GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

OBSAE Observatorio de Administración Electrónica

GUÍA PARA LA INCORPORACIÓN DE IPv6 COMO REQUISITO DE COMPRA PÚBLICA

Marzo 2012

Estudio realizado por el Instituto Nacional de Tecnologías de la Comunicación S.A. (INTECO) en colaboración con el Ministerio de Hacienda y Administraciones Públicas

Las opiniones expresadas en este estudio son las de los autores y no reflejan necesariamente el punto de vista del Ministerio de Hacienda y Administraciones Públicas.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. RESUMEN EJECUTIVO

Dentro del conjunto de medidas incluidas en el Plan de fomento para la incorporación del Protocolo de Internet versión 6 (IPv6) en España, aprobado en el Acuerdo de Consejo de Ministros de 29 de Abril de 2011, se establece que el Ministerio de Política Territorial y Administraciones Públicas (actual Ministerio de Hacienda y Administraciones Públicas), *"impulsará la incorporación de IPv6 como requisito en la compra pública en productos y servicios de tecnologías de la información y comunicaciones".*

Con el fin de dar cumplimiento a este objetivo, se ha llevado a cabo un estudio en el que, partiendo de un análisis de la situación actual respecto a la consideración del protocolo IPv6 en las compras públicas y de una valoración de las mejores prácticas, se proponen una serie de recomendaciones de carácter práctico que permiten a los compradores públicos incorporar IPv6 en los procedimientos de adquisición relacionados con la aplicación de las Tecnologías de la Información en las Administraciones Públicas.

En primer lugar, el estudio revisa los antecedentes existentes sobre la incorporación de IPv6 en políticas de compras. A nivel internacional, se presentan las experiencias de EEUU (comparando los distintos enfoques entre el Gobierno Federal, el NIST y el Departamento de Defensa), el Gobierno de Tasmania, Arabia Saudí y Reino Unido. Aunque la forma de abordar los requisitos de compatibilidad con IPv6 es variada, la aproximación general es basarse en el cumplimiento de estándares. En el ámbito nacional, se dan referencias de cómo se han definido los requisitos para IPv6 tanto a nivel estatal (Criterios SNC de la AGE; RedIRIS; Ministerio de Sanidad, Servicios Sociales e Igualdad; Ministerio de Industria, Turismo y Comercio), como autonómico (Gobierno de Aragón, Junta de Andalucía) y local (Diputación de Cáceres), poniendo de nuevo de manifiesto las diferentes aproximaciones a la hora de especificar esos requisitos (desde cláusulas de carácter general hasta listados detallados de los estándares a cumplir).

A continuación, el estudio aborda el concepto de compatibilidad IPv6, presentando las diferentes iniciativas internacionales orientadas la certificación de dispositivos compatibles con IPv6: ISO/IEC 17025, USGv6, IPv6 Ready logo Program, IPv6-to-Standard, UNH-IOL IPv6 Testing Consortium, DoD (JITC /DISA) IPv6 Product Certification, para después analizar el impacto de IPv6 en los componentes básicos de los productos y servicios de tecnologías de la información: hardware (comparando los modelos de clasificación más usados: DoD, USGv6, RIPE-501, RIPE-501bis), software (distinguiendo los diferentes tipos y modalidades de contratación), servicios de telecomunicaciones y capacidades de los equipos humanos.

Posteriormente el estudio presenta un conjunto de buenas prácticas en la definición de requisitos IPv6 en compras públicas:

- En lo que respecta a cuestiones generales, las buenas prácticas sugieren: identificar y planificar necesidades de compras, consultar el mercado antes de iniciar la licitación, involucrar a todas las partes interesadas, definir las características del ofertante, reflejar claramente los requisitos técnicos, definir los criterios de

evaluación, buscar la mejor relación calidad-precio y aprender de la experiencia de cara al futuro.

- En lo que respecta al hardware, sugieren usar un modelo de clasificación de los equipos en 7 niveles, basado en RIPE-501bis, y establecer la compatibilidad en base al cumplimiento o no cumplimiento de aquellos RFCs asociados a IPv6 que cubran las necesidades particulares a considerar para el dispositivo evaluado, en la ubicación concreta de la red donde se requiere su utilización.

- Para el software, se debe exigir que cualquier aplicación que se comunique vía protocolo IP, soporte tanto IPv4 como IPv6 manteniendo el mismo nivel y calidad de servicio establecido. Cualquier desarrollo deberá tener en consideración las pautas generales de calidad de desarrollo de software y los aspectos particulares de IPv6, los cuales aparecen reflejados en los RFCs correspondientes. En particular, las aplicaciones utilizarán nombres de dominio y las correspondientes librerías o APIs de resolución DNS, evitando el uso de direcciones IP literales.. Además, para la evaluación del cumplimiento se sugiere solicitar demostraciones en el caso de desarrollos a medida o la presencia en bases de datos de aplicaciones compatibles en el caso de software comercial.

- En cuanto al tratamiento de las competencias relativas a IPv6 en equipos humanos, se sugiere articularlo mediante compromisos de servicio en el caso de contratos de mantenimiento. En el caso de equipos de desarrollo, las capacidades del equipo humano se reflejarán en las demostraciones y auditorías de código a realizar durante el desarrollo del producto. Por otra parte, en función del nivel de conocimientos IP necesarios para la labor a desempeñar, se deberían considerar como mejoras en los criterios de valoración las certificaciones personales, prefiriendo aquellas neutrales como "IPv6 Ready" del IPv6 Forum, frente a las de fabricantes.

- En cuanto a las comunicaciones y conectividad, las buenas prácticas indican que se debe exigir al proveedor un nivel de servicio independiente del protocolo, sin necesidad de interfaces físicas diferenciadas para IPv4 e IPv6, evaluando su cumplimiento mediante cuestionarios con requisitos específicos dependiendo del tipo de servicio (conectividad a Internet, conectividad VPN, DNS, correo, DataCenter, etc.). Junto con estos cuestionarios se deberá definir un modelo de evaluación para determinar los requisitos de obligado cumplimiento, cuáles son opcionales y cómo se valorarán las mejoras.

Por último, el estudio concluye con recomendaciones concretas para la elaboración de cláusulas a incluir en pliegos técnicos u otros documentos formales:

- Se recomienda incluir a modo de introducción la siguiente cláusula general.

  "Todo sistema (hardware, software, firmware, etc.) o servicio relacionado directa o indirectamente con la transmisión, manipulación o procesamiento de información por medio del Protocolo de Internet (IP), independientemente del

régimen bajo el cual se regule la relación con dicho elemento (adquisición, desarrollo, explotación, contratación, etc.), debe ser capaz de operar plenamente de acuerdo a los estándares comerciales establecidos para el Protocolo de Internet versión 6 (IPv6) y a los aspectos definidos en el RFC2460 (Internet Protocol Version 6 Specification) y el resto de RFCs relacionados con IPv6.

En esta circunstancia, el sistema o servicio debe mantener o mejorar los niveles de servicio, calidad y confianza preestablecidos, tanto con el protocolo IPv4 como con IPv6. Asimismo, el proveedor deberá aportar, durante el periodo de garantía establecido, soporte técnico para ambos protocolos.

Para cualquier excepción al uso o compatibilidad con IPv6 será necesaria autorización explícita y por escrito por parte de la entidad contratante."

- En cuanto al hardware, se recomienda reflejar en el documento principal la descripción funcional del activo, indicando de manera explícita las necesidades de compatibilidad con IPv6, e incluir como anexo el procedimiento para indicar el grado de compatibilidad, el listado de estándares a cumplir y el mecanismo para recopilar la información de cumplimiento.

- En cuanto al software a medida, se recomienda exigir en el pliego el cumplimiento de las buenas prácticas de desarrollo (entre ellas, el uso de nombres DNS en lugar de direcciones literales), la identificación en la fase de toma de requisitos de los requisitos relacionados con la compatibilidad IPv6 y evidencias de realización satisfactoria de pruebas sobre entornos IPv6 equivalentes al de producción.

- En cuanto al software comercial, se recomienda exigir al proveedor una confirmación formal y por escrito de la compatibilidad IPv4 e IPv6 (mediante nombres de dominio) y capacidad funcional sobre el entorno objetivo del software solicitado, complementándola de manera opcional con certificaciones de terceros y en casos específicos, con demostraciones.

- En el caso de equipos humanos, se recomienda seguir la misma aproximación que en el caso del hardware: descripción en el documento principal de las competencias solicitadas y en anexos, procedimientos para evaluar el cumplimiento, especificación detallada de las competencias y modelos para indicar el grado de cumplimiento.

- En el caso de servicios de comunicaciones y conectividad, se recomienda incluir en el documento principal las necesidades de compatibilidad IPv6 requeridas, sin necesidad de interfaces adicionales a las de IPv4 y exigir de forma expresa al proveedor el mantenimiento de los niveles de servicio independientemente del protocolo, dejando en los anexos los procedimientos para evaluar el cumplimiento, el listado con las preguntas específicas junto con los criterios de evaluación y los mecanismos para recopilar esta información.

2. INTRODUCCIÓN

En la Orden PRE/1716/2011, de 9 de junio, se publica el Acuerdo de Consejo de Ministros de 29 de abril de 2011, por el que se aprueba el Plan de fomento para la incorporación del Protocolo de Internet versión 6 (IPv6) en España [1].

El Plan persigue dinamizar la incorporación de IPv6, dando respuesta al gran crecimiento de Internet e impulsando la innovación tecnológica y el despliegue de nuevos servicios en el ámbito de la Sociedad de la Información (reforzando la seguridad de la información y la conectividad y facilitando la administración de redes).

Dentro de las diez medidas incluidas inicialmente en el plan, la número nueve establece la Incorporación de IPv6 como requisito de la compra pública:

"9. El Ministerio de Política Territorial y Administración Pública impulsará la incorporación de IPv6 como requisito en la compra pública en productos y servicios de tecnologías de la información y comunicaciones, tomando como referencia para ello preferentemente normas o recomendaciones internacionales."

Para la definición de los requisitos asociados a IPv6 a introducir en una política pública es necesario analizar el concepto de "compatibilidad IPv6". En los últimos años, varias organizaciones internacionales conscientes de este problema, han invertido un importante esfuerzo en la creación de certificaciones de compatibilidad IPv6. La mayor parte del esfuerzo se ha centrado en la compatibilidad de dispositivos hardware, sin embargo, una política de compras públicas debe englobar otros aspectos como son el software, la contratación de servicios de comunicaciones, contratación de equipos de personas, etc.

Por tanto, todos estos aspectos deben ser considerados, puestos en contexto con respecto a la legislación vigente y documentados en base a experiencias nacionales e internacionales para dar una garantía en la definición de las recomendaciones para los requisitos relacionados con IPv6 en las compras públicas que trata de recoger este documento.

3. CONTEXTO

3.1. LEY DE CONTRATACIÓN DEL SECTOR PÚBLICO

En el ámbito de las Administraciones Públicas españolas, la definición de los requisitos de compras públicas debe desarrollarse bajo el marco definido por la Ley 30/2007, de 30 de octubre, de Contratos del sector público [2][1]. Esta Ley tiene por objeto regular la contratación del sector público, a fin de garantizar que la misma se ajusta a los principios de libertad de acceso a las licitaciones, publicidad y transparencia de los procedimientos, y no discriminación e igualdad de trato entre los candidatos, y de asegurar, en conexión con el objetivo de estabilidad presupuestaria y control del gasto, una eficiente utilización de los fondos destinados a la realización de obras, la adquisición de bienes y la contratación de servicios mediante la exigencia de la definición previa de las necesidades a satisfacer, la salvaguarda de la libre competencia y la selección de la oferta económicamente más ventajosa.

Para el caso concreto del objeto de este documento, que son las compras y contrataciones públicas influenciadas por la incorporación de IPv6 como protocolo de comunicación, los tipos de contratos definidos en la dicha Ley que puede verse afectados son:

- **Contratos de suministro**, definidos inicialmente en el artículo 9 y desarrollados en el Libro IV Efectos, cumplimiento y extinción de los contratos administrativos, Título II Normas especiales para contratos de obras, concesión de obra pública, gestión de servicios públicos, suministros, servicios y de colaboración entre el sector público y el sector privado, Capítulo IV Contratos de Suministro.

  Este apartado recoge la adquisición y el arrendamiento de equipos y sistemas de telecomunicaciones o para el tratamiento de la información, sus dispositivos y programas, y la cesión del derecho de uso de estos últimos. Lo cual será identificado en el presente documento como Hardware (ver apartados 5.2.1 y 6.2) y Software de carácter comercial (ver apartados 5.2.2 y 6.3.2).

- **Contratos de servicio**, definidos inicialmente en el artículo 10 y desarrollados en el Libro IV Efectos, cumplimiento y extinción de los contratos administrativos, Título II Normas especiales para contratos de obras, concesión de obra pública, gestión de servicios públicos, suministros, servicios y de colaboración entre el sector público y el sector privado, Capítulo V Contratos de Servicio.

  Para el caso particular de los Contratos de Servicio, la Ley incluye el Anexo II en el que se reflejan las categorías de servicios referidos para dichos contratos. Dentro de este listado, son de interés:

  - Categoría 1. “Servicios de mantenimiento y reparación”
  - Categoría 5. “Servicios de telecomunicaciones”
  - Categoría 7. “Servicios de informática y servicios conexos”

[1] Nótese que, el 15 de diciembre de 2011 entró en vigor el Texto Refundido de la Ley de Contratos del Sector Público aprobado por Real Decreto legislativo 3/2011 de 14 de noviembre [3] que deroga a la Ley 30/2007 que, aunque no ha cambiado el contenido, sí introduce cambios en la numeración de algunos preceptos.

Estos aspectos aparecen reflejados en este documento como Equipo Humano (ver apartados 5.2.3 y 6.3.3), Comunicaciones y Conectividad (ver apartados 5.2.4 y 6.5) y Software desarrollado a medida (ver apartados 5.2.2.1 y 6.3.1).

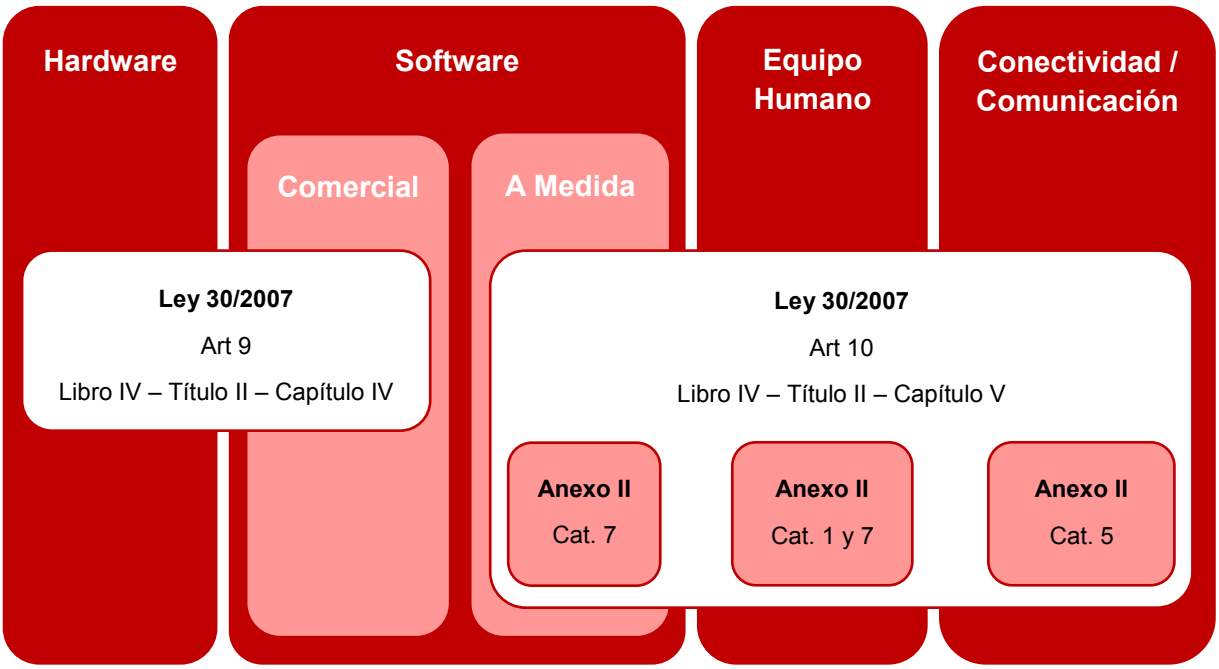


Figura 1: Relación entre los puntos de impacto y su definición en la Ley 30/2007 de Contratos del Sector Público.

Por último, es importante resaltar lo indicado en el Artículo 101 Reglas para el establecimiento de prescripciones técnicas, en el subapartado 3, en el cual se insta a que las prescripciones técnicas se hagan "…en base a especificaciones técnicas contenidas en normas nacionales que incorporen normas europeas, a documentos de idoneidad técnica europeos, a especificaciones técnicas comunes, a normas internacionales, a otros sistemas de referencias técnicas elaborados por los organismos europeos de normalización …".

3.2. GUÍA SOBRE COMPRA PÚBLICA INNOVADORA

La Estrategia Estatal de Innovación (e2i) [3] aprobada por Acuerdo del Consejo de Ministros de 2 de julio de 2010, e incorporada a la Ley de la Ciencia, la Tecnología y la Innovación, se configura como el marco de referencia estable a largo plazo mediante el cual se pretende implicar a todos los agentes políticos, sociales y económicos en la consecución del objetivo común de favorecer la innovación para transformar la economía española en una economía basada en el conocimiento.

La e2i se compone de 5 ejes de actuación, de los cuales el eje 2 persigue potenciar el crecimiento de los mercados innovadores a través de la compra pública para alcanzar una convergencia entre las prioridades sociales y los mercados innovadores.

