**Propuesta Proyecto UNITAL**

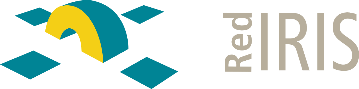
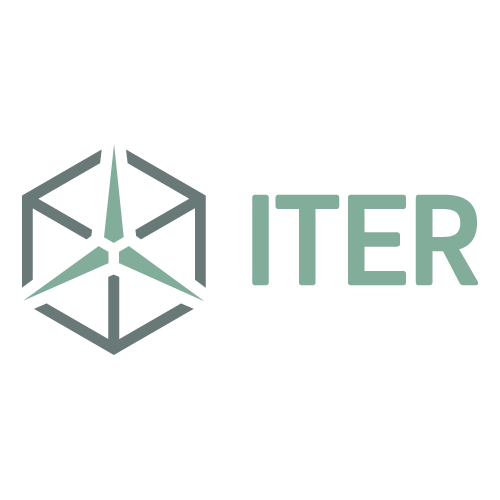
**Borrador versión 6**

**Coordinadores: UC3M, Telcaria, Rediris**

**Autores: ITER, UNEX, CESGA,**

**UVIGO, UDC, UHA**

**Fecha: xxxx 2019**



# Tabla de Contenidos

[Tabla de Contenidos 1](#_Toc14805791)

[Lista Figuras 3](#_Toc14805792)

[Lista de Tablas 4](#_Toc14805793)

[1. Introducción 5](#_Toc14805794)

[1.1 Estructura de la propuesta 5](#_Toc14805795)

[1.2 Identificación 5](#_Toc14805796)

[1.2.1 Datos del Proyecto 5](#_Toc14805797)

[1.2.2 Duración 5](#_Toc14805798)

[1.3 Resumen Proyecto 5](#_Toc14805799)

[1.4 Proyecto Objetivo 6](#_Toc14805800)

[1.5 Participantes 7](#_Toc14805801)

[1.5.1 Listado de participantes 7](#_Toc14805802)

[1.5.2 Justificación de Interés 8](#_Toc14805803)

[1.5.3 Justificación de Utilización 9](#_Toc14805804)

[1.6 Prioridad temática 9](#_Toc14805805)

[2. Proyecto Objetivo 10](#_Toc14805806)

[2.1 Análisis del tejido empresarial 10](#_Toc14805807)

[2.2 Estado del Arte 10](#_Toc14805808)

[2.3 Marco Regulatorio y Legal 11](#_Toc14805809)

[2.3.1 Derechos de Propiedad Intelectual 11](#_Toc14805810)

[2.3.2 Marco Regulatorio 12](#_Toc14805811)

[2.4 Impacto Socioeconómico 12](#_Toc14805812)

[3. Tecnología a Desarrollar 14](#_Toc14805813)

[3.1 Arquitectura 14](#_Toc14805814)

[3.1.1 Slicing con federación 14](#_Toc14805815)

[3.1.2 Seguridad 16](#_Toc14805816)

[3.1.3 Red inalámbrica 18](#_Toc14805817)

[3.1.4 Monitorización 30](#_Toc14805818)

[3.2 Módulos 32](#_Toc14805819)

[3.2.1 HPaaS 32](#_Toc14805820)

[3.2.2 Gestión de Energía 32](#_Toc14805821)

[3.2.3 Seguridad Avanzada 34](#_Toc14805822)

[4. Pruebas y validación 35](#_Toc14805823)

[4.1 Validación funcionalidad general 35](#_Toc14805824)

[4.1.1 Escalabilidad 35](#_Toc14805825)

[4.1.2 Renumeración 35](#_Toc14805826)

[4.1.3 Pruebas de carga 35](#_Toc14805827)

[4.1.4 Pruebas alta disponibilidad 36](#_Toc14805828)

[4.2 Validación arquitectura y módulos 36](#_Toc14805829)

[4.2.1 Validación Arquitectura 36](#_Toc14805830)

[4.2.2 Validación Módulos 36](#_Toc14805831)

[5. Presupuesto del proyecto y división de tareas 38](#_Toc14805832)

[5.1 Presupuesto 38](#_Toc14805833)

[5.2 Presupuesto por Paquetes de Trabajo 38](#_Toc14805834)

[5.2.1 PT 1: Gestión y dirección 38](#_Toc14805835)

[5.2.2 PT 2: Desarrollo Arquitectura 39](#_Toc14805836)

[5.2.3 PT3: Desarrollo Módulos 39](#_Toc14805837)

[5.2.4 PT4: Capacitación 39](#_Toc14805838)

[5.2.5 PT4: Implantación 39](#_Toc14805839)

[Bibliografía 40](#_Toc14805840)

# Lista Figuras

[Figura 4.1: Conexión de Regiones FEDER 7](#_Toc11312798)

[Figura 6.1: Jerarquía grupos de seguridad 17](#_Toc11312799)

[Figura 6.2: Integrantes grupos de seguridad 18](#_Toc11312800)

[Figura 6.3: Reglas grupos de seguridad 18](#_Toc11312801)

[Figura 6.3: Diseño sistema monitorización 19](#_Toc11312802)

# Lista de Tablas

[*Tabla 1.1: Datos del Proyecto* 5](#_Toc11169336)

[*Tabla 1.2: Duración del Proyecto* 5](#_Toc11169337)

[*Tabla 7.1: Localidades red* 15](#_Toc11169338)

[*Tabla 8.1: Presupuesto* 17](#_Toc11169339)

# Introducción

## Estructura de la propuesta

Esta propuesta se ha estructurado en los siguientes capítulos:

1. **Introducción:** breve resumen de las motivaciones y objetivos que se esperan alcanzar en el proyecto, junto con sus principales características.
2. **Proyecto Objetivo:** en este capítulo se comentará la solución propuesta directamente relacionada con la Necesidad Pública, junto con un análisis actual del mercado. Se evaluará además el marco legal y regulatorio del proyecto y su impacto socioeconómico.
3. **Tecnología a Desarrollar:** aquí se describe el producto, con sus principales características técnicas y funcionales, destacando las innovaciones tecnológicas que presenta y el estado de desarrollo de éstas.
4. **Pruebas y Validación:** esta sección se reserva al estudio y diseño del entorno de validación, así como las herramientas y medidas que podrán usarse para evaluar el estado de desarrollo y realizar un seguimiento de su avance.
5. **Presupuesto del proyecto y división de tareas:** presupuesto total estimado del proyecto. Vendrá justificado por paquetes de trabajo, tareas a realizar y otros gastos en fungible, capacitación y equipamiento.

## Identificación

### Datos del Proyecto

En la siguiente tabla se muestra el resumen de datos del proyecto ya presentado en la call de expresiones de interés del CDTI el 30 de mayo:

|  |  |
| --- | --- |
| Expediente | EXP - 00121064 / SIOD-20190251 |
| Título | PROYECTO UNIVERSIDAD DIGITAL - UNITAL |
| Nivel Actual | TRL 5 - Tecnología validada en un entorno relevante |
| Nivel Alcanzable | TRL 7 - Demostración de prototipo en entorno operacional |
| Temática | Tecnologías de la Información y Comunicación (TICs) |

*Tabla 1.1: Datos del Proyecto*

### Duración

En la siguiente tabla se indica la duración del proyecto, basada en la planificación del proyecto (ver capítulo 4), y la fecha de inicio de éste calculada en función de las fechas orientativas de adjudicación del CDTI.

|  |  |
| --- | --- |
| Duración | 24 meses |
| Fecha Inicio | 01/01/2020 |

*Tabla 1.2: Duración del Proyecto*

## Resumen Proyecto

Las universidades tienen unas necesidades de gestión de computación y comunicaciones mucho más complejas, diversas y cambiantes que las empresas. Deben atender investigación muy diversa, laboratorios docentes muy diversos, enorme rotación de usuarios, usuarios poco confiables, uso intensivo de WiFi, eventos con asistentes externos, y otras múltiples características específicas.

Al mismo tiempo, las universidades (sobre todo si tienen titulaciones TIC) tiene una fuerte necesidad de incorporar los últimos avances tecnológicos en gestión de computación y comunicaciones. Las universidades fueron pioneras en internet, redes locales, videoconferencia y otros servicios avanzados. Ahora demandan virtualización, slicing, SLAs, self-organizing networks, operación basada en inteligencia artificial, data analytics, laboratorios mediante realidad aumentada, gestión de servicios IoT, supercomputación, content-based networks, servicios 5G (URLLC, mMTC y eMBB), drones y vehículos autónomos en los campus, y otras funcionalidades avanzadas.

Estas necesidades específicas no se ven cubiertas por los productos comerciales de gestión de computación y comunicaciones en el mercado, dado que estos se orientan al gran mercado de las redes empresariales y de la administración. El mercado universitario, siendo sin duda de un volumen muy atractivo, es en cualquier caso mucho menor que el total del mercado empresarial y de la administración por lo que las grandes empresas no atienden sus necesidades específicas.

Por tanto, es necesario un orquestador de computación y comunicaciones que satisfaga los requisitos específicos de las universidades, y muy importante, capaz de evolucionar para continuar atendiendo a la naturaleza cambiante de los mismos. Nuestro orquestador UNITAL no solo satisfará los requisitos de servicios, sino mucho más que eso, realizará un proceso de transformación digital de la actividad universitaria, rediseñando todas las actividades en base a las nuevas tecnologías.

## Proyecto Objetivo

Desarrollaremos un prototipo de UNITAL, un orquestador de computación y comunicaciones, basado en NFV/SDN, con las funcionalidades específicas requeridas por las universidades y centros de investigación.

La funcionalidad principal de UNITAL es la gestión integrada de slices de computación y comunicación. Un slice consiste en un conjunto de máquinas virtuales, con una configuración específica (SO, IP, recursos, software instalado, parámetros, ...), interconectadas entre sí de una determinada manera (direcciones IP, direcciones y protocolos filtrados/permitidos, recursos de red, ...), e interconectada al exterior (a otros slices o a internet), de una determinada manera (direcciones y protocolos filtrados/permitidos, recursos de red, ...). Ejemplos de usos de slices son la reconfiguración programada de aulas informáticas, slices distintas para administración, investigación y docencia, o slices para experimentos científicos. Se integrará red fíja y WiFi, IPv4 y v6, y se soportará federación de slices.

UNITAL tendrá una interfaz batch basada en descriptores y otra gráfica. La interfaz batch permitirá la programación de creación, modificación y destrucción de slices completas. La interfaz gráfica permitirá la monitorización, modificación y destrucción de slices de forma interactiva. UNITAL tendrá además tres componentes principales:

Ciberseguridad: firewalling multicabecera distribuido, plano de control cifrado y autenticado, y plano de usuario cifrado (bajo demanda), y compatibilidad con firewalls standalone.

