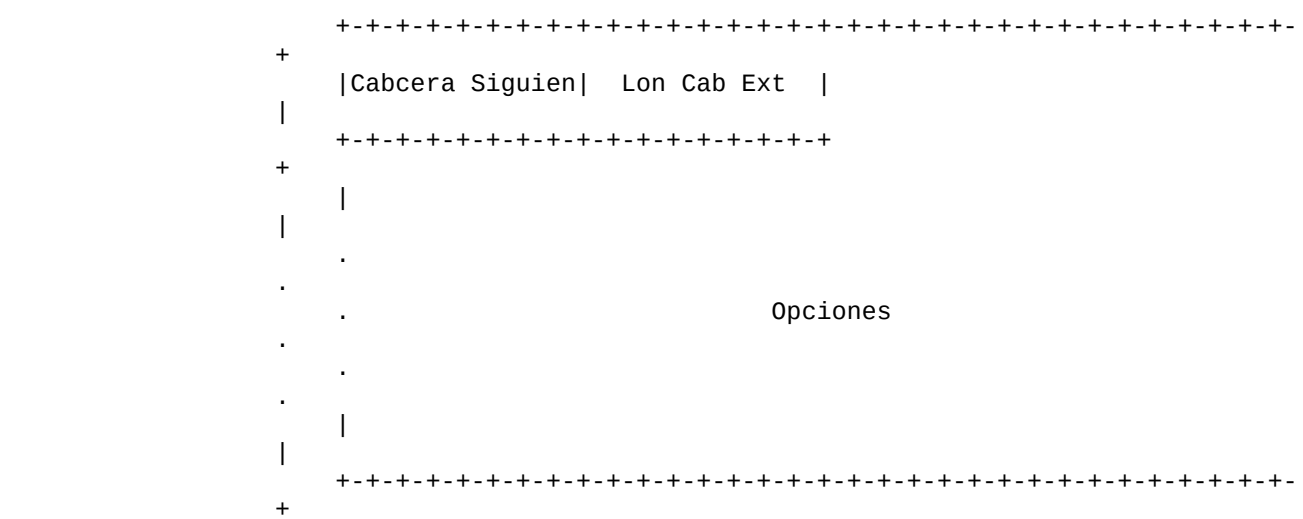
No se espera que las siguientes condiciones ocurran, pero no se consideran errores si lo hacen:

El número y contenido de las cabeceras que preceden a la cabecera
Fragmento de fragmentos diferentes del mismo paquete original pueden diferir. Cualesquiera de las cabeceras que estén presentes, precediendo a la cabecera Fragmento en cada paquete fragmento, se procesan cuando los paquetes llegan, previamente a que los fragmentos hagan cola para el reensamblaje. Sólo aquellas cabeceras en el paquete fragmento de Desplazamiento cero se retienen en el paquete reensamblado.

Los valores Cabecera Siguiente en las cabeceras Fragmento de fragmentos diferentes del mismo paquete original pueden diferir.
Sólo el valor del paquete fragmento de Desplazamiento cero se usa para el reensamblaje.

4.6 Cabecera Opciones de Destino

La cabecera Opciones de Destino es usada para llevar información opcional que necesita ser examinada solamente por el(los) nodo(s) destino del paquete. La cabecera Opciones de Destino es identificada por un valor Cabecera Siguiente de 60 en la cabecera inmediatamente precedente, y tiene el siguiente formato:



Cabecera Siguiente Selector de 8 bits. Identifica el tipo de

	cabecera que sigue inmediatamente a la cabecera Opciones de Destino. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC-1700 et seq.].
Lon Cab Ext	Entero sin signo de 8 bits. Longitud de la cabecera Opciones de Destino en unidades de 8 octetos, no incluye los primeros 8 octetos.
Opciones	Campo de longitud variable, de longitud tal que la cabecera Opciones de Destino completa es un entero múltiplo de 8 octetos de largo. Contiene uno o más opciones codificadas TLV, tal como se describe en la sección 4.2.

Las únicas opciones de destino definidas en este documento son las opciones Pad1 y PadN especificadas en la sección 4.2.

Notar que hay dos posibles maneras de codificar información de destino opcional en un paquete IPv6: como una opción en la cabecera Opciones de Destino, o como una cabecera de extensión separada. La cabecera Fragmento y la cabecera Autenticación son ejemplos de la más reciente propuesta. Qué propuesta puede ser usada depende de qué acción es deseada de un nodo destino que no entiende la información opcional:

- Si la acción deseada es que el nodo destino descarte el paquete y, sólo si la Dirección Destino del paquete no es una dirección multienvío, enviar un mensaje ICMP Tipo No reconocido a la Dirección Origen del paquete, luego la información puede ser codificada como una cabecera separada o como una opción en la cabecera Opciones de Destino cuyo Tipo de Opción tiene el valor 11 en sus dos bits de más alto orden. La elección puede depender de factores tales como cual toma menos octetos, o cual rinde mejor alineación o más eficiente análisis.

- Si alguna otra acción es deseada, la información debe ser codificada como una opción en la cabecera Opciones de Destino cuyo Tipo de Opción tiene el valor 00, 01, o 10 en sus dos bits de más alto orden, especificando la acción deseada (ver sección 4.2).

4.7 Cabecera No Hay Siguiente

El valor 59 en el campo Cabecera Siguiente de una cabecera IPv6 o de cualquier cabecera de extensión indica que nada hay siguiendo esa cabecera. Si el campo Longitud de la Carga Útil de la cabecera IPv6 indica la presencia de octetos más allá del final de una cabecera cuyo campo Cabecera Siguiente contiene 59, esos octetos deben ignorarse, y pasarse inalterados si el paquete se reenvía.

