Título: Servicios telemáticos transeuropeos entre administraciones: TESTA II y la EXTRANET del Consejo de la Unión Europea.

Autor: Miguel A. Amutio Gómez

Resumen: TESTA II materializa la interconexión de las redes administrativas de los Estados miembros de la Unión Europea a través de una red troncal común, de forma que hace posible la implantación de aplicaciones telemáticas transeuropeas de intercambio de datos entre Administraciones.
La Extranet del Consejo de la Unión Europea, que tiene abierta la posibilidad de utilizar la infraestructura y servicios de TESTA II en un futuro próximo, resulta de gran interés por el tratamiento de los aspectos de seguridad realizado en su ámbito.

TESTA II y la Extranet permiten la integración de nuestra Administración en las redes administrativas transeuropeas y constituyen, además, una referencia técnica para el desarrollo de la Intranet Administrativa.

Biografía: Miguel A. Amutio Gómez es Consejero Técnico de la Subdirección General de Coordinación de Recursos Tecnológicos de la AGE, Ministerio de Administraciones Públicas. Es asesor técnico del Grupo de Usuarios de Telcomunicaciones en la Administración (GTA). Participa en diversos Comités y Grupos de Trabajo del ámbito de la Comisión Europea y del Consejo de la Unión Europea. Es miembro de la delegación española en el 'Comité de Telemática entre Administraciones' que asiste a la Comisión Europea en relación con el Programa IDA (Intercambio de Datos entre Administraciones); y del 'Grupo de trabajo de conexiones electrónicas - seguridad de datos' del ámbito del Consejo de la Unión Europea.

1. Las Redes Administrativas Telemáticas Transeuropeas

La prestación de servicios a través de todo el territorio de la Unión Europea por parte de las administraciones a los ciudadanos, empresas y a otras administraciones requiere y genera a la vez numerosos intercambios de información. Se pueden destacar, por ejemplo, los relativos a empleo y seguridad social; asistencia sanitaria y farmacovigilancia; introducción y gestión de la moneda única; información entre empresas y administraciones en temas de aduanas y fiscalidad; marcas y tráfico ilegal de bienes culturales; datos estadísticos; diversidad biológica y medio ambiente; normas técnicas y regulaciones; mercado de las telecomunicaciones; y un largo etc.

Para abordar el establecimiento efectivo de la interoperabilidad de los sistemas de información de los Estados miembros, se lanzó en 1995 la acción IDA I, mediante la *Decisión (5/468/CE) del Consejo de la Unión Europea, de 6 de noviembre de 1995, sobre la contribución comunitaria al intercambio telemático de datos entre las administraciones en la Comunidad*. La acción IDA I perseguía el desarrollo de una infraestructura de servicios telemáticos y evitar así la creación de barreras innecesarias debidas a la adopción descoordinada de soluciones particulares.

Posteriormente, en 1999, se lanzaron las decisiones IDA II:

- *Decisión 1719/1999/CE del Parlamento Europeo y del Consejo de 12 de julio de 1999, sobre un conjunto de orientaciones, entre las que figura la identificación de los proyectos de interés común, relativo a redes transeuropeas destinadas al intercambio electrónico de datos entre administraciones (IDA).*
- *Decisión 1720/1999/CE del Parlamento Europeo y del Consejo de 12 de julio de 1999, por la que se aprueba un conjunto de acciones y medidas al objeto de garantizar la interoperabilidad de las redes telemáticas transeuropeas.*

Estas dos decisiones conceden especial atención al desarrollo de los servicios telemáticos genéricos:

- La Decisión 1719/1999 establece que los Proyectos IDA, así como otras redes sectoriales, se realizarán sobre la base de las acciones y medidas horizontales comunitarias, en particular, en lo que se refiere a los servicios genéricos.
- La Decisión 1720/1999 tiene por objeto establecer un conjunto de medidas que permitan la convergencia de las redes telemáticas administrativas establecidas en los Estados miembros y entre la Comunidad y los Estados

miembros. Todo el esfuerzo va encaminado a garantizar la interoperabilidad entre las distintas infraestructuras físicas, servicios y contenido de la información, lograr una interfaz telemática común, acelerar la creación de nuevas redes, realizar un intercambio de datos seguro y fiable, controlar los costes, y lograr capacidad de respuesta y flexibilidad, así como adaptación a los cambios tecnológicos.