Gestión integrada de Wireless: virtualización de la red wirless (WiFi y 5G), integrada con red fija.

Monitorización: adquisición y consolidación de datos de tráfico, con detalle de aplicaciones y servicios, horario, incidencias, en series temporales, y postprocesado de los datos.

Finalmente, UNITAL incorporará tres aplicaciones avanzadas: detección de intrusiones basada en IA, gestión de supercomputación como servicio, y gestión de ahorro energético.

El prototipo será instalado para su validación en:

* Andalucía
* Canarias
* Extremadura
* Castilla La Mancha
* Galicia

Será un despliegue en producción, a nivel nacional, con latencias extremo a extremo e interconectado a través de RedIRIS. Para más detalle sobre la utilización y validación del prototipo ver la sección 4.1.



Figura 4.1: Conexión de Regiones FEDER

## Participantes

En el proyecto participarán Telcaria junto con otra empresa española, encargadas del desarrollo y dirección del proyecto, la Universidad Carlos III de Madrid y Rediris como entidades organizadoras y de apoyo a UNITAL, y otras 7 universidades y 2 centros de supercomputación españoles de 5 comunidades autónomas distintas (listados en 1.5.1) como receptoras del bien.

### Listado de participantes

**UNIVERSIDAD CARLOS III DE MADRID**, una Universidad española (CIF: Q2818029G) con sede social en C/ Madrid, 126 28903 Getafe, ESPAÑA, representada por su Grupo de Investigación NETCOM, del Departamento de Ingeniería Telemática (en adelante referida como “UC3M”).

**TELCARIA IDEAS S.L.**, una Sociedad Mercantil Estatal radicada en España (CIF: B87003125) y con sede comercial en C/Barrionuevo, 8 28911 Leganés, ESPAÑA (en adelante referida como "Telcaria").

**FUNDACIÓN CENTRO TECNOLÓXICO DE SUPERCOMPUTACIÓN DE GALICIA**, un centro público de investigación español (CIF: G15852981) con sede social en Avenida de Vigo, s/n Campus Sur. 5705. Santiago de Compostela, ESPAÑA (en adelante referida como "CESGA").

**INSTITUTO TECNOLÓGICO Y DE ENERGÍAS RENOVABLES**, un centro de investigación español (CIF: A38259115) con sede en Polígono Industrial de Granadilla s/n, 38600 Granadilla de Abona, Santa Cruz de Tenerife, ESPAÑA (en adelante referida como "ITER").

**UNIVERSIDADE DA CORUÑA**, una Universidad española (CIF: Q6550005J) con sede social en Rúa Maestranza 9, 15001 La Coruña, ESPAÑA (en adelante referida como "UDC").

**UNIVERSIDAD DE EXTREMADURA**, una Universidad española (CIF: Q0618001B) con sede social en el Campus Universitario Avenida de Elvas s/n 06006 Badajoz, ESPAÑA (en adelante referida como "UEX").

**UNIVERSIDAD DE VIGO**, una Universidad española (CIF: Q8650002B) con sede social en el Campus de Marcosende s/n, 36310 Vigo, ESPAÑA (en adelante referida como "UVIGO").

**UNIVERSIDAD DE ALCALÁ**, una Universidad española (CIF: Q2818018J) con sede social en Plaza de San Diego s/n, 28801 Alcalá de Henares, Madrid, ESPAÑA y sede a los efectos de la propuesta UNITAL en el Campus de Guadalajara de la Universidad de Alcalá, Calle de Cifuentes, 28, 19003 Guadalajara, ESPAÑA, representada por su grupo de investigación GIST, del Departamento de Automática (en adelante referida como "UAH"), representada por Juan Ramón Velasco Pérez, Coordinador del grupo de investigación GIST.

### Justificación de Interés

Telcaria: Mejorar justificación interés una vez terminadas las secciones de “Tecnología a Desarrollar”

Las cuatro comunidades autónomas han mostrado su apoyo al proyecto mediante cartas de interés firmadas a nivel de director general o superior. En ellas han manifestado su completo apoyo y se comprometen a la aceptación de los derechos que sean transferidos a la Comunidad Autónoma al final del proyecto, resaltando además que los objetivos y resultados del prototipo UNITAL se alinean perfectamente con la estrategia RIS3 de estas cinco comunidades autónomas.

UNITAL supone una transformación completa en la forma de prestar y gestionar los servicios TIC académicos, y un gran avance en la transformación digital de las universidades y centros de I+D. La utilización de slices aumenta enormemente la flexibilidad de los servicios, alcanzando un gran nivel de automatización de la operación.

Todas las comunidades autónomas participantes disponen de servicios de gestión de redes y comunicaciones con técnicos muy competentes., pueden por tanto dar el apoyo necesario tanto en el proceso de licitación del prototipo como en el ensayo y evaluación del prototipo desarrollado.

Éstas tienen competencias en educación universitaria, motivo por el cual están perfectamente legitimadas para demandar una solución de gestión integrada de comunicaciones y computación de servicios académicos.

### Justificación de Utilización

Por parte de las cuatro comunidades autónomas, el prototipo se utilizará para comprobar la necesidad expresada por las mismas en esta licitación. Determinarán si realmente permite el proceso de transformación digital de las universidades y probarán algunas de las posibles funciones virtualizadas que pueden correr sobre UNITAL. La implementación de la solución en múltiples entidades y en zonas geográficamente distantes es un elemento clave para poder validar la escalabilidad de UNITAL, que deberá reaccionar y adaptarse al crecimiento topológico y de carga de trabajo sin perder calidad en los servicios ofrecidos (entre los que se incluyen las VNFs).

En Galicia el prototipo le permitirá hacer una simulación de la red de RECETGA pasando del actual diseño de CPD basado en protocolos legacy como STP, a una red definida por software. Entre las funciones que se podrán probar, está el balanceo de carga entre múltiples links y el uso de proxies en distintos nodos posibles para la descarga de recursos externos.

En Canarias la utilización del sistema posibilitará su adaptación a TEIDE HPC, el superordenador con capacidades de almacenamiento y cómputo que presta servicios a la comunidad académica. UNITAL será utilizado para la evaluación de una mejor gestión del acceso a recursos propios por parte de terceros (entre los que se incluye la supercomputación como servicio, HPCaaS) y para la prestación de servicios de recuperación ante desastres (que vendrá facilitada por el entorno de interoperación ofrecido por el sistema).

## Prioridad temática

El proyecto evidencia un alineamiento pleno con el objetivo “Retos de la Sociedad y Economía Digital”, del eje prioritario 5.5 de EECTI 2013-2020, así como, con las siguientes prioridades RIS3: P4.4 “Agenda Digital” de Canarias, Desafío 1 “Reformular el sistema de I+D+i” de Castilla La Mancha, PI3.3 “Desarrollo de infraestructuras de telecomunicaciones avanzadas” y la Agenda Digital de Extremadura, y P.2.3 “Economía del Conocimiento: TIC y TFE” de Galicia.

# Proyecto Objetivo

## Análisis del tejido empresarial

Debido a lo reciente y disruptiva que es la tecnología en la que se basa la solución propuesta, existen pocas empresas a nivel nacional que pudiesen ser capaces de desarrollar el prototipo de UNITAL, así como de realizar las pruebas de validación.

Telcaria es capaz de acometer este desarrollo y pruebas porque ya ha desarrollado Alviu, un producto muy avanzado, gracias a su fuerte actividad de investigación a través de múltiples proyectos de I+D de NFV/SDN y 5G como el FP7 Netide, los H2020 Superfluidity, 5GEVE, 5G-Coral y 5Growth, dos proyectos de doctorados industriales, y proyectos empresariales como el Onlife de Telefónica. Adicionalmente, Telcaria realizará el desarrollo con una participación sustancial de grupos de investigación punteros en distintas áreas clave (NFV, hipervisores, 5G, controladores, ...) pertenecientes a varias universidades y centros de investigación españoles.

La principal competencia para UNITAL es la multinacional Cisco, seguida de Nokia, BigLeaf, Cato y Speedify. Todas ellas son empresas internacionales con sedes principales en el extranjero.

Este mercado está claramente dominado por Cisco, el cual sustenta el 60% de routers empresariales, el 37% de routers de proveedores de servicio y el 57% del mercado global de ethernet switching[[1]](#footnote-2). Sin embargo, la diversidad de necesidades y la complejidad del mercado deja espacio para múltiples otras empresas que buscan espacios rentables. Estos espacios pueden ser en cuanto a segmentos de mercado, como Juniper que se especializó en routers de altas prestaciones, en cuanto a servicios, como PaloAlto y Fortinet, que se especializan en firewalls, o en cuanto a tecnología, como Edgecore y Noviflow, que se especializan en switches SDN. Se puede concluir por tanto que, a pesar de la gran dominancia de Cisco, existen oportunidades muy atractivas en este mercado para empresas de menor tamaño, siempre que se posicionen de forma muy certera.

## Estado del Arte

Telcaria: Ampliar

Los productos existentes más avanzados son:

BigLeaf Networks:

Su servicio SD-WAN está centrado en la optimización de recursos, pero enfocado a entornos de la nube. Resuelven la falta de visibilidad en la red a través de la integración con un amplio repertorio de aplicaciones y entornos cloud, desarrollando funcionalidades específicas para éstos.

Cato Networks:

Utiliza dos niveles complementarios, Cato Cloud Network and Cato Security Services y resuelve la complejidad de las políticas de firewall distribuidas mediante protección de acceso móvil y cloud y protección avanzada contra intrusos.

Speedify:

Optimiza la distribución de recursos mediante técnicas de load balancing y bonding para combinar múltiples conexiones a Internet en un solo túnel.

Cisco:

Enfoque clásico de inteligencia de la red en cada nodo, corriendo las funciones de enrutamiento y otras políticas en hardware. Su solución SD-WAN consiste básicamente en la automatización de la configuración de estos equipos a través de Sw específico.

Respecto a la virtualización de computación, actualmente se utilizan discos de arranque con múltiples sistemas operativos, y en algunos casos hipervisores para disponer de máquinas virtuales. Los hipervisores tipo 1 (bare metal) más utilizados en el entorno universitario son Vmware y Xen. Los tipo 2 (over SO) son Vmware, Virtualvox , Parallels y UEMU.

Ninguno de los productos anteriores permite la configuración integrada de máquinas virtuales y de switches de la red, ni tampoco la creación y gestión de slices sobre distintas máquinas físicas, si bien usando Openstack se puede obtener una funcionalidad parcial.

El prototipo UNITAL es la siguiente generación de nuestro producto Alviu. Alviu permite el control centralizado de la red, sobre ONOS, utilizando Openflow y white-box switches. Alviu gestiona slices de red, firewalls virtuales, zero-touch configuration, renumbering y otras funciones avanzadas. La principal limitación de Alviu es que no es capaz de gestionar de forma única las slices de red y las de computación.