5. Cuestiones de Tamaño del Paquete

El IPv6 requiere que cada enlace en la internet tenga una MTU de 1280 octetos o mayor. En cualquier enlace que no pueda llevarse un paquete de 1280 octetos en una pieza, debe proporcionarse fragmentación y reensamblaje especifico al enlace en una capa debajo del IPv6.

Los Enlaces que tienen una MTU configurable (por ejemplo, enlaces PPP [RFC-1661]) deben configurarse para tener una MTU de por lo menos 1280 octetos; se recomienda que sean configurados con una MTU de 1500 octetos o mayor, para alojar posibles encapsulaciones (es decir, tunelizar) sin incurrir en la fragmentación de la capa IPv6.

De cada enlace al cuál un nodo se conecta directamente, el nodo debe poder aceptar paquetes tan grandes como la MTU de ese enlace.

Se recomienda fuertemente que los nodos IPv6 implementen el Descubrimiento de la MTU de la Ruta [RFC-1981] con el propósito de descubrir y tomar ventaja de las rutas con MTUs mayores que 1280 octetos. Sin embargo, una implementación IPv6 mínima (por ejemplo, en una ROM de inicio) puede restringirse simplemente a enviar paquetes no más grandes que 1280 octetos, y omitir la implementación del Descubrimiento de la MTU de la Ruta.

Con el propósito de enviar un paquete más grande que la MTU de la ruta, un nodo puede utilizar la cabecera Fragmento IPv6 para fragmentar el paquete en el origen y tenerlo reensamblado en el(los) destino(s). Sin embargo, el uso de tal fragmentación se desalienta en cualquier aplicación que pueda ajustar sus paquetes para satisfacer la MTU de la ruta medida (es decir, por debajo de los 1280 octetos).

Un nodo debe poder aceptar un paquete fragmentado que, después del reensamblaje, sea tan grande como de 1500 octetos. Se permite a un nodo aceptar paquetes fragmentados de tal manera que reensamblan a más de 1500 octetos. Un protocolo o aplicación de capa superior que depende de la fragmentación IPv6 para enviar paquetes más grandes que la MTU de una ruta no debe enviar paquetes más grandes que 1500 octetos a menos que tenga la certidumbre que el destino es capaz reensamblar paquetes de esos tamaños tan grandes.

En contestación a un paquete IPv6 que se envía a un destino IPv4 (es decir, un paquete que experimenta la traducción del IPv6 al IPv4), el nodo IPv6 originante puede recibir un mensaje ICMP Paquete Demasiado Grande reportando de una MTU del Salto Siguiente menor a 1280. En ese caso, no se exige que el nodo IPv6 reduzca el tamaño de los paquetes subsiguientes a menos de 1280, pero debe incluir una cabecera Fragmento en esos paquetes para que el enrutador traductor de IPv6 a

IPv4 pueda obtener un valor Identificación apropiado para usar en los fragmentos IPv4resultantes. Note que esto significa que la carga útil puede tener que ser reducida a 1232 octetos (1280 menos 40 para la cabecera IPv6 y 8 para la cabecera Fragmento), y más pequeña todavía si se usan cabeceras de extensión adicionales.

6. Etiquetas de Flujo

El campo Etiqueta de Flujo de 20 bits en la cabecera IPv6 puede ser usado por un origen para etiquetar secuencias de paquetes para los cuales solicita un manejo especial por los enrutadores IPv6, tal como la calidad de servicio no estándar o el servicio en "tiempo real".
Este aspecto del IPv6 está, al momento de escribir, todavía experimental y sujeto a cambio conforme los requisitos para dar soporte a flujos en la Internet se vuelvan más claros. Se exige a los hosts o a los enrutadores que no dan soporte a las funciones del campo Etiqueta de Flujo poner el campo a cero al originar un paquete, pasar el campo inalterado al reenviar un paquete, e ignorar el campo al recibir un paquete.

El Apéndice A describe la semántica y uso del campo etiqueta de flujo pretendido en vigencia.

7. Clases de Tráfico

El campo de 8 bits Clase de Tráfico en la cabecera IPv6 está disponible para usarse por nodos originantes y/o enrutadores reenviantes para identificar y distinguir entre las diferentes clases o prioridades de paquetes IPv6. En el momento en que esta especificación está siendo escrita, hay un cierto numero de experimentos en camino en cuanto al uso de los bits Tipo de Servicio IPv4 y/o Anterioridad para proporcionar varias formas de "servicio diferenciado" para paquetes IP, además de a través del uso de un flujo establecido explícito. El campo Clase de Tráfico en la cabecera IPv6 esta proyectado para permitir similar funcionalidad que será soportada en el IPv6.

Se espera que esos experimentos conduzcan eventualmente hacia un acuerdo en que orden las clasificaciones de tráfico son mas útiles para los paquetes IP. Las definiciones detalladas de la sintaxis y semántica de todos o algunos de los bits Clase de Tráfico IPv6, si es experimental o proyectado para eventual estandarización, serán proporcionados en documentos separados.

Los siguientes requisitos generales se aplican al campo Clase de Tráfico:

- La interface de servicio para el servicio IPv6 dentro de un nodo debe proporcionar un medio para que un protocolo de capa superior proporcione el valor de los bits Clase de Tráfico en los paquetes originados por ese protocolo de capa superior. El valor por defecto debe ser cero para todos los 8 bits.