- Finalmente, ambas decisiones establecen que los proyectos IDA técnicamente estarán basados en normas europeas o especificaciones de acceso público, como las normas abiertas de Internet, al objeto de garantizar un elevado nivel de interoperabilidad.

Por otra parte, el Programa IDA gestionado por la Dirección General de Empresa de la Comisión Europea, se encarga de proporcionar, en el marco de las citadas decisiones, el soporte a la implantación de estas redes telemáticas transeuropeas. A grandes rasgos, persigue definir reglas para la construcción de los sistemas telemáticos, proponer recomendaciones organizativas y técnicas para estos sistemas, respetando el principio de subsidiariedad, e impulsar y promover la propia construcción y desarrollo de los sistemas telemáticos y de los servicios genéricos.

La acción TESTA es la materialización del desarrollo de servicios telemáticos genéricos que apoyen la implantación de aplicaciones telemáticas transeuropeas de intercambio de datos entre Administraciones.

2. Los Servicios Telemáticos Transeuropeos entre Administraciones: TESTA

2.1. TESTA

La acción TESTA (*Trans-European Services for Telematics Between Administrations*) se lanzó en 1995, en el marco de IDA I, con el objetivo de proporcionar un catálogo completo y bien estructurado de servicios telemáticos que facilitasen el intercambio de datos y asegurasen la interoperabilidad. Este catálogo incluía servicios relativos a correo electrónico, directorio, EDI, servicios IP, X.25, *Frame Relay*, acceso *dial-up*, líneas dedicadas punto a punto, VSAT, ATM, así como otros servicios de soporte y de supervisión de la red. La Comisión Europea mediante concurso público adjudicó la prestación de los servicios TESTA al operador Global One en 1996.

Durante el período entre los años 1996 y 2000, las redes TESTA se implementaron sectorialmente, es decir, en función de la demanda de un sector determinado (farmacia,

agricultura, estadística, etc.). Este enfoque dio lugar al desarrollo de numerosas conexiones *ad hoc,* independientes unas de otras, con la consecuencia de elevados costes para los usuarios y existencia de enlaces duplicados.

Por otra parte, en esta etapa se fue madurando el concepto denominado TESTA IPNet, como solución para aquellos usuarios de servicios telemáticos en el contexto de IDA que deseasen disponer de servicios de red IP como plataforma de ámbito europeo. Se trata de una visión de red europea administrativa IP, que permita que una administración pueda comunicarse telemáticamente con cualquier otra, teniendo en cuenta la creciente capilaridad en las relaciones entre administraciones, extendida hasta los niveles regional y local. Según este enfoque, cada proyecto IDA que conecta a una comunidad de usuarios a través de los Estados miembros, hace uso de una plataforma de servicios telemáticos basada en servicios de red IP, aislada de Internet, sobre la cual se pueden definir *extranets* para cada comunidad de usuarios de un proyecto IDA.

La evolución de TESTA durante este período mostró, por una parte, el agotamiento de un modelo según el cual se establecían conexiones *ad hoc* según las necesidades de los proyectos sectoriales y, por otra parte, la conveniencia de avanzar hacia un enfoque global de red IP administrativa transeuropea común.