La novedad principal de UNITAL sobre los productos actuales es la creación de slices conjuntas de computación y comunicación, con características programables a través de descriptores. UNITAL permite la creación, monitorización, modificación y destrucción de slices. Las slices se pueden aplicar a la operación de aulas de informática, reconfigurándolas por completo en función del horario de asignaturas. Las slices permiten la separación de servicios de administración, investigación y docencia, proporcionando a cada uno las características y recursos necesarios. Permiten la integración de IPv4 e IPv6, y la integración de la red fija y la red Wireless, combinando WiFi, 5G y LiFi. UNITAL por tanto satisfará las diversas y cambiantes necesidades de comunicaciones y computación de las entidades académicas.

## Marco Regulatorio y Legal

### Derechos de Propiedad Intelectual

A excepción del SO PicOS de los whitebox switches, todos los programas y herramientas sobre los que el diseño e implementación de este proyecto se han fundado son componentes open source bajo licencia de Apache 2.0. La licencia Apache 2.0 es bastante flexible en cuanto a comercialización, permitiendo a los desarrolladores tener derecho sobre las extensiones y componentes adicionales que desplieguen. Sin embargo, la licencia GPL es más restrictiva, estableciendo que tanto los componentes bajo esta licencia como sus extensiones deben ser distribuidas sobre los mismos términos (libertad para ejecutar, estudiar, compartir y modificar el software). Por este motivo, UNITAL no incluirá ningún componente con licencia GNU General Public License (GPL).

Los elementos principales se van a monetizar son el controlador y el orquestador, y éstas son las licencias relevantes para la propiedad intelectual del producto. ONOS está registrado bajo la licencia de Apache 2.0, por lo que los módulos desarrollados encima de ONOS pueden ser registrados y comercializados bajo una licencia de copyright o licencias más restrictivas. Asimismo, el orquestador ha sido desarrollado desde cero sin ningún tipo de código de terceros, siendo código 100% propietario. Ambos están protegidos bajo un registro de marca con el nombre de Alviu, y se plantea la posibilidad de proteger la propiedad intelectual de éstos bajo una patente. Sin embargo, las patentes no son demasiado efectivas en este tipo de productos ya que es difícil proteger la funcionalidad de los módulos bajo este tipo de acreditaciones. Por eso, el servicio correrá en la nube o en servidores propios, asegurando que nadie, ni siquiera los clientes, puedan tener acceso al código.

### Marco Regulatorio

El producto cumplirá con la LOT garantizando mediante cifrado la confidencialidad de las comunicaciones.

El procesamiento y control de datos de los usuarios de la red, tanto en los módulos de seguridad como los usados para la optimización del uso de recursos dentro de la red mediante IA, deberán adherirse al Reglamento General de Protección de Datos de la Unión Europea (GDPR). Para ello, habrá que tener en cuenta las bases legales bajo las cuales los receptores finales puedan hacer uso de estos datos.

Adicionalmente, el equipamiento de red deberá cumplir la legislación de la UE que permita la libre circulación del producto dentro del mercado europeo con la marca CE (requiriendo, principalmente, las certificaciones de RoHS y WEEE).

## Impacto Socioeconómico

El mercado mundial de routers y switches asciende a $9,6 millardos anuales (datos de IDC de Q1-2018)[[2]](#footnote-3) [[3]](#footnote-4), con un crecimiento en torno al 7% anual. A esta cifra hay que añadir las ventas de servicios que están en torno a $7,3 millardos anuales. El mercado de routers está bastante concentrado, con Cisco como líder (ventas de $1,6 millardos), seguido de Juniper, Nokia y Huawei como grandes suministradores. El mercado de switches está mucho más atomizado, y hay docenas de fabricantes. Nuestros competidores

Cisco, BigLeaf, Cato y Speedify están orientados al mercado corporativo, y no disponen (ni anuncian) productos con las características de UNITAL, aptos para satisfacer el mercado de universidades y centros de I+D. Por otro lado, Nuage tiene un producto de controlador virtualizados, pero totalmente enfocado al mercado Telco, que en absoluto se adapta al mercado universitario. Otros posibles competidores son Mirantis, pero se centra en computacion en el borde con una alianza con Juniper, y OnApp, centrado en cloud management.

Nuestra estrategia se basa en atacar el mercado de servicios y redes universitarias, sustancialmente diferente del corporativo, ocupando un espacio que nuestros competidores no están cubriendo adecuadamente. En base a datos obtenidos directamente de las universidades, su gasto anual promedio en computación y comunicaciones es de una ratio de 23€/alumno. Esto supone un mercado anual de 45 M€/año solo en España. Proyectando a nivel europeo, el mercado universitario sería de 360 M€/año, y a nivel mundial ascendería a 1.430 M€/año.

Como consecuencia de la adjudicación de esta licitación, Telcaria hará una ampliación de capital para transformar el prototipo de UNITAL, ya validado, en un producto comercial. Esta ampliación de capital se realizará mediante inversión de los socios, e inversión de un fondo de capital riesgo. La ampliación de capital se complementará con fondos de proyectos europeos, en los que Telcaria tiene un track-record demostrado. La ampliación de capital ascenderá a 8 millones de euros, en dos rondas, complementada con dos millones de euros de fondos europeos, incluyendo RIA, IA y SME instrument.

La creación de empleo directo de este proyecto estará en torno a 42 puestos, la gran mayoría para profesionales altamente cualificados en el sector de las telecomunicaciones, telemática e informática. Éstos se dividirían en cuanto a participación en el proyecto en Ingenieros Backend, Ingenieros de virtualización de redes, Ingenieros de devOps, automatización de pruebas, frontend, técnico de bases de datos y project managers. Por otro lado, se estima que de forma indirecta induzca la creación de 10 puestos de trabajo en el ámbito de la investigación y la i+d

La igualdad de género se tendrá en cuenta en todo momento durante la contratación de personal, no discriminando ni dando preferencia a ningún candidato en base a su género. Cabe destacar además que el porcentaje de mujeres dentro de los empleados de Telcaria está por encima de la media del sector (19,3% en España) y que la actual CEO de la empresa es mujer.

El desarrollo del software de control tendrá en cuenta aspectos de eficiencia energética en el equipamiento de conmutación y routing de la red, además de en los servidores y otros recursos de computación bajo su control, optimizando el uso de los mismos al facilitar la compartición de recurso y escalando de forma dinámica el despliegue de éstos para evitar el consumo energético por parte de servidores u otro equipamiento que no se esté utilizando.

Este es un proyecto transformador a nivel nacional, apoyado conjuntamente por Canarias, Castilla La Mancha, Extremadura y Galicia, contando adicionalmente con la participación de RedIRIS y de la U. Carlos III. Telcaria se presentará a la licitación con otra empresa española, proporcionando conjuntamente una amplia solvencia técnica y económica.

# Tecnología a Desarrollar

## Arquitectura

En este paquete se desarrollará la primera fase identificada en 5.2 para la creación de la infraestructura base.

### Slicing con federación

Telcaria: ampliar/mejorar

#### Consola de configuración y operación

Interfaz gráfica unificada para el control total de la red SDN, permitiendo controlar las políticas de routing, calidad de servicio y seguridad. Estará integrada además con alarmas configurables con el aviso de ciertos eventos en la red y de logs. Los perfiles de seguridad permitirán ademar delegar con facilidad ciertas tareas a departamentos o personal investigador, dando acceso por ejemplo al administrador de unos servidores de pruebas dentro de un departamento para instalar sus propias reglas de entrada a las máquinas (sin necesitar el uso de otras herramientas como iptables, y mejorando la transparencia).

#### Funcionalidades básicas

* Compatibilidad con protocolos estándar: BGP, iBGP y OSPF**,** permitiendo la interoperabilidad con redes legacy.
* Creación de VLANs a través de red WAN, sobre transporte IP
* Dual stack IPv4 e IPv6 en toda la red

#### Descubrimiento & Configuración Zero-touch de dispositivos

La creación de ciertas plantillas por defecto para que cuando se añada un nuevo nodo a la red, éste se conecte de forma automática al controlador y sea configurado sin la necesidad de intervención manual. Además, al añadirle a específicos slices o grupos de la red (como al de Departamentos en el ejemplo anterior), éste heredará de forma automática todas las políticas ya configuradas en esta red.

#### Integración computación y comunicaciones

UNITAL no solo pretende converger las distintas tecnologías de acceso a la red mencionadas en 1.2.1, sino que pretende integrarse con la interconexión WAN y las plataformas de gestión de recursos de cómputo y almacenamiento. Dicha integración, permitirá a UNITAL, desplegar slices integradas en todos los dominios mencionados, para poder instanciar las slices con una mayor granularidad, asignando recursos de red, cómputo y almacenamiento, necesarios para cumplir con el ASN, que los servicios de los verticales están demandando.

En su mayor exponente, UNITAL podría ser capaz de integrar las tecnologías de Serverless computing con Networkless networking introducido por el slicing de la red planteado. Abstrayendo a los desarrolladores e investigadores la complejidad de desplegar y mantener testbeds/escenarios, compuestos de equipamiento de red, cómputo y almacenamiento.

Se propone un piloto para analizar la implantación en la UDC de una plataforma de red de comunicaciones abierta basada en redes definidas por software y virtualización de los servicios de comunicaciones.

El objetivo es poner a disposición de los grupos de investigación de la Universidad los servicios de comunicaciones globales, abiertos y dinámicos que posibiliten el trabajo tanto en entornos colaborativos, como en entornos con necesidades de redes de muy alta capacidad, o en proyectos con necesidades de comunicaciones muy diferentes que deben ser provistos de forma automatizada y dinámica.

La implantación de las nuevas tecnologías de muy alta capacidad como son las redes 100G en los campus universitarios hacen necesarios nuevos sistemas para la prestación de los servicios de comunicaciones que deben poder adaptarse de forma flexible a las nuevas necesidades cambiantes de los entornos de investigación y docencia, permitiendo así, afrontar con éxito los nuevos retos en comunicaciones, servicios y seguridad.