La Guía sobre Compra Pública Innovadora [5], sobre la que ha informado favorablemente la junta consultiva de contratación administrativa (JCCA) el 28 de octubre de 2011, tiene el compromiso de orientar el desarrollo eficaz de la compra pública innovadora que se abordará trabajando desde el lado de la demanda, esto es, del gestor público que saca a licitación los contratos de compra publica innovadora y desde el lado de la oferta, es decir, de las empresas que compiten en las licitaciones ayudándolas en el juego competitivo a participar y presentar ofertas innovadoras en dichos procedimientos de contratación. Está dirigida a las Administraciones Públicas y demás organismos y entidades del sector público contratantes para la mejor y más adecuada aplicación de los procedimientos de contratación y adjudicación de la contratación pública innovadora.

Si bien esta guía no tiene una implicación directa aplicable al ámbito de los requisitos de compras públicas con IPv6, sí podrían ser tomadas en consideración algunas de las recomendaciones que recoge para aspectos como la definición de criterios de evaluación o la interacción con los ofertantes.

4. ANTECEDENTES SOBRE LA INCORPORACIÓN DE IPv6 EN POLÍTICAS DE COMPRAS

Para complementar el contexto y fundamentos anteriormente expuestos, en este apartado se incluyen una serie de experiencias tanto nacionales como internacionales en el tratamiento de IPv6 en las compras públicas.

Dado el alto volumen de referencias y experiencias disponibles sobre todo a raíz del agotamiento del direccionamiento IPv4, se recogen a continuación sólo los casos considerados como más representativos.

4.1. EVOLUCIÓN DE LAS POLÍTICAS DE COMPRAS PÚBLICAS

Como ya se ha indicado, la problemática de la compatibilidad IPv6 es reciente ya que, a pesar de que el protocolo ya es conocido desde 1992, la incorporación de las particularidades IPv6 en los procesos de compras y contratación públicas tardó bastante tiempo en extenderse. Ha sido en los últimos años, ante la inminente necesidad de realizar la transición a IPv6 por el progresivo agotamiento de direcciones IPv4, cuando la problemática de la compatibilidad IPv6 ha pasado al primer plano.

Antes de esto, las compras y contrataciones públicas apenas consideraban las particularidades de IPv6, por lo que muchas organizaciones se han encontrado y se encontrarán en situaciones en que determinadas adquisiciones realizadas, como por ejemplo dispositivos hardware de comunicaciones, aun cuando por capacidad su vida útil no se ha agotado, no son compatibles con IPv6. Este problema va más allá de un gasto económico dado que puede impactar negativamente en planificaciones más globales, como el despliegue IPv6 a nivel de toda la organización o la capacidad de comunicación con otros agentes.

Por su parte, los fabricantes han sido progresivamente conscientes de las futuras necesidades de sus clientes desde el punto de vista de IPv6, por lo que se realizaron esfuerzos para la adaptación. Ejemplo de ello es que ya en mayo de 2001 CISCO publicó la primera versión comercial de Cisco IOS Software con soporte IPv6 [17] y a partir de octubre de 2001 Microsoft Windows XP [21] ya contaba con pila IPv6.

Progresivamente, alrededor de 2003 (coincidiendo por ejemplo con algunas iniciativas internacionales como la publicación del plan estratégico de adopción de IPv6 del Departamento de Defensa de los EEUU [22] y el lanzamiento de la fase 1 del programa IPv6 Ready Logo [12] en septiembre de 2003) las organizaciones profundizaron en incluir cláusulas en sus pliegos para introducir los requisitos de IPv6, pero esta labor ha sido en general discreta, quedando reducida a añadir frases del tipo “el dispositivo debe ser compatible con IPv6”. Estas indicaciones se incorporaron de forma progresiva en las políticas de compras públicas, sin embargo, la complejidad del protocolo y la ambigüedad que ello genera en el concepto de “compatibilidad IPv6”, junto con el escaso conocimiento técnico sobre IPv6, hacían que no fuesen suficientes para asegurar que las adquisiciones son realmente “compatibles” con el nuevo protocolo.

En este escenario, surgieron varias iniciativas destinadas especificar el concepto de compatibilidad, algunas de las cuales desembocaron en certificaciones de uso extendido (ver apartado 5.1). El objetivo era definir unas pautas para evitar que una adquisición no fuese compatible con IPv6, un protocolo conocido y del que se era consciente que iba a ser aplicado a medio plazo. El resultado fue que a partir de 2005 aproximadamente, surgieron definiciones de políticas y recomendaciones para las compras públicas muy específicas, basadas en listados de RFCs y conjuntos de pruebas exhaustivos. Esta circunstancia coincide en el tiempo, por ejemplo, con el lanzamiento de la fase 2 del programa IPv6 Ready Logo en febrero de 2005.

Esta solución, que ya aseguraba la idoneidad presente y futura de las adquisiciones tenía el inconveniente de que la propia evolución de IPv6, al igual que ocurre con IPv4, generaba actualizaciones en RFCs existentes e incluso nuevos RFCs a considerar, lo que obligaba a la casi continua actualización de las políticas de compras definidas.

En este sentido, desde 2010 la tendencia es la definición de políticas de compras públicas en las que se introduzcan los aspectos generales a cumplir con respecto a IPv6 apoyadas en artefactos que permitan definir las necesidades de bajo nivel, como son los RFCs y las pruebas a realizar.

Este mecanismo permite disponer de una política definida y estática, cuya ejecución práctica se base en elementos con información de bajo nivel y actualizados, pero siempre coherentes con la política, como se puede observar en la experiencia de Tasmania y del Gobierno de EEUU.

Figura 2: Cronograma evolución IPv6.

4.2. INTERNACIONALES

4.2.1. EEUU

La hoja de ruta de EEUU para la transición a IPv6 siempre ha separado la evolución para el gobierno, el ejército y la industria.

Todas las compras del sector público, con la excepción de las del ejército, tienen que seguir la estricta política de contratación IPv6.

El ejército es responsable de su propia política de compras y, hasta hace poco, mantuvo un proceso separado pero similar a otras entidades gubernamentales. En la actualidad, utilizan esencialmente la misma política que el gobierno federal, esto es, el listado de leyes y planes orientados a la adopción de IPv6 por el Gobierno de EEUU que se puede consultar en [23].

A continuación se describe en detalle la evolución y tratamiento de IPv6 en cada uno de los ámbitos identificados en EEUU.

4.2.1.1. Gobierno de EEUU

La primera referencia a la transición a IPv6 por parte del gobierno de Estados Unidos quedó reflejada en el Memorandum 05-22. "Transition Planning for Internet Protocol version 6 (IPv6)" [7] de agosto de 2005. En este memorando se establece Junio de 2008 como fecha para que toda la infraestructura de las agencias gubernamentales hubiese realizado la transición a IPv6. También se incluía la obligación de que los equipos pudieran manejar tanto IPv4 como IPv6 para asegurarse la conectividad con ambos protocolos.

Posteriormente fueron apareciendo nuevas regulaciones como, por ejemplo, en diciembre de 2009 se publicó la norma "Federal Acquisition Regulations" [24], en cuya redacción colaboraron el Department of Defense (DoD), General Services Administration (GSA) and National Aeronautics and Space Administration (NASA). Esta norma refleja la obligatoriedad de introducir los requisitos específicos de IPv6 en los procedimientos de compras y contrataciones públicas de activos o servicios tecnológicos.

En la actualidad el gobierno de los Estados Unidos cuenta con una base de datos de cláusulas de contratos destinada a facilitar la redacción de las ofertas y contratos con sus proveedores. En esta base de datos, para IPv6 se incluye una cláusula específica [25], con fecha de última actualización marzo de 2011:

> ***Title 48: Federal Acquisition Regulations System***
>
> *PART 3452—SOLICITATION PROVISIONS AND CONTRACT CLAUSES*
>
> *Subpart 3452.2—Text of Provisions and Clauses*
>
> *3452.239-70 Internet protocol version 6 (IPv6).*
>
> *As prescribed in 3439.701, insert the following clause in all solicitations and resulting contracts for hardware and software:*
>
> *Internet Protocol Version 6 (MAR 2011)*
>
> *(a) Any system hardware, software, firmware, or networked component (voice,*

video, or data) developed, procured, or acquired in support or performance of this contract shall be capable of transmitting, receiving, processing, forwarding, and storing digital information across system boundaries utilizing system packets that are formatted in accordance with commercial standards of Internet protocol (IP) version 6 (IPv6) as set forth in Internet Engineering Task Force (IETF) Request for Comments (RFC) 2460 and associated IPv6-related IETF RFC standards. In addition, this system shall maintain interoperability with IPv4 systems and provide at least the same level of performance and reliability capabilities of IPv4 products.

(b) Specifically, any new IP product or system developed, acquired, or produced must—

(1) Interoperate with both IPv6 and IPv4 systems and products; and

(2) Have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.

(c) Any exceptions to the use of IPv6 require the agency's CIO to give advance, written approval.

(End of clause)

4.2.1.2. NIST (National Institute of Standards and Technology)

EL NIST publicó en 2008 una guía cuya finalidad era ayudar a las Agencias Federales en la formulación de sus planes para la adquisición de tecnología IPv6. Para conseguirlo se establecieron una serie de perfiles estándar para IPv6 [26] en el Gobierno para que pudieran ser aplicables a todos los usos futuros de IPv6 para entornos no clasificados ni de seguridad nacional.

Estos perfiles pretendían definir una clasificación simple de los equipos de red más comunes y de los requisitos IPv6 mínimos que debían cumplir, así como proporcionar una fuente técnica común sobre la que las políticas del gobierno pudieran sustentarse. Para este fin, los perfiles se definieron como un compendio de especificaciones de protocolos que podían ser obligatorias, recomendadas o deseables.

Además el NIST tiene un completo programa de pruebas de productos, de forma que los vendedores que quieran vender al Gobierno de EEUU deben de probar sus equipos para confirmar que cumplen con los estándares pedidos y, como tal, queda reflejado en un documento con carácter contractual [27][28]. Si posteriormente surge algún tipo de problema con estos equipos en relación con sus capacidades IPv6, estos documentos pueden utilizarse para la gestión de responsabilidades.

4.2.1.3. Departamento de Defensa

En Febrero de 2009 el Departamento de Defensa de EEUU incluyó las pruebas de IPv6 como parte de su procedimiento general de evaluación, certificación e inclusión en la Lista

de Productos Aprobados (UCAPL) [29] (ver apartado 5.1.6). Antes de esta fecha mantenían un programa de pruebas y certificación separado de las pruebas del Gobierno.

4.2.2. Gobierno de Tasmania

Los requisitos de compras públicas y auditoría del Gobierno de Tasmania resumen en un documento de seis páginas una serie de trasfondos, objetivos, definiciones, normas y auditorías para IPv6 [30].

Aunque no surte de ninguna asistencia técnica a sus organizaciones para cumplir estos estándares, esta política es particularmente interesante precisamente por su reducida extensión, lo cual es coherente con la tendencia observada en los últimos tiempos dentro de este campo.

En su contenido, lo más relevante es el modo en el que condensa en un solo punto todo el núcleo de la política, solventando los siguientes aspectos: qué dice la política, cual es su objetivo, qué elementos se ven afectados, qué se considera compatibilidad IPv6 y qué se considera IPv6 nativo.

Estos aspectos se resumen en la siguiente tabla:

Tabla 1: Traducción de la Normativa del Gobierno de Tasmania[2].

Estándar	Las Organizaciones se asegurarán que todos los **nuevos** Activos de Comunicación cuya vida útil se estime que se prolongue más allá del 30 de Junio de 2014[3] tendrán capacidad IPv6 (véase la definición) el día 30 de Junio de 2014.
Objetivo	Permitir a los Organizaciones una transición suave del uso del Protocolo de Internet IPv4 a IPv6 que realizará el Gobierno de Tasmania.
Definición; Activo de Comunicación	Un Activo de Comunicación es un sistema de comunicación, aplicación equipo, periférico servicio, contrato o infraestructura.
Definición: Capacidad IPv6	Se define la "Capacidad IPv6" de un sistema a la capacidad de recibir, procesar y transmitir paquetes IPv6 y/o relacionarse con otros sistemas y protocolos de la misma forma que mediante IPv4. Los criterios para otorgar esta categoría son: Cumplir el perfil estándar IPv6 contenido en el Registro de Estándares del Departamento de Defensa de EEUU (DISR) (una publicación americana al no existir ninguna australiana), manteniendo la interoperabilidad en ambientes heterogéneos con IPv4; compromiso de

[2] Contenido extraído y traducido de [30]

[3] Es de destacar que en el contexto actual de agotamiento de IPv4 el 3 de Febrero de 2011, la fecha indicada de 30 de Junio de 2014 queda tal vez demasiado lejana, teniendo en cuenta además que el 6 de Junio de 2012 se ha confirmado que se produce la puesta en marcha definitiva de IPv6 por parte de grandes proveedores de contenidos y servicios de Internet, de forma global

	actualización a medida que el estándar de IPv6 evoluciona y disponibilidad por parte del licitador de soporte técnico IPv6.
Definición: "IPv6 Nativo"	Se define como "IPv6 Nativo" a aquellos sistemas o productos que son capaces de recibir, procesar y reenviar paquetes de IPv6 y/o relacionarse con otros sistemas y protocolos únicamente mediante IPv6.

Es importante matizar que la definición de IPv6 nativo adoptada por esta norma no es completamente correcta desde un punto de vista técnico, pues IPv6 no ha sido diseñado por IETF para un funcionamiento autónomo e independiente de IPv4, al menos no en la primera etapa de transición y coexistencia, por lo que debería de interpretarse como "…y/o relacionarse con otros sistemas y protocolos mediante IPv6 en coexistencia con IPv4.".

4.2.3. Arabia Saudí

El gobierno Saudí ha establecido una hoja de ruta para implementar IPv6 [31] en su infraestructura. Se ha incluido como requisitos la compatibilidad con IPv6 en un intento de mejorar la inclusión del soporte de IPv6 en las infraestructuras de Telecomunicaciones y fomentar el uso de IPv6.

Obliga que todas las compras de productos de electrónica de red sean capaces de operar en IPv4, IPv6 y un entorno doble-pila IPv4+IPv6, tanto en los sectores públicos como privados e insta a los proveedores de comunicaciones a que sean completamente compatibles con IPv6.

Por último advierte a todos los contratistas que no sean compatibles con IPv6 que pueden correr el riesgo de asumir los costes de conversión cuando se acaben las direcciones disponibles en IPv4 si tienen que realizar cambios urgentes para adaptarse a IPv6.

4.2.4. Reino Unido

En 2009 el Reino Unido publicó un documento llamado "*Next Generation Networks: Procurement Standards, Guidance and Model Clauses*" con el fin de ayudar en la transición hacia a IPv6.

El objetivo de este documento era generar unas guías de buenas prácticas con las que ayudar a los compradores de servicios de telecomunicación de NGN (*Next Generation Networks*, o Redes de Nueva Generación), así como fijar los estándares que los proveedores que desearan trabajar con el gobierno deberían de cumplir. Dichas guías incluían una serie de cuestionarios para proveedores así como clausulas para contratos y guía para la gestión de los contratos y los proveedores.

En la actualidad este documento ha pasado a "archivado" y actualmente los documentos referidos al *Public System Netwok* (PSN) incluyen IPv6 como un requisito a pedir en el futuro [32].

4.3. NACIONALES

4.3.1. Criterios de Seguridad, Normalización y Conservación de las Aplicaciones Utilizadas para el Ejercicio de Potestades

Este documento [33], elaborado por el Consejo Superior de Informática para el impulso de la Administración Electrónica y publicado con fecha 24 de Junio de 2004, expone las pautas para la normalización en los servicios electrónicos prestados por los órganos y entidades del ámbito de la Administración General del Estado con el objeto de facilitar la compatibilidad técnica, la disponibilidad y la interoperabilidad.

En la redacción de dicho documento, aun no tratando de forma particular aspectos relacionados con las compras públicas, ya se queda reflejada la recomendación explicita de utilizar IPv6 siempre que sea posible, así como el uso de tecnologías de tecnologías de conectividad extremo a extremo basadas en IPsec [34][4].

Posteriormente, en 2010, el contenido de este documento fue sustituido por lo establecido en el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica [35], regulado por el Real Decreto 4/2010, de 8 de enero, y el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica [36], regulado por el Real Decreto 3/2010, de 8 de enero.

4.3.2. Gobierno de Aragón: Aragonesa de Servicios Telemáticos

Aragonesa de Servicios Telemáticos, entidad dependiente del Gobierno de Aragón, en 2007 introduce el soporte IPv6 entre las características deseables para los nodos de la Red Urbana u otros equipamientos aunque su cumplimiento no es obligatorio:

> *"Nivel de soporte de IPv6 y funcionalidades disponibles relativas a este protocolo."*

Esta referencia ha sido extraída del "Pliego de prescripciones técnicas para la contratación de los servicios para la mejora de la red de comunicaciones de los centros sanitarios dependientes del departamento de salud" [37] de Noviembre de 2007.

4.3.3. Red.es, RedIRIS y Universidades

Red.es, como responsable de RedIRIS, es uno de los organismos en España cuyos pliegos de contratación obligan la compatibilidad IPv6. De hecho, actualmente RedIRIS es una de las pocas redes Españolas con el certificado del logo "*IPv6 Ready*".

Un ejemplo de esto es el pliego de Agosto de 2011 con nombre "Pliego de prescripciones técnicas que regirán la realización del contrato de "mejora de la infraestructura de

[4] Es de destacar que el uso de IPsec extremo a extremo solo se puede garantizar de manera general en un entorno IPv6, no en IPv4, dada la existencia de direcciones privadas, NAT y la no-obligatoriedad de implementar IPsec en pilas IPv4.

comunicaciones de Red.es" [38]. En este pliego se introducen requisitos de los equipos con capacidad IPv6. Específicamente:

> *"El equipo debe soportar IPv6 según se especifica en el RFC2460 con particular atención a los protocolos y mecanismos siguientes: OSPFv3 (RFC2740), IS-IS, ICMPv6 (RFC2463) MP-BGP (RFC2545) PIMv2 Sparse Mode, MLD, Embedded RP, SNMP, IGMPv3 para IPv6"*

Gracias al empuje de RedIRIS, las universidades españolas están empezando a incluir en sus pliegos la compatibilidad IPv6 en las renovaciones o contrataciones de nuevos equipos.

