TEMA 120. LAS REDES PÚBLICAS DE TRANSMISIÓN DE DATOS. LA RED SARA. LA RED TESTA. PLANIFICACIÓN Y GESTIÓN DE REDES.

Actualizado a 16/04/2023

1. ALCANCE DEL TEMA

Este documento pretende describir las principales características de la red **SARA** y el servicio de red **TESTA**. Así como los fundamentos de la planificación y gestión de redes.

2. RED SARA

La **Red SARA** (Sistemas de Aplicaciones y Redes para las Administraciones) es un conjunto de infraestructuras de comunicaciones y servicios básicos que conecta las redes de las Administraciones Públicas Españolas e Instituciones Europeas facilitando el intercambio de información y el acceso a los servicios.

2.1. CONTEXTO NORMATIVO

A continuación se incluye tabla resumen con el contexto normativo, tanto vigente como derogado, de la red SARA:

NORMA	ESTADO DE LA NORMA	COMENTARIOS
Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.	**DEROGADA**	**Artículo 43.** **Red de comunicaciones de las Administraciones Públicas españolas**. La Administración General del Estado, las Administraciones Autonómicas y las entidades que integran la Administración Local, así como los consorcios u otras entidades de cooperación constituidos a tales efectos por éstas, adoptarán las medidas necesarias e incorporarán en sus respectivos ámbitos las tecnologías precisas para posibilitar la interconexión de sus redes con el fin de crear una red de comunicaciones que interconecte los sistemas de información de las Administraciones Públicas españolas y permita el intercambio de información y servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados Miembros.
Real Decreto 4/2010 por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica	**VIGENTE**	**Artículo 13. Red de comunicaciones de las Administraciones públicas españolas.** 1. Al objeto de satisfacer lo previsto en el artículo 43 de la Ley 11/2007, de 22 de junio, las Administraciones públicas utilizarán preferentemente la Red de comunicaciones de las Administraciones públicas españolas para comunicarse entre sí, para lo cual conectarán a la misma, bien sus respectivas redes, bien sus nodos de interoperabilidad, de forma que se facilite el intercambio de información y de servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados miembros. La Red SARA prestará la citada Red de comunicaciones de las Administraciones públicas españolas.

		2. Para la conexión a la Red de comunicaciones de las Administraciones públicas españolas serán de aplicación los requisitos previstos en la disposición adicional primera. **Artículo 14. Plan de direccionamiento de la Administración.** Las Administraciones Públicas aplicarán el Plan de direccionamiento e interconexión de redes en la Administración, desarrollado en la norma técnica de interoperabilidad correspondiente, para su interconexión a través de las redes de comunicaciones. (*Se modifica por la disposición final 2.3 del Real Decreto 203/2021, de 30 de marzo. Ref. BOE-A-2021-5032*)
Resolución de 19 de julio de 2011 que aprueba la NTI de requisitos de conexión a la red de comunicaciones de las Administraciones Públicas españolas	**VIGENTE**	Tiene por objeto establecer las condiciones en las que cualquier órgano de una Administración, o Entidad de Derecho Público vinculada o dependiente de aquélla (en adelante, organización), accederá a la Red SARA
RD 806/2014, art. 1 0 Declaración de Servicios Compartidos. CETIC (15/09/2015)	**VIGENTE**	Servicio de nube híbrida (nube SARA) Servicios de computación y almacenamiento en nube híbrida para la AGE y sus OO.PP., mediante la configuración de nodos de consolidación tanto en CPDs de la Administración (nube privada) como de proveedores externos (nube pública)

Resaltamos, además, que el Real Decreto 203/2021, en su Disposición final segunda(punto 8) modifica la Disposición adicional primera del ENI (RD 4/2010) por la que se incluye el mandato de desarrollar nuevas normas técnicas de interoperabilidad que serán de obligado cumplimiento por parte de las Administraciones Públicas. Entre ellas destacamos la **Norma Técnica de Interoperabilidad de Plan de Direccionamiento** que tratará reglas aplicables a la asignación y requisitos de direccionamiento IP para garantizar la correcta administración de la Red de comunicaciones de las Administraciones Públicas españolas y evitar el uso de direcciones duplicadas. A fecha de redacción de este tema, la citada norma técnica aún no ha sido elaborada.

2.2. OBJETIVOS

- ✓ **Comunicar a la Administración General del Estado, a las Comunidades Autónomas y a los Entes Locales**, aplicando criterios de racionalidad técnica y económica, y a todos ellos con **la Unión Europea y sus Estados Miembros**.
- ✓ Proporcionar un conjunto integrado de servicios telemáticos para el **intercambio electrónico seguro de información** entre las **distintas Unidades de la Administración.**
- ✓ Establecimiento de una **Política de Seguridad Común.**

2.3. CARACTERÍSTICAS

- **Fiabilidad**: Red completamente mallada, sin puntos únicos de fallo, tecnología de última generación y soporte 24x7x365.
- **Seguridad**: Tráfico cifrado y Sistema de Alerta Temprana ante incidentes de seguridad, en colaboración con el CCN-CERT.
- **Capacidad**: Ancho de banda de 10 Gbps en Ministerios y 100 Mbps en Comunidades Autónomas.
- **Calidad de Servicio (QoS)**: Cada dato se trata según su naturaleza.

- **Interoperabilidad**: Gateway IPv6 común, para que los servicios de Administración Electrónica puedan ser accesibles a los ciudadanos utilizando conexiones IPv6.