Requisitos:

* Abstracción de las tecnologías físicas de acceso del usuario (cableado, inalámbrico) para la prestación de servicios de comunicaciones independientes del tipo de conexión utilizado
* Control de acceso a usuarios centralizado y único para redes cableadas e inalámbricas, basado en 802.1x y portal WEB, y utilizando roles del LDAP/RADIUS/dirección MAC/profiling del dispositivo
* Utilizar la información de acceso usuario/dispositivo/conexión para activar ACLs/políticas/seguridad basado en el usuario/grupo/dispositivo
* Posibilidad de extender redes de nivel 2 sobre la red IP
* Protocolos de redundancia/balanceo de red alternativos al STP. Por ejemplo: SPB
* Creación de servicios dinámicos definidos por usuario
* Disponer en los controladores técnicas de control de aplicación y gestión de ancho de banda
* Auditoría de navegación WEB
* Auditoría de sesiones de usuarios, con detalle de IP/MAC/host/puerto\_conmutador/AP WiFi/horario
* Aplicación de gestión de usuarios con búsquedas e informes basadas en la auditoría del punto anterior
* Aplicación web de supervisión en tiempo real de toda la red.
* Reconfiguración dinámica de la red en función de calendarios (laboratorios que dependiendo de la hora acceden a unos servidores o a otros), incluso con cambio de IPs de hosts.
* Gestión del DHCP e IPAM
* Permitir el despliegue de servicios de las comunicaciones en topologías multicampus centralizando la gestión de los servicios
* Aplicación WEB para la gestión de los conmutadores, con permisos granulares basados en grupos de usuarios, y con las operaciones más habituales (asignación de VLANs a puertos, ver configuración de puertos, …)
* Aplicación web de supervisión en tiempo real de toda la red

#### Inteligencia en las capas de servicio y de datos

Una diferencia clave en 5G y en adelante es la posibilidad de tener una red basada en la recopilación de datos mediante el uso de las tecnologías de ML y AI para la optimización de la red y permitiendo la introducción de innovadoras aplicaciones que aporten un valor añadido. Una de las principales ventajas de un Sistema Edge integrado es que los datos pueden ser colectados y gestionados desde un único sistema de almacenamiento distribuido ubicado en la infraestructura del Edge. Esta recolección de los datos tendrá en cuenta las diferentes alternativas de protocolos y topologías (como por ejemplo, una red inalámbrica en mesh).

#### Calidad de servicio

QoS es un fuerte de SDN y OVS, te permite configurar muy fácilmente políticas de QoS y modificar los parámetros de configuración de cada cola. Al igual que con la gestión de grupos de seguridad, la asignación de calidad de servicio se puede hacer por slices o grupos de red, facilitando la gestión global de las colas y criterios de clasificación, pudiendo así configuración una clasificación más allá de las colas para voz sobre IP. Se plantea además (en relación con alguno de los verticales en 1.5) la posibilidad de asignar colas de forma dinámica para por ejemplo reservar cierto caudal de tráfico y así garantizar que se cumplan las condiciones deseadas de red. Esto puede ser de interés para reservar recursos para pruebas de carga, experimentos por parte del personal de investigación que requieran cierta cantidad de recursos de red o para otros eventos dentro de la universidad.

##### Authentication Aware Routing

Esa facilidad de configuración y gestión de las políticas de QoS, evolucionará para integrarse con los mecanismos de AAA que existan en la red en forma de Authenticated QoS Aware Routing (AQoSAR). AQoSAR será uno de los percusores para desplegar slices en la red autenticadas.

##### Monitorización Acuerdos de Nivel de Servicio (ANS)

La dinamicidad en la gestión de colas de los switches que propone UNITAL, será utilizada por los elementos de orquestación para que junto con la monitorización avanzada del plano de datos propuesta en 1.3, permitan identificar si los acuerdos de nivel de servicio (ANS) se están cumpliendo y como consecuencia de ello, modificar la slice de red para que mantenga el ANS de forma automatizada, sin necesidad de intervención manual por parte del administrador de red.

### Seguridad

CESGA: ampliar/mejorar

El principal objetivo en cuanto a seguridad en UNITAL será el de vulnerabilidades internas, asumiendo que para la prevención y control de ataques perimetrales las universidades ya cuentan con firewall standalone como aquellos de Paloalto o Fortinet.

Esta sección se divide en 3 subsecciones, cubriendo la seguridad en la herramienta de control y gestión de UNITAL, la funcionalidad del firewall distribuido para la monitorización y filtrado de tráfico interno y por último la autenticación de usuarios en la red.

#### Herramienta de control

Autenticación

Autenticación de usuarios por nombre y contraseña. Se podría incluir también autenticación basada en infraestructura de clave pública (PKI). Protocolos como Kerberos podrían ser utilizados. Los usuarios están organizados a su vez en grupos de seguridad.

Perfiles de seguridad

Estos grupos de seguridad en los que se dividen los usuarios establecen permisos de:

* Crear/eliminar usuarios
* Ver resumen general del dashboard
* Ver los logs para cada uno de los grupos de seguridad
* Leer/editar reglas de firewall para cada uno de los grupos de seguridad

Los grupos o slices de seguridad son entidades abstractas que agrupan múltiples elementos dentro de la red. Los criterios para crear estas zonas pueden ser en base a los switches, agrupaciones de puertos o por subredes/dominios de IP (para más detalle ver 1.1.2).

#### Firewall tráfico interno

Grupos de seguridad

Para facilitar la administración de la red y de las diferentes reglas de seguridad que establecen el tráfico permitido dentro de la red, se hace uso de la división jerárquica de la red en grupos. Estos grupos se organizan a su vez en una estructura de árbol, teniendo cada grupo un único padre (del cual hereda toda la configuración) y cero o varios hijos. Habrá un grupo por defecto que incluirá todos los elementos/nodos de la red SDN y del cual heredaran los demás grupos. Dentro de estos grupos, se podrán agrupar las entidades de la red según los siguientes criterios:

* Switches físicos o virtuales
* Puertos
* Dominios/redes virtuales

Una vez creados estos grupos, se podrá crear las diferentes reglas de acceso entre ellos. En estas reglas, se puede especificar uno o más grupos origen y destino, filtrando el tráfico con reglas hasta nivel 4, especificar cómo tratar el tráfico y si se desea registrar en los logs. Para no tener problemas de escalabilidad, este firewall no guardará estado de las sesiones abiertas, pudiendo especificar reglas reflexivas para obtener una funcionalidad parecida.

Esta implementación puede observarse en el siguiente ejemplo:

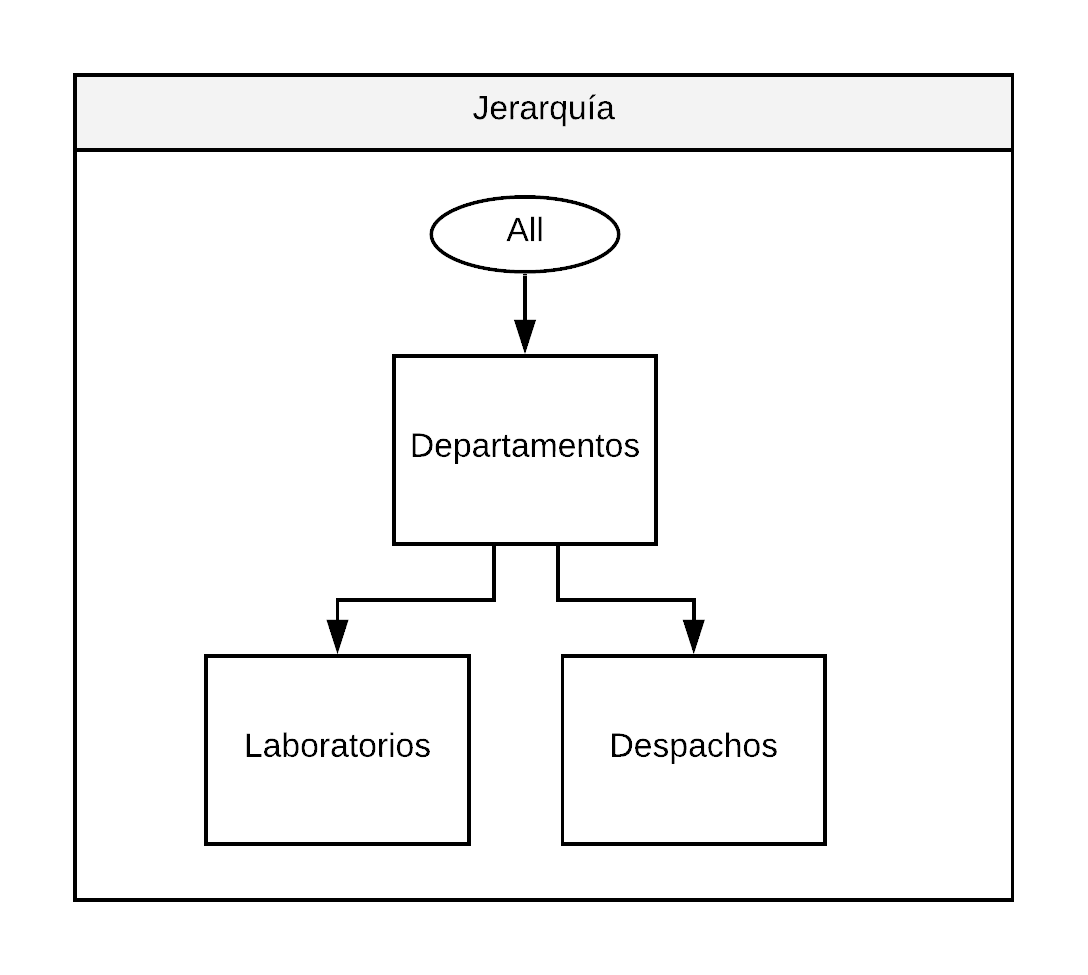


Figura ‎3.1: Jerarquía grupos de seguridad

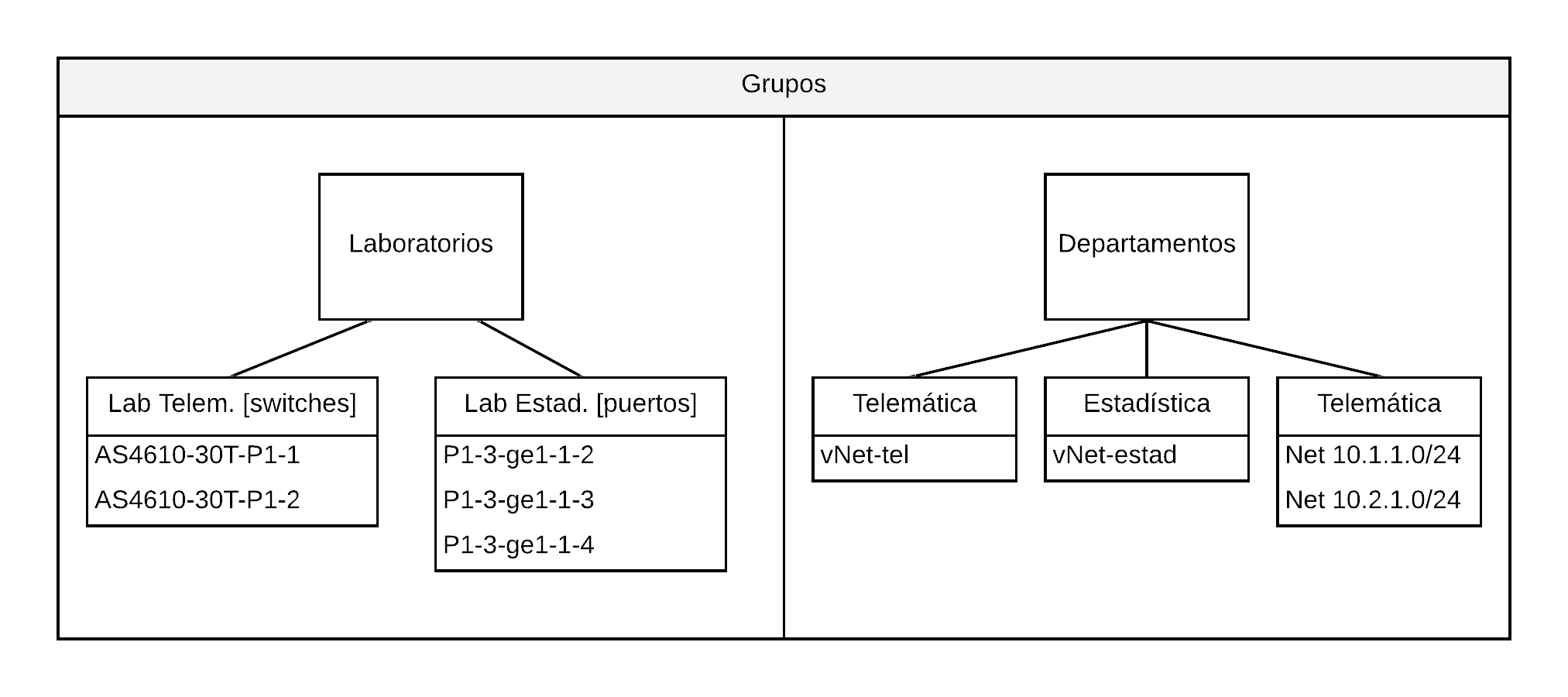


Figura 6.2: Integrantes grupos de seguridad

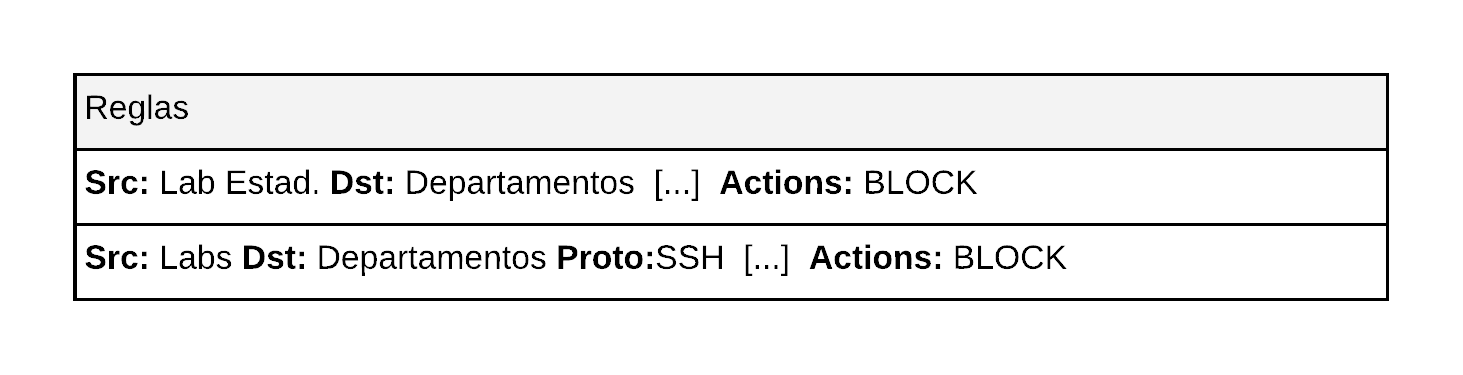


Figura 6.3: Reglas grupos de seguridad

Otras funcionalidades

* IP spoofing – bloqueo de tráfico saliente de una subred con una IP distinta a su prefijo
* Limitar número máximo de conexiones que puede abrir una máquina/subred
* Storm control: limitar tráfico broadcast de ARP y de multicast

#### Autenticación en red

Para la autenticación de los usuarios deseando conectarse a la red, se propone la autenticación a través del protocolo 802.1X, usando al controlador SDN como entidad que proporciona el servicio de AAA, implementando el protocolo Diameter. Para dispositivos que no soporten la autenticación 802.1X (como algunas impresoras de red o sensores), se podría incluir un mecanismo de autenticación basado en DHCP, el cual autenticaría los dispositivos en base a su MAC. Adicionalmente, esta funcionalidad se administraría desde el dashboard de control, advirtiendo por ejemplo de nuevos dispositivos no reconocidos que hayan intentado conectarse a la red y dando la opción de permitir su acceso.

Por último, se plantea la implementación de Authentication Aware Routing como herramienta de integración entre la lógica de routing y la autenticación. Los detalles de su funcionamiento vienen explicados en más detalle en 1.2.3.1.

### Red inalámbrica

Las comunicaciones inalámbricas han tenido un crecimiento continuado durante la última década, y son el segmento de la industria de las telecomunicaciones con mayores expectativas de crecimiento, innovación y aplicaciones futuras. En los últimos años se ha producido una explosión de tráfico de los usuarios móviles, y se prevé que su crecimiento en los próximos 5 años se multiplique por siete [Cisco\_VNI].

El número total de teléfonos inteligentes y tabletas superará el 50% del total de dispositivos y conexiones móviles a escala mundial (6.200 millones). En 2016 en España existían un total de 35 millones de teléfonos inteligentes y el 80% de las viviendas disponía de conexión móvil de banda ancha [INTEF\_TIC].

Los dispositivos móviles actuales y futuros pueden utilizar indistintamente redes de operador 4G y 5G, y redes WIFI públicas o privadas. En los últimos años las redes WIFI han tenido un crecimiento importante debido a distintos factores:

* Los operadores de telecomunicaciones siguen fijando, en su gran mayoría, un límite a los usuarios en el consumo mensual de datos por redes 3G y 4G, haciendo que los usuarios conmuten a redes WIFI públicas o privadas tan pronto como pueden.
* Se están desplegando redes WIFI por parte de operadores de telecomunicaciones para reducir la carga sobre sus redes móviles (traffic offloading).
* Los usuarios académicos, empresariales y residenciales prefieren cada vez más las redes inalámbricas a las cableadas, buscando movilidad y un escritorio sin cables.

El número total de zonas WIFI públicas y privadas, tanto de empresas como de particulares, se ha multiplicado por 8 en los 4 últimos años. Este elevado número de redes y usuarios requieren, especialmente en los entornos empresariales y académicos, de potentes y complejos sistemas de gestión y control de los usuarios e infraestructuras inalámbricas que garanticen la seguridad d elas comunicaciones y la flexibilidad de los servicios prestados en dichas redes.

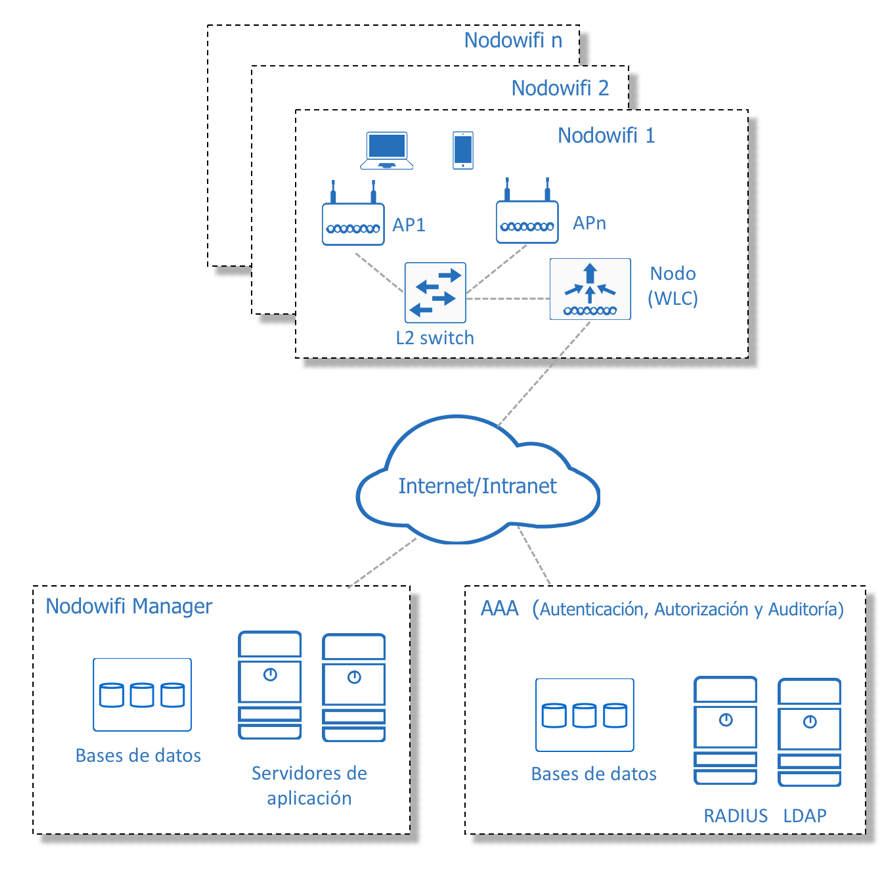
Dichos sistemas de gestión y control tienen que contemplar por un lado las funciones de Autenticación, Autorización y Contabilización (AAA *Authentication, Authorization and Accounting*) de los usuarios de la red, que en grandes despliegues WIFI pueden contarse por decenas de miles de usuarios, equipos y sesiones en un solo día. Por otro lado, es necesario gestionar a nivel físico y lógico toda la infraestructura de puntos de acceso, routers, conmutadores, establecer las políticas de seguridad, gestionar los canales de radio de acuerdo a la normativa, fijar los anchos de banda, etc.

En redes WIFI de tamaño mediano y grande, de decenas a miles de APs, las funciones de AAA y gestión de la red están normalmente delegadas en los Controladores de Red Local Inalámbrica (WLC *Wireless LAN Controller*) comerciales.

#### Solución actual Nodowifi.

La arquitectura hardware y software se compone de tres grandes elementos funcionales (Figura 1):

* Controladores de Red Local Inalámbrica (Nodowifi).
* Aplicación web de administración y gestión (Nodowifi Manager).
* Servidores de autenticación, autorización y contabilización AAA.