2.2. TESTA II

TESTA II persigue la interconexión de las redes administrativas de los Estados miembros a través de una red troncal común (conocida como *EuroDomain*), de forma que sean posibles los intercambios de datos transeuropeos. Las redes administrativas nacionales (conocidas como *Local Domains*), conectadas a través de la red troncal del *EuroDomain,* pueden acceder a ésta por medio de ubicaciones específicas (conocidas como *EuroGates*). Dicho de otra forma, se proporciona a cada red administrativa nacional un enlace de conexión con TESTA II, en un esquema de red privada virtual que permite la conexión *any-to-any*. La figura 1 muestra este modelo conceptual adoptado por TESTA II.

La prestación de los servicios de TESTA II a nivel europeo (*EuroDomain backbone services*) y a nivel local (*Local Domain Services*) fue adjudicada por la Comisión Europea mediante concurso al operador Global One a finales de 1999.

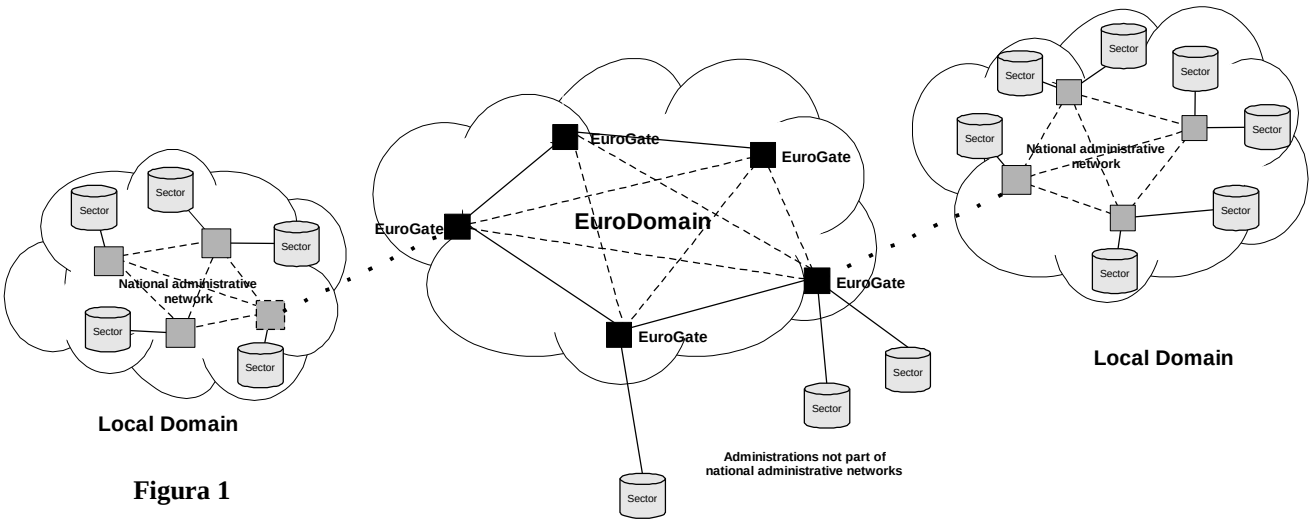

Figura 1

TESTA II es, por tanto, una red de redes, no conectada a Internet (salvo por ciertos puntos de conexión seguros), cuyos servicios se apoyan en la familia de protocolos TCP/IP y en la solución de red privada virtual aportada por el operador de la misma, que se apoya sobre ATM para servicios de transporte. La solución de red privada virtual se ha implantado en base a tecnología propietaria CISCO de encaminadores que facilite la posterior evolución hacia la norma *Multi-Protocol Label Switching* (MPLS) elaborada por IETF (RFC 2547). Por otra parte, esta red privada virtual puede soportar protocolos de acceso tales como ATM, *Frame Relay* o IP nativo.

2.2.1. Servicios prestados por TESTA II

Los servicios proporcionados por TESTA II a los Estados miembros son, esencialmente, enlaces de las respectivas redes administrativas nacionales a la red troncal europea, a través de un enlace y de una línea de acceso dedicada, con unas características determinadas de ancho de banda y calidad del servicio. De esta forma, cada Estado miembro dispondrá de un enlace con TESTA II para canalizar el tráfico de las aplicaciones sectoriales con las Instituciones Europeas, Agencias Europeas, las administraciones de otros Estados miembros, etc.