Así, la **Universidad de Burgos**, dentro de las características mínimas exigidas para los denominados equipos de conectividad de acceso, los equipo de CORE, se indica que deben ser:

> *"Equipamiento compatible con IPv6"*

En este caso, ya se considera una condición de obligado cumplimiento, pero no se detalla exactamente el concepto de compatibilidad, en su "Pliego de prescripciones técnicas para el concurso de renovación de la electrónica de red de la Universidad de Burgos" [41] de Junio de 2010.

La **Universidad de Cantabria**, en su "Pliego de prescripciones técnicas para la contratación del suministro e instalación de un sistema unificado de comunicaciones para toda la red de la Universidad de Cantabria (UNICAN)" [42] de Agosto 2010 incluye como característica de todos los equipamientos "IPv6 Routing Protocol".

Las Universidades de Murcia **y Valencia** tienen desplegadas sus redes con IPv6, con el direccionamiento proporcionado por RedIRIS. En sus pliegos no suelen introducir cláusulas específicas de IPv6, al ir englobado en el mantenimiento global de la red.

4.3.4. Ministerio de Sanidad y Consumo (Actual Ministerio de Sanidad, Servicios Sociales e Igualdad)

Este Ministerio incluye en sus prescripciones técnicas referencias a la compatibilidad IPv6 a fin de que los equipos adquiridos sean capaz de integrarse en la nueva tecnología.

En concreto, por ejemplo en el "Pliego de prescripciones técnicas que regirá en el concurso por procedimiento abierto convocado por el Instituto Nacional de Gestión Sanitaria para la contratación del suministro, instalación y configuración del equipamiento de los servicios de voz, datos, vigilancia, control de accesos y presencia, televisión y audiovisuales, así como el servicio de soporte y mantenimiento del mismo, para el nuevo hospital de Ceuta" [39], de Mayo 2008, en la descripción de los conmutadores de nivel 3 se indica:

> *"2 Procesadoras de alto de alto rendimiento, incluyendo conmutador de tramas por hardware y enrutamiento de paquetes IPv4 y IPv6 velocidad de cable… Routing IPv6 hasta 200 Mpps (En Hardware)"*

Para los equipos de firewall:

> *"Soporte multicast, IPv6, routing y QoS, permitiendo la integración dentro de la red sin interrumpir el tráfico por la misma ni el uso de las aplicaciones"*

Para los conmutadores de nivel 2:

> *"Soporte multicast, IPv6, routing y QoS, permitiendo la integración dentro de la red sin interrumpir el tráfico por la misma ni el uso de las aplicaciones"*

Lo más destacado de este pliego es que incluye un apartado de "Normativa en el que se detallan los estándares (IEEE y REF) que se deben cumplir y a qué tipo de elemento afecta cada RFC, utilizando la siguiente clasificación:

- SP: Sistema Perimetral
- CCN: Conmutador de Conectividad de Núcleo
- CCC: Conmutador de Conectividad Capilar
- PAW: Punto de acceso WIFI

En este sentido se incluyen ya referencias a RFCs relacionados con IPv6, como el RFC 2030) [40].

4.3.5. Ministerio de Industria, Turismo y Comercio (Actual Ministerio de Industria, Energía y Turismo)

Este Ministerio también incluye en sus prescripciones técnicas referencias a la compatibilidad IPv6. En particular, en el pliego de comunicaciones de voz y datos para el Ministerio, tramitado en 2011, se incluye la siguiente cláusula:

> *"Se solicita que tanto el software como el hardware en los equipos y líneas a instalar por el adjudicatario sean compatibles tanto con el protocolo IPv4 como con el protocolo IPv6"*

4.3.6. Junta de Andalucía

En el "Pliego de prescripciones técnicas para la contratación de la red corporativa de telecomunicaciones de la Junta de Andalucía" [43] de Junio de 2010, convocado por la Consejería de Economía, Innovación y Ciencia, se incluyen los siguientes requisitos para los equipos de comunicaciones:

> *"Aquéllos equipos que implementen funcionalidades de encaminamiento deberán soportar las especificaciones de IPv6, permitiendo si fuera requerida la posibilidad de implantarlo en la totalidad de la red, así como de desarrollar en cualquier momento distintos escenarios parciales que requieran las funcionalidades de dicha especificación. Los licitadores valorarán en sus ofertas el coste adicional de las actualizaciones de software si éstas fueran necesarias."*

Para el equipamiento utilizado en cada una de las redes se indica lo siguiente:

> *"El equipamiento suministrado para la solución técnica […] tendrá la posibilidad de soportar protocolo IPv6 de serie o mediante actualización software. Se valorarán soluciones que permitan la incorporación del protocolo IPv6 como solución técnica de conectividad."*

A modo de resumen, dentro de los requisitos globales, se indica:

> *"De forma general, aquellos equipos que implementen funcionalidades de encaminamiento deberán soportar las especificaciones de IPv6, permitiendo si fuera requerido por las necesidades del servicio, la posibilidad de implantarlo como solución global, así como desarrollar en cualquier momento distintos escenarios parciales que requieran las funcionalidades de dicha especificación."*

4.3.7. Diputación de Cáceres

El Área de Hacienda, Economía y Patrimonio de la Diputación de Cáceres, en Abril de 2011, en su "Pliego de cláusulas administrativas particulares que regirá la contratación del servicio de telecomunicaciones de la Excma. Diputación provincial de Cáceres, centros dependientes, organismos autónomos, sociedad Agropecuaria y consorcio medio XXI" [44], dentro de las premisas de las condiciones generales de este pliego indica lo siguiente:

> *"Soporte IPv6, en todo el equipamiento incluido en el contrato, donde dicha característica sea aplicable"*

En las descripciones particulares de los elementos incluidos en la licitación se hacen referencias como las siguientes:

> *"Balanceador de carga y proxy inverso: "Gateway IPv4/IPv6".*
>
> *Equipos de chasis (electrónica de red): "Soporte de protocolos de redundancia tipo VRRP y VRRPv3 (IPv6)."*

5. COMPATIBILIDAD IPv6

5.1. MODELOS DE COMPATIBILIDAD IPv6

Para asentar las pautas para la realización de compras de activos y contrataciones de servicios orientadas a la futura compatibilidad de estos con IPv6, el primer paso es establecer el concepto de "compatibilidad" con IPv6.

En los últimos años, ante la falta de una definición global del término de compatibilidad IPv6, varias organizaciones han generado su propia especificación, lo cual ha desembocado en la aparición de varias iniciativas internacionales orientadas la certificación de dispositivos compatibles con IPv6.

Estas certificaciones simplifican los procesos de análisis de compatibilidad a realizar por una organización, siempre y cuando los requisitos para la certificación sean coherentes con las necesidades de ésta y la entidad certificadora sea de confianza.

En este sentido existen varias iniciativas internacionales, entre las que destacan:

5.1.1. ISO/IEC 17025

En ella se describen todos los requisitos que los laboratorios de ensayo y calibración deben cumplir si desean demostrar que son técnicamente competentes y que son capaces de producir resultados técnicamente válidos.

Esta norma se utiliza como referencia para los programas de compatibilidad [3].

5.1.2. USGv6[5]

En el *OMB Memorandum M-05-22 [7]* se insta al *National Institute of Standards and Technology* (NIST) al desarrollo de la infraestructura técnica necesaria para el soporte a gran escala de la adopción del IPv6 en el gobierno de Estados Unidos (US Government – USG).

Como respuesta, el NIST desarrolló un perfil de los estándares técnicos a cumplir para la adquisición de dispositivos de red con capacidades IPv6 [8]. Este perfil incluye los RFCs involucrados y otras capacidades opcionales para estos elementos.

Además del perfil, se estableció un programa que permitiese a los laboratorios acreditados la realización de test de cumplimiento del perfil definido [9].

Finalmente, el Gobierno de EEUU publicó la **USGv6 Buyer's Guide[10],** que es una guía destinada a las Agencias que pretendan adquirir equipamiento de red, incluyendo hardware (equipos, elementos de infraestructura o protección) y software.

[5] La descripción completa del caso de Estados Unidos se incluye en el apartado 4.2.1.

5.1.3. Programa "IPv6 Ready Logo"

El IPv6 Forum [11] (consorcio internacional formado por entidades pertenecientes a la Industria, Investigación y Educación con la misión de promover IPv6) creó en 2003 el *Programa IPv6 Ready Logo* [12]: un programa de pruebas de interoperabilidad y conformidad de dispositivos con IPv6 orientado a incrementar la confianza de los usuarios demostrando que IPv6 está disponible y preparado para su uso [13].

Las especificaciones de este test están coordinadas por un comité y sus principales objetivos son:

- Verificación de la implementación e interoperabilidad de los productos IPv6.
- Proporcionar acceso a herramientas gratuitas de autocomprobación.
- Disponer de laboratorios en todo el mundo dedicados a proporcionar asistencia o servicios de pruebas.

Una vez certificado un producto, este podrá hacer uso del logo acreditativo. Además, estos productos aparecen en una lista disponible en la web del programa en la cual se presentan dos niveles de clasificación:

- Fase 1 – IPv6 Ready Logo Silver. Productos que han superado un total de 170 pruebas. Este modelo ha sido descontinuado.
- Fase 2 – IPv6 Ready Logo Gold. Productos que han superado un total de 450 pruebas. Modelo de referencia en este momento.

5.1.4. IPv6-to-Standard

Los equipos de trabajo IETF (*Internet Engineering Task Force*) IPv6 y el IPv6 Maintenance (6man) trabajan de forma conjunta para avanzar el núcleo de las especificaciones IPv6 hacia el último paso del proceso de estandarización de IETF.

Los protocolos IETF son elevados a nivel de *Internet Standard (STD)*, un nivel de referencia para tecnologías y metodologías aplicables a Internet, cuando se ha obtenido una experiencia operativa significativa y satisfactoria.

En este marco, "IPv6-to-Standard" insta a los proveedores de hardware, software, servicios, aplicaciones (y otros) con soporte IPv6 a participar en este proceso identificando sus productos compatibles con IPv6, los cuales quedan registrados en la página web del proyecto [14].

Sin embargo, aunque es una referencia válida, recientemente el IETF ha decidido que la situación de facto por la cual la industria global considera como estándares los RFCs, y la falta de recursos por parte de la comunidad IETF para elevar los mismos a la categoría de STD, hacen necesario cancelar el estatus de "STD". Así por ejemplo muchos protocolos actuales de MPLS son solo RFCs y no llegarán a la fase de STD, por su discontinuación, y exactamente ocurrirá con los referidos a IPv6 y cualesquiera otros protocolos.

5.1.5. UNH-IOL IPv6 Testing Consortium

La InterOperability Laboratory de la Universidad de New Hampshire (UNH-IOL), como parte del programa IPv6 Ready Logo, ofrece programas colaborativos de pruebas de más de 20 tecnologías de almacenamiento y gestión de redes de datos. Cada uno de estos programas, denominados "*consortiums*" [15], representan la colaboración entre los principales elementos de la industria, los equipos de pruebas y proveedores de servicios con el objetivo conseguir un beneficio mutuo en los siguientes aspectos:

- Reducción de gastos en gestión de calidad e investigación y desarrollo.
- Disposición de una verificación por un agente externo de confianza.
- Reducción del tiempo de lanzamiento de un producto.
- Orientación para la aceptación por parte de la industria.

En el caso particular del *consortium* de IPv6, está orientado a la reducción del tiempo de lanzamiento de los productos de los participantes y a la aceleración de la adopción de IPv6. Con el fin de mantener y fortalecer los servicios, este *consortium* cumple la certificación ISO/IEC 17025 y ofrece test acreditados USGv6 en la línea del *Programa IPv6 Ready Logo*.

5.1.6. DoD (JITC /DISA) IPv6 Product Certification

El programa de certificación de productos IPv6 del Departamento de Defensa de los Estados Unidos surge en 2005 con el fin de generar una base de datos de productos compatibles con IPv6 a ser utilizada para todos los procesos de adquisición de equipamiento TI por parte del Departamento de Defensa.

Se generó un documento que recogía la definición particular del Departamento de Defensa del concepto "capacidad IPv6". En él se clasificaban los productos en seis clases y se indicaba su correspondencia con los RFC, atendiendo a los siguientes niveles de obligatoriedad:

- *MUST*: El estándar es obligatorio.
- *MUST NOT*: El estándar o comportamiento no debe darse.
- *SHOULD*: El estándar es opcional, pero recomendable.
- *SHOULD NOT*: El estándar o comportamiento no es deseable.
- *MAY*: El estándar o comportamiento es opcional.
- *SHOULD+*: El estándar es opcional en este momento, pero será requerido a corto plazo.

Los requisitos planteados en este programa por el DoD han quedado obsoletos y actualmente el DoD utiliza los procedimientos habituales del Gobierno de EEUU.

5.2. PUNTOS DE IMPACTO

Dentro de los contratos públicos, existen varios tipos de elementos que pueden verse afectados por el uso de la tecnología IPv6. Por tanto, a la hora de preparar los pliegos y especificaciones técnicas para estos tipos de elementos, es necesario tener en cuenta el impacto que puede suponer considerar la compatibilidad IPv6 como requisito ineludible.

En general, no basta con determinar que el elemento es “compatible con IPv6”, concepto abierto a interpretación, sino que además al existir un periodo de coexistencia con IPv4, el equipo debe de ser capaz de funcionar con IPv4 (en modelo doble-pila y únicamente con IPv6), sin que su funcionamiento afecte negativamente a dispositivos que sigan operando sólo en IPv4 o sólo en IPv6. En estos casos en los que los elementos proporcionen otros mecanismos de transición entre IPv4 e IPv6, se habrá de determinar también qué funcionalidad ofrecen dentro de qué arquitectura de transición.

5.2.1. Hardware

El tipo de elemento que más claramente se ve afectado por la incorporación del protocolo IPv6 es el hardware. En este sentido, por su alta implicación, se ha invertido un gran esfuerzo en estandarizar el concepto de “compatibilidad IPv6” aplicado al hardware, generalmente basándose en determinados RFCs que el dispositivo debe cumplir.

El termino hardware es una generalización ya que no todo el hardware se verá afectado por el proceso de transición a IPv6. Ciertos dispositivos que no están directamente relacionados con procesos de comunicación o conectividad quedan fuera del grupo de elementos afectados, como son los periféricos (monitores, teclados,…) o componentes internos no relacionados con conectividad (memoria, tarjetas de video,…), obviamente salvo que se comuniquen con IP.

Para generalizar y facilitar la definición de compatibilidad, lo habitual es establecer una clasificación de alto nivel de los tipos de dispositivos afectados y determinar, para cada uno de ellos, cuales son los RFCs de obligatorio cumplimiento, cuales son recomendables y cuales opcionales.

Muy relacionado con el hardware, otro aspecto a tener en cuenta en ciertos dispositivos es el firmware. Debe analizarse la incidencia de la transición a IPv6 en el firmware de los dispositivos, el cual debe evolucionar a la vez que evolucionan los estándares de IPv6. Si bien esta actualización no podrá exigirse desde el punto de vista del pliego, por quedar en manos de los grandes fabricantes, si deberá tenerse en consideración estas actualizaciones a la hora de definir contratos de mantenimiento.

A continuación se recogen los diferentes modelos de clasificación más utilizados para los dispositivos hardware en el ámbito de IPv6.

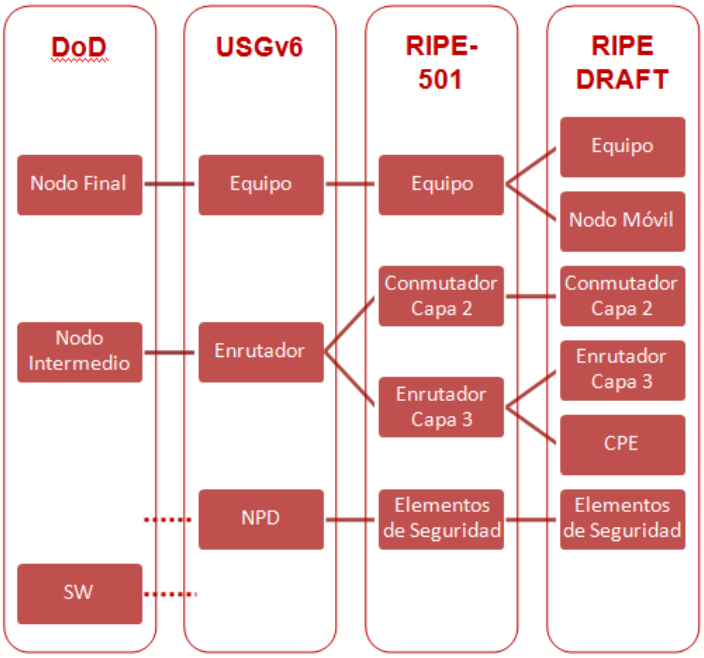


Figura 3: Relación entre las propuestas de clasificación de dispositivos hardware afectados por la compatibilidad IPv6.

5.2.1.1. Clasificación de elementos según USGv6

De cara a USGv6, los dispositivos que pueden verse afectados por la incorporación de IPv6 y por tanto son susceptibles de ser testeados, se clasifican de la siguiente forma:

- **Enrutador**: Nodo que interconecta subredes para el envío de paquetes. Su principal propósito es soportar los protocolos necesarios para permitir la interconexión de distintas subredes a nivel de capa de red.
- **Equipo**: cualquier nodo que no sea un enrutador. Su principal propósito es dar soporte a protocolos de aplicación que son origen o destino de la comunicación.
- **NPD**: Cortafuegos y dispositivos de protección y/o prevención de intrusos que examinan, bloquean o modifican el tráfico de red en virtud de la seguridad.

5.2.1.2. Clasificación de elementos según DoD (JITC /DISA) IPv6 Product Certification

Este proyecto, en la Guía "IPv6 Standard Profiles for IPv6 Capable Products Versión 5.0" de julio de 2010, establece una clasificación de los productos de acuerdo a su arquitectura y rol en una red IPv6.

- **Nodo final**: dispositivos con comportamiento de Equipo.
  - Equipo / Estación de trabajo
  - Elemento de Red o Servidor sencillo
  - Servidores
- **Nodo intermedio**: dispositivos con comportamiento de enrutador

  - Enrutador
  - Encaminador
  - Activo de Información
- **Software compatible con IPv6**: elementos software.