1. Elementos funcionales de la arquitectura Nodowifi.

Los servicios necesarios para implementar la arquitectura expuesta corren sobre servidores con sistema operativo Linux, lo que ha permitido incluir las funcionalidades y características de los controladores inalámbricos comerciales, y añadir otras funcionalidades adicionales mediante paquetes del sistema operativo o programación software específica.

Algunas funcionalidades añadidas son:

* La integración de un proxy-cache transparente por controlador.
* Autoconfiguración remota de los controladores.
* Análisis de las sesiones para optimización de la red.
* Autenticación mediante certificado o DNI electrónico.
* Soluciones de eficiencia energética de la red mediante el apagado de los nodos y los puntos de acceso sin uso, por la noche o en días no lectivos (proyecto Ecowifi).

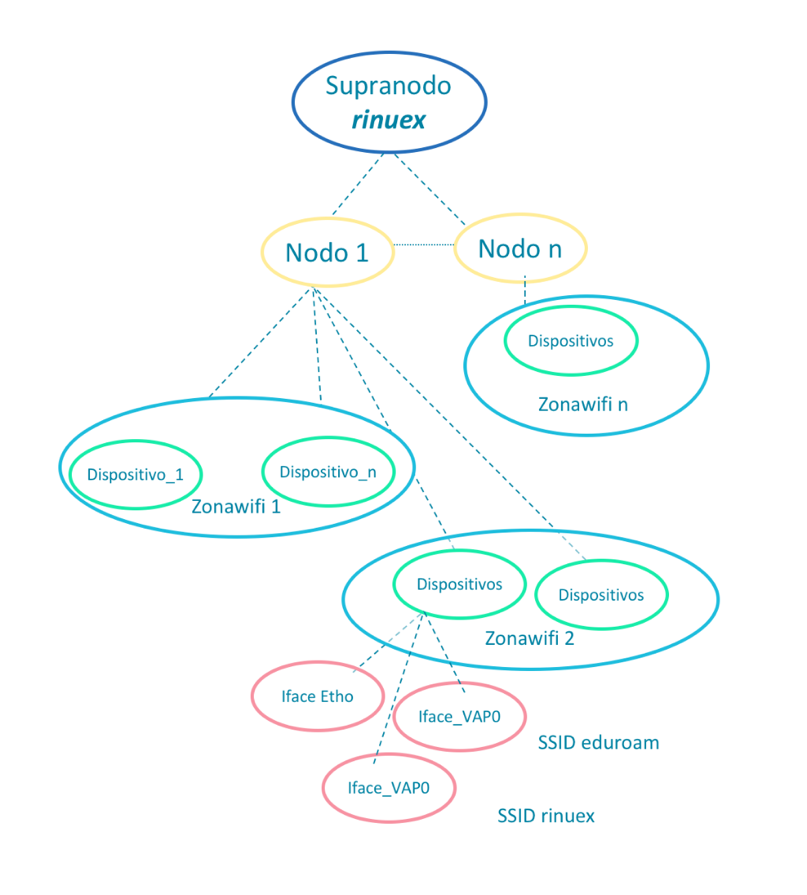
##### Nodowifi Manager.

Es una aplicación web basada en una arquitectura software **LAMP** (**Linux, Apache, MySQL, PHP)** que permite la administración y supervisión de toda la red inalámbrica: usuarios, sesiones, seguridad e infraestructura hardware.

En la Figura 2 se representa gráficamente la estructura jerárquica de la arquitectura de Nodowifi. En el diseño inicial de la arquitectura se tuvo en cuenta la posibilidad de gestionar grandes redes Wi-Fi con miles de puntos de acceso y decenas de miles de usuarios concurrentes; para ello, se definió una estructura altamente escalable y a la vez flexible, que permitiera múltiples escenarios y configuraciones de nodos, y que pudiera adaptarse a las nuevas tecnologías que han ido apareciendo.

A continuación, se enumeran y detallan cuáles son los elementos lógicos que definen una red gestionada y auditada por la arquitectura Nodowifi:

* Supranodo: Es la entidad lógica de mayor nivel, la cual agrupa toda la información administrativa de la red y supervisa a los Nodos de la red.
* Nodo: Entidad lógica que agrupa todos los dispositivos, servicios y redes de un Nodo. Los nodos se implementan sobre uno o más servidores Nodowifi y el número de servidores por nodo puede variar en función del número de usuarios, dispersión geográfica o requisitos de alta disponibilidad.
* Dispositivos: Son todos los elementos hardware que componen la red. Pueden ser: un servidor Nodowifi, puntos de acceso de diferentes fabricantes y tecnologías, antenas, sensores, routers, etc.
* Zonawifi: Se trata de una agrupación lógica de dispositivos, normalmente APs, por un criterio o zona común. En el caso de un campus, una zona wifi puede estar dividida en facultades, edificios, biblioteca, etc.
* Interfaces: Conexión a la red cableada o inalámbrica de los Dispositivos. Los interfaces son el enlace con los servicios de red.
* Servicios: Distintos servicios de Internet o Intranet prestados en el Supranodo. Por ejemplo: eduroam, servicio de navegación web o servicios de voz sobre IP.



1. Representación gráfica de la estructura jerárquica de la arquitectura.

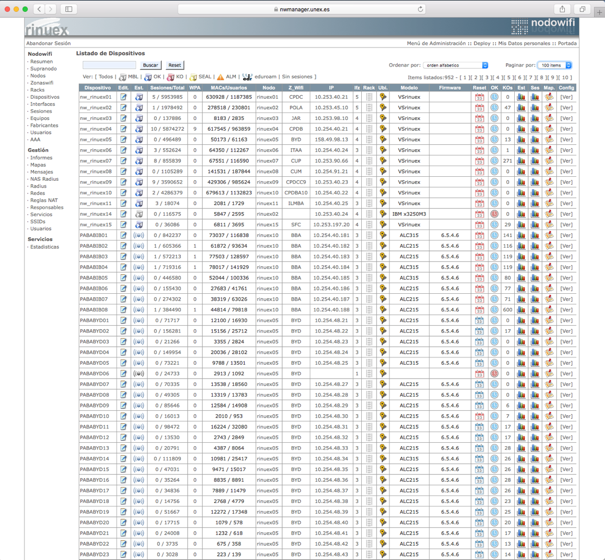
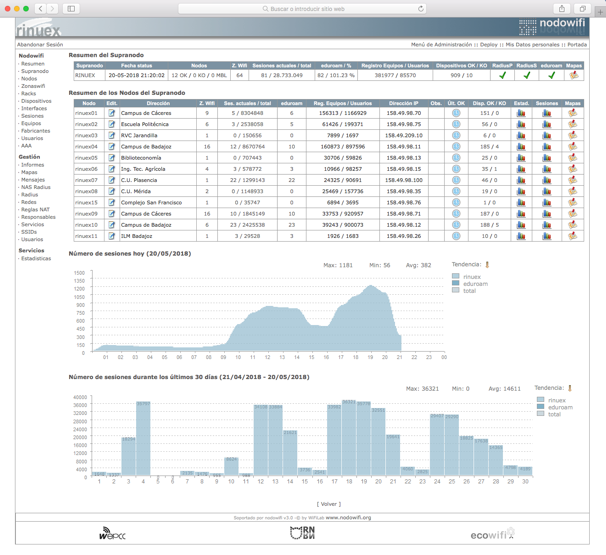
Las características principales del software de supervisión y administración implementado por Nodowifi Manager son:

* Portal web de supervisión en tiempo real del Supranodo de la red.
* Base de datos para la información administrativa y de supervisión de la red.
* Exportación de las configuraciones, función Deploy, desde el Manager a los servidores Nodowifi.
* Auditoría de las sesiones: nombre de usuario, dirección IP, Dirección MAC de acceso al medio, nombre de host, fecha y hora de inicio y fin, volumen de datos transmitidos/recibidos y roamings entre APs del usuario, etc.
* Posibilidad de auditoría de la navegación web de los usuarios, con información del número peticiones, direcciones web (URL, Uniform Resource Locator) solicitadas por los usuarios, fecha, navegador, sistema operativo y fallo/acierto de la cache.
* Estadísticas de sesiones, usuarios, equipos y fallos, por múltiples criterios.
* Gráficas en tiempo real de las sesiones y fallos, por Supranodo, Nodo, Dispositivo y Servicio.
* Gestión de alarmas y eventos.
* Administración de los datos de los servidores corporativos de autenticación (RADIUS, Remote Authentication Dial-In User Service).

###### Portal de gestión Nodowifi Manager.

Se trata de una aplicación web para la administración y supervisión de las redes y usuarios de los distintos Supranodos, con las siguientes características principales:

* Permite gestionar múltiples Supranodos en un sólo Manager, con configuraciones y seguridad diferenciadas.
* Interfaz visual orientado a administrar y supervisar según la jerarquía lógica antes descrita.
* Permite definir usuarios con diferentes perfiles de Administrador, Operador, Responsable de Nodo.
* Permite delegar la gestión de un Nodo o nodos con sus usuarios a un responsable, por ejemplo: una residencia universitaria, biblioteca, hospital, etc.



1. Capturas de pantalla de la página de Resumen del Supranodo.

##### Controladores de acceso Nodowifi Server.

Se trata de un servidor o clúster de servidores en modo activo/pasivo o balanceo de carga, que integran a modo *appliance* las funcionalidades de control de acceso a la red mediante portal cautivo u 802.1x. Es el elemento principal de la arquitectura, en el que recae entre otras funciones el control de acceso, firewall, gestión de la calidad de servicio, proxy de navegación y monitor de red.

En la actualidad, el Nodowifi esta implementado sobre un servidor virtualizado con arquitectura x86 de 64 bits y sistema operativo Linux. Cuenta con doble interfaz de red a 1/10/20 Gigabit Ethernet en función del hardware de virtualización. Los requisitos de memoria y CPU del servidor dependerán del número de usuarios concurrentes y el ancho de banda a gestionar, con un coste que puede variar de trescientos a cuatrocientos euros para un Nodo de una pyme, biblioteca, residencia o telecentro que gestione hasta 100 usuarios con interfaces 1 Gigabit Ethernet, y de mil o dos mil euros para un Nodo de campus con más de 1.000 usuarios concurrentes e interfaces 10/20 Gigabit Ethernet. Estos costes por Nodo son muy inferiores a las controladoras comerciales.

La ‎Figura 38 muestra cómo el Nodo actúa como un *gateway* entre la parte privada (usuarios Wi-Fi) y la red pública (Intranet/Internet).