2.4. SERVICIOS

SERVICIOS DE RED

- **Conectividad:** Transporte cifrado, **a través de la Red Troncal de tecnología VPLS,** de cualquier tipo de tráfico, aplicando mecanismos de Calidad de Servicio-QoS (Quality of Service)
  - **Voz sobre IP - VoIP (Voz over IP)**
  - **MallaB (red de telefonía de altos cargos)**
  - **Videoconferencia**
  - **Datos de Aplicaciones**
- **Servicios Telemáticos Básicos:** Se proporcionan a través de Áreas de Conexión (AC) instaladas en cada uno de los Proveedores de Acceso (PAS) en los que la Red SARA tiene un punto de presencia.
  - **DNS (DomainNameSystem)**
  - **SMTP (Simple Mail Transfer Protocol)**
  - **NTP (Network Time Protocol) – Hora Oficial Española proporcionada por el ROA**
  - **Proxy/Proxy Inverso**
  - **Videocolaboración Web (proyecto Reúnete)**
- **Seguridad Perimetral**: De manera coordinada con los responsables de seguridad de la Administración Pública conectada y del CCN-CERT, se proporcionan excelentes niveles de seguridad mediante:
  - **Cortafuegos**
  - **Detectores de Intrusos - IDS (Intrusion Detection System)**
  - **Análisis de Vulnerabilidades**
  - **Correlación de Logs**

SERVICIOS HORIZONTALES A LAS ADMINISTRACIONES PÚBLICAS

Son los servicios comunes, promovidos directamente por la SGAD, que facilitan la consolidación de servicios y sistemas en general, algunos de los cuales favorecen el despliegue de la oferta de administración electrónica. Las diferentes administraciones pueden ser usuarias de ellos para integrarlos con los servicios finales que prestan a sus ciudadanos:

- **Suite de productos y servicios de Firma Electrónica**
- **Sistema de Intermediación de Datos**
- **Centro de Transferencia de Tecnología**
- **Correo Multidominio, Acceda, ORVE, InSIDE, SIR**
- **Reuniones Virtuales (proyecto Reúnete)**

SERVICIOS VERTICALES DE LAS ADMINISTRACIONES PÚBLICAS

Son los servicios que proveen las Administraciones Públicas, **en el marco de sus competencias y bajo su responsabilidad,** que utilizan la Red SARA como mecanismo para su interoperabilidad. Ej.: Servicios Verticales relacionados con Protección Civil y Emergencias (112), servicios de peticiones de becas universitarias, etc.

2.5. ROLES

El apartado V de la NTI de requisitos de conexión a la red de comunicaciones de las Administraciones Públicas españolas incluye los distintos roles que interactúan con la red SARA, así como sus responsabilidades, que pasamos a resumir a continuación:

ROL	RESUMEN DE RESPONSABILIDADES
Ministerio de Asuntos Económicos y Transformación Digital (MAETD)	-Instalará, administrará y mantendrá una conexión de capacidad suficiente y alta disponibilidad ubicada en las dependencias que la Administración pública determine -Proporciona a los responsables del PAS la documentación técnica (arquitectura y AC) Servicio de soporte 24x7 para garantizar la continuidad del servicio -Gestionará el portal web www.redsara.es, como espacio para facilitar información general sobre la Red SARA -Adoptarán las medidas de seguridad necesarias para proteger debidamente la información transmitida, mediante el cifrado de las comunicaciones y la detección temprana de incidentes en colaboración con el CNN-CERT
PAS (Proveedores de Acceso a la Red SARA)	- Realizará las labores de conectividad y despliegue pertinentes para poder acceder desde sus propias dependencias o instalaciones a la Red SARA a través del AC -Gestionará y mantendrá los elementos activos que conecten a su red corporativa a la Red SARA -Garantizarán condiciones adecuadas en la ubicación del AC (condiciones medioambientales, suministros eléctricos, cableado, etc.) con el fin de asegurar la continuidad del servicio -Mantendrán un servicio de soporte, **a ser posible** 24x7, facilitando al MAETD los contactos, tanto de los responsables del PAS como de los Centros de Soporte, CAUs o equivalentes -Colaborará con el MAETD en la gestión de incidentes y problemas -Facilitará, promoverá y sostendrá el acceso a la Red SARA a sus Organismos y Entidades de Derecho Público dependientes y adicionalmente, en el caso de las CCAA, a las Administraciones Locales de su ámbito territorial, con la tecnología, mecanismos y procedimientos que estos

	acuerden, garantizando la continuidad del servicio y las condiciones adecuadas de seguridad en la parte que le corresponde -Colaborarán con el MAETD en el mantenimiento del catálogo de servicios y conexiones
Usuario Final	- Aplicarán las condiciones particulares del PAS del que dependen - Aplicarán condiciones particulares de servicio horizontales y verticales que utilizan a través de la Red SARA

2.6. ARQUITECTURA

El acceso a la Red SARA se realizará a través de lo que se denomina **Punto de Presencia (PdP)** entendido como cualquier sede en la que existe una conexión directa a la Red SARA, sin presencia de ninguna organización intermedia.

Entre los PdPs de la Red SARA podrán distinguirse los siguientes tipos:

1) Proveedores de Acceso a la Red SARA (**PAS**).
    a) Ministerios, AEAT, TGSS, SPEE
    b) Comunidades Autónomas, Ceuta y Melilla
    c) Órganos Constitucionales y Organismos Independientes
        i) Casa de S.M. El Rey
        ii) Consejo General del Poder Judicial
        iii) Tribunal de Cuentas
        iv) Defensor del Pueblo
        v) Consejo de Estado
        vi) Senado
        vii) Agencia Española de Protección de Datos
        viii) Consejo de Seguridad Nuclear
        ix) Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda
        x) Banco de España
2) Centros de Proceso de Datos (**CPD**) de SARA.
3) Red **TESTA** (Trans-European Services for Telematics between Administrations).
4) **Centros externos de monitorización**.
5) **Prestadores de servicios de certificación**.
6) **Otros**: como son las Ventanillas Únicas Empresariales

Finalmente, aunque originalmente se diseña únicamente para interconectar Administraciones Públicas entre sí, a partir de una **Resolución de 4 de julio de 2017 de la SEFP**, se abre la puerta a que entidades privadas que den servicios de administración electrónica en la nube a Administraciones Públicas ubicada en al menos dos Comunidades Autónomas puedan establecer un Punto de presencia (PdP) en la Red SARA. https://administracionelectronica.gob.es/ctt/redsara/masmas#.ZDwPC3ZBxD8

El esquema del Área de Conexión (AC) de un PAS funcionará como punto único de conexión entre la red de la **Administración pública correspondiente y sus organizaciones dependientes o asignadas al PAS**, a las redes de otras **administraciones y Entidades públicas conectadas a la Red SARA, así como a la Red TESTA** de la Comisión Europea. El acondicionamiento físico de las **instalaciones del PAS cumplirá lo establecido a tal efecto en el Real Decreto 311/2022,** de 3 de mayo, por el que se regula el **Esquema Nacional de Seguridad** en el ámbito de la Administración Electrónica de manera que se asegure la continuidad del servicio.