5.2.1.3. Clasificación de elementos según RIPE

El RIPE proporciona un documento, el RIPE-501 "Requirements For IPv6 in ICT Equipment" [16], en el cual se establece una clasificación de equipos en 4 grupos:

- **Equipo**: cliente o servidor.
- **Conmutador de capa 2**
- **Enrutador, o conmutador de capa 3.**
- **Elementos para asegurar la seguridad en la red** (Cortafuegos, IDS, etc.).

Como se puede observar, esta clasificación es similar a la definida por USGv6, simplemente separando en un grupo propio los elementos de red de nivel 2.

Sin embargo, en la actualidad se está trabajando en una nueva versión de este documento (RIPE-501bis), de la cual ya existe una versión en borrador, en la cual se pasa de 4 a 7 grupos:

- **Equipo**: cliente o servidor.
- **Conmutador de capa 2.**
- **Enrutador, o conmutador de capa 3.**
- **Elementos para asegurar la seguridad en la red** (Cortafuegos, IDS, etc.).
- **CPE (*Customer Premises Equipment)***, que agrupa los dispositivos que se encuentran en las instalaciones u hogares de los clientes con el fin de servir de puntos de conexión. A pesar de que estos dispositivos son generalmente enrutadores, los requisitos exigibles son diferentes a los de un enrutador para empresa.
- **Nodo móvil (Mobile node)**, en este contexto se considera que un nodo móvil es un dispositivo que se conecta vía alguna especificación 3GPP (como por ejemplo 3G, GPRS/UMTS o LTE).
- **Balanceador de Carga (Load balancer)**, dispositivo de red que distribuye el trabajo entre múltiples equipos, servidores u otros recursos con el objetivo de optimizar el uso de los recursos, maximizar el rendimiento, minimizar el tiempo de respuesta y evitar la sobrecarga.

5.2.2. Software

El siguiente punto de impacto a considerar en la transición a IPv6 son las aplicaciones software. La definición de las pautas para medir la compatibilidad IPv6 en este ámbito es un aspecto complejo y, sobre todo, un aspecto en el que se ha hecho poco hincapié porque la

mayoría de las aplicaciones están desarrolladas de forma que pueden abstraerse de los protocolos de comunicación[6]..

Inicialmente una posible clasificación de los tipos de software a considerar en relación a IPv6 sería la siguiente:

- **Firmware**: bloque de instrucciones de programa para propósitos específicos, grabado en una memoria de tipo no volátil, que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo. La mayoría de los dispositivos de comunicación cuentan con un firmware, el cual debe contar con la capacidad de gestionar las particularidades de IPv4 e IPv6, de forma aislada o conjunta (doble-pila o pila-híbrida). Por sus características se considera tanto una parte del hardware (está diseñado para un dispositivo concreto) como software, ya que proporciona la lógica de la aplicación. A nivel de este documento, el caso particular del firmware se tratará como un elemento del hardware.
- **Sistema operativo (SO)**: software de una estación de trabajo o servidor que proporciona el entorno sobre el que otras aplicaciones podrán ejecutarse. El SO incluye el software de comunicaciones (drivers) que proporciona la capacidad de interacción con el protocolo IPv4 e IPv6 y un interfaz de programación de aplicaciones (API) que permite que las aplicaciones compatibles con IPv4 e IPv6 hagan uso de estas características.
- **Middleware:** software que proporciona una capa de funcionalidad entre el sistema operativo y las aplicaciones o entre el hardware de la plataforma y el sistema operativo.
- **Aplicación:** software con una funcionalidad determinada. La evaluación de si una aplicación es o no compatible con IPv4 e IPv6 depende de si maneja o no direcciones IPv4 e IPv6 y otras características específicas de IPv4 y/o IPv6 disponibles a través del API.

[6] La excepción es cuando una aplicación, software o incluso una página web utiliza direcciones IP literales, lo cual impacta lógicamente no solo en IPv6 sino también en IPv4

Figura 4: Capas de software.

En este sentido, los fabricantes deben analizar el código de sus aplicaciones y determinar el grado de compatibilidad con IPv6. Es importante considerar que una aplicación o sistema operativo no puede ser analizado de forma aislada sino que es necesario tener en cuenta la interacción con el hardware u otro software, aunque son relativamente extraños los casos en que esto pueda tener implicaciones al respecto de IPv6.

Para definir el impacto de la transición a IPv6 en lo relativo al software podríamos distinguir dos niveles:

- **Pérdida de funcionamiento**: Si al realizar la transición, el software deja de funcionar. Esta situación puede ser debida a que en el proceso de arranque de la aplicación necesite algún tipo de dato como la dirección IP del sistema y al encontrarse con un dato diferente a una dirección IPv4 sea incapaz de gestionarla y falle en este proceso. La mayoría de las aplicaciones tienen la capacidad de abstraerse de los protocolos de red si utilizan nombres DNS en lugar de direcciones literales, por lo que las pérdidas de funcionamiento suelen quedar restringidos a tipos muy concretos de software.

- **Pérdida de funcionalidad,** si cuando se realiza la transición, el software se pierde alguna capacidad. Esta pérdida puede ser debida a que las direcciones IPv4 y las direcciones IPv6 no son consideradas por la aplicación como el mismo tipo de datos, por lo que algunas aplicaciones pueden tener problemas para manejar direcciones IPv6.

  El impacto de la perdida de funcionalidad y la complejidad y urgencia de la adaptación de la aplicación depende del objetivo de la misma: una aplicación que disponga de un apartado de configuración de acceso a Internet vía proxy, una aplicación de recopilación de información de registro con una base de datos de direcciones IP, etc.

En un proceso de adquisición habría que distinguir dos tipos software: desarrollos a medida o aplicaciones comerciales, independientemente de las tipologías y posibles impactos identificados anteriormente. El tratamiento de compatibilidad y adaptación para cada uno de los tipos requiere un análisis diferenciado.

5.2.2.1. Software desarrollado a medida

Las aplicaciones desarrolladas o adaptadas por encargo son uno de los puntos más delicados a la hora de analizar la compatibilidad IPv6 ya que puede resultar difícil conocer el impacto real de los cambios necesarios para la adaptación del software, siendo la empresa encargada del desarrollo la fuente más fiable para realizar el análisis del impacto de los cambios necesarios sobre la aplicación. En este sentido, es poco probable que la empresa responsable del desarrollo avance en la compatibilidad IPv6 si no existe un compromiso anterior o nueva obligación para con su cliente[7].

5.2.2.2. Aplicaciones comerciales

Par las aplicaciones comerciales, es el fabricante quien debe garantizar la compatibilidad con IPv6 generando nuevas versiones o parches, por lo que la primera fuente de información en este sentido es la documentación oficial ofrecida por el desarrollador. Sin embargo, debido a la falta de consenso existente en términos como “compatibilidad IPv6” o “preparado para IPv6”, varias organizaciones independientes ha generado bases de datos de compatibilidad de aplicaciones de uso habitual y han publicado esta información[8].

5.2.3. Equipo Humano

Se engloban en esta categoría aquellas relaciones con proveedores en las que, como parte de su oferta, se incluye la descripción de perfiles personales atendiendo a unas exigencias mínimas en cuanto a conocimiento en IPv6.

Un aspecto muy importante es que, en estos casos, no todo el personal incluido en contratos relacionados con IPv6 necesita certificar sus conocimientos, sino que sería necesario restringir estas exigencias a aquel personal que necesite aplicar estos conocimientos de forma directa y continua en el desempeño de sus funciones.

Algunos ejemplos de contratos a los que les aplicaría este punto de impacto serían: equipo humano encargado de tareas de soporte y mantenimiento asociadas a un hardware o software, personal de los Servicios de Asistencia Técnica de los proveedores de comunicaciones, formadores, etc.

---

[7] En particular, es fundamental exigir y comprobar que las aplicaciones no utilizan direcciones literales, sino nombres DNS, y que llaman a las librerías o APIs adecuadas para su resolución. En el caso en que almacenen dichos datos, aun de forma temporal, los registros o bases de datos donde se produzca dicho almacenamiento han de contemplar un tamaño mínimo de 128 bits. Además, si es necesario “interpretar” o procesar de algún modo dichas direcciones, se debe tener en cuenta la diferencia entre el formato de las mismas.

[8] En este caso, aunque en menor grado, también podría darse la situación descrita para el caso anterior de uso de direcciones literales.

Obsérvese que este punto puede presentar una cierta dificultad. Si bien el grado de complejidad de IPv6 es equiparable al de IPv4 (y en algunos aspectos, significativamente menor), sus características implican cambios importantes en la forma de trabajar respecto de las prácticas habituales en IPv4. Para evitar el impacto negativo de hacer las cosas en IPv6 igual que con IPv4 (lo que puede afectar a la seguridad, estabilidad y visibilidad de la red), es conveniente disponer de personal con experiencia real de campo en IPv6, que pueda complementar con la práctica la información existente en los RFCs y resto de documentos técnicos.

Del mismo modo que ocurre con el resto de puntos de impacto, es necesario establecer pautas que permitan evaluar de forma objetiva qué consideramos por "conocimiento en IPv6". Para ello, una buena referencia puede ser el programa neutral del IPv6 Forum "IPv6 Ready", independiente de fabricantes y por tanto con un enfoque objetivo.

5.2.4. Comunicaciones y Conectividad

Esta categoría incluye la relación con los proveedores de comunicaciones que prestan servicios a una organización. En estos contratos es necesario poder determinar si el proveedor tiene capacidad para cubrir los requisitos actuales y futuros de la entidad contratante, pero manteniendo los requisitos de calidad y capacidad adecuados.

A este respecto, diferentes organismos y proveedores han publicado documentación sobre los requisitos de comunicaciones y conectividad, tales como:

- **IPv6 Act Now**. Proyecto soportado por RIPE NCC en el que se aporta información a cada uno de los interesados en la transición a IPv6: Pequeñas y grandes empresas, ISPs y Gobiernos [17].
- **CISCO**, dentro de la documentación aportada desde su Wiki, presenta una lista de preguntas a realizar a un proveedor de conectividad para determinar su capacidad con respecto a IPv6 [18].
- **Energy Sciences Network (ESnet)**. Red de comunicaciones servida por el Departamento de Energía de los EEUU para la colaboración entre laboratorios, universidades y otros centros de investigación a nivel internacional. Entre la documentación ofrecida, aporta una guía de implementación IPv6 [19].

6. BUENAS PRÁCTICAS EN LA DEFINICIÓN DE REQUISITOS IPv6 EN COMPRAS PÚBLICAS

La definición o actualización de una política que regule la contratación de servicios y/o la adquisición recursos siempre que aparece una nueva tecnología de uso masivo es fundamental para asegurar que las compras o contratos a realizar se lleven a cabo con la suficiente confianza, eficiencia y ahorro de recursos públicos.

A continuación se analizan las particularidades de cada uno de los puntos de impacto identificados en el punto 5.2, concretando qué aspectos deben de considerarse en cada caso.

6.1. ASPECTOS GENERALES

En general, tomando como referencia estándares internacionales, existen más de 500 RFCs [27][45][46] relacionados en mayor o menor medida con el protocolo IPv6. Además, cada uno de estos RFCs puede tener diferente grado de influencia sobre uno o más tipos de elemento (puntos de impacto).

Para que este planteamiento sea manejable, es necesario establecer una organización adecuada para la preparación de las condiciones de contratación o compra (pliegos y contratos) de los licitadores y, también, indicar a los ofertantes como deben justificar el cumplimiento de estas condiciones de forma sencillamente evaluable.

Por tanto, los requisitos establecidos en las compras públicas deben concretarse en las tres fases que corresponden a cualquier contratación:

- **Definición de los requisitos técnicos**, lo que incluiría la forma y redacción que toman dichos requisitos en un determinado pliego, es decir, cómo presentar la información a los ofertantes.
- **Elaboración de ofertas** que deberán acreditar o justificar el cumplimiento de los requisitos establecidos en el pliego correspondiente, es decir, cómo los ofertantes aportan la información requerida.
- **Valoración de ofertas**, fase en la que es necesario disponer de los recursos necesarios para valorar convenientemente tanto los requisitos definidos como obligatorios como deseable u opcional, es decir, cómo evaluar la información aportada por los ofertantes.

6.1.1. Características de una Política de Compras Públicas

Una Política de Compras Públicas, como mecanismo para la garantía de los requisitos establecidos en un proceso de contratación, debería contemplar las siguientes características:

- Efectivo: asegura que el producto que pase la validación sea adecuado para su objetivo.
- Sencillo: la realización de dicha validación debe ser lo más sencilla posible.

- Concreto: no debe generar ambigüedades ni para el licitador ni para el ofertante.
- Flexible: la definición de la validación debe cubrir las necesidades generales, adaptándose a las diferentes circunstancias que puedan darse.

6.1.2. Buenas Prácticas en Políticas de Compras Públicas

A continuación se indican una serie de buenas prácticas generales orientadas a la definición de una política de compras públicas adecuada, flexible y de uso extendido.

Identificar y planificar necesidades de compras

- Disponer de personal técnico formado y capaz de gestionar la adquisición de soluciones acordes a las necesidades reales.

Consultar el mercado antes de iniciar la licitación

- Identificar soluciones existentes en el mercado consultanto a potenciales proveedores siempre que se respete la transpariencia del proceso.
- Lanzar consultas a organismos equivalentes sobre las soluciones adoptadas antes problemas similares.
- Mantener actualizada la información sobre certificaciones, bases de datos de compatibildiad y RFC relacionados.

Involucrar a todas las partes interesadas

- Identificar a expertos técnicos y asesores legales.
- Asegurar su participación a lo largo del procedimiento.

Definir las características del ofertante

- Prestar atención al cumplimiento por parte del ofertante de los requisitos de solvencia técnica y financiera.
- Solicitar y tener en consideración experiencias similares aportadas por el ofertante.

Reflejar claramente los requisitos técnicos

- Aportar esta información en el proceso de licitación.
- Definir claramente el alcance de estos requisitos, determinan qué elemento se ve afectado por cada aspecto.
- Aportar mecanismos que faciliten y simplifiquen a los ofertantes informar sobre el cumplimiento de dichas especificaciones.

Definir los criterios de evaluación

- Especificar todos los criterios automáticos (disponer de una certificación, cumplir un RFC) y su peso en la evaluación.

Buscar la mejor relación calidad-precio

- Aplicar el criterio de oferta económica más ventajosa: conjunta los costes totales de toda la vida del contrato y otros aspectos importantes como la calidad y méritos técnicos de la oferta.
- Decidir criterios que reflejen estos aspectos y reflejarlos de forma clara en las licitaciones.

Aprender de la experiencia de cara al futuro

- Documentar y compartir con otras administraciones las experiencias obtenidas.
- Establecer procedimientos de evaluación para mejorar los procedimientos de compra pública.

6.1.3. Tipos de Contratos

Los puntos de impacto analizados en el apartado 5.2 sirven para acotar las condiciones que deben ser cumplidas por el ofertante y para modelar mecanismos específicos de comprobación. Sin embargo, es poco probable encontrar contratos en el que se aborde únicamente uno de estos tipos de elementos, sino que lo habitual es que cuando una organización prepara una licitación, el propio objetivo de la misma haga necesario incluir varios puntos de impacto de los aquí identificados.

De esta forma, según cuál sea el objeto del contrato, será necesario identificar los puntos de impacto relacionados de forma que se consideren los requisitos específicos de IPv6 de cada uno de ellos.

En este apartado se citan, con carácter meramente orientativo, los principales casos de caso de contratación con los que pueden encontrarse las organizaciones y cuáles serían los

puntos de impacto aplicables en cada caso. En este sentido, los principales tipos de contratos o compras identificados serían:

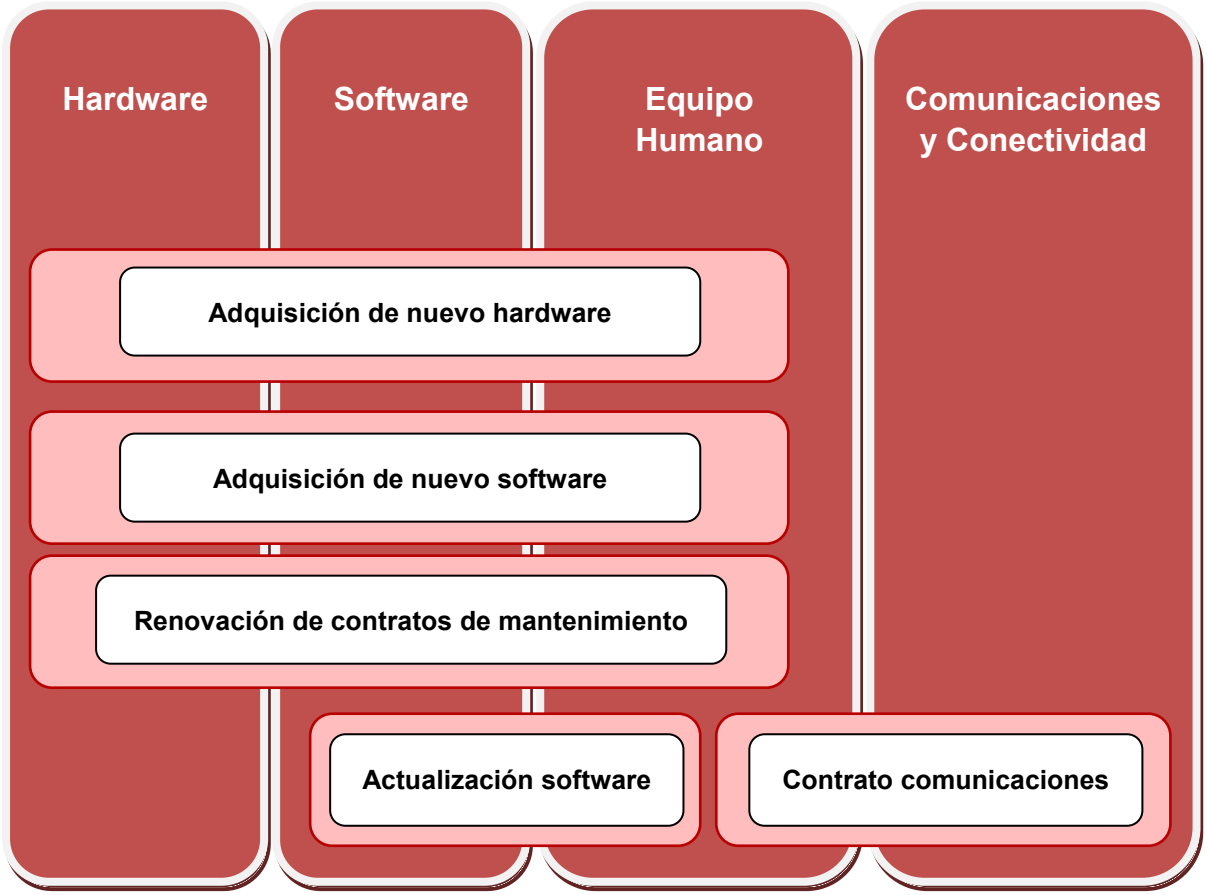


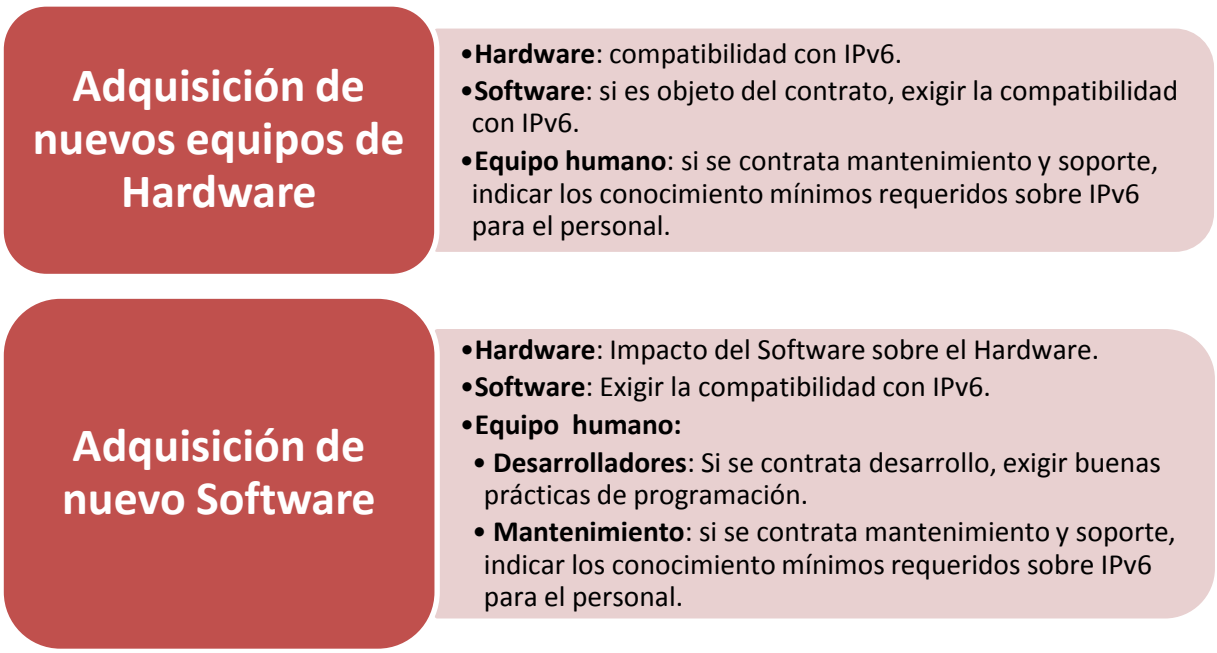
Figura 5 . Relación Contratos Tipo - Puntos de impacto.

- **Adquisición de nuevos equipos hardware**. Este tipo de contrato tiene como principal punto de impacto el hardware, el cual es el objetivo principal del mismo y debe de ser compatible con IPv6. Además, debe de tenerse en cuenta el software asociado al dispositivo si este también está incluido en el contrato, sobretodo aspectos como la capacidad IPv6 ofrecida por el Sistema Operativo. Por último, si el contrato incluye un servicio de soporte y mantenimiento, será necesario establecer los conocimientos con respecto a IPv6 mínimos requeridos por el equipo humano que desempeñe esta actividad.
- **Adquisición de nuevo software**. En cualquier adquisición de software debe de garantizarse la compatibilidad con IPv6 y el uso de nombres DNS (en contraposición al de direcciones literales) desde el momento inicial o en un momento dado, siempre acorde con la planificación de transición de la organización. Si el software es comercial y esta compatibilidad no está en el plan del fabricante, la contratación debería de orientarse hacia otra aplicación. Como en al caso anterior, si junto con el

software se contrata un servicio de mantenimiento y soporte, será necesario establecer los conocimiento mínimos en IPv6 del equipo de trabajo.

- **Renovación de contratos de mantenimiento**. Si una organización tiene previsto iniciar su proceso de transición a IPv6 dentro de la duración establecida en un contrato de mantenimiento, debe de asegurarse de que el nuevo equipo de mantenimiento cuente con los conocimientos IPv6 necesarios. Así mismo, si el contrato de mantenimiento se refiere a un hardware o Software concreto, dentro de las competencias del nuevo contrato se debe de incluir la actualización del firmware del hardware y de la instalación o generación de nuevas versiones del software para garantizar su funcionamiento en el periodo de transición IPv6.
- **Contrato de comunicaciones**. Es necesario asegurar que el proveedor de comunicación tiene la capacidad necesaria para dar soporte a la organización contratante en su proceso de transición a IPv6 sin que esto suponga una pérdida de calidad de servicio o se incumplan los niveles de servicio establecidos. Asimismo, puede exigirse que el equipo de trabajo que forme parte del Servicio de Asistencia Técnica tenga conocimiento suficiente sobre IPv6.
- **Actualización de Software**: Si la organización dispone de un Software que debe de ser actualizado a causa de la transición a IPv6, deberá de exigirse un plan de desarrollo por personal especializado, un desarrollo siguiendo guías de buenas prácticas y que el software sea independiente de la capa de red. Además deberá de pedirse un plan de actualización en caso de que sea necesario modificar el software en un futuro cercano.

En la siguiente figura se muestra un resumen de estos tipos de contrato y las consideraciones para cada impacto:



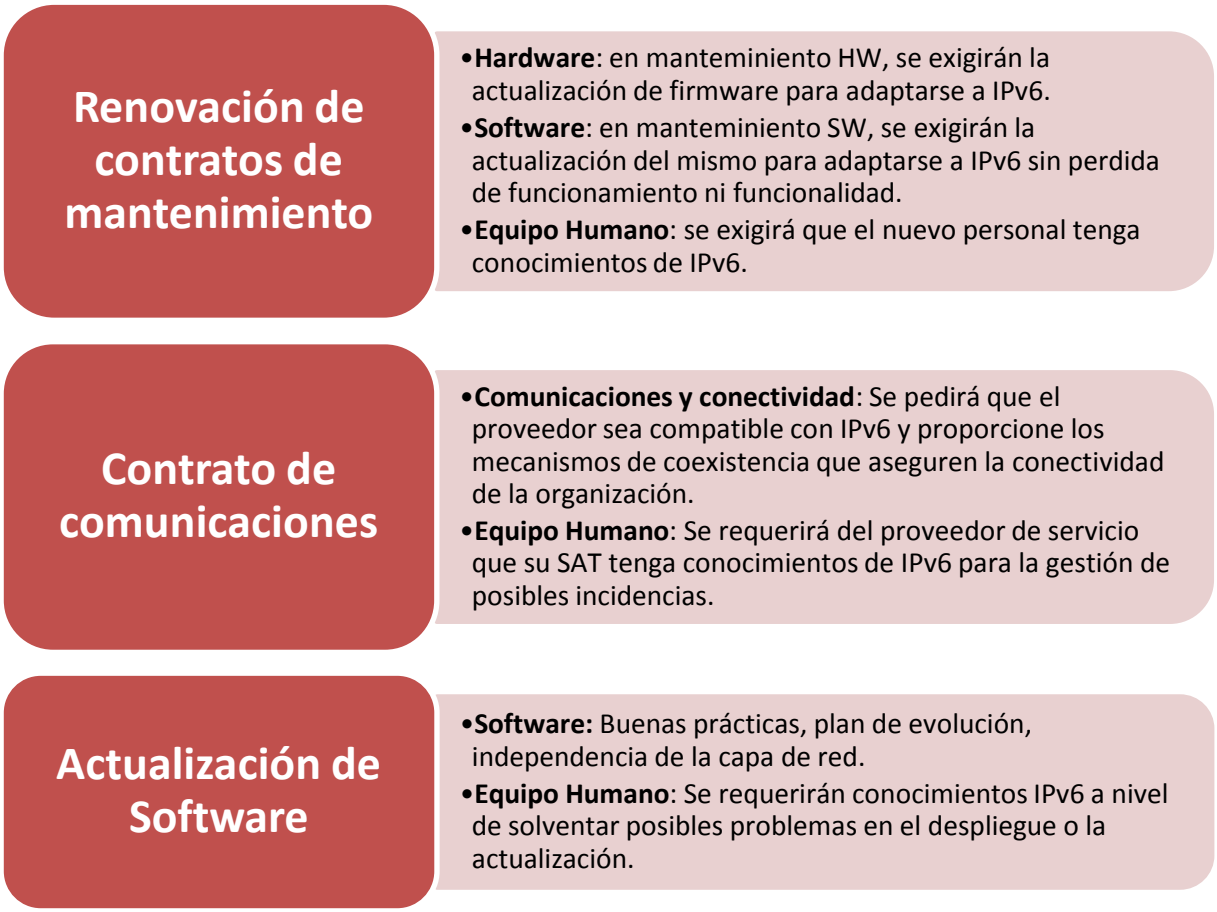


Figura 6 . Resumen de Contratos Tipo.

6.2. HARDWARE

Como ya se explicó en el apartado 5.2.1, el hardware es el primer punto de impacto en la transición IPv4-IPv6 y probablemente sobre el que más se ha profundizado. Para este punto de impacto, el objetivo es disponer de un mecanismo que permita evaluar la idoneidad de un dispositivo hardware.

6.2.1. Mecanismos Generales de Análisis de Dispositivos Hardware

En primera instancia, existen dos planteamientos para la definición de este mecanismo:

- **Tomar como referencia las certificaciones de productos compatibles con IPv6** (ver apartado 5.1). De esta forma, si se indica que un determinado producto cuenta con una certificación concreta, directamente se puede asumir que este producto cumple con las expectativas de compatibilidad IPv6.
  Este modelo tiene como ventaja su simplicidad puesto que se delega el proceso de validación del producto en una entidad externa de confianza. Sin embargo, también existen varias desventajas que pueden descartar el uso exclusivo de este planteamiento:

  - El hecho de no disponer de una de estas certificaciones no quiere decir que el producto no sea compatible y funcional con IPv6. Ninguna certificación es exhaustiva, abordando todos los productos del mercado.
  - Es necesario analizar con detenimiento las pruebas que se realizan por las entidades certificadoras. Estas pruebas pueden ser profundas, pero pueden no cubrir el 100% de las funcionalidades IPv6, por lo que para necesidades particulares, disponer de un certificado de compatibilidad no asegura su funcionamiento.
- **Definir un listado de RFCs a cumplir** adecuado a unas necesidades particulares. Es más laboriosa llevar a cabo este planteamiento (como ya se ha indicado, existen más de 500 RFCs relacionados en mayor o menor medida con IPv6) y requiere un análisis muy detallado. La principal ventaja de este planteamiento es que asegura que el producto que cumpla todos los RFC indicados en el listado será adecuado para su objetivo. Sin embargo, las desventajas que presenta este modelo son las siguientes:
  - El análisis exhaustivo de todos los RFCs es una tarea muy compleja.
  - Dicho análisis tendrá que hacerse en varias ocasiones, puesto que las necesidades pueden cambiar según el objetivo final del dispositivo.
  - Una vez realizado el análisis, es necesario realizar las pruebas de conformidad a dichos RFCs para garantizar su cumplimiento.

6.2.2. Prácticas Recomendadas

La primera premisa para la definición de requisitos de compras públicas de hardware es que todos los dispositivos deben soportar los protocolos IPv4 e IPv6 con un nivel y calidad de funcionamiento similar en ambos casos. Estas diferencias deben estar identificadas y evaluadas de forma cuantificable.

Para poder concretar las necesidades particulares de cada elemento hardware, se propone el siguiente modelo:

- Definir 7 niveles de clasificación de los equipos hardware, que se corresponderán con el modelo extendido reflejado en el documento de RIPE-501bis (Ver apartado 5.2.1.3):
  - **Equipo**.
  - **Conmutador de capa 2.**
  - **Enrutador, o conmutador de capa 3.**
  - **Elementos para asegurar la seguridad en la red** (Cortafuegos, IDS, etc.).
  - **CPE (*Customer Premises Equipment).***
  - **Nodo móvil (Mobile node).**
  - **Balanceador de Carga (Load balancer).**
- Definir una clasificación de los RFCs relacionados con IPv6 indicando cuales serán de obligado cumplimiento, cuales dependen de las funcionalidades deseadas y cuales serán opcionales. Un ejemplo de cómo abordar esta clasificación de RFCs se incluye como Anexo I (Apartado 9).

- Generar una serie de cuestionarios en un formato suficientemente extendido, por ejemplo un documento con formato de tabla o un formulario web, que permitan a los licitadores justificar su compatibilidad IPv6 mediante respuestas de tipo SI/NO y valorar de forma objetiva cada una de las ofertas en referente a esta compatibilidad. Estos cuestionarios deben evolucionar de forma paralela al protocolo IPv6. Un modelo de cuestionario para el tratamiento del cumplimiento de las RFCs relacionadas se incluye como Anexo II (Apartado 10).
  El hecho de que un hardware cuente con una certificación oficial de compatibilidad con IPv6 únicamente se debería de considerar una mejora o extra, no deberá de sustituir la cumplimentación de los cuestionarios de compatibilidad con RFCs. En caso de tener en consideración este aspecto, en la licitación se deberá de indicar que certificaciones serán aceptadas como mejora.
  El cumplimiento de los cuestionarios puede tener un carácter contractual, estableciéndose medidas en caso de incumplimiento bien para sancionar al licitador o bien para forzar el cumplimiento de las mismas.

6.3. SOFTWARE

El análisis de la compatibilidad con IPv6 del software es muy diferente al análisis del hardware puesto que, como se trató en 5.2.2, no existen certificaciones de uso extendido para el software y son pocos los RFCs que tratan cuestiones relacionadas con la adecuación de las aplicaciones a IPv6.

Una política de compras de software sirve para asegurar las nuevas adquisiciones cumplan con los requisitos IPv6 existentes. Sin embargo, existe una diferencia importante con respecto al hardware: una aplicación software es actualizable. Esto, unido al hecho de que generalmente las aplicaciones software suelen abstraerse de los protocolos de red, hace que una de las opciones a analizar sea la actualización del software existente como alternativa a la adquisición de nuevas aplicaciones.

A continuación se analizan las posibles circunstancias en las que se puede encontrar una organización de acuerdo a los diferentes tipos de aplicaciones.

6.3.1. Software a Medida

Las aplicaciones desarrolladas a medida son aquellas creadas por petición expresa de una entidad y, en general, no distribuidas a ningún otro cliente. Este software puede ser desarrollado de forma externa o interna a la organización y la realización de cualquier evolución del mismo deberá de analizarse en función de las condiciones establecidas en el contrato (para desarrollos externos) o en la disponibilidad (para desarrollos internos).

El desarrollador (entendido como el fabricante externo o el equipo de desarrollo interno según corresponda) es la primera fuente de información para el estudio de compatibilidad con IPv6.

Como primera premisa ante cualquier desarrollo se debe de exigir el cumplimiento estricto de las normas de Calidad de Software [48], lo cual aportará la robustez y flexibilidad necesarias para que las aplicaciones desarrolladas se adapten a las necesidades del

usuario final. La aplicación de estas normas supone, de forma implícita, solventar las particulares de desarrollo relacionadas con IPv6. Sin embargo, con el fin de aclarar estos aspectos, se indican las buenas prácticas, estándares y particularidades relacionadas con IPv6 a considerar durante el desarrollo de software.

- Con respecto a las **buenas prácticas**, RIPE [49]) define las siguientes:
  - Todo el software debe soportar IPv4 e IPv6 y ser capaz de gestionar la comunicación solo con IPv4, solo con IPv6 y en modo doble-pila.
  - Todos los parámetros de configuración local o remota deberán soportar también configuración IPv6.
  - Todas las características que son ofrecidas sobre IPv4 deben de estar disponibles con IPv6.
  - Los usuarios no deben percibir ninguna diferencia significativa cuando están operando sobre IPv6 o cuando están sobre IPv4, al menos que esto proporcione un beneficio claro sobre IPv6.
  - Se considera una mala práctica utilizar el uso de direcciones literales en el código fuente, tal y como se describe en el RFC3484 [50].
- Con respecto a los **estándares**, el DoD de Estados Unidos ha recopilado el siguiente listado de normas y estándares [51] a considerar en el desarrollo de aplicaciones compatibles con IPv6:
  - IEEE Standard 1003.1-2001, basado en la especificación de servicios XNS.
  - RFC3542, Advanced Sockets Application Program Interface (API) for IPv6 [52].
  - RFC4038, Applicacion Aspects of IPv6 Transition [53].
  - RFC4584, Extension to Sockets API for Mobile IPv6 [54], para algunas aplicaciones móviles de nodos MIPv6.
  - RFC5014, IPv6 Socket API for Source Address Selection [55].
  - RFC3678, Socket Interface Extension for Multicast Source Filtering [56].
  - RFC3986, Uniform Resource Identifiers [57], sintaxis genérica para la representación de direcciones IPv6 en interfaces de usuario.

- Además de seguir estas recomendaciones y estándares, es recomendable incluir en el contrato que la aplicación sea capaz de evolucionar a medida que lo hagan los estándares de IPv6, incluyendo nuevos estándares.

Con el fin de asegurar la compatibilidad del software desarrollado, se recomienda aportar al desarrollador información sobre la planificación de la transición IPv6 de la organización que pueda afectar a la aplicación desarrollada y las particularidades IPv6 del entorno en el que va a ejecutarse dicha aplicación.