Internet/Intranet

Nodowifi

Manager

Nodo 1



AP1

L2 switch

Nodo

(WLC)

AAA

RADIUS

LDAP

802.1Q

SSID1 “eduroam” VLAN 20

SSID1 “rinuex” VLAN 21

Gestión VLAN 22

Trunk  
802.1Q

Trunk  
802.1Q

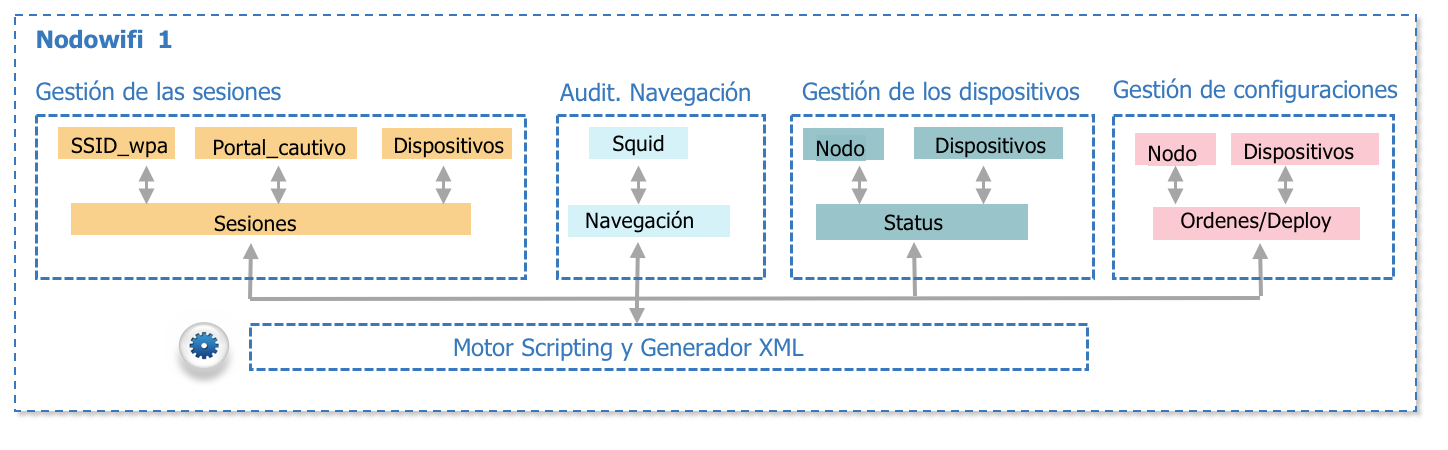
1. Los APs de cada nodo se conectan mediante un trunk 802.1Q a la electrónica de red, separando el tráfico de los distintos servicios Wi-Fi y la red de gestión.

* Permite implementar arquitecturas mono-nodo o multi-nodo, auto-configurables y distribuidas geográficamente, con autenticación, gestión y accounting centralizados.
* Alta disponibilidad con capacidad de redundancia y balanceo de carga.
* Autenticación de los usuarios contra distintos orígenes de datos locales (PAM) o remotos.
* Soporte de tramas 802.1q y asignación de VLANs mediante RADIUS.
* Permite que coexistan clientes inalámbricos y cableados en un mismo Nodo: aulas de libre acceso, laboratorios, etc.
* Gestión de los usuarios con calidades y funcionalidades basadas en perfiles.
* Permite integrar y reutilizar Puntos de Acceso y Antenas de distintos fabricantes.
* Compatible con redes basadas en tecnologías de xDSL y FTTH con balanceo de carga en la salida a red pública.
* Actúa como proxy/cache trasparente de navegación, con la posibilidad de almacenar los registros log para su procesado y correlación con la información de las sesiones.
* Supervisa y configura los elementos de la red inalámbrica, reportando la información de eventos y alarmas al Manager.

Como se indicaba anteriormente, el Nodo está implementado sobre un núcleo Linux de 64bits, en la UEX sobre servidores Debian. Para poder ejecutar las funciones anteriormente descritas, se requieren adicionalmente los paquetes Apache, Perl, MySQL, OpenSSL, Squid, PGP y PHP.

A nivel de sistema operativo, se utilizan adicionalmente, entre otros, los servicios SSH, DHCP, TFTP, NTP, Iptables, IPRoute2, CBQ y TCL.

En la Figura 5 se observa el diagrama de bloques de un Nodo, y cómo se conecta con el Manager, el cual procesa y almacena toda la información recibida vía XML/HTTPS desde los servidores Nodowifi, los cuales actúan como colectores de la información de las sesiones, alarmas, etc.



1. Diagrama de bloques software de un Nodowifi.

###### Flujo y control del tráfico.

El corazón del Nodo está basado en Iptables, que es un potente firewall integrado en el kernel de Linux y que forma parte del proyecto Netfilter.

Iptables es una herramienta de cortafuegos que permite, entre otras funciones, filtrar y redireccionar paquetes IP, realizar traducción de direcciones de red u obtener logs del tráfico. La herramienta tiene soporte para IPv4 (iptables) y para IPv6 (ip6tables).

La estructura por defecto de Iptables se compone de: Tablas, Cadenas y Reglas. Los tres tipos de tablas de mayor uso son:

* MANGLE.
* NAT.
* FILTER.

MANGLE.

Esta tabla se encarga de modificar los paquetes, para lo cual utiliza distintos tipos de modificadores:

* Tipo de servicio TOS (Type Of Service): Define el tipo de servicio de un paquete y se usa para establecer cómo se debe enrutar el paquete.
* Tiempo de vida TTL (Time To Live): Permite cambiar el campo tiempo de vida de un paquete.
* MARK: Permite marcar paquetes con valores específicos, y se puede emplear para limitar el ancho de banda y generar colas mediante CBQ (Class Based Queuing) o definir diferentes enrutamientos con Iproute2.

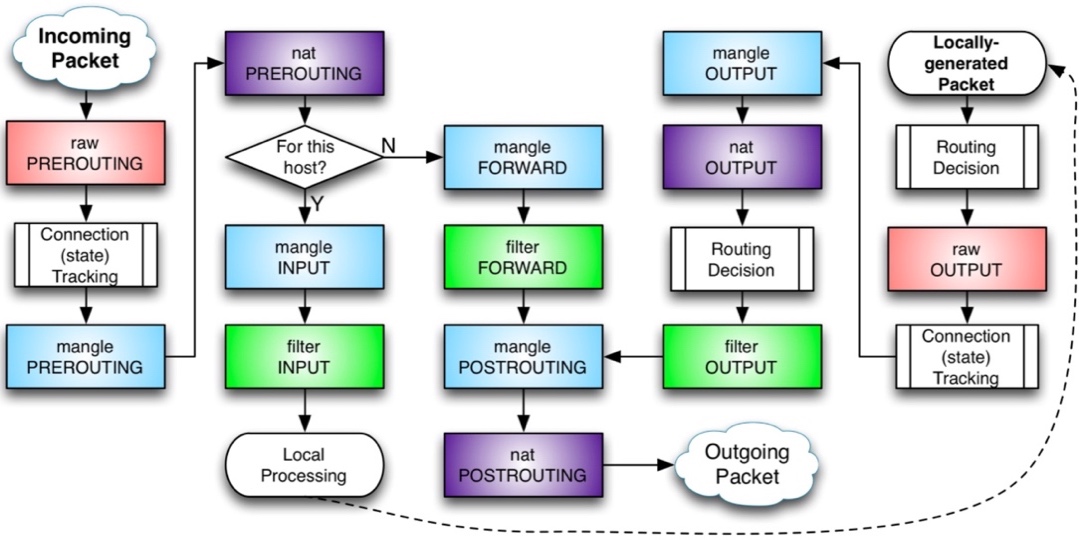
NAT.

* Las tablas NAT (Network Address Translation) se utilizan para traducir direcciones de red y permiten compartir una IP pública entre muchos equipos, por lo que en la actualidad resultan imprescindibles en el protocolo IPv4, dadas las limitaciones en el número de direcciones IP.
* Las tablas NAT permiten añadir reglas para modificar las direcciones IP de los paquetes, y contienen dos reglas:
* SNAT (IP Masquerading): Para la dirección de origen.
* DNAT (Port Forwarding): Para las direcciones destino.
* Las modificaciones se pueden hacer en las cadenas:
* PREROUTING: Para modificar paquetes tan pronto como lleguen al equipo.
* OUTPUT: Para la salida de paquetes que se generan localmente y van a ser enrutados para su salida.
* POSTROUTING: Modificar paquetes que estén listos para salir del equipo.

FILTER:

Es la tabla utilizada por defecto para gestionar paquetes de datos. Estas son las tablas más habituales y son responsables del filtrado de los paquetes según se ha configurado el cortafuegos o filtro. Todos los paquetes pasan a través de esta tabla, y para la modificación tiene tres opciones predefinidas:

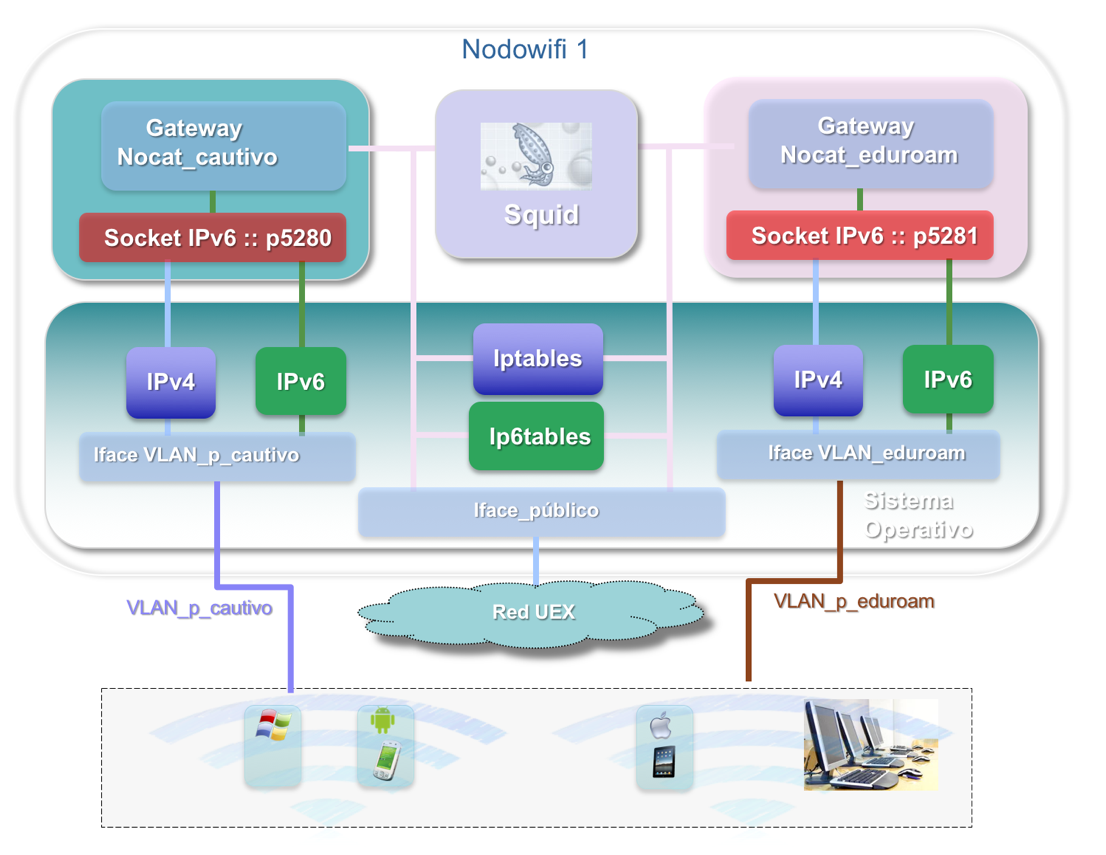
* INPUT: Todos los paquetes destinados a entrar en nuestro sistema deben pasar por esta cadena.
* OUTPUT: Todos los paquetes creados por el sistema y que van a salir de él hacia otro dispositivo.
* FORWARD: Los paquetes de redireccionan a su nuevo destino, afectando a todos los paquetes que pasan por esta cadena.
* Adicionalmente, existen las tablas de menor uso:
* RAW: Filtra los paquetes antes que cualquier otra tabla. Se utiliza principalmente para configurar exenciones de seguimiento de conexiones en combinación con el target NOTRACK.
* SECURITY: Utilizada para reglas de conexión de red del tipo Mandatory Access Control.
* En la Figura 6 se observa el diagrama de flujo de los paquetes entrantes, salientes y generados por un sistema con Iptables.