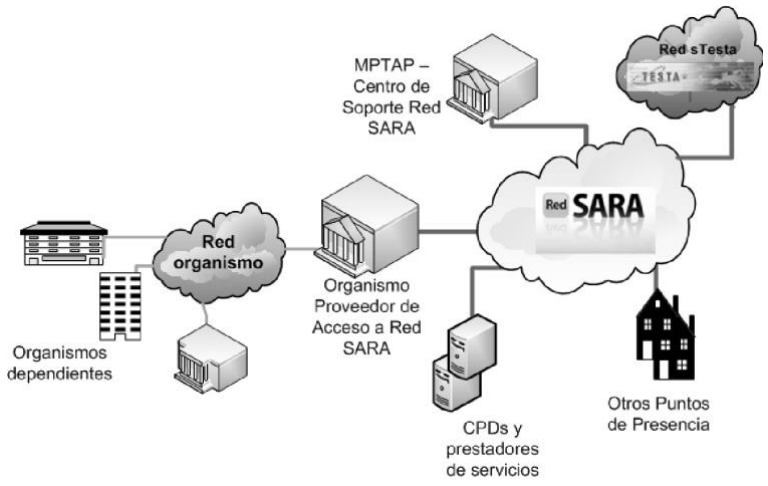
Los elementos del AC, además de proporcionar seguridad perimetral, albergarán los servicios telemáticos básicos prestados por la Red SARA: DNS, SMTP, NTP, Proxy y Proxy inverso**.**

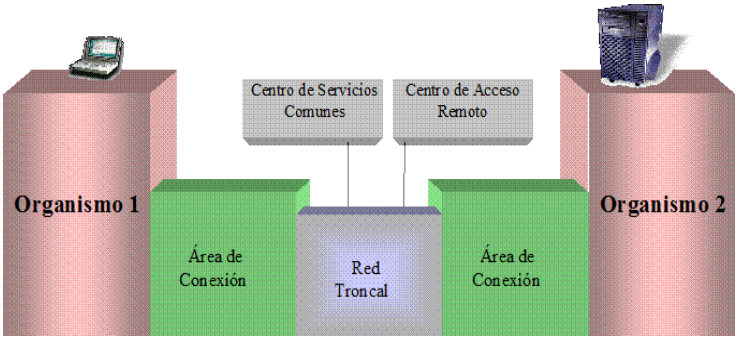
En la zona intermedia, **DMZ**, será **posible conectar cualquier equipo que la organización considere conveniente utilizar para la comunicación con el resto de organizaciones que componen la Red. Estos equipos envían sus alertas al CSC (Centro de Servicios Comunes).**

La red SARA para la **integración y gestión de soporte** consta de los siguientes elementos:

- ✓ **Centro de Atención a Integradores y Desarrolladores**: Encargado de dar soporte de primer y segundo nivel de las peticiones de servicio e incidencias.
- ✓ **Centro de Soporte de la Red SARA**: Servicio **24x7 y 365** días al año, existe **colaboración con el CCN-CERT** para la detección y coordinación temprana de amenazas.
- ✓ **Centro de Transferencia Tecnológica CTT:** repositorio común software para la reutilización de aplicaciones

Nota: Se recomienda la lectura de la guía de aplicación de la NTI de requisitos de conexión a red de comunicaciones de las AAPP españolas, así como de la Resolución de la SEFP sobre los Puntos de Presencia.





2.7. PLAN DE DIRECCIONAMIENTO E INTERCONEXIÓN DE REDES

El Plan de direccionamiento e interconexión de redes en la Administración es necesario para:

- La **interconexión de las redes** de las Administraciones Públicas y en particular a y a través de la Red SARA (Sistema de Aplicaciones y Redes para las Administraciones).
- El **despliegue de servicios** de administración electrónica sobre la Red SARA.
- **La interconexión con redes de Administraciones** de otros Estados miembros de la UE, el despliegue y acceso a los servicios paneuropeos de administración electrónica **a través de la Red SARA y de su enlace con la red transeuropea sTESTA** que tiene a su vez su propio plan de direccionamiento. **La política de direccionamiento IP de TESTA usa unos rangos de direcciones IP asignados por RIPE (Autoridad de Registro IP para Europa**), no encaminables por Internet, y administrados por el operador de TESTA en nombre de la Comisión Europea. **Este rango es el 62.62.0.0.**