6.3.2. Software Comercial

Las aplicaciones comerciales son aquellas desarrolladas por un fabricante y comercializadas a varios clientes. Para estas aplicaciones, es el fabricante el que define y gestiona su evolución y, por su propio interés, el que debería de encargarse de generar los parches y/o nuevas versiones que aseguren la compatibilidad IPv6 de sus herramientas.

Como en el caso del software desarrollado a medida, el fabricante es la primera fuente de información sobre la compatibilidad de sus productos. Para el software comercial a adquirir, el fabricante o distribuidor deberán aportar la información necesaria sobre la compatibilidad de su software. Se deberá indicar si es o no compatible, a partir de que versión se establece esta compatibilidad y, en caso de que no exista compatibilidad o esta sea parcial, indicar la planificación de la evolución de la aplicación.

Al no existir certificaciones de compatibilidad IPv6 equivalentes a las de hardware, para evitar el análisis reiterado de las aplicaciones de uso más común, varias organizaciones han generado bases de datos con el estado de compatibilidad de las aplicaciones más utilizadas. Algunas de las bases de datos más representativas son:

- 6DISS (IPv6 DISSemination and Exploitation) IPv6 Applications Database [58]: Recopilación de información sobre varias aplicaciones y herramientas de uso extendido y su estado con respecto a IPv6: en cuales está IPv6 disponible, en que versión y si es necesario o no un parche La información está clasificada por categoría, sistema operativo y modo de compatibilidad (integrado o por medio de parche). Sin embargo, esta base de datos sólo ha sido mantenida hasta el año 2006, aproximadamente, con lo cual nuevas aplicaciones podrían no aparecer en ella.
- IPv6-to-Standard [14]: Base de datos que incluye aplicaciones, productos y servicios con soporte IPv6 exclusivamente según los RFCs básicos.
- University of Wisconsin-Madison IPv6 Application Compatibility List [59]: Listado de aplicaciones de uso extendido y su estado de compatibilidad con respecto a IPv6. En algunos casos, se incluye un enlace a la página web oficial del producto donde se trata el tema de la compatibilidad.
- NIFFI (National Information Infrastructure Development Institute) Campus IPv6 Wiki [60]: Listado de compatibilidad de aplicaciones de uso extendido

El hecho de que una aplicación aparezca en una o varias de estas bases de datos puede servir de garantía de compatibilidad, aunque en todo caso, se recomienda que sea el fabricante el que se encargue de indicar las capacidades de su producto.

Tabla 2: Resumen de las recomendaciones para el software.

SW	A MEDIDA	COMERCIAL
	Exigir el cumplimiento de buenas prácticas y estándares. Aportar información sobre la transición IPv6 y el entorno. Realizar una prueba de funcionamiento.	Solicitar información al desarrollador/fabricante. Confirmar versión compatible o planificación para la compatibilidad. Tomar como referencia las bases de datos de entidades de confianza.

6.3.3. Prácticas Recomendadas

Como en el caso del hardware, cualquier aplicación que se comunique vía protocolo IP debe soportar tanto IPv4 como IPv6 manteniendo el mismo nivel y calidad de servicio establecido. Además, este cambio debe pasar desapercibido por los usuarios, salvo que las propias particularidades inherentes de cada protocolo, como por ejemplo las direcciones IP, sean datos manejados por ellos. En este sentido, se debe destacar también la conveniencia de no utilizar direcciones literales, sino nombres DNS[9],.

Además, se propone lo siguiente:

- Generar una lista de RFCs recomendables y de obligatorio cumplimiento para toda nueva adquisición de software (tanto comercial como desarrollos a medida) para lo que se definirían requisitos y plantillas similares a las tratadas como Anexo I (Apartado 9) y Anexo II (Apartado 10) respectivamente.
- En el caso de desarrollo a medida, exigir una demostración de que el desarrollo funciona correctamente en los entornos sólo IPv4, sólo IPv6 y en modo doble-pila IPv4-IPv6.
- En el caso de software comercial, será suficiente con aparecer en dos de las bases de datos disponibles para asegurar la compatibilidad con IPv6. Las bases de datos que se deben usar estarán incluidas en la licitación. En caso de que el software no aparezca en estas bases de datos, el fabricante deberá demostrar el funcionamiento del mismo en entornos IPv4, IPv6 y en doble-pila por medio de una demostración.
- Estos documentos podrán tener carácter contractual y serán de obligado cumplimiento. En caso de incumplimiento se incurrirá en penalizaciones, rescisión de contrato o cualquier otro mecanismo de la Administración.

6.4. EQUIPO HUMANO

En el caso en el que el contrato exija la definición y/o incorporación de un equipo de trabajo, se requiere que la oferta del proveedor sea capaz de reflejar y justificar los siguientes aspectos:

- El equipo de trabajo destinado al desarrollo del contrato es suficientemente grande como para poder abordar todas las necesidades del mismo.
- Los miembros de este equipo cuentan con los conocimientos en IPv4 e IPv6 necesarios para realizar su trabajo.
- La calidad de los servicios ofrecidos es acorde a los requisitos, tanto para IPv4 como para IPv6.

La forma más adecuada de justificar la preparación de los miembros del equipo de trabajo en relación a IPv6 es por medio de las certificaciones personales. En el caso de IPv6, existen varias certificaciones acreditadas, como por ejemplo:

[9] Salvo que precisamente se trate de aplicaciones de gestión de DNS, y por tanto se requiera la manipulación de ambos parámetros (dirección y nombre DNS)

- El proyecto 6DEPLOY de la Comisión Europea, en coordinación con el IPv6 Forum [61], está poniendo en marcha certificaciones neutrales e independientes de fabricantes, para cursos, ingenieros y formadores. Por el momento sólo ha sido certificado para facilitar estos cursos, y por tanto, para que los ingenieros y formadores reciban dicha certificación el propio proyecto 6DEPLOY y sus participantes, concretamente en España y resto de países de lenguas españolas, Consulintel. Estas certificaciones exigen un examen presencial tras la formación, lo que permite contrastar los conocimientos adquiridos por el participante.
- Hurricane Electric Free IPv6 Certification [62]. Certificación gratuita la cual ofrece un entorno de pruebas interactivo, on-line y no presencial, que permite obtener diferentes niveles de certificación (si bien carece de un mecanismo de contraste de los conocimientos adquiridos al no disponer de un examen presencial).
- El IPv6 Institute [63], en colaboración con el Campus Global de la Universidad de Arkansas, ha lanzado un conjunto de certificaciones IPv6, denominadas IPv6Cert. El objetivo es aportar conocimientos demostrables en el desarrollo, transición y aplicaciones relacionadas con IPv6.

Disponer de alguna certificación relacionada con IPv6 junto con la participación en otros proyectos en las que esta tecnología fuese uno de los aspectos de peso, pueden considerarse suficientes para determinar que un miembro del equipo de trabajo cuenta con conocimientos relacionados con IPv6.

6.4.1. Prácticas Recomendadas

La propuesta para el tratamiento de las competencias relativas a IPv6 en equipos humanos se basa en los siguientes puntos:

- En caso de contratos de mantenimiento (servicios de personal con dedicación puntual) se establecerán unos compromisos de servicio. Estos compromisos serán independientes de IPv6, por lo que si el licitador no dispone del conocimiento necesario podrá verse penalizado económicamente, rescindido su contrato y/o excluido de procesos posteriores.
- En el caso de equipos de desarrollo bastará con exigir una demostración de que el desarrollo funciona correctamente en los entornos sólo IPv4, sólo IPv6 y en doble-pila IPv4-IPv6. Si bien, durante la validación de la entrega del producto, se deberá realizar una auditoría de calidad de código centrándose, en particular, en las particularidades de IPv6.
- Si bien el hecho de disponer de una certificación no puede ser una exigencia, en función de la labor a desempeñar, puede ser conveniente considerarlo como una mejora orientada a garantizar los conocimientos necesarios sobre IPv6.

En cualquier caso, como medida para el tratamiento de estas cuestiones en procesos de compra pública se impondría la necesidad de aportar los perfiles profesionales a través de formatos de Curriculum Vitae normalizados de alta difusión como es el formato Europass [64] que podría complementarse con tablas de experiencia y conocimientos específicos por perfil como la reflejada en el Anexo III (Apartado 11).

6.5. COMUNICACIONES Y CONECTIVIDAD

En el caso de los contratos con proveedores de conectividad y comunicaciones, es necesario asegurar que la configuración interna de dicho proveedor no desemboque en un impacto negativo de cara al servicio que deseamos recibir, tanto si nos encontramos en IPv4 o en IPv6.

Los principales requisitos a solicitar a un proveedor son:

- Posibilidad de mantener comunicación doble-pila IPv4/IPv6 a través del proveedor.
- Los Acuerdos de Nivel de Servicio deben definirse de forma independiente a la tecnología y configuración interna del proveedor y al hecho de que estemos utilizando solo IPv4, en transición IPv4-IPv6, solo IPv6 o en doble-pila IPv4/IPv6.
- Las especificaciones de ancho de banda, latencia, paquetes perdidos, etc. deben ser independientes de que estemos utilizando solo IPv4, en transición IPv4-IPv6, solo IPv6 o doble-pila IPv4/IPv6.
- Con respecto al direccionamiento, según las necesidades del contratante, el proveedor debe ser capaz de aportar un direccionamiento adecuado a las necesidades (Direccionamiento “PA”, Dependiente del Proveedor) y/o tener la capacidad de gestionar un direccionamiento propio perteneciente al contratante (Direccionamiento “PI”, Independiente del Proveedor).

6.5.1. Prácticas Recomendadas

Lo más importante es asegurar si el proveedor tiene capacidad para cubrir las necesidades IPv6 del contratante y para poder realizar este análisis, es necesario conocer el estado actual del contratante y cuál es su planificación de transición IPv4-IPv6.

Se debe exigir al proveedor establezca un nivel y calidad de servicio independiente del protocolo, es decir, no es admisible utilizar el proceso de transición IPv4-IPv6 o la activación de servicios IPv6 como justificación para una reducción de las prestaciones de los servicios afectados.

Una estrategia para poder determinar si el soporte IPv6 ofrecido por el proveedor cumple con las expectativas es generar un conjunto de preguntas directas sobre estos aspectos, a modo de encuesta, las cuales deberán ser respondidas por el proveedor con carácter vinculante. En el Anexo III (Apartado 11) se incluye, a modo de ejemplo, un conjunto de preguntas y cómo evaluar la respuesta de cada una de ellas.

En estas encuestas todas las preguntas se englobarían en tres categorías:

- Obligatorio: el incumplimiento del requisito es excluyente del concurso, debido a que es fundamental para la implantación del servicio.
- Deseable: el incumplimiento del requisito no es excluyente, pero se valorará muy positivamente que se cumpla.
- Opcional: el incumplimiento del requisito no es excluyente, pero se valorará que se cumpla.

Desde el punto de vista del contenido, los requisitos específicos responderían a las siguientes preguntas:

- ¿Qué tipo de conectividad ofrece el operador en IPv6?
- ¿Qué tipo de servicios de conectividad ofrece el operador en IPv6?
- ¿Cómo ofrece el servicio de conectividad internamente el operador?
- ¿Qué servicios adicionales ofrece el operador en IPv6?

En lo que se refiere a servicios de comunicaciones extremo a extremo se pueden diferenciar dos grandes grupos, debido a sus características diferenciadas:

- **Servicios de conectividad a Internet**: donde el operador tiene que garantizar una conexión a Internet, con IPv4 e IPv6 fiable y robusta en la que se prestaría especial atención a que:
  - No debería utilizar mecanismos túneles internamente a su red.
  - Debe tener una estructura de upstreams IPv6 fiable.
  - Debe proporcionar mecanismos de alta disponibilidad.
  - Debe de tener visibilidad, y por tanto tránsito y/o peering (directa o indirectamente), del 100% de la tabla de enrutamiento global, tanto IPv4 como IPv6.
- **Servicios de conectividad VPN**: donde el operador proporciona un servicio de conectividad interna entre las sedes del cliente:
  - No debería utilizar mecanismos túneles internamente a su red.
  - Debe proporcionar diferentes mecanismos de encaminamiento al cliente (dinámico y estático).
  - Dentro de los dinámicos tendría que soportar BGP, siendo OSPFv3, IS-IS y RIPng deseables, según las necesidades del contratante.

Por último, otros servicios que debería ofrecer en IPv6, aunque no obligatoriamente, serían:

- Servicio DNS accesible en IPv6.
- Servicios de correo accesible en IPv6.
- Servicios de DataCenter (hosting/housing) accesibles en IPv6.

7. RECOMENDACIONES PARA LA INTRODUCCIÓN DE REQUISITOS IPv6 EN PLIEGOS TÉCNICOS DE ADQUISICIONES

A continuación se indica un modelo de cláusula general propuesto a modo de introducción para la integración de características IPv6 en los procesos de adquisición de sistemas o servicios.

> *"Todo sistema (hardware, software, firmware, etc.) o servicio relacionado directa o indirectamente con la transmisión, manipulación o procesamiento de información por medio del Protocolo de Internet (IP), independientemente del régimen bajo el cual se regule la relación con dicho elemento (adquisición, desarrollo, explotación, contratación, etc.), debe ser capaz de operar plenamente de acuerdo a los estándares comerciales establecidos para el Protocolo de Internet versión 6 (IPv6) y a los aspectos definidos en el RFC2460 (Internet Protocol Version 6 Specification) y el resto de RFCs relacionados con IPv6.*
>
> *En esta circunstancia, el sistema o servicio debe mantener o mejorar los niveles de servicio, calidad y confianza preestablecidos, tanto con el protocolo IPv4 como con IPv6. Asimismo, el proveedor deberá aportar, durante el periodo de garantía establecido, soporte técnico para ambos protocolos.*
>
> *Para cualquier excepción al uso o compatibilidad con IPv6 será necesaria autorización explícita y por escrito por parte de la entidad contratante."*

La cláusula propuesta no se aplicaría a los procesos de contratación de equipos de trabajo que no estén asociados a un servicio concreto, para los cuales se recomienda seguir el modelo indicado en el apartado 6.4.1 y en el Anexo III (apartado 11).

Con su inclusión en un documento formal (contrato, pliego de licitación, etc.), esta cláusula tiene el objetivo de introducir, de forma clara y concisa, la necesidad de que cualquier elemento solicitado de forma directa o indirecta deberá contar con compatibilidad IPv6 y asegurar un mínimo de calidad de servicio en este escenario.

Para afianzar esta necesidad, aun en contra de la recomendación de delegar la especificación de los estándares solicitados a Anexos de las políticas y contratos, se hace referencia directa al RFC2460 "Internet Protocol version 6 Specification" por su carácter de definición básica del protocolo y, por tanto, primera premisa de obligado cumplimiento en cualquier definición de compatibilidad con IPv6.

Posteriormente, en la redacción del documento formal, se deben desarrollar las necesidades particulares desde el punto de vista de la compatibilidad con IPv6 de aquellos elementos o servicios objeto del documento.

A continuación se detallan las consideraciones para la redacción de documentos formales, particularizadas en cada uno de los puntos de impacto. Tal y como se indica en el apartado 6.1.3, lo más habitual es que estos documentos tengan como objetivo de forma simultánea

más de un punto de impacto, sin embargo, este aspecto no influye a las recomendaciones indicadas.

7.1. HARDWARE

En aquellos documentos formales en los que se haga referencia a activos hardware, se recomienda seguir el siguiente planteamiento para la redacción de su especificación:

- Redactar la descripción funcional de cada uno de los activos, indicando de forma explícita las necesidades de compatibilidad con IPv6.
- Indicar el procedimiento por el cual se aportará la información de compatibilidad y el carácter vinculante de la información aportada. Este procedimiento y los elementos en los que se apoya, se incluirán en un anexo.
- Definir el listado de estándares (RFCs) a cumplir de forma obligatoria o recomendada por el activo. Los estándares indicados deben estar alineados con la descripción funcional.
- Aportar un mecanismo o artilugio que facilite al ofertante un modo claro de indicar el cumplimiento de los estándares solicitados y al encargado de analizar la oferta le aporte un mecanismo sencillo de evaluación del grado de cumplimiento.

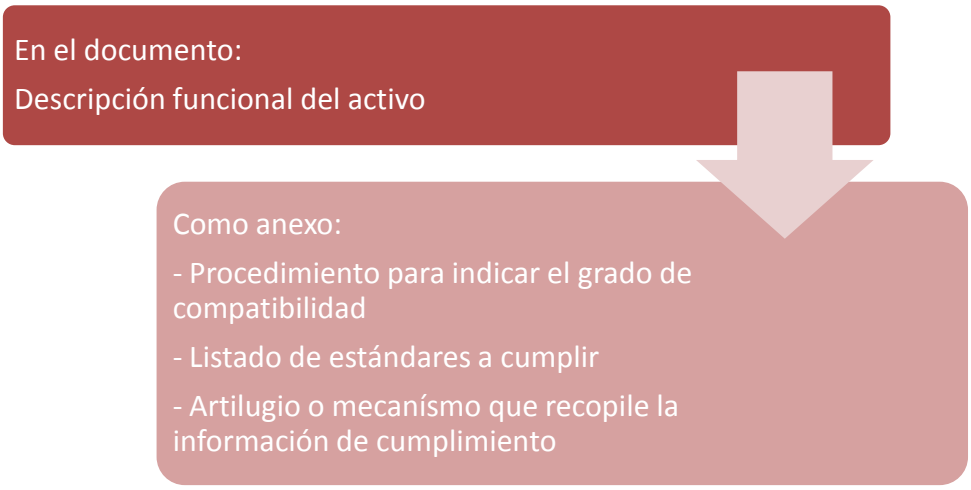


Figura 7 . Redacción de documentos en los que se soliciten activos hardware.

Para más información sobre las particularidades del hardware, ver el apartado 6.2.

7.2. SOFTWARE

En aquellos documentos formales en los que se solicite software, será necesario hacer una diferencia dependiendo de si se está solicitando software desarrollado a medida o software comercial.