- Los nodos que soportan un uso (experimental o estándar eventual) especifico de algunos o todos los bits Clase de Tráfico se les permite cambiar el valor de esos bits en los paquetes que ellos originan, reenvían, o reciben, como sea

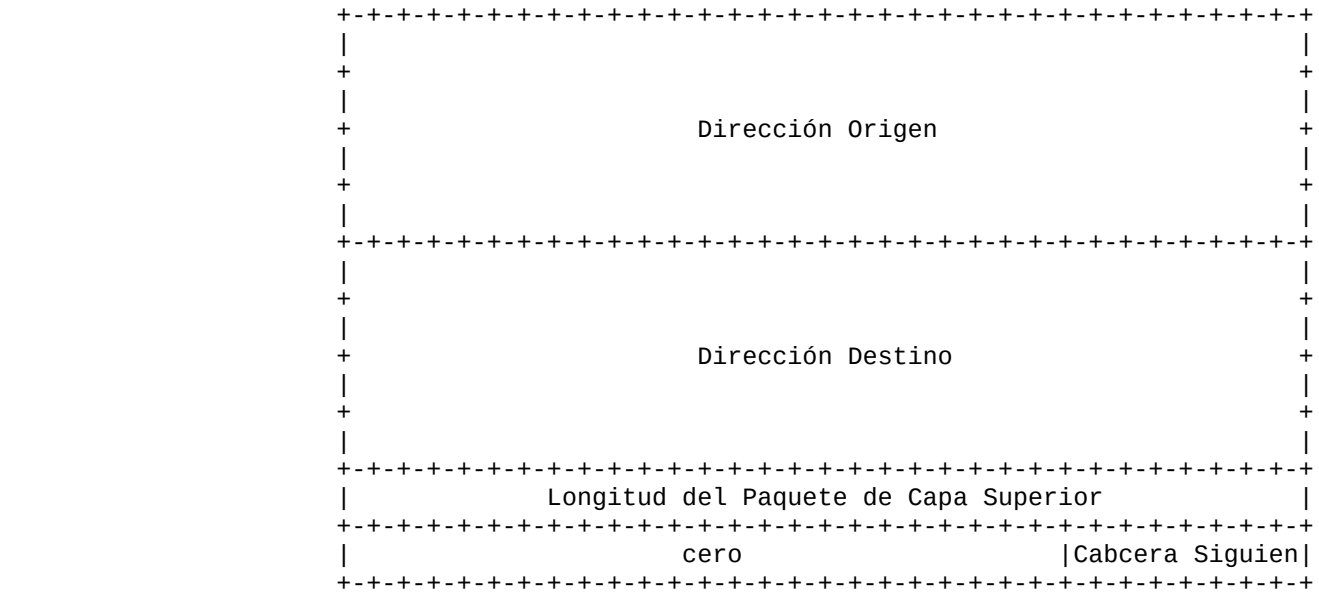
requerido para ese uso específico. Los nodos deben ignorar y dejar sin alterar a cualesquiera de los bits del campo Clase de Tráfico para los cuales no dan soporte a un uso específico.

- Un protocolo de capa superior no debe asumir que el valor de los bits Clase de Tráfico en un paquete recibido son los mismos que el valor enviado por el origen del paquete.

8. Problemas de Protocolo de Capa Superior

8.1 Sumas de Verificación de Capa Superior

Cualquier protocolo de transporte u otro de capa superior que incluya las direcciones de la cabecera IP en su cálculo de suma de verificación debe modificarse para el uso sobre el IPv6, para incluir las direcciones IPv6 de 128 bits en lugar de las direcciones IPv4 de 32 bits. En particular, la siguiente ilustración muestra la "pseudo cabecera" TCP y UDP para el IPv6:



- Si el paquete IPv6 contiene una cabecera Enrutamiento, la Dirección Destino usada en la pseudo cabecera es la del destino final. En el nodo originante, esa dirección estará en el último elemento de la cabecera Enrutamiento; en el(los) receptor(res), esa dirección estará en el campo Dirección Destino de la cabecera IPv6.

- El valor Cabecera Siguiente en la pseudo cabecera identifica el

protocolo de capa superior (por ejemplo, 6 para el TCP, o 17
para el UDP). Diferirá del valor Cabecera Siguiente en la
cabecera IPv6 si hay cabeceras de extensión entre la cabecera
IPv6 y la cabecera de capa superior.

- La Longitud del Paquete de Capa Superior en la pseudo cabecera es la longitud de la cabecera de capa superior y los datos (por ejemplo, la cabecera TCP más los datos TCP). Algunos protocolos

de capa superior llevan su propia información de longitud (por ejemplo, el campo Longitud en la cabecera UDP); para tales protocolos, esa es la longitud usada en la pseudo cabecera. Otros protocolos (como el TCP) no llevan su propia información de longitud, en cuyo caso la longitud usada en la pseudo cabecera es la Longitud de la Carga Útil de la cabecera IPv6, menos la longitud de cualquier cabecera de extensión presente entre la cabecera IPv6 y la cabecera de capa superior.

- A diferencia del IPv4, cuando los paquetes UDP son originados por un nodo IPv6, la suma de verificación UDP no es opcional. Es decir, siempre que se origine un paquete UDP, un nodo IPv6 debe calcular una suma de verificación UDP sobre el paquete y la pseudo cabecera, y, si ese cálculo produce un resultado de cero, debe cambiarse al hexadecimal FFFF para la colocación en la cabecera UDP. Los receptores IPv6 deben descartar los paquetes UDP que contengan una suma de verificación cero, y deben registrar el error.