Más en detalle, para cada red administrativa nacional conectada a TESTA II se contemplan los siguientes servicios:

- Un puerto de acceso a la red TESTA II (*EuroGate*) con una características de ancho de banda, servicio y perfil de tráfico determinados (puerto de acceso a la red privada virtual proporcionada por el operador).
  En nuestro país, la Red Interministerial de Comunicaciones, embrión de la futura Intranet Administrativa, se conecta mediante un encaminador CISCO

3620 *Customer Edge - CE*), ubicado en instalaciones del Ministerio de Administraciones Públicas, conectado a través una línea dedicada *Frame-relay* con el encaminador (*Provider Edge - PE*) ubicado en instalaciones del operador, que es el *EuroGate* propiamente dicho.

- Una línea dedicada con capacidad de hasta 2Mb/s para acceso desde la red administrativa nacional al *EuroGate*. En nuestro caso se dispone de una línea dedicada *Frame-Relay* conectada al encaminador (CE) ubicado en el Ministerio de Administraciones Públicas con un ancho de banda de 256 Kbps.
- Un enlace RDSI que sirve de *backup* de la línea dedicada, incluyendo el equipamiento de *backup* y la propia RDSI. En nuestro caso se han habilitado dos líneas RDSI que proporcionan un ancho de banda conjunto de 256 kbps.
- También se incluye un modem *dial-in* para configuración y mantenimiento remotos del encaminador CE.
- Configuración de red privada virtual y del encaminador según un esquema definido de direccionamiento, perfil de tráfico, etc.
- Servicios de gestión de red y encaminamiento que incluyen un seguimiento proactivo 24 horas al día por 7 días a la semana.

La figura 2 muestra un esquema detallado del modelo de conexión de una red administrativa nacional a TESTA II.

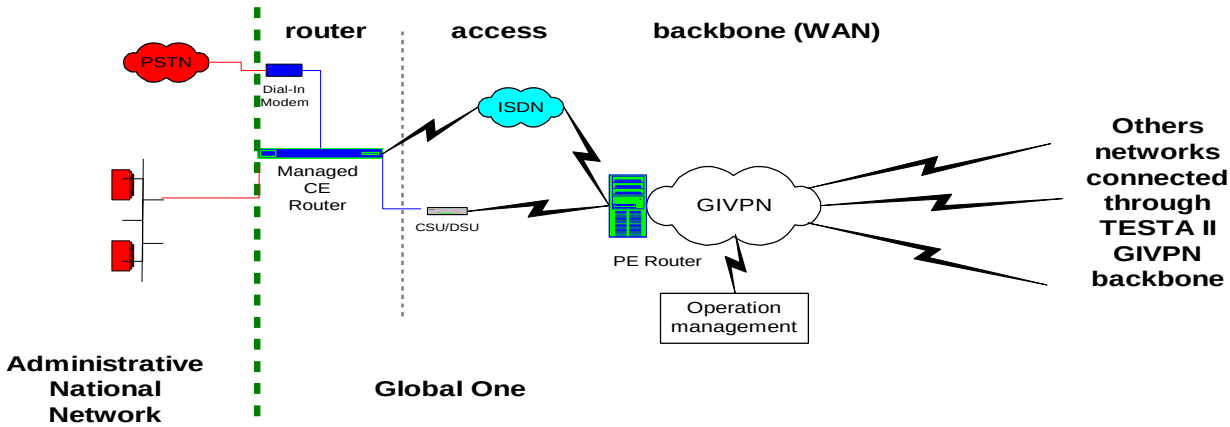

Figura 2

Como se puede observar en el gráfico, la frontera (línea punteada gruesa) se establece en el puerto de red local del encaminador (CE) instalado en la red administrativa nacional. Obviamente el Dominio Local es responsable de la gestión de sus propias redes incluyendo el diseño, la configuración, el rendimiento y la explotación. En la zona entre las dos líneas punteadas se ubican los elementos de

interconexión entre la correspondiente red administrativa nacional y la red troncal TESTA II.