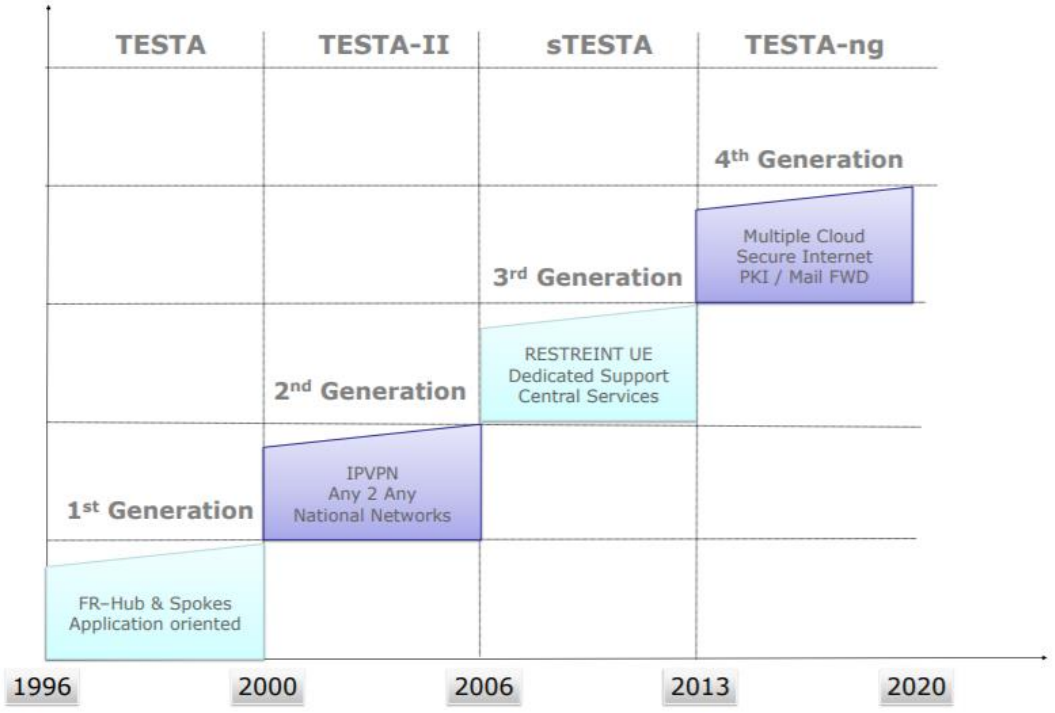
Rango de direcciones IP	Entidad u Organismo
10.252.0.0 /16	Red SARA
10.253.0.0/16	Red SARA
10.254.0.0/16	Cloud de la AGE

3. RED TESTA

En 1996, las instituciones de la Unión Europea se conectaban por primera vez a través de **TESTA (Trans European Services for Telematics between Administrations),** implementada bajo IDA, un programa predecesor de ISA.

En la actualidad el **servicio de red TESTA (Trans European Services for Telematic Administrations) proporciona una red de backbone europea para el intercambio de datos entre administraciones públicas**. La red usa los protocolos de Internet IP **pero es operada por la Comisión Europea separada de Internet**, intercambiando **información clasificada y no clasificada** entre las instituciones europeas.

Gráfica evolución

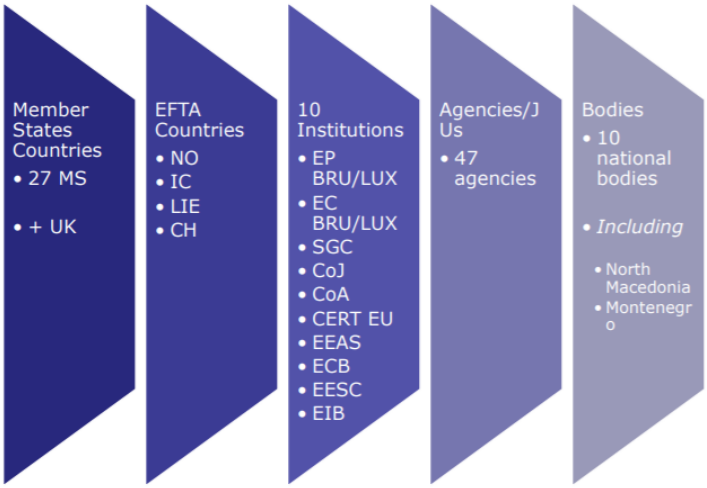


Para la red TESTA, la red SARA es la "National Network" de España, con un punto único de acceso al Eurodomain.

La red **TESTA** es utilizada por:

- **Estados miembros y administraciones públicas**. Los ciudadanos y las empresas están fuera del alcance si bien se benefician indirectamente debido a la protección de los datos personales en la red.
- Varias **redes de diversos sectores** están usando los **servicios TESTA** para sus **aplicaciones sectoriales (OLAF**, DG TREN, ESTAT, DG JLIS, DG SANCO, FISH, DG ENV y DG TRADE). DG: dirección general **OLAF: Oficina anti fraude europea.**
- La red está usada habitualmente por las **instituciones europeas y las agencias europeas**. Además el **framework TESTA** es ampliamente usado por **DG HOME para la implementación de las redes SIS II y VIS II** (espacio **Schengen** y sistema de intercambio de **visados**) y **EUROPOL.**
- Por otro lado, la **Secretaría General del Consejo** está usando **TESTA** para la implementación de **la red FADO (**FALSE AND AUTENTHIC DOCUMENTS ONLINE), la extranet del Consejo y las redes de cortesía.
- La red TESTA se usa también **en proyectos no comunitarios** por los estados miembros y organizaciones, **bajo ciertas condiciones** descritas en el Memorandum, con casos de éxito dentro del contexto del **tratado de Prüm** y l**a unidad de inteligencia financiera** en temas de blanqueo de dinero, **FIUNET.**

Current EURODOMAIN Clients / Profiles



OBJETIVOS

Los objetivos de desarrollo de la red TESTA son los siguientes:

- **Conectividad:** la provisión de una infraestructura de comunicaciones altamente confiable, extensible, flexible y segura entre las administraciones públicas de Europa para que las necesidades actuales y futuras entre esas administraciones puedan ser cubiertas.
- **Consolidación** de redes de datos existentes en la actualidad, diseminadas en diferentes contratos y gestionadas por otras instituciones u organismos europeos.
- **Seguridad:** provisión de una infraestructura de comunicaciones segura, restringida a la UE, acreditable si se requiere.
- **Soporte:** provisión de una única infraestructura de soporte que puede actuar como una entidad simple para afrontar problemas, apoyar a sectores y administraciones, gestión de alertas y de informes.
- **Gestión:** la gestión completa del proyecto así como la gestión del servicio y administrativa de los servicios de red TESTA.
- **Asistencia:** la provisión de servicios de asistencia dedicados al control y auditoría de los servicios de red operacionales.