La versión IPv6 del ICPM [ICMPv6] incluye la pseudo cabecera citada arriba en su cálculo de suma de verificación; éste es un cambio a diferencia de la versión IPv4 del ICMP, el cual no incluye una pseudo cabecera en su suma de verificación. La razón para el cambio es para proteger al ICMP de una mala entrega o corrupción de aquellos campos de la cabecera IPv6 de los que depende, los qué, a diferencia del IPv4, no son cubiertos por una suma de verificación de la capa internet. El campo Cabecera Siguiente en la pseudo cabecera para el ICMP contiene el valor 58, que identifica la versión IPv6 del ICMP.

8.2 Tiempo de Vida Máximo de un Paquete

A diferencia del IPv4, no se exigen a los nodos IPv6 cumplir con el

tiempo de vida máximo de un paquete. Ésa es la razón por la que el campo "Tiempo de Vida" del IPv4 se renombró a "Límite de Saltos" en el IPv6. En la práctica, muy pocas, si alguna, implementaciones IPv4 adoptan el requisito de limitar el tiempo de vida de un paquete, asi que esto no es un cambio en la práctica. Cualquier protocolo de capa superior que depende de la capa internet (ya sea IPv4 o IPv6) para limitar el tiempo de vida de un paquete debe actualizarse para proporcionar sus propios mecanismos de detección y descarte de paquetes obsoletos.

8.3 Tamaño Máximo de la Carga Útil de Capa Superior

Al calcular el tamaño máximo de carga útil disponible para los datos de capa superior, un protocolo de capa superior debe tener en cuenta el tamaño más grande de la cabecera IPv6relativo a la cabecera IPv4. Por ejemplo, en el IPv4, la opción MSS del TCP se calcula como el tamaño máximo de paquete (un valor por defecto o un valor aprendido a través del Descubrimiento de la MTU de la Ruta) menos 40 octetos (20 octetos para la longitud mínima de la cabecera IPv4 y 20 octetos para la longitud mínima de la cabecera TCP). Al usar TCP sobre IPv6, el MSS debe calcularse como el tamaño máximo de paquete menos 60 octetos, puesto que la longitud mínima de la cabecera IPv6 (es decir, una cabecera IPv6 sin cabeceras de extensión) es 20 octetos más larga que la longitud mínima de la cabecera IPv4.

8.4 Contestando a Paquetes que Llevan Cabeceras Enrutamiento

Cuando un protocolo de capa superior envía uno o más paquetes en contestación a un paquete recibido que incluía una cabecera Enrutamiento, el(los) paquete(s) respuesta no debe(n) incluir una cabecera Enrutamiento que se derivó automáticamente "invirtiendo" la cabecera Enrutamiento recibida A MENOS QUE se hayan verificado la integridad y autenticidad tanto de la Dirección Origen como de la cabecera Enrutamiento recibida (por ejemplo, mediante el uso de una cabecera Autenticación en el paquete recibido). En otras palabras, se permiten sólo los siguientes tipos de paquetes en contestación a un paquete recibido que lleva una cabecera Enrutamiento:

- Los paquetes respuesta que no llevan cabeceras Enrutamiento.

- Los paquetes respuesta que llevan cabeceras Enrutamiento que NO se derivaron invirtiendo la cabecera Enrutamiento del paquete

recibido (por ejemplo, una cabecera Enrutamiento proporcionada
por configuración local).

- Los paquetes respuesta que llevan cabeceras Enrutamiento que se derivaron invirtiendo la cabecera Enrutamiento del paquete recibido SI Y SÓLO SI la integridad y autenticidad de la Dirección Origen y de la cabecera Enrutamiento del paquete recibido han sido verificadas por el contestador.

Apéndice A. Uso y Semántica del Campo Etiqueta de Flujo

Un flujo es una secuencia de paquetes enviada desde un origen determinado hacia un destino (unienvío o multienvío) determinado para el cual el origen desea un tratamiento especial por los enrutadores intermedios. Podría transmitirse la naturaleza de ese tratamiento especial hacia los enrutadores por un protocolo control, tal como el protocolo reservación de recurso, o por información dentro de los mismos paquetes del flujo, por ejemplo, en una opción de salto a salto. Los detalles de tales protocolos control u opciones están fuera del ámbito de este documento.

Pueden haber flujos activos múltiples desde un origen hacia un destino, así como también tráfico que no esta asociado con algún flujo. Un flujo se identifica singularmente por la combinación de una dirección origen y una etiqueta de flujo no cero. Los paquetes que no pertenecen a un flujo llevan una etiqueta de flujo de cero.

Una etiqueta de flujo se asigna a un flujo en el nodo origen del flujo. Deben escogerse nuevas etiquetas de flujo (pseudo) aleatoriamente y uniformemente del rango 1 al FFFFF en hexadecimal. El propósito de la asignación al azar es para hacer cualquier conjunto de bits dentro del campo Etiqueta de Flujo adecuado para el uso como una clave por los enrutadores, para buscar el estado asociado con el flujo.

Deben enviarse todos los paquetes que pertenecen al mismo flujo con la misma dirección origen, dirección destino, y etiqueta de flujo. Si alguno de esos paquetes incluye una cabecera Opciones de Salto a Salto, entonces todos ellos deben originarse con los mismos contenidos de cabecera Opciones de Salto a Salto (excepto el campo Cabecera Siguiente de la cabecera Opciones de Salto a Salto). Si alguno de esos paquetes incluye una cabecera Enrutamiento, entonces todos ellos deben originarse con los mismos contenidos en todas las cabeceras de extensión e incluso la cabecera Enrutamiento (excepto el

campo Cabecera Siguiente en la cabecera Enrutamiento). Se permiten a los enrutadores o destinos, pero no se exige, verificar que estas condiciones se cumplen. Si una violación se detecta, debe reportarse al origen en un mensaje ICMP Problema de Parámetro, Código 0, apuntando al octeto de mayor orden del campo Etiqueta de Flujo (es decir, desplazamiento 1 dentro del paquete IPv6).