Inicialmente se ha configurado una única red privada virtual para toda la red TESTA II. Dado que se ofrece conectividad *'any to any'*, desde la Intranet Administrativa se pueden intercambiar datos con cualquier otra red que esté conectada al *EuroDomain* TESTA II.

El contrato en curso de TESTA finaliza en diciembre del año 2000, por lo que en la segunda mitad de este ejercicio y principios del 2001 se está procediendo a realizar la migración de los enlaces *ad hoc* de TESTA, que mantienen todavía algunas aplicaciones sectoriales, a la nueva infraestructura de servicios de TESTA II, una vez que los respectivos enlaces con las redes administrativas nacionales de los Estados miembros se hayan establecido.

2.2.2. Direccionamiento IP y DNS en TESTA II

La política de direccionamiento IP de TESTA II contempla la utilización de rangos de direcciones IP asignados por RIPE (Autoridad de Registro IP para Europa) que serán administrados por el operador de TESTA II en nombre de la Comisión Europea. De hecho ya se ha reservado una clase B para TESTA II (62.62.0.0). La citada política cuenta con supuestos tales como los siguientes:

- Todos los servidores ubicados en dominios locales a los que se acceda vía la red TESTA II tendrán direcciones IP registradas correspondientes al rango asignado por RIPE a TESTA II. Los dominios locales deben asegurarse de que ninguna de estas direcciones sea propagada a través de Internet.
- Sólo se encaminarán por la red troncal de TESTA II las direcciones citadas en el punto anterior. Las direcciones que no pertenezcan a este conjunto no serán encaminadas. Las direcciones registradas que puedan estar siendo utilizadas por los dominios locales fuera del rango asignado a TESTA II tampoco serán encaminadas por el *EuroDomain*.
- No se encaminará el tráfico Internet por el *EuroDomain*.
- El tráfico desde los dominios locales hacia Internet no será encaminado por el *EuroDomain*. La conexión a Internet tendrá lugar en el ámbito de los propios dominios locales, de forma que los aspectos de seguridad resultantes de esta conexión serán gestionados a nivel del dominio local y no formarán parte del ámbito de TESTA II.
- Los requisitos de seguridad de los dominios locales en relación con la conexión a TESTA II serán determinados y controlados dentro de los mismos.

El uso de direcciones IP públicas da lugar a ciertos riesgos en el caso de que, de forma inadvertida, estas direcciones internas de TESTA II se den a conocer en Internet. Esta situación se puede dar si un dominio local anuncia las rutas internas de TESTA II a través de su conexión a Internet y pudiera resultar en que la red troncal TESTA II fuera visible para cualquiera que fuera capaz de superar las barreras de seguridad del dominio local.

En cuanto al DNS se contempla una estructura bajo 'testa.eu.int'. De esta forma los servicios disponibles para los dominios locales a través de TESTA II deberán usar un nombre DNS bajo el dominio TESTA (por ejemplo: subnivel.testa.eu.int).

3. Extranet del Consejo de la Unión Europea

La creación de la Extranet del Consejo de la Unión Europea responde a un mandato realizado por los Estados miembros a la Secretaría General del Consejo de la Unión Europea. Este mandato se refiere al establecimiento de una red privada IP que enlace telemáticamente la citada Secretaría con la Representaciones Permanentes de los Estados miembros, en Bruselas, y con las Administraciones nacionales, en las correspondientes capitales, para el intercambio de información de carácter institucional.