En el caso del software a medida, se recomienda lo siguiente:

- Exigir que el cumplimiento de las buenas prácticas de desarrollo, lo cual, por sí solo, debería ser suficiente para asegurar que los aspectos relacionados con la

compatibilidad IPv6 fuesen correctamente identificados y tratados durante el desarrollo (incluyendo el uso de nombres DNS en lugar de direcciones literales),.

- Solicitar que, durante la toma de requisitos, se identifiquen de forma explícita y diferenciada aquellos requisitos relacionados con el cumplimiento de la compatibilidad IPv6 en base al entorno sobre el que se vaya a desplegar la aplicación.
- Solicitar evidencias de que, durante el periodo de pruebas, se han realizado pruebas específicas sobre entornos IPv6 equivalentes con el entorno objetivo del software desarrollado y que el resultado de estas pruebas ha sido satisfactorio.

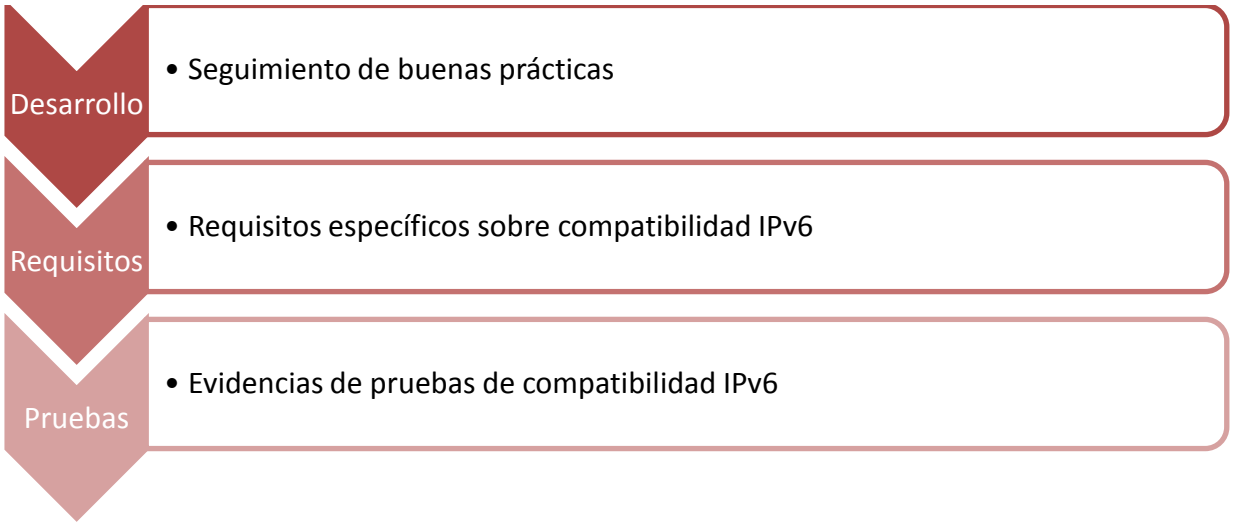


Figura 8 . Redacción de documentos en los que se solicite software a medida.

En el caso del software comercial:

- Exigir al proveedor una confirmación formal y por escrito de la compatibilidad del software solicitado con IPv6 y de su capacidad funcional de operar con la misma calidad sobre el entorno objetivo del software, incluyendo el uso de nombres DNS en lugar de direcciones literales.
- Opcionalmente, solicitar al proveedor la certificación o confirmación de la compatibilidad IPv6 del software por parte de una entidad ajena y de confianza. Al no existir ni bases de datos ni entidades certificadoras de uso extendido destinadas a la compatibilidad IPv6 del software, no debe ser una exigencia.
- En caso de necesitar una confirmación específica de la compatibilidad para el entorno objetivo del software, se puede solicitar una demostración.

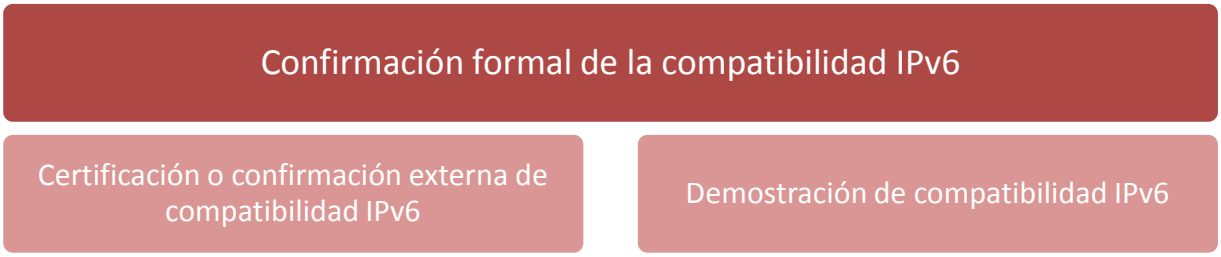


Figura 9 . Redacción de documentos en los que se solicite software comercial.

Para más información sobre las particularidades del software, ver el apartado 6.3.

7.3. EQUIPO HUMANO

En el caso particular de la definición de perfiles de trabajo, no existen recomendaciones específicas con respecto a la descripción de los conocimientos o capacidades en IPv6. A pesar de que existen certificaciones en IPv6 destinadas a profesionales (entre ellas "IPv6 Ready" del IPv6 Forum, de carácter neutral), aun no están suficientemente extendidas como para tomarlas como referencia, por lo que en este sentido, se recomienda que las certificaciones sean consideradas dependiendo de la cualificación requerida para la función a desempeñar. Es conveniente complementar las certificaciones con la experiencia demostrada, dado que la formación teórica, debido a la relativa novedad de IPv6 para algunos profesionales, puede en muchas ocasiones no ser suficiente para la actividad a realizar.

De cara a abordar la redacción de documentos formales, se recomienda seguir un modelo similar al del hardware:

- Descripción de las competencias solicitadas.
- Procedimiento para indicar el cumplimiento de las competencias.
- Especificación técnica de las competencias.
- Modelo para la indicación del grado de cumplimiento de la especificación.

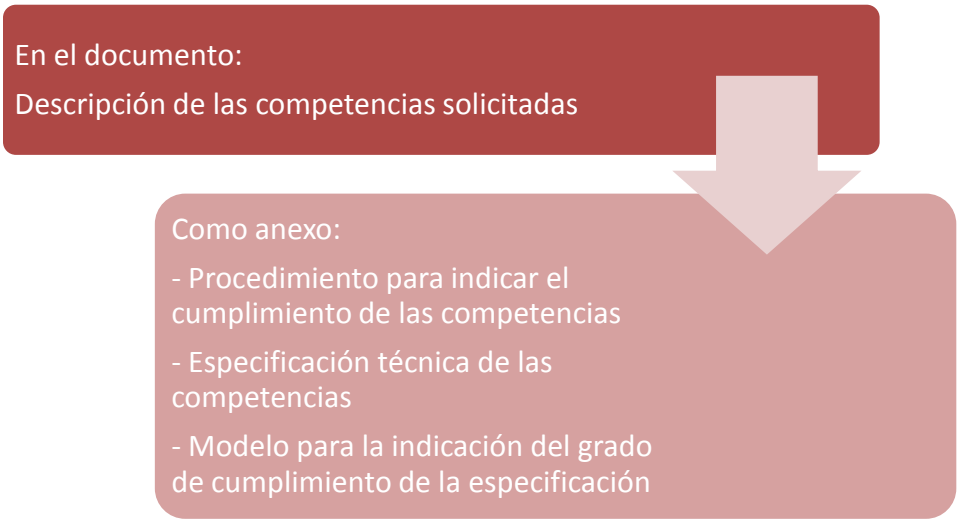


Figura 10 . Redacción de documentos en los que se especifiquen perfiles de trabajo.

Para más información sobre las particularidades de los equipos de trabajo, ver el apartado 6.4.

7.4. COMUNICACIONES Y CONECTIVIDAD

Para aquellos documentos formales en los que se soliciten servicios de comunicación y conectividad, se recomienda seguir el siguiente planteamiento:

- Identificar las necesidades de compatibilidad IPv6 requeridas.
- Solicitar de forma expresa la confirmación por parte del proveedor de que los niveles de calidad de servicio establecidos seguirán cumpliéndose independientemente del protocolo utilizado y de la fase de transición IPv4-IPv6 en la que se pueda encontrar el proceso.
- Explicar el procedimiento por el cual se va a recabar información del proveedor sobre el cumplimiento de las necesidades IPv4-IPv6. Se recomienda que esta información y los elementos que soportarán el proceso para su puesta en práctica se aporten en un anexo.
- Definir un conjunto de preguntas específicas para recabar información sobre el cumplimiento de las necesidades de compatibilidad IPv6 solicitadas al proveedor. Además, se indicará el modo de evaluación de la respuesta, diferenciando entre los valores mínimos y deseables.
- Aportar un mecanismo o artilugio que facilite al proveedor un modo claro de indicar el cumplimiento de las necesidades solicitadas y que al encargado de analizar la oferta le aporte un mecanismo sencillo de evaluación del grado de cumplimiento.

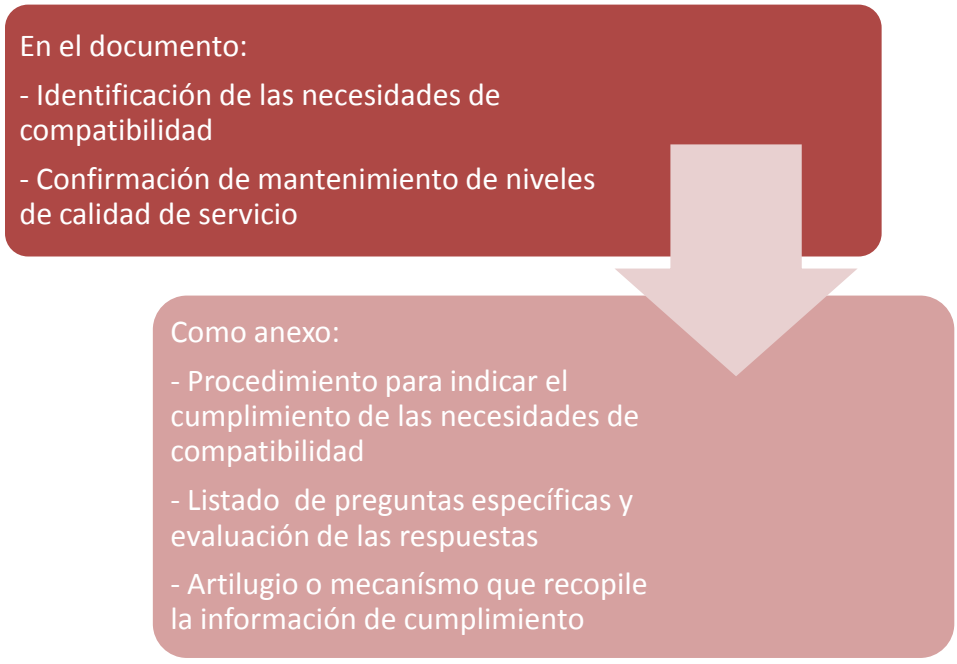


Figura 11 . Redacción de documentos para servicios de comunicación y conectividad.

8. REFERENCIAS

[1] Plan de Fomento para la Incorporación del Protocolo de Internet versión 6 (IPv6) en España.

http://www.ipv6.es/es-ES/transicion/Documents/BOE-A-2011-10786.pdf

[2] Ley 30/2007, de 30 de octubre, de Contratos del Sector Público.

http://www.boe.es/boe/dias/2007/10/31/pdfs/A44336-44436.pdf

[3] Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.

http://www.boe.es/boe/dias/2011/11/16/pdfs/BOE-A-2011-17887.pdf

[4] Estrategia Estatal de Innovación E2I.

http://www.micinn.es/portal/site/MICINN/menuitem.7eeac5cd345b4f34f09dfd1001432ea0/?vgnextoid=72cfb53b972e4210VgnVCM1000001d04140aRCRD

[5] Guía sobre Compra Pública Innovadora.

http://www.micinn.es/stfls/MICINN/Innovacion/FICHEROS/Politicas_Fomento_Innv./Guia.CPI.pdf

[6] La nueva Norma Europea EN ISO/IEC 17025.

http://argo.urv.es/quimio/general/iso.pdf

[7] Memorandum 05-22. “Transition Planning for Internet Protocol version 6 (IPv6)”.

http://usgv6-deploymon.antd.nist.gov/govmon.html

[8] USGv6.

http://w3.antd.nist.gov/usgv6/

[9] Interoperability Laboratory.

http://www.iol.unh.edu/services/testing/ipv6/USGv6.php

[10] USGC Buyer’s Guide.

http://www.antd.nist.gov/usgv6/BuyersGuide.html

[11] IPv6 Forum.

http://www.ipv6forum.org

[12] IPv6 Logo Program.

https://www.ipv6ready.org/db/index.php/public/

[13] IPv6 Logo Approved List.

https://www.ipv6ready.org/db/index.php/public/

[14] IPv6-to-Standard.

http://www.ipv6-to-standard.org/

[15] IPv6 Consortiums.

http://www.iol.unh.edu/services/testing/ipv6/

[16] Requirements For IPv6 in ICT Equipment.

http://www.ripe.net/ripe/docs/ripe-501

[17] IPv6 Act Now.

http://www.ipv6actnow.org/info/how-to/enterprise/talk/

[18] What To Ask From Your Service Provider About IPv6.

http://docwiki.cisco.com/wiki/What_To_Ask_From_Your_Service_Provider_About_IPv6

[19] IPv6 Implementation Checklist.

http://www.es.net/services/ipv6-network/ipv6-implementation-checklist/

[20] Cisco IPv6 At-A-Glance.

http://www.cisco.com/web/strategy/docs/gov/ipv6_aag.pdf

[21] MSR IPv6.

http://research.microsoft.com/en-us/projects/msripv6/

[22] Memorandum DOD Internet Protocol v6.

http://www.defense.gov/news/Jun2003/d20030609nii.pdf

[23] Estimating USG IPv6 & DNSSEC External Service Deployment Status.

http://usgv6-deploymon.antd.nist.gov/govmon.html

[24] Federal Acquisition Regulations.

http://edocket.access.gpo.gov/2009/pdf/E9-28931.pdf

[25] Electronic Code of Federal Regulations.

http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=ccc0e7cb6de6089743dc9825f1eaca91&rgn=div8&view=text&node=48:7.0.3.23.28.1.1.22&idno=48

[26] A Profile for IPv6 in the U.S. Government.

http://w3.antd.nist.gov/usgv6/docs/usgv6-v1.pdf

[27] USGv6-v1 Capability Checklist Description and Instructions.

http://w3.antd.nist.gov/usgv6/docs/usgv6-v1-ccl-v1.1.xls

[28] Suppliers Declaration of Conformity for USGv6 Products: Notes Page and Detailed Test Results Summary.

http://w3.antd.nist.gov/usgv6/docs/usgv6-v1-sdoc-v1.6.xls

[29] Approved Products Lists Integrated Tracking System.

https://aplits.disa.mil/

[30] IPv6 Procurement and Audit Standard.

http://www.egovernment.tas.gov.au/__data/assets/pdf_file/0017/113237/IPv6_procurement_and_audit_standards.pdf

[31] Saudi Arabia IPv6 Task Force.

http://www.ipv6.sa/documents

[32] Technical Domain Description Public Services Network Programme.

http://www.cabinetoffice.gov.uk/sites/default/files/resources/technical-domain-description-v2.0.pdf

[33] Criterios de Seguridad, Normalización y Conservación de las Aplicaciones Utilizadas para el Ejercicio de Potestades.

http://www.csi.map.es/csi/pg5c10.htm

[34] Security Architecture for the Internet Protocol.

http://www.ietf.org/rfc/rfc2401.txt

[35] Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

http://www.csi.map.es/csi/pg5e41.htm

[36] Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

http://www.csi.map.es/csi/pg5e42.htm

[37] Pliego de prescripciones técnicas para la contratación de los servicios para la mejora de la red de comunicaciones de los centros sanitarios dependientes del departamento de salud.

http://benasque.aragob.es:443/cgi-bin/BRSCGI?CMD=VEROBJ&MLKOB=241230632929

[38] Pliego de prescripciones técnicas que regirán la realización del contrato de "Mejora de la Infraestructura de Comunicaciones de Red.es.

http://www.red.es/procedimiento/detail.action;jsessionid=985BE9649998DFC27D5103DB9BEDB139.vertebra_appl17?id=992&request_locale=es

[39] Pliego de prescripciones técnicas que regirá en el concurso por procedimiento abierto convocado por el Instituto Nacional de Gestión Sanitaria para la contratación del suministro, instalación y configuración del equipamiento de los servicios de voz, datos, vigilancia, control de accesos y presencia, televisión y audiovisuales, así como el servicio de soporte y mantenimiento del mismo, para el nuevo hospital de Ceuta.

http://www.ingesa.msc.es/ciudadanos/licitaciones/archivos/080091/PliegoTecnicoDatosVozCeuta.pdf

[40] RFC2030 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI.

http://www.faqs.org/rfcs/rfc2030.html

[41] Pliego de prescripciones técnicas para el concurso de renovación de la electrónica de red de la Universidad de Burgos.

http://contrataciondelestado.es/wps/wcm/connect/?MOD=PDMProxy&TYPE=personalization&ID=NONE&KEY=NONE&LIBRARY=%2FcontentRoot%2Ficm%3Alibraries[17]&FOLDER=%2FDefault%2F61054%2F7186553%2F&DOC_NAME=%2FcontentRoot%2Ficm%3Alibraries[17]%2FDefault%2F61054%2F7186553%2FDOC2010071310525410072+SARA+SM++PPT+Electronica+de+red.pdf&VERSION_NAME=NONE&VERSION_DATE=NONE&IGNORE_CACHE=false&CONVERT=NONE&MUST_CONVERT=false

[42] Pliego de prescripciones técnicas para la contratación del suministro e instalación de un sistema unificado de comunicaciones para toda la red de la Universidad de Cantabria (UNICAN).

http://www.unican.es/NR/rdonlyres/DC5420B4-39EC-43C9-897F-7E7417761097/58342/PPT_EXP_359_2010.pdf