El tiempo de vida máximo de cualquier flujo en estado de tratamiento establecido a lo largo de la ruta de un flujo debe especificarse como parte de la descripción del estado del mecanismo de establecimiento, por ejemplo, el protocolo reservación de recurso o la configuración de la opción de salto a salto de flujo. Un origen no debe reusar una etiqueta de flujo para un nuevo flujo dentro del tiempo de vida máximo de cualquier flujo en estado de tratamiento que se podría haber establecido para el uso anterior de esa etiqueta de flujo.

Cuando un nodo detiene y reinicia (por ejemplo, como resultado de una "caída"), debe tener el cuidado de no usar una etiqueta de flujo que podría haber usado para un flujo anterior cuyo tiempo de vida pueda no haber expirado aún. Esto puede lograrse registrando el uso de las etiquetas de flujo sobre un almacenamiento estable para que pueda tenerse presente durante las caídas, o absteniéndose de usar cualquier etiqueta de flujo hasta que el tiempo de vida máximo de cualquier posible flujo previamente establecido haya expirado. Si se conoce el tiempo mínimo para reinicializar el nodo, ese tiempo puede descontarse del periodo de espera necesario antes de empezar a asignar las etiquetas de flujo.

No hay ningún requisito que todos, o incluso la mayoría, de los paquetes pertenezcan a flujos, es decir, que lleven etiquetas de flujo no cero. Esta observación se pone aquí para recordar a los diseñadores e implementadores de protocolos no asumir lo contrario. Por ejemplo, sería desacertado diseñar un enrutador cuyo rendimiento sólo sería adecuado si la mayoría de los paquetes pertenecieran a flujos, o diseñar un esquema de compresión de cabecera que sólo trabaje sobre paquetes que pertenezcan a flujos.

Apéndice B. Pautas de Formateo para las Opciones

Este apéndice da algunos consejos en cómo disponer los campos al diseñar nuevas opciones para ser usadas en la cabecera Opciones de Salto a Salto o en la cabecera Opciones de Destino, tal como se describe en la sección 4.2. Estas pautas se basan en las siguientes suposiciones:

- Una característica deseable es que cualquier campo multiocteto dentro del área Datos de la Opción de una opción se alinean en sus límites naturales, es decir, los campos de ancho de n octetos deben ser colocados en un entero múltiplo de n octetos desde el inicio de la cabecera Opciones de Salto a Salto o de la cabecera Opciones de Destino, para n = 1, 2, 4, o 8.

- Otra característica deseable es que la cabecera Opciones de Salto a Salto o la cabecera Opciones de Destino ocupe tan poco espacio como sea posible, sujeto al requisito que la cabecera sea un entero múltiplo de 8 octetos de largo.

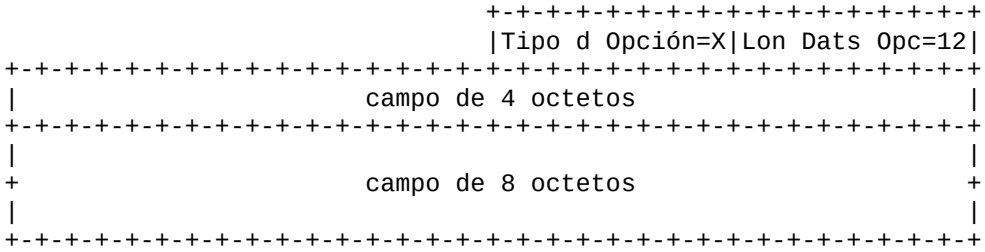
- Puede asumirse que, cuando ambas cabeceras que tienen opciones están presentes, llevan un número muy pequeño de opciones, usualmente solo una.

Estas suposiciones sugieren la siguiente propuesta para disponer los campos de una opción: ordenar los campos desde el más pequeño hasta el más grande, sin relleno interior, luego deducir el requisito de alineación para la opción entera en base al requisito de alineación del campo más grande (hasta una alineación máxima de 8 octetos). Esta propuesta se ilustra en los siguiente ejemplos:

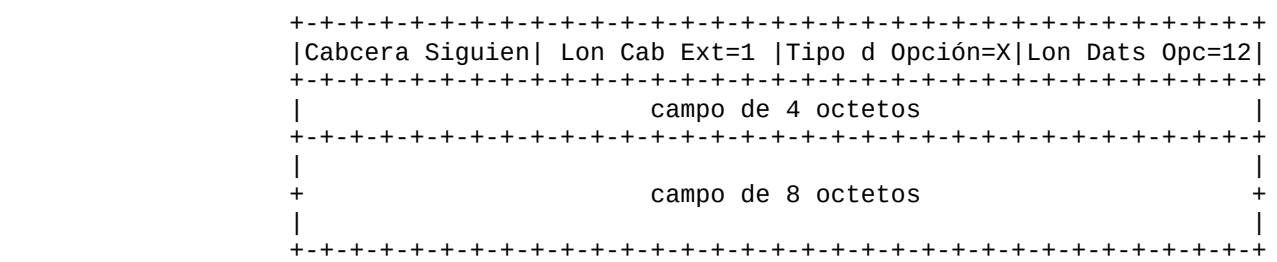
Ejemplo 1

Si una opción X requiere dos campos datos, uno de longitud de 8 octetos y uno de longitud de 4 octetos, se dispondrían tal como

sigue:

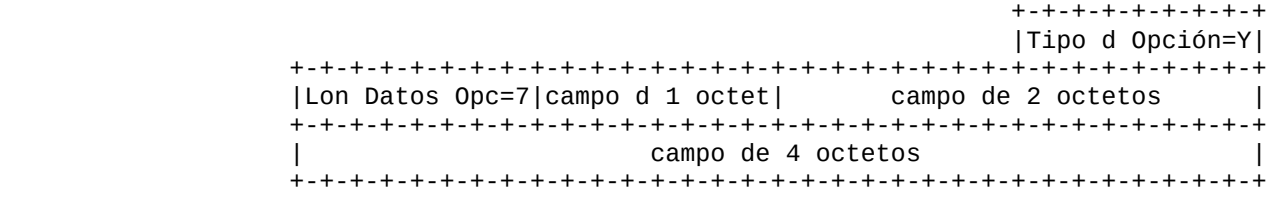

|Tipo d Opción=X|Lon Dats Opc=12|
campo de 4 octetos
campo de 8 octetos

Su requisito de alineación es 8n+2, para asegurar que el campo de 8 octetos comience en un desplazamiento múltiplo de 8 a partir del inicio de la cabecera circundante. Una cabecera Opciones de Salto a Salto completa o una cabecera Opciones de Destino completa que contiene esta única opción se vería como sigue:

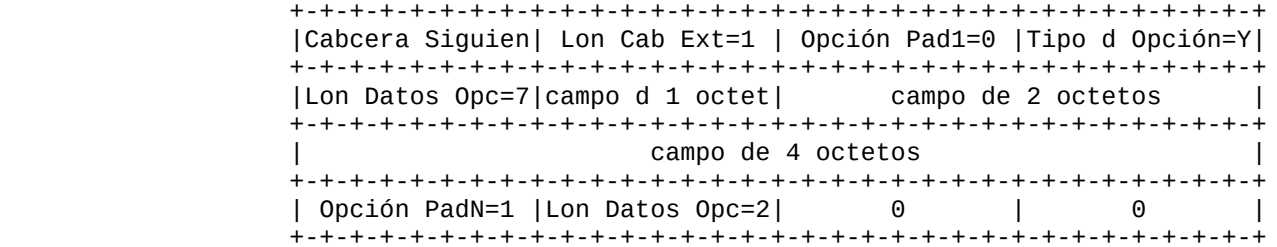


Ejemplo 2

Si una opción Y requiere tres campos datos, una de longitud de 4 octetos, una de longitud de 2 octetos, y una de longitud de 1 octeto, se dispondrían tal como sigue:

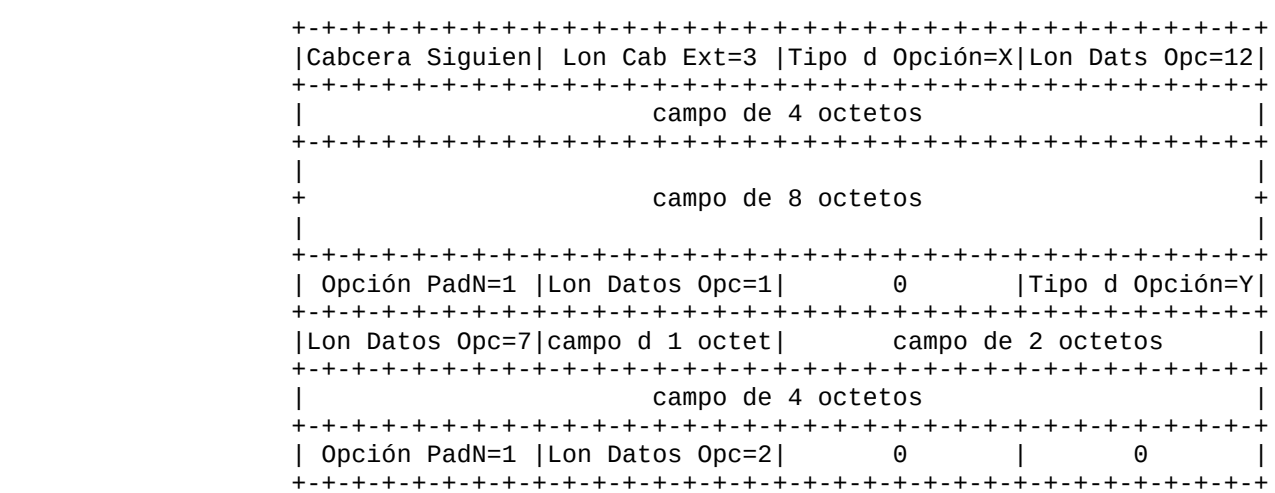


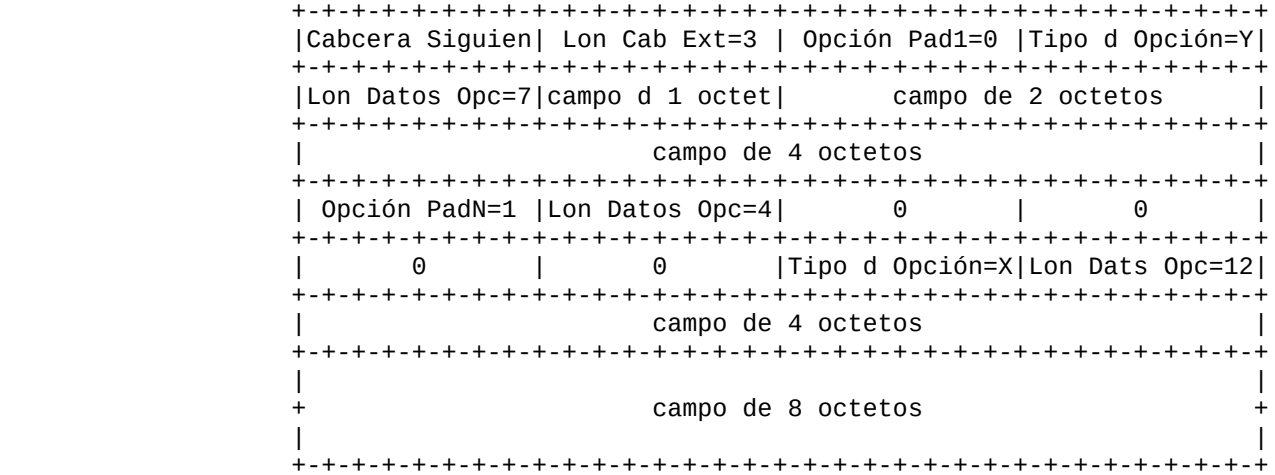
Su requisito de alineación es 4n+3, para asegurar que el campo de 4 octetos comience en un desplazamiento múltiplo de 4 a partir del inicio de la cabecera circundante. Una cabecera Opciones de Salto a Salto completa o una cabecera Opciones de Destino completa que contiene esta única opción se vería como sigue:



Ejemplo 3

Una cabecera Opciones de Salto a Salto o una cabecera Opciones de Destino que contiene ambas opciones X e Y de los Ejemplos 1 y 2 tendría uno de los dos siguientes formatos, dependiendo en que opción apareciera primero:





Consideraciones de Seguridad

Las características de seguridad del IPv6 se describen en la Arquitectura de Seguridad para el Protocolo Internet [RFC-2401].

Reconocimientos

Los autores agradecidamente reconocen el gran número de sugerencias útiles de los miembros del grupo de trabajo IPng, del grupo de investigación de Protocolos de Extremo a Extremo, y de la Comunidad Internet En General.

Direcciones de los Autores

Stephen E. Deering
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Teléfono: +1 408 527 8213
Fax: +1 408 527 8254
Correo Electrónico: deering@cisco.com

Robert M. Hinden
Nokia
232 Java Drive
Sunnyvale, CA 94089
USA

Teléfono: +1 408 990-2004
Fax: +1 408 743-5677
Correo Electrónico: hinden@iprg.nokia.com

Dirección del Traductor al Castellano

Percy Luis Ché Castillo
UPAO
Av. América Sur 3145
Urb. Monserrate, Trujillo
PERÚ

Teléfono: +51 044 201880
Fax: +51 044 286111
Correo Electrónico: percychecastillo@yahoo.com

Referencias

[RFC-2401] Kent, S. y R. Atkinson, "Arquitectura de Seguridad para el Protocolo Internet", RFC 2401, Noviembre 1998.

[RFC-2402] Kent, S. y R. Atkinson, "Cabecera Autenticación del IP", RFC 2402, Noviembre 1998.

[RFC-2406] Kent, S. y R. Atkinson, "Seguridad del Encapsulado de la Carga Útil (ESP)", RFC 2406, Noviembre 1998.

[ICMPv6] Conta, A. y S. Deering, "ICMP para el Protocolo Internet Versión 6 (IPv6)", RFC 2463, Diciembre 1998.

[ADDRARCH] Hinden, R. y S. Deering, "Arquitectura de Direccionamiento para la Versión 6 del IP", RFC 2373, Julio 1998.

[RFC-1981] McCann, J., Mogul, J. y S. Deering, "Descubrimiento de la MTU para la versión 6 del IP", RFC 1981, Agosto 1996.

[RFC-791] Postel, J., "Protocolo Internet", STD 5, RFC 791, Setiembre 1981.

[RFC-1700] Reynolds, J. y J. Postel, "Números Asignados", STD 2, RFC 1700, Octubre 1994. Ver también: http://www.iana.org/numbers.html

[RFC-1661] Simpson, W., "El Protocolo Punto a Punto (PPP)", STD 51, RFC 1661, Julio 1994.

CAMBIOS A PARTIR DE LA RFC-1883

Este memorándum tiene los siguientes cambios a partir de la RFC-1883.
Los números identifican la versión del Bosquejo Internet en la cual
se hizo el cambio.

02) Se quitaron todas las referencias a datagramas de tamaño gigante

y la opción Carga Útil de Tamaño Gigante (se movió hacia un documento separado).

02) Se movió la mayor parte de la descripción de la Etiqueta de Flujo de la sección 6 hacia el (nuevo) Apéndice A.

02) En la descripción de la Etiqueta de Flujo, ahora en el Apéndice A, se corrigió el valor Etiqueta de Flujo máximo de FFFFFF a FFFFF (es decir, un "F" menos) debido a la reducción del tamaño del campo Etiqueta de Flujo de 24 bits a 20 bits.

02) Se reenumeró (se reletreó?) el anterior Apéndice A para ser el Apéndice B.

02) Se cambió la redacción de la sección Consideraciones de Seguridad para evitar bucle dependencia entre esta especificación y las especificaciones del IPsec.

02) Se actualizó la dirección de correo electrónico y la afiliación de compañía de R. Hinden.