La Extranet del Consejo de la Unión Europea, que corresponde a lo que en la antes citada Decisión 1719/1999 se denomina 'Otras redes sectoriales' y cuyos servicios de red IP se han adjudicado en el interludio entre TESTA y TESTA II a British Telecom, tiene abierta la posibilidad de utilizar la infraestructura y servicios de TESTA II en un futuro próximo y resulta de gran interés por el tratamiento de los aspectos de seguridad realizado en su ámbito.

3.1. Arquitectura

La arquitectura de la Extranet responde al esquema general que se muestra en la figura 3. Donde los globos TOE (*Target of Evaluation*) A, B, C, D, etc., constituyen dominios ubicados en los Estados miembros, la Secretaría General del Consejo y la Comisión que contienen los recursos a los que acceden exclusivamente los usuarios de la Extranet. Por otra parte, los globos Intranet A, B, C, D, etc., fuera del ámbito de la Extranet, corresponden a las respectivas redes administrativas nacionales de los Estados miembros.

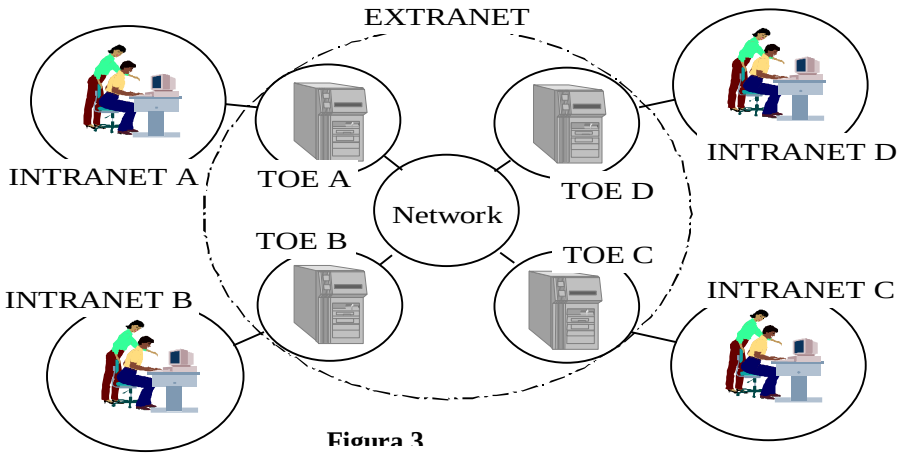

Figura 3

3.2. Servicios

La Extranet persigue que los Estados miembros puedan disponer, con mayor agilidad y en menor plazo, de los documentos oficiales del Consejo de la Unión Europea, así como facilitar el acceso a fuentes de información que son de gran interés para las respectivas administraciones nacionales. Las funcionalidades contempladas son las siguientes:

- En primer lugar, la remisión de documentos oficiales del Consejo desde la Secretaría a los Estados miembros (*pushing* de documentos).
- En segundo lugar, que los Estados miembros puedan acceder, a través de los usuarios autorizados, a los repositorios de información de la Secretaría ubicados en Bruselas para recuperar documentos (*pulling* de documentos).
- Adicionalmente, se contempla la posibilidad de disponer de otras funcionalidades tales como correo electrónico oficial, correo electrónico interpersonal, acceso al archivo histórico de documentos oficiales, acceso a la base de datos de reuniones del COREPER, del Consejo y de los Grupos de trabajo. Asimismo, podrá proporcionar acceso a otras fuentes de información de interés como, por ejemplo, la base de datos de notas de prensa del Consejo y otros puntos de información que los Estados miembros puedan poner a disposición.

De forma que el proceso podrá realizarse en las dos direcciones; en un sentido recepción de documentos; y en el otro sentido, navegación y búsqueda de documentos.

Estos servicios se prestarán a un número de usuarios potenciales cercano a 10.000, estructurado en más de 200 grupos de trabajo.

Por la Extranet circularán, de acuerdo con la clasificación de información en el ámbito del Consejo, los documentos de las categorías ***Limité*** y ***Restreint***. Los documentos de las

categorías superiores *Confidential* y *Secret* quedan fuera de la Extranet.