BENEFICIOS

Los **beneficios** que se obtendrán son:

- **Prevención de la proliferación de las redes sin control**. Acceso a **una red segura trans europea** para el intercambio de datos
- **Acceso a un servicio de red trans europeo seguro** y gestionado para el intercambio de datos con requisitos específicos de **disponibilidad y seguridad**
- Evitar la **implementación innecesaria** de estructuras de red **costosas**
- **Permitir el uso en el contexto de proyectos no comunitarios** por los estados miembro, organismos e instituciones actuando en su nombre, estimulando el uso de una estructura de red existente
- **Proteger** el uso de los **datos personales** en la red.

ENFOQUE ORGANIZATIVO

Más de 91 aplicaciones (**EURODAC, CECIS, FIDES**…) están utilizando **TESTA** para el intercambio de información.

Action / Policy	Description of relation
Eurodac	Council Regulation No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention. Eurodac Legal Basis
CARE	Council Decision of 30 November 1993 on the creation of a Community database on road accidents CARE Legal Basis
FIDES	COUNCIL REGULATION (EC) No 2371/2002 of 20 December 2002 on the conservation and sustainable exploitation of fisheries resources under the Common Fisheries Policy FIDES Legal Basis
HOLIS	Council Regulation (EC) No 1257/96 of 20 June 1996 concerning humanitarian aid HOLIS Legal Basis
SIS II	Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II). SIS II Legal Basis
CECIS	Council Decision 2007/779/EC, Euratom of 8 November 2007 establishing a Community Civil Protection Mechanism. CECIS Legal Basis
SIGL	COUNCIL REGULATION (EEC) No 3030/93 of 12 October 1993 on common rules for imports of certain textile products from third countries. SIGL Legal Basis
Prüm	Trans-border police cooperation in a non-community programme
FIUNET	Financial Intelligence Network (non-community programme)

ENFOQUE DE GOBERNANZA

El enfoque de TESTA es **colaborativo**. Se construye sobre los esfuerzos nacionales de establecer redes de administraciones nacionales, regionales o locales forjándolas a través de una red transeuropea. Cada dominio interconectado deberá cumplir los requisitos necesarios de seguridad, rendimiento y organizativos para acceder a la red TESTA.

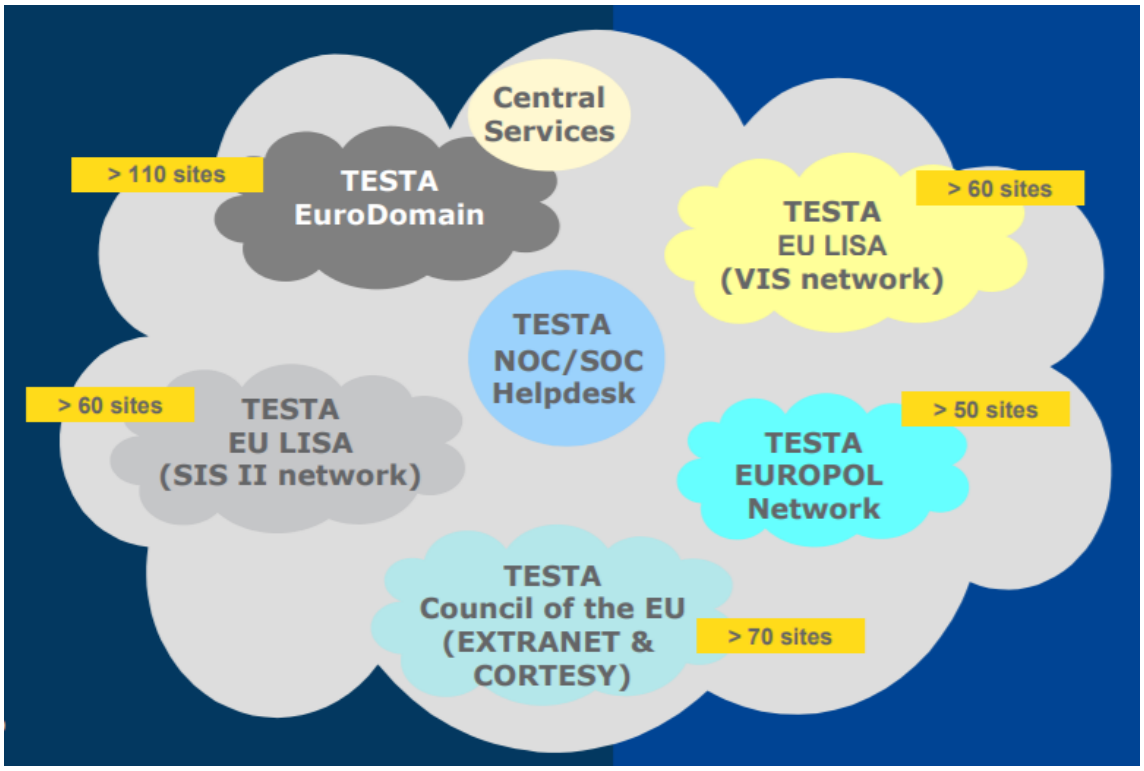
El impacto presupuestario de esa decisión será responsabilidad de las administraciones. La red será controlada por un servicio central de soporte y operaciones, responsable de todos los asuntos operacionales, incluyendo la gestión de seguridad del encriptado de los dispositivos.