---

01) En la sección 3, se cambió el nombre del campo "Clase" a "Clase de Tráfico" y se aumentó su tamaño de 4 a 8 bits. Se disminuyó el tamaño del campo Etiqueta de Flujo de 24 a 20 bits para compensar el aumento en el campo Clase de Tráfico.

01) En la sección 4.1, se restituyó el orden de la Cabecera Autenticación y la Cabecera ESP, las cuales fueron intercambiadas equivocadamente en la versión 00 de este memorándum.

01) En la sección 4.4, se suprimió el campo Mapa de Bits Estricto/Impreciso y la funcionalidad enrutamiento estricto de la cabecera Enrutamiento de Tipo 0, y se quitó la restricción sobre el número de direcciones que pueden ser llevadas dentro de la cabecera Enrutamiento de Tipo 0 (fue limitado a 23 direcciones, debido al tamaño del mapa de bits estricto/impreciso).

01) En la sección 5, se cambió la mínima MTU IPv6 de 576 a 1280 octetos, y se añadió una recomendación que los enlaces con una MTU configurable (por ejemplo, enlaces PPP) sean configurados para tener una MTU de por lo menos 1500 octetos.

01) En la sección 5, se suprimió el requisito que un nodo no debe enviar paquetes fragmentados de tal manera que reensamblan a más de 1500 octetos sin conocimiento del tamaño del búfer de

reensamblaje destino, y se lo reemplazó con una recomendación
que los protocolos o las aplicaciones de capa superior no deberían hacer eso.

01) Se reemplazó la referencia hacia la especificación Descubrimiento de la MTU de la Ruta para el IPv4 (RFC-1191) con la referencia hacia la especificación Descubrimiento de la MTU de la Ruta para el IPv6 (RFC-1981), y se suprimieron las Notas al final de la sección 5 respecto al Descubrimiento de la MTU de la Ruta, dado que esos detalles ahora son cubiertos por la RFC-1981.

01) En la sección 6, se suprimió la especificación de flujo establecido "oportunista", y se quitaron todas las referencias al tiempo de vida máximo de 6 segundos para el estado de flujo establecido oportunamente.

01) En la sección 7, se suprimió la descripción provisional de la estructura interna y semántica del campo Clase de Tráfico, y se especificó que tales descripciones sean proporcionadas en documentos separados.

---

00) En la sección 4, se corrigió el valor Código para indicar "encontrado tipo de Cabecera Siguiente desconocido" en un mensaje ICMP Problema de Parámetro (se cambió de 2 a 1).

00) En la descripción del campo Longitud de la Carga Útil en la sección 3, y del campo Longitud de la Carga Útil de Tamaño Gigante en la sección 4.3, se aclaró que las cabeceras de extensión están incluidas en el conteo de la longitud de la carga útil.

00) En la sección 4.1, se intercambió el orden de la cabecera Autenticación y la cabecera ESP. (NOTA: esto fue un error, y el cambio fue desecho en la versión 01).

00) En la sección 4.2, se aclaró que las opciones son identificadas por un Tipo de Opción de 8 bits completo, no por los 5 bits de bajo orden de un Tipo de Opción. Se especificó también que el mismo espacio de enumeración del Tipo de Opción es usado tanto por la cabecera Opciones de Salto a Salto como por la cabecera Opciones de Destino.

00) En la sección 4.4, se añadió una sentencia exigiendo que los nodos que procesan una cabecera Enrutamiento deben enviar un mensaje ICMP Paquete Demasiado Grande en contestación a un paquete que es demasiado grande para caber en el enlace de salto

siguiente (en lugar de, digamos, llevar a cabo fragmentación).

00) Se cambió el nombre del campo Prioridad IPv6 a "Clase", y se reemplazó la descripción anterior de Prioridad en la sección 7 con una descripción del campo Clase. También, se excluyó este campo del conjunto de campos que deben permanecer de la misma forma para todos los paquetes en el mismo flujo, tal como se especificó en la sección 6.

00) En la pseudo cabecera en la sección 8.1, se cambió el nombre del campo "Longitud de la Carga Útil" a "Longitud del Paquete de Capa Superior". Se aclaró también que, en el caso de protocolos que llevan su propia información de longitud (como el datagrama de tamaño no gigante UDP), es la longitud derivada de la capa superior, no la longitud derivada de la capa IP, la que es usada en la pseudo cabecera.

00) Se añadió la sección 8.4, especificando que los protocolos de capa superior, al contestar a un paquete recibido que llevó una cabecera Enrutamiento, no deben incluir el inverso de la cabecera Enrutamiento en el(los) paquete(s) respuesta a menos que la cabecera Enrutamiento recibida fuese autenticada.

00) Corregidos algunos errores tipográficos y errores gramaticales.

00) Actualizada la información de contacto de los autores.

---

motivo de su traducción a otras lenguas aparte del Inglés.

Los permisos limitados concedidos más arriba son perpetuos y no serán revocados por la Sociedad Internet o sus sucesores o cesionarios.

Este documento y la información contenida en él se proporcionan en su forma "TAL CUAL" y LA SOCIEDAD INTERNET Y LA FUERZA DE TRABAJO EN INGENIERÍA INTERNET RECHAZAN CUALESQUIERA GARANTÍAS, EXPRESAS O IMPLÍCITAS, INCLUYENDO, PERO NO LIMITADAS A, CUALQUIER GARANTÍA DE QUE EL USO DE LA INFORMACIÓN AQUÍ EXPUESTA NO INFRINGIRÁ NINGÚN DERECHO O GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN PROPÓSITO ESPECÍFICO.