- *Limité*. Se trata de documentos para uso interno solamente; es la asignación por defecto y quien tiene acceso a este tipo de documentos es el personal que trabaja para la Administración en condiciones de sigilo. Representa el acceso mínimo y por defecto.
- *Restreint*. Se trata de documentos a los que se accede según el principio de 'necesidad de conocer' determinado por la pertenencia a un determinado grupo de trabajo. El acceso a este tipo de documentos viene justificado por la función.

3.3. Enfoque de seguridad

La salvaguarda de la autenticidad, confidencialidad, integridad y disponibilidad, tanto de la información intercambiada, como de los servicios proporcionados por la Extranet, requiere el acuerdo sobre objetivos, procedimientos, clasificación de la información y medidas de seguridad. El 'Grupo de Conexiones Electrónicas - Seguridad de Datos', formado por representantes de los Estados miembros, la Secretaría del Consejo y la Comisión tiene el mandato de definir la política de seguridad de la Extranet.

La política de seguridad de la Extranet se articula en torno a las siguientes piezas clave:

- el 'Perfil de Protección de la Extranet (EPP2)';
- el '*Memorandum* sobre el tratamiento de la información clasificada en la Extranet';
- otros documentos adicionales, sobre política de control de acceso, etc.

3.3.1. Arquitectura de seguridad

La figura 4 muestra la arquitectura de seguridad de la Extranet que se articula en torno a 5 elementos principales:

1. Dominio privado. Corresponde a las redes administrativas nacionales de los Estados miembros, de la Comisión y del Consejo y redes locales de las Representaciones Permanentes en Bruselas que se conectan a la Extranet. Equivale a lo que en el ámbito de TESTA II se conoce como *Local Domain*.
2. Cortafuegos. Constituye una barrera cuya función principal es el filtrado del tráfico IP.
3. Servidores de la Extranet. Soportan servicios visibles desde la Extranet, tales como servicios *web*, bases de datos, correo, etc.

4. Dispositivo de cifrado de tráfico IP. Realiza las funciones de cifrado y descifrado del tráfico IP, saliente o entrante entre el dominio accesible por la Extranet y la red IP.
5. Proveedor de servicios de red IP. Proporciona los servicios de red IP. Equivale a la red troncal de TESTA II.

En esta estructura la Secretaría del Consejo es una parte más al mismo nivel que los Estados miembros, de tal forma que todos los dominios deben compartir un nivel similar de protección.