[43] Pliego de prescripciones técnicas para la contratación de la red corporativa de telecomunicaciones de la Junta de Andalucía.

http://www.porandalucialibre.es/documentos/doc_view/350-pliego-prescipciones-tecnicas-red-corporativa-moviles.html

[44] Pliego de cláusulas administrativas particulares que regirá la contratación del Servicio de Telecomunicaciones de la Excma. Diputación Provincial de Cáceres, Centros Dependientes, Organismos Autónomos, Sociedad Agropecuaria y Consorcio Medio XXI.

http://www.dip-caceres.es/comun/galerias/galeriaDescargas/caceres/Economia/PLIEGO_CLAUSULAS_ADMINISTRATIVAS_TECNICAS_ANEXO_TELECOMUNICACIONES.pdf

[45] Lista de RFC aprobados por el IETF.

http://www.consulintel.es/html/ForoIPv6/RFCs.htm

[46] IPv6 RFCs and Standards Working Groups.

http://ipv6now.com.au/RFC.php

[47] DRAFT: Requirements for IPv6 in ICT Equipment.

https://www.ripe.net/ripe/docs/other-documents/requirements-for-ipv6-in-ict-equipment/

[48] INTECO: Calidad TIC:

http://www.inteco.es/landing/calidad_TIC/

[49] Requirements For IPv6 in ICT Equipment – new vision:

http://go6.si/wp-content/uploads/2011/06/Requirements-for-IPv6-in-ICT-equipment-v.1.pdf

[50] RFC3484 Default Address Selection for Internet Protocol version 6 (IPv6).

http://www.ietf.org/rfc/rfc3484.txt

[51] Normas y Estándares DoD.

https://www.us.army.mil/suite/doc/23263297

[52] RFC3542 Advanced Sockets Application Program Interface (API) para IPv6.

http://www.ietf.org/rfc/rfc3542.txt

[53] RFC4038 Applicacion Aspects of IPv6 Transition.

http://www.ietf.org/rfc/rfc4038.txt

[54] RFC4584 Extension to Sockets API form Mobile IPv6.

http://www.ietf.org/rfc/rfc4584.txt

[55] RFC5014 IPv6 Socket API for Source Address Selection.

http://www.ietf.org/rfc/rfc5014.txt

[56] RFC3678 Socket Interface Extension for Multicast Source Filtering.

http://www.ietf.org/rfc/rfc3678.txt

[57] RFC3986 Uniform Resource Identifiers.

http://www.ietf.org/rfc/rfc3986.txt

[58] 6DISS IPv6 Applications Database.

http://applications.6pack.org/

[59] IPv6 Application Compatibility List.

http://kb.wisc.edu/helpdesk/page.php?id=11691

[60] IPv6 Application and Patch Database.

http://ipv6.niif.hu/m/ipv6_apps_db

[61] Certificaciones.

http://www.ipv6.es/es-ES/transicion/quees/Paginas/Certificaciones.aspx

[62] IPv6 Certifications.

http://ipv6.he.net/certification/

[63] The IPv6 Institute.

http://www.ipv6institute.com/index.html

[64] Modelo de CV Europass

http://europass.cedefop.europa.eu/europass/home/hornav/Introduction.csp

[65] RFC2460, Internet Protocol, Version 6 (IPv6).

http://www.ietf.org/rfc/rfc2460.txt

[66] RFC1752 The Recommendation for the IP Next Generation Protocol.

http://www.ietf.org/rfc/rfc1752.txt

[67] RFC1550, IP: Next Generation (IPng) White Paper Solicitation.

http://www.ietf.org/rfc/rfc1550.txt

[68] RFC1726, Technical Criteria for Choosing IP the Next Generation (IPng).

http://www.ietf.org/rfc/rfc1726.txt

[69] RFC 5555, Mobile IPv6 Support for Dual Stack Hosts and Routers.

http://www.ietf.org/rfc/rfc5555.txt

[70] RFC4877, Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture.

http://www.ietf.org/rfc/rfc4877.txt

9. ANEXO I – LISTADO DE RFC PARA COMPATIBILIDAD IPv6

A modo de ejemplo, para la definición de RFC a contemplar para la compatibilidad IPv6, actualmente RIPE cuenta con la norma RIPE-501 para "regular" el modo en que especifica la compatibilidad de los componentes hardware. Además, se está trabajando activamente en un borrador de la nueva versión 501bis [49] de una nueva norma que sustituirá a RIPE-501, manteniendo el mismo objetivo y espíritu que la anterior.

Tal y como se ha indicado, se recomienda seguir el mismo modelo para especificar las necesidades de compatibilidad en la definición de la política de compras públicas. A modo de ejemplo, a continuación se muestra un fragmento de cómo RIPE organiza esta información en concreto para los componentes de tipo "Host":

…

Requirements for "host" equipment

Mandatory support:

- *IPv6 Basic specification [RFC2460]*
- *IPv6 Addressing Architecture basic [RFC4291]*
- *Default Address Selection [RFC3484(bis)]*
- *Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]*
- *ICMPv6 [RFC4443]*
- *DHCPv6 client [RFC3315]*
- *SLAAC [RFC4862]*
- *Path MTU Discovery [RFC1981]*
- *Neighbor Discovery [RFC4861]*
- *Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213]*
- *IPsec-v2 [RFC2401, RFC2406, RFC2402]*
- *IKE version 2 (IKEv2) [RFC4306, RFC4718]*
- *ISAKMP [RFC2407, RFC2408, RFC2409]*
- *If support for mobile IPv6 is required, the device needs to comply to "MIPv6" [RFC3775, RFC5555] and "Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture" [RFC4877]*
- *DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]*

- *DNS message extension mechanism [RFC2671]*
- *DNS message size requirements [RFC3226]*

Optional support:

- *Revised ICMPv6 [RFC5095]*
- *IPv6 Router Advertisement Options for DNS Configuration [RFC6106]*
- *Extended ICMP for multi-part messages [RFC4884]*
- *SEND [RFC3971]*
- *SLAAC Privacy Extensions [RFC4941]*
- *Stateless DHCPv6 [RFC3736]*
- *DS (Traffic class) [RFC2474, RFC3140]*
- *Cryptographically Generated Addresses [RFC3972]*
- *IPsec-v3 [RFC4301, RFC4303, RFC4302]*
- *SNMP protocol [RFC3411]*
- *SNMP capabilities [RFC3412, RFC3413, RFC3414]*
- *Multicast Listener Discovery version 2 [RFC3810]*
- *Packetization Layer Path MTU Discovery [RFC4821]*

…

Este modelo tiene las siguientes particularidades:

Mandatory support:

Listado de los RFC de obligado cumplimiento para los dispositivos correspondientes a la clase en cuestión.

Optional support:

Listado de los RFC opcionales.

• IPv6 Basic specification [RFC2460]

Dentro de las secciones de RFC obligatorios y opcionales, se indica, a modo de lista, cada uno de los RFC correspondientes.

• If support for mobile IPv6 is required, the device needs to comply to "MIPv6"

[RFC3775, RFC5555] and "Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture" [RFC4877]

Dentro del apartado de RFC obligatorios, existe la posibilidad de determinar que ciertos RFC son obligatorios únicamente si se desea disponer de un determinado servicio o funcionalidad. En el ejemplo resaltado, si se desea disponer de soporte para IPv6 móvil, será necesario soportar el RFC5555 [69] y el RFC4877 [70].

10. ANEXO II – PLANTILLA DE CUMPLIMIENTO DE RFC

Una de las principales recomendaciones a la hora de poner en práctica una política de compras es disponer de artilugios que soporten las necesidades reales asociadas a dicha política. Las principales características de estos elementos son:

- Fácilmente actualizable: es necesario que el soporte del artilugio permita ser actualizado de forma sencilla.
- Fácilmente utilizable: dicho elemento será distribuido a ofertantes para su cumplimentación y, posteriormente, será evaluado por parte del licitador, por lo que debe de ser manejable para ambos objetivos.

En el proyecto USGv6 se ha definido un archivo Excel [28] en el que entre otras cosas, los licitadores deben de indicar el grado de cumplimiento de los RFC, tal y como se ve en la siguiente captura:

	Spec / Reference	Section	USGv6-v1 Requirements: Title / Definition	Context / Configuration Option	USGv6-V1 Rec: Host	Router	NPD	Notes about requested USGv6-v1 Capabilities.
30			**IPv6 Basic Requirements**					
31	RFC2460		**IPv6 Specification**	IPv6-Base	M	M		
32		2	IPv6 Packets: send, receive	IPv6-Base	M	M		
33		2	IPv6 packet forwarding	IPv6-Base		M		
34		4	Extension headers: processing	IPv6-Base	M	M		
35		4,3	Hop-by-Hop & unrecognized options	IPv6-Base	M	M		
36		4,5	Fragment headers: send, receive, process	IPv6-Base	M	M		
37		4,6	Destination Options extensions	IPv6-Base	M	M		
38	RFC5095		**Deprecation of Type 0 Routing Headers**	IPv6-Base	M	M		
39	RFC2711		**IPv6 Router Alert Option**	IPv6-Base		M		
40								
41	RFC4443		**ICMPv6**	IPv6-Base	M	M		
42	RFC4884		**Extended ICMP for Multi-Part Messages**		S+	S+		
43	RFC1981		**Path MTU Discovery for IPv6**	IPv6-Base	M	M		
44		4	Discovery Protocol Requirements	IPv6-Base	M	S+		
45	RFC2675		**IPv6 Jumbograms**		O	O		
46								
47	RFC4861		**Neighbor Discovery for IPv6**	IPv6-Base	M	M		
48		4.1, 4.2	Router Discovery	IPv6-Base	M	M		
49		4.6.2	Prefix Discovery	IPv6-Base	M	M		
50		7,2	Address Resolution	IPv6-Base	M	M		
51		7.2.5	NA and NS processing	IPv6-Base	M	M		
52	(RFC4862)	7.2.3	Duplicate Address Detection	IPv6-Base	M	M		
53		7,3	Neighbor Unreachability Detection	IPv6-Base	M	M		
54		8	Redirect functionality		S	M		
55	RFC5175		**IPv6 Router Advertisement Flags Option**		S	S		
56	RFC4191		**Default Router Preference**		S+	S+		
57	RFC3971		**Secure Neighbor Discovery**	SEND	c(M)	c(M)		
58			**Auto Configuration**					
59	RFC4862		**IPv6 Stateless Address Autoconfig**	SLAAC	c(M)			
60		5,3	Creation of Link Local Addresses	SLAAC	M	M		
61	(RFC4861)	5,4	Duplicate Address Detection	SLAAC	M	M		
62		5,5	Creation of Global Addresses	SLAAC	c(M)			
63		•	Ability to Disable Creation of Global Addrs	SLAAC	c(M)			
64	RFC4941		**Privacy Extensions for IPv6 SLAAC**	SLAAC & PriAddr	c(M)			
65		•	<2nd context for MIP Mobile Node>	SLAAC & MIP	c(S+)			
66								
67	RFC3736		**Stateless DHCP Service for IPv6**	SLAAC	c(S+)			
68								
69	RFC3315		**Dynamic Host Config Protocol (DHCPv6)**	DHCP-Client	c(M)			
70		•	Ability to Administratively Disable	DHCP-Client	c(M)			
71			DHCP Client Functions	DHCP-Client	c(M)			
72	RFC4361		**Node-specific Client IDs for DHCPv4**	DHCP-Client & IPv4	c(S+)			
73	RFC3633		**Prefix Delegation**	DHCP-Prefix		c(M,S+)		
74								
75			**Addressing Requirements**					
76	RFC4291		**IPv6 Addressing Architecture**	Addr-Arch	M	M		
77	RFC4007		IPv6 Scoped Address Architecture	Addr-Arch	M	M		
78		•	Ability to manually configure Addresses	Addr-Arch	M	M		
79	RFC4193		Unique Local IPv6 Unicast Address		O	O		
80	RFC3879		Deprecating Site Local Addresses	Addr-Arch	M	M		
81	RFC3484		Default Address Selection for IPv6	Addr-Arch	M	M		
82		2,1	Configurable Selection Policies		S+	S+		
83	RFC2526		Reserved IPv6 Subnet Anycast Addresses	Addr-Arch	M	M		

Product Summary | Stack-1 DOC | Stack-1 Notes | SDOC-How-to-Complete

Listo

Figura 12 . Fragmento de la plantilla Excel del USGv6.

La complejidad de los artilugios está condicionada por el carácter grado de carácter contractual del mismo. Según la legislación vigente, estos elementos podrán considerar legalmente vinculantes o complementos de aporte de información. En el primero de los

casos, la información solicitada y su organización debe de cuidarse en extremo por las implicaciones asociadas.

11. ANEXO III – MODELO DE TABLA PARA VALORACION DE COMPETENCIAS Y EXPERIENCIA

Para la justificación de los conocimientos de los miembros del equipo de trabajo se propone el siguiente modelo:

- En la redacción del pliego, incluir una tabla resumen con las competencias y conocimiento a evaluar para cada tipo de perfil solicitado. Para estos conocimientos y competencias se definirán los requisitos mínimos y deseables para facilitar el aporte de información por parte del ofertante.

  A continuación se puede ver un modelo para esta tabla:

Tabla 3: Plantilla de tabla de competencias y conocimientos

Competencias / Requisitos	Mínimo	Deseable
Conocimiento x	Formación / Certificación	Experiencia mínima de 1 año
Competencia y	Experiencia de 2 años	Experiencia superior
…	…	

- El ofertante deberá de cumplimentar una tabla equivalente a la anterior en la que se indique, para cada conocimiento o competencia, el grado de cumplimiento del mismo.

  Para este fin, el licitador debe aportar una plantilla a rellenar por el ofertante para cada individuo incluido en la oferta o incluir dicha información en un modelo de resumen de Curriculum Vitae como el que se muestra a continuación, el cual puede solicitarse como complemento de un Curriculum Vitae en formato Europass [64]. En este modelo el apartado de competencias y modelos debe generarse de forma paralela a la taba de competencias anterior.

Tabla 4: Modelo de resumen de CV incluyendo conocimiento y competencias

Identificación de oferta:	<Denominación y código de la oferta>
Empresa licitante:	**<Nombre de la empresa>**
Nombre y apellidos del empleado:	**<Nombre del empleado>**

Antigüedad en empresa, antigüedad en categoría y experiencia					
Empresa	**Categoría**	**F-alta**	**F-baja**	**Meses**	**Actividad Relacionada**
<Empresa 1>	…	…	…	…	…
<…>	…	…	…	…	…

Titulación académica			
Título académico	**Centro**	**Años**	**F-exped.**
<Titulo 1>	…	…	…
<…>	…	…	…

Formación						
	Entorno del proyecto			**Otros entornos**		
Curso	**Horas**	**Empresa**	**F-Inicio**	**Horas**	**Empresa**	**F-Inicio**
<Curso 1>	…	…	…	…	…	…
<…>	…	…	…	…	…	…

Competencias y Conocimientos (según tabla de competencias y conocimientos)	
	Grado de Cumplimiento
Conocimiento x	<Experiencia y/o formación que justifique el conocimiento x>
Competencia y	<Experiencia y/o formación que justifique la competencia y>
…	…

Idiomas			
Inglés	**Francés**	**Alemán**	**Otros (especificar)**

12. ANEXO IV – MODELO DE ENCUESTA PARA PROVEEDORES DE COMUNICACIONES

A modo de ejemplo, se muestran un conjunto de preguntas que podrían realizarse para determinar las capacidades del proveedor en los servicios de conectividad extremo a extremo, concretamente, en lo referente a la conectividad con Internet.

Junto con cada pregunta se aporta información orientada a la evaluación de la respuesta de la misma estableciendo la siguiente clasificación:

- Obligatorio: mínimo exigido para el aspecto sobre el que se pregunta. Es bloqueante.
- Deseable: mejora sobre el mínimo de obligado cumplimiento que se tendrá en cuenta en la evaluación, aportando más valor. Identifica la solución más apropiada.
- Opcional: mejora o particularidad que habitualmente excede de lo deseable y, por tanto, se valorará como mejora.
- Comentario: apreciación de apoyo para la generación de la respuesta por el ofertante o para la evaluación de la respuesta por parte del licitador.

Tabla 5: Ejemplo de listado de preguntas a realizar a un proveedor de conectividad

Nº	Preguntas	
1	Número y nombre de los upstreams IPv6 que utiliza y que prevé utilizar en el futuro.	
	Obligatorio	Al menos deberá disponer de dos upstreams IPv6 y que sean de primer nivel y en ambos sea visible el 100% de la tabla de rutas.
2	Tipo de técnica utilizada para el transporte de IPv6 en el ISP.	
	Obligatorio	El transporte IPv6 no se realizará utilizando mecanismos túnel.
	Deseable	El transporte IPv6 se realizará utilizando doble pila, 6PE ó 6VPE.
	Opcional	El transporte IPv6 se realizará utilizando softwires.
3	Conectividad IPv4 e IPv6 con el cliente.	
	Obligatorio	Los circuitos establecidos entre el cliente y el ISP podrán soportar simultáneamente IPv4 e IPv6 en el mismo circuito físico.

	Opcional	Será posible el establecimiento de circuitos físicos o lógicos dedicados para IPv6 exclusivamente[10]
4	Protocolos de encaminamiento con el cliente.	
	Obligatorio	Se soportará enrutamiento estático y BGP.
	Deseable	Se soportará RIPng.
	Opcional	Se soportará OSPFv3 e IS-IS y se soportará EIGRP para IPv6.
5	Anuncio de la tabla completa de enrutamiento de IPv6.	
	Obligatorio	El operador deberá disponer de la capacidad de anunciar la tabla completa de rutas IPv6. El operador deberá ser capaz de anunciar una ruta por defecto al cliente.
6	Máxima longitud de prefijo permitido en los anuncios IPv6, tanto por el proveedor como por sus upstreams.	
	Obligatorio	El operador y sus upstreams deben ser capaces de admitir prefijos /48.
	Opcional	Soporte de prefijos más específicos.

Como apoyo a la generación de las listas de preguntas, se sugiere el análisis de las recomendaciones publicadas por CISCO [18].

[10] Pensando en el momento en que se desee desactivar IPv4, aunque previsiblemente no a corto plazo.