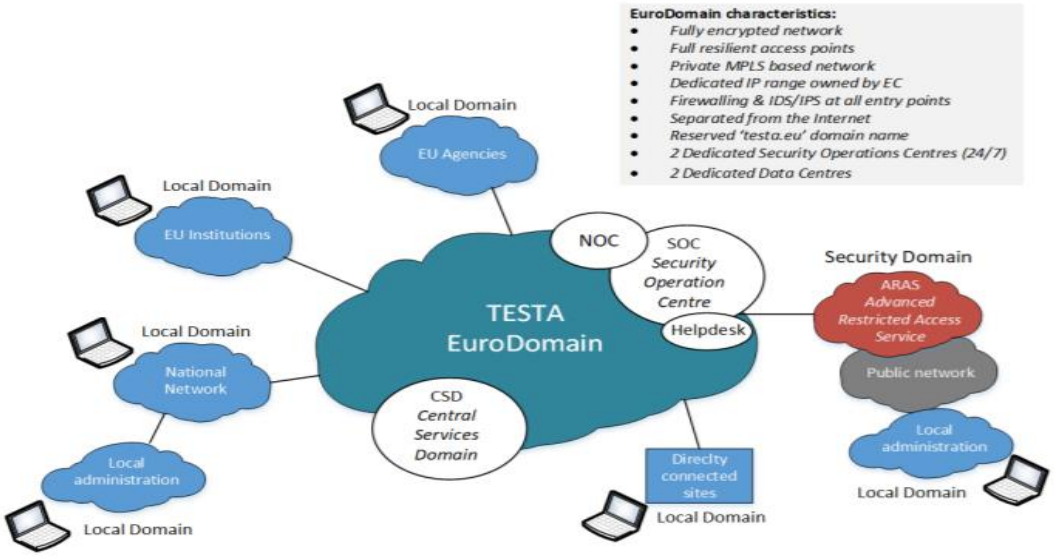
ENFOQUE TÉCNICO

TESTA está basada en una infraestructura completamente resiliente **MPLS encriptada mediante IPSEC.**

La infraestructura está gestionada por un **centro de seguridad operacional (SOC)** y los **servicios genéricos** se proporcionan a través de un dominio altamente securizado **(CSD) Central Service Domain.**

La infraestructura de gestión de red TESTA será totalmente resiliente a través de localizaciones **de backup para SOC y CSD**, de manera que se pueda garantizar la continuidad en caso de desastre. Durante la migración, un *bridge* resiliente será creado entre los dos entornos para que la migración tenga lugar de manera gradual.





.

4. PLANIFICACIÓN Y GESTIÓN DE REDES

La **planificación de redes** debe tener en cuenta en el diseño las estrategias que permitan mantener el servicio ante fallos y procurar que los elementos de red dispongan de las capacidades necesarias. Por su parte, la **gestión de redes** debe establecer los mecanismos para recoger información relevante de seguimiento de la red y que permitan actuar sobre los sistemas de información (red, servidores).

4.1. PLANIFICACIÓN DE REDES

La planificación estratégica de las comunicaciones debe estar integrada o al menos ligada al Plan de sistemas y comunicaciones de la organización. Si la organización es un departamento ministerial, se plasmará en el **Plan director de comunicaciones del Ministerio**, exigido por RD 541/2001.

El Plan Director de Telecomunicaciones proyectará las necesidades globales de servicios de telecomunicación del Departamento y sus Organismos en un período de cinco años, así como las estrategias para su licitación, y estará sujeto a revisiones anuales. Se desarrollará en programas, cuya vigencia será de dos años, que comprenderán los siguientes servicios de telecomunicaciones:

- Telefonía fija.
- Telefonía móvil.
- Alquiler de circuitos.
- Servicios de transmisión de datos.
- Comunicaciones corporativas.
- Servicios de Internet y otros servicios telemáticos e interactivos.
- Otros servicios de valor añadido.

Los pasos recomendados para llevarlo a cabo son los siguientes:

- **Recogida de información y requerimientos**: Recoger entre las distintas unidades, entre otras, información sobre la distribución física de las instalaciones, estructura departamental, servicios necesarios, requerimientos de acceso a la red interna y externo. La información se puede obtener fundamentalmente a través de 2 vías: cuestionarios y herramientas de gestión de red. Estas últimas si están bien diseñadas y configuradas pueden proporcionar estadísticas de uso de la red, inventario de los equipos y enlaces de comunicación e información de interconexión y direccionamiento.
- **Análisis de la situación actual**: Con la información recogida sobre tecnología empleada, equipamiento utilizado, planes de direccionamiento, esquemas de interconexión, presupuestos dedicados a este concepto, personal interno y externo dedicados a estas tareas, etc; se determinan las acciones de mejora necesarias para que la red de comunicaciones responda a los objetivos estratégicos y tácticos de la organización.
- **Solución propuesta**: Las acciones de mejora se agrupan y consolidan en proyectos, y con estos se conforma el plan de proyectos para su planificación e implantación. El plan de proyectos debe contener para cada proyecto: la programación temporal, la dotación de RRHH, las fuentes de financiación y su priorización.
- **Contratación**: En el caso de una Administración, es necesario la sujeción a los procedimientos y condiciones de la contratación administrativa. El RD 541/2001 establece la licitación conjunta de todos los servicios de comunicaciones de los diferentes departamentos y la posibilidad de declarar determinados servicios de comunicaciones como de contratación centralizada a través de la Dirección General de Patrimonio del Estado. El concurso unificado de comunicaciones de cada Departamento debe ser un instrumento básico y horizontal para llevar a cabo buena parte de las acciones de mejora determinadas en el análisis de la situación actual. Se fomenta la división de las necesidades del Departamento Ministerial en **lotes.**

4.2. GESTIÓN DE REDES

La gestión de red puede definirse como el conjunto de procedimientos, facilidades y utilidades que permiten la coordinación, supervisión, mantenimiento y control de recursos distribuidos en una red. Implica asegurar la correcta operación de la red, supervisando el uso de sus componentes, manteniéndolos operativos, planificando los cambios de la red y produciendo informes periódicos sobre su operación.