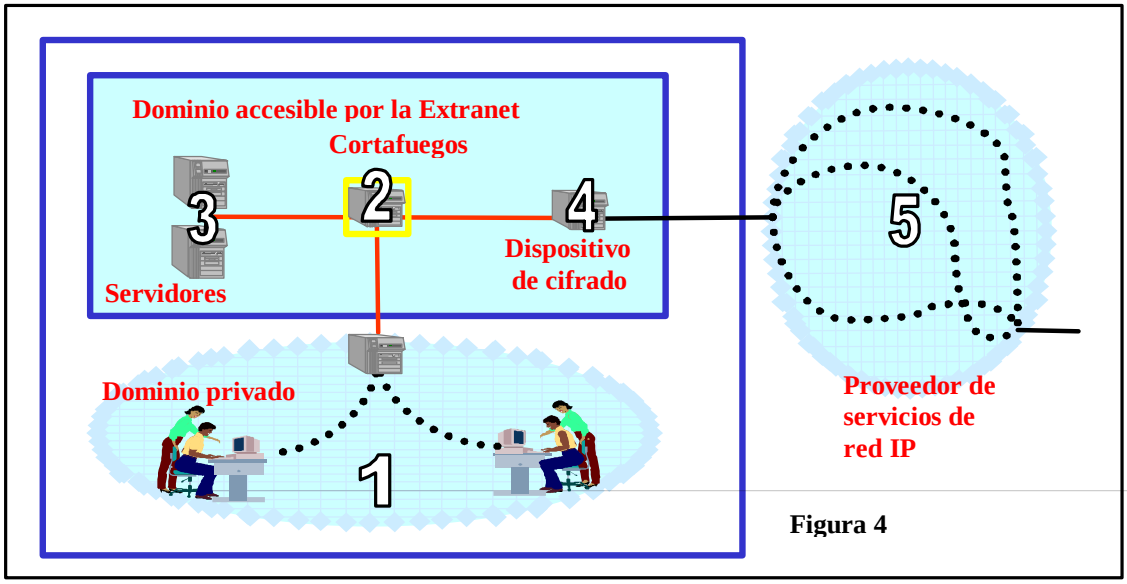

Figura 4

3.3.2. El Perfil de Protección de la Extranet

El 'Perfil de Protección EPP2 para la Extranet del Consejo' se ciñe al ámbito del 'Dominio accesible por la Extranet'. Este ámbito forma el *Target of Evaluation* (TOE) en el que se incluyen el cortafuegos (2), los servidores de la Extranet (3) y el dispositivo de cifrado (4). Si bien el dominio privado (1) y el proveedor de servicios de red IP (5) quedan fuera del TOE, el perfil de protección incluye para ellos requisitos mínimos de seguridad que se convierten en recomendaciones y cláusulas de seguridad a satisfacer respectivamente.

El perfil de protección constituye un instrumento para la formalización:

- de la descripción de los dominios de seguridad ubicados en la Secretaría General del Consejo, en las Representaciones Permanentes y en las capitales de los Estados miembros;
- de los supuestos, objetivos y políticas de seguridad;
- de las posibles amenazas;

- de las funciones de seguridad requeridas;
- de los requisitos de aseguramiento requeridos.

Además permite:

- La definición de los requisitos de seguridad que deben ser satisfechos por la Extranet, de manera que también puedan utilizarse como prescripciones técnicas para la adquisición de determinados elementos del sistema.
- El intercambio de información y la construcción del consenso entre los participantes en su elaboración, en relación con la especificación de los aspectos de seguridad del sistema.

Este Perfil de Protección se basa en la aplicación de los Criterios Comunes para la Evaluación de la Seguridad de la Tecnología de la Información, del documento ISO/IEC WD 15446, "*Guide on the production of PPs and STs*" y del perfil de protección CS2.

El hecho de que los Criterios Comunes de Evaluación de la Seguridad de la Tecnología de la Información se hayan convertido recientemente en la norma internacional ISO/IEC 15408, refuerza la decisión de elaborar las recomendaciones de seguridad de la Extranet como un perfil de protección basado en su aplicación. Este enfoque es cualitativamente superior a cualquier otro que carezca de un soporte formal semejante y resulta de gran interés como modelo para su aplicación en proyectos que se desenvuelven en un entorno tecnológico similar.

4. Conclusiones

TESTA II y la Extranet permiten la integración efectiva de nuestra Administración en las redes administrativas transeuropeas. Constituyen, además, una referencia técnica para el desarrollo de la Intranet Administrativa en cuanto a los criterios y recomendaciones relativos a las opciones tecnológicas, a la infraestructura física, a los servicios prestados y a las medidas de seguridad que se definan.

Tanto TESTA II como la Extranet configuran un modelo en el que las respectivas redes administrativas (*intranets*) de los Estados miembros y de instituciones de la Unión Europea se interconectan mediante enlaces con una red troncal. Al igual que nuestro país con la Intranet Administrativa, los demás Estados miembros o bien ya disponen de *intranets* administrativas o bien se encuentran en fase de desarrollarlas.

Referencias:

- Información sobre IDA en: http://www.ispo.cec.be/ida/
- Criterios Comunes en: http://csrc.nist.gov/cc/