MODELO DE GESTIÓN

La organización ISO desarrolló un modelo estándar de gestión de red, donde se definen las áreas funcionales que todo sistema de gestión de red debe cubrir y que son las siguientes:

- **Gestión de fallos:** Proporciona mecanismos de detección, aislamiento, diagnóstico y corrección de averías de la red y condiciones de error. En redes cuya caída es crítica, la gestión de fallos debe ser preventiva. En redes donde el tiempo no operativo no es tan crítico, la gestión de fallos debe ser correctiva. El proceso de actuación básico ante una incidencia incluye: determinar los síntomas y aislar el problema, reparar el fallo y probar la solución y registrar la incidencia.

- **Gestión de contabilidad**: Permite evaluar el uso de los recursos de la red y establecer su coste, así como definir la política de tarificación de los servicios y recursos de red utilizados y controlar el uso masivo o abusivo de determinados recursos.

- **Gestión de configuración e identificación**: Persigue hacer el seguimiento, control y actualización de los elementos de red instalados, su nivel de software (versión), sus parámetros operativos,

sus interconexiones, etc. Toda esta información debe recogerse y actualizarse en una base de datos de configuración de red a modo de inventario.

- **Gestión de prestaciones**: Proporciona diferentes parámetros relativos al rendimiento de la red (pej. eficiencia de red, los tiempos de respuesta al usuario y el grado de utilización de los enlaces, etc), con el fin de mantenerlos en unos niveles aceptables mediante el ajuste de la configuración. Puede tener 2 enfoques: reactivo o proactivo.

- **Gestión de seguridad**: Controla el acceso a los recursos de la red, según las políticas de seguridad de red definidas por la organización, para evitar que la red sea saboteada, o que personas sin autorización tengan acceso a información sensible. Se encarga, entre otras cosas de: altas/bajas de usuarios y recursos, autentificación de usuarios, controlar el acceso a recursos o proteger información confidencial.

ESTÁNDARES

En un sistema de gestión de red, los agentes de gestión localizados en los elementos de red, son sondeados periódicamente por la entidad gestora, utilizando un protocolo de gestión. Los principales estándares de gestión de red son:

- **OSI**: Estándar desarrollado por ISO/IEC (7498/4) en colaboración con ITU-T (X.700) para entornos OSI. Los principales elementos del estándar son:
    - Arquitectura: Se basa en la teoría de objetos. Un conjunto de interacciones entre uno o más procesos de gestión (o gestores) residentes en el sistema de gestión y uno o más procesos gestionados (o agentes) residentes en los elementos de red gestionados. Un proceso agente es responsable de uno o más objetos gestionados que son representaciones abstractas de un recurso (ej.: un switch, una cuenta de usuario, etc)
    - Management Information Base (MIB): Repositorio conceptual de datos que contiene toda la información sobre los objetos gestionados, agrupada en función de atributos asociados con los objetos y donde cada atributo de un objeto tiene un valor. Está estructurada jerárquicamente en forma de árbol, en el que cada variable u "hoja" puede representarse de forma simbólica (todo el camino) o mediante forma numérica (secuencia de números).
    - Servicios de Gestión. CMIS (*Common Management Information Service*): Conjunto de servicios para la manipulación, por parte de un proceso gestor, de la información de gestión que mantiene cada proceso agente. El transporte de dicha información se realiza a través de un protocolo de gestión. CMIS proporciona servicios para:
        - Recuperar (Get) y modificar (Set) valores de atributos.
        - Crear (Create) y borrar (Delete) objetos.
        - Controlar (Action) objetos, provocando acciones físicas especiales.
        - Notificar (Event-Report) la ocurrencia de algún suceso.
        - Confirmar eventos.

    - Protocolo de Gestión. CMIP (*Common Management Information Protocol*): Su evolución CMOT (Common Management Over TCP/IP) intenta extender el uso de los estándares de la gestión OSI en el entorno Internet, pero finalmente se abandonó en beneficio del modelo SNMP.

El **modelo OSI** presenta como **limitaciones**: Ser extremadamente complejo y prolijo. Su proceso de desarrollo llevó demasiado tiempo, lo que propició el desarrollo de estándares alternativos. Los sistemas de gestión de red basados en el modelo OSI son más caros que los basados en SNMP.

- **SNMP**: Estándar creado por el IETF que nació para la gestión de redes tipo TCP/IP, y en particular de la red Internet, pero gracias a su simplicidad y pragmatismo se ha popularizado en toda clase de redes. La base de este modelo de gestión es su protocolo SNMP (*Simple Network Management Protocol*), creado como extensión al protocolo SGMP. Del protocolo SNMP están publicadas por IEFT las siguientes RFCs (Request for Comments):

    - SNMPv1, RFC 1157
    - MIB-II, RFC 1213
    - SNMPv2, RFC 1441-1452 y 1901-1908
    - SNMPv3, RFC 3410-3418

    Los principales elementos de este estándar son:

    - **Protocolo de gestión de red (SNMP)**: Define los mensajes que pueden intercambiar la entidad de gestión y los agentes. También define los nombres y direcciones de gestores y agentes. La última versión es SNMPv3 que introduce mecanismos de autenticación, privacidad y control de accesos sólidos, mediante el uso de claves compartidas entre agente y gestor, mecanismos de cifrado común y el uso de funciones hash. Algunos tipos de Operaciones:
        - Get: Obtener pequeños bloques de información de los agentes.
        - GetNext: Lanzar una secuencia de peticiones.
        - Response: responder a las anteriores.
        - Set: escribir un dato en el agente o en la base de datos de gestión.
        - Trap: Envío de un mensaje no solicitado al gestor.
        - GetBulk: Recuperar bloques arbitrariamente grandes del agente.
        - Inform: Los agentes informan de forma espontánea al gestor de un evento.
        - Report: El agente informa espontáneamente de excepciones y errores.

    - Estructura y contenido de la información de gestión: Se compone de:
        - **Lenguaje de definición de datos: SMI** (*Structure of Management Information*). Permite representar los modelos de objetos que van a ser gestionados y establecer los tipos de datos de las variables de gestión que contienen esos objetos. Está basado en ASN.1.
        - **La base de información de gestión (MIB)**: Conjunto de todos los objetos que posee cada agente. La MIB informa a la aplicación de gestión acerca de qué funciones de gestión están disponibles para cada dispositivo de red. Existen MIB's estándar (definidos por el IAB y que todos los agentes y gestores conformes a SNMP deben soportar) y MIB's definidos por cada fabricante. Un tipo especial de MIB es la *Remote Monitoring* (RMON). Se trata de una MIB que permite a un gestor delegar funciones de monitorización en un tipo especial de agentes SNMP conocidos como sondas RMON (RFC 4502).
- **TMN** (Telecommunication Management Network): Toma del modelo de gestión OSI el concepto gestor-agente o el uso de una metodología orientada a objetos. Sin embargo, el modelo TMN contempla una red separada para el intercambio de la información de gestión mientras que el modelo OSI emplea para el intercambio de información de gestión los propios elementos de red gestionados. Con una red de gestión separada de la red gestionada se puede mantener el acceso a los elementos de la red a pesar de los fallos en la red gestionada. En contrapartida habrá que incurrir en costes adicionales por la implantación de la red de gestión.
    - Recomendaciones ITU-T M.3000 y M.3010.

- TMN es especialmente apropiado para las redes de conmutación de circuitos (voz) de los grandes operadores públicos de telecomunicaciones, que no son particularmente adecuadas para el intercambio de información de gestión (datos). Y en particular en aquellas redes estandarizadas por el ITU-T como RDSI o ATM.

GESTIÓN INTEGRADA

En las grandes organizaciones, lo más común es encontrar una gestión de red basada en múltiples soluciones de gestión proporcionadas por distintos proveedores, donde además existirán soluciones para la gestión de sistemas.

El gran reto de la gestión de red es conseguir proporcionar **sistemas de gestión de red integrados**, que proporcionen toda la funcionalidad de gestión que se requiere para operar una red heterogénea, mediante una solución completa en lugar de hacerlo mediante soluciones parciales que normalmente son difícilmente interoperables. Las ventajas de la gestión de red integrada son:

- Se reducen las necesidades de formación del personal de gestión de red.
- Las necesidades de personal adicional para atender otros sistemas de gestión desaparecen.
- Se reduce la necesidad de operación manual de los técnicos de gestión ya que, no es preciso saltar de gestor en gestor para realizar una única intervención en la red; por tanto, se reducen los costes de operación.
- Disminuye la necesidad de mantener datos de gestión de red duplicados entre las diferentes aplicaciones de gestión de red y sincronizarlos convenientemente.
- Será mucho más fácil integrar la gestión de red con otras funciones de la organización como por ejemplo la planificación de red.

Con las arquitecturas estándar de gestión de red se soluciona el problema de los modelos de gestión propietarios, pero no desaparece la necesidad de integración entre sistemas de gestión basados en modelos de gestión estándar diferente. O la integración de sistemas de gestión basados en un mismo modelo estándar pero desarrollados por distintos fabricantes para sus propios equipos. Se hace necesario establecer mecanismos que posibiliten la interoperabilidad entre los diversos dominios de gestión implicados. Existen 2 tendencias para integrar los sistemas de gestión de red de una organización:

a) **Gestión vía plataforma**: Los vendedores de plataformas de gestión suelen facilitar kits de desarrollo que permiten incorporar nuevas capacidades a la plataforma. Además, muchas aplicaciones de gestión de terceras partes suelen estar preparadas para la integración directa con las plataformas de gestión más populares.

b) **Gestión vía una solución de integración a medida**: Integrar a medida el conjunto de gestores que la red requiere; la infraestructura de gestión resultante se denomina solución. Este enfoque suele darse en organizaciones que ya han hecho una considerable inversión en sistemas de gestión específicos para diferentes dominios de gestión y que desean aprovechar ese esfuerzo.

PLATAFORMAS DE GESTIÓN

Algunas de las plataformas de gestión más conocidas son:

- **Cisco Prime**: Integra las siguientes soluciones:
  - Cisco Prime LAN Management Solutions (LMS): Gestión convergente de usuarios y acceso, gestión del ciclo de vida de redes inalámbricas, y configuración y supervisión integradas de los enrutadores.

- Cisco Prime Network Control System (NCS): Gestión simplificada de Cisco Borderless Networks.
- Cisco Prime Collaboration Manager (CM): Monitoreo y diagnóstico sobre las soluciones de video y telepresencia en tiempo real.
- Cisco Prime Network Analysis Module (NAM): Ofrece una amplia visibilidad de los recursos para lograr una rápida resolución de problemas.

- **HP BTO** (Business Technology Optimization) (sustituye a la familia OpenView): Familia de productos para gestión de red entre los que se incluyen:
  - Network Node Manager (NNM): Muestra un esquema de la topología de red fácil de leer que muestra los dispositivos, con sus conexiones físicas, y las notificaciones y alertas que ocurren.
  - Operations Manager.
  - Performance Manager: Herramienta de análisis y planificación gráfica para analizar y proyectar la utilización de recursos futuros y las tendencias de rendimiento.
  - OpenView Reporter: Transforma los datos de disponibilidad y rendimiento enriquecidos con información de gestión, y proporciona informes con los niveles de calidad del servicio (tiempos de respuesta de las aplicaciones, disponibilidad del servicio, etc)

- **IBM Tivoli Monitoring**: supervisa y gestiona aplicaciones del sistema y de la red en una gran variedad de sistemas operativos, hace un seguimiento de la disponibilidad y del rendimiento y proporciona informes para hacer un seguimiento de las tendencias y resolver problemas.