1. Diagrama del flujo general de un paquete por las tablas y cadenas de Iptables. *Fuente: Phil Hagen SANS FOR572: Advanced Network Forensics and Analysis*.

###### Marcado y rutado de los paquetes.

Como se ha indicado, el Nodo es diseñado para actuar como un Gateway entre las redes denominadas privadas donde se encuentran los usuarios inalámbricos o cableados, y la red denominada pública que da acceso a los servicios de red o Internet (Figura 7).

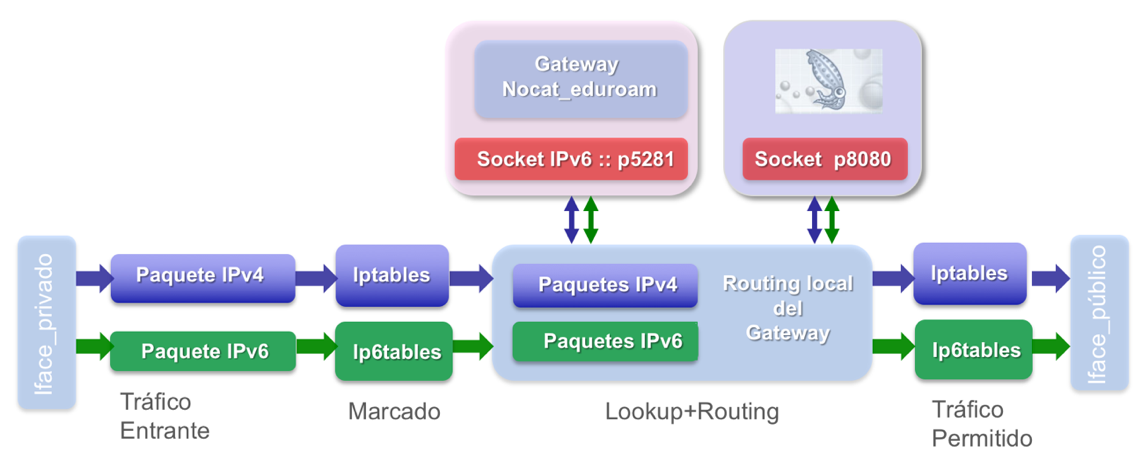
****

1. Arquitectura Iptables de un Nodo: los nodos están configurados en doble pila (IPv4/IPv6) y el tráfico se separa por servicios mediante VLANs independientes.

Los servicios prestados por un nodo pueden diferir en función de su ubicación, pero suelen ser una combinación de las dos siguientes opciones:

* Usuarios cableados o Wi-Fi mediante portal cautivo. Cuando un usuario se conecta a una red de este tipo, al intentar navegar se le redirecciona de forma automática a un portal web donde debe autenticarse vía una página HTTPs. Este es el modelo de implantación para zonas Wi-Fi de alto tránsito y que no disponen de soporte a los usuarios, como hoteles, aeropuertos, zonas de ocio, etc. No requieren de configuración en el cliente y suelen complementar la seguridad con una clave precompartida. Son fáciles de configurar, pero bastante inseguras.
* Usuarios 802.1x. Son usuarios que utilizan un cliente (suplicante) con soporte WPA2 empresarial. El punto de acceso o conmutador al que se conectan (autenticador), actúa como proxy entre el cliente y el servidor de autenticación RADIUS. Requieren de configuración en el cliente para validar los certificados de los servidores RADIUS.

La solución Nodowifi permite una combinación de ambos tipos de clientes y redes, separando el tráfico en VLANs con reglas de navegación y seguridad diferenciadas. La Figura 8 muestra la arquitectura de red de un Nodo y su integración con Iptables.



1. Marcado y rutado de paquetes dentro de un Nodo mediante iptables e ip6tables.

En función de la configuración y ubicación del Nodo, la navegación de todos los usuarios de la parte privada se puede enmascarar mediante NAT, permitiendo compartir una única dirección IP pública a decenas o cientos de usuarios simultáneamente.

##### Puntos de acceso.

###### Fit AP

Las redes actuales utilizan puntos de acceso híbridos denominado Fit AP. Este tipo de redes apareció como evolución de los primeros WLC, donde los APs asumen de nuevo funciones de gestión del tráfico a nivel 2 y 3 y cifrado, especialmente en despliegues de redes de campus con seguridad WPA2, descargando al controlador central de dicho trabajo (Figura 9).



Puntos de acceso híbridos



AP1

AP2



WLC en la nube

1. Red WIFI con dos APs híbridos (Fit APs) y un Controlador de Red Local Inalámbrica (WLC) en el CPD o nube.

La administración y gestión de políticas reside en el controlador, que se conecta con múltiples APs, de cientos a miles, mediante túneles. Dado que el tráfico de red ya no pasa por los controladores en la mayoría de los casos, estos han reducido sus requerimientos hardware o incluso se han convertido en controladores virtualizados desplegados en los Centros de Procesos de Datos (CPD) de las instituciones o de los fabricantes de los APs.

La principal ventaja de este tipo de redes es que permiten administrar despliegues complejos de forma centralizada, sin los problemas de escalado y cuellos de botella de las controladoras centralizadas. Permiten incluso el despliegue en sedes remotas sin necesidad de equipos adicionales.

Las principales desventajas son: la falta de interoperabilidad entre fabricantes, el elevado coste de licenciamiento y la falta de flexibilidad en entornos de investigación o académicos.

###### Puntos de acceso soportados

Al utilizar una arquitectura híbrida con puntos inteligentes, los APs pueden ser de distintos fabricantes. La solución se ha integrado con éxito con puntos de los siguientes fabricantes:

* Alcatel Lucent.
* Hewlett Packard
* Aruba.
* Cisco.
* 3Com.
* Ubiquiti.
* Mikrotic.
* Nomadix.
* Buffalo.
* Comtrend.

##### Limitaciones de la solución actual.

A pesar de que el diseño de la Arquitectura Nodowifi se ha realizado para poder escalar a grandes redes WiFi de miles de APs y decenas de miles de usuarios concurrentes, la gestión y explotación diaria de una gran de red de campus o empresarial se ve limitada por las capacidades de configuración y administración de la electrónica de red clásica, dificultando las tareas de:

* Reconfiguración dinámica de equipos.
* Creación de VLANs bajo demanda.
* Seguridad de la infraestructura y los usuarios.
* Roaming de las sesiones.
* Almacenamiento y proceso de información de alarmas, eventos y estadísticas.

##### Mejora de Nodowifi con la solución UNITAL

SDN puede tener una potencia transformadora en redes de campus al poder dar solución a los problemas y limitaciones planteados en el apartado anterior.

El hecho de que la red *edge* permita la inclusión del paradigma SDN puede suponer que se prioricen aplicaciones clave sobre la red virtual, lo que asegura una experiencia de usuario consistente. Una red de acceso más ágil puede gestionar mejor la alta (y variable) demanda de aplicaciones y servicios, permitiendo proporcionar más servicios de red a una mayor velocidad con menos o los mismos recursos.

La gestión integrada de la red fija y WiFi mediante UNITAL, da la posibilidad de usar end-to-end slicing entre la red fija y WiFi, permitiendo crear slices en ambos dominios y que sean interoperables.

#### Solución Nodowifi UNITAL

##### Integración con la red cableada

Una vez vistos los beneficios que puede aportar la incorporación del paradigma SDN a las redes de campus, la integración del controlador WLC propuesto y el controlador SDN en un único orquestador mediante la solución UNITAL, facilitaría la integración de los servicios prestados mediante la red cableada y la red WiFi.

Para ello, se propone migrar la actual arquitectura Nodowifi multifabricante de controladores Wireless implementados en software de la UEx, a una nueva solución basada en redes definidas por software y funciones de red virtuales, integrada en la solución UNITAL e implementada sobre sistemas abiertos y estándares de la industria.

En concreto, al incorporar SDN a redes WiFi se podrá:

1. **Gestionar mediante un interfaz gráfico integrado.** Unificar la gestión de la red fija y de la red inalámbrica mediante un único interfaz gráfico, simplifica las operaciones de red y reduce los costes. Los administradores de la red ven a los usuarios utilizar una única herramienta, sin importar en la red en la que se encuentran. Asimismo ganan visibilidad en la red unificada.
2. **Crear y forzar a cumplir políticas unificadas en la red.** Con SDN, las políticas se definen una única vez y se aseguran consistentemente a lo largo de las LANs fijas e inalámbricas. Los usuarios tienen una experiencia uniforme, independientemente de su método de acceso.
3. **Construir una red de campus más inteligente que se adapte a requisitos cambiantes necesita “programabilidad”.** Con SDN, la red de campus se convierte en más inteligente y cambia dinámicamente como respuesta a las necesidades de aplicaciones y lógicas de negocio. El hecho de desplegar SDN en la red hace que se puedan definir diferentes niveles de servicio automáticamente para conseguir el rendimiento de red, calidad de servicio o seguridad necesarios. Las APIs basadas en estándares abiertos permiten crear aplicaciones SDN fácilmente que comunican directamente los requisitos de la red y el comportamiento deseado al controlador SDN.
4. **Tener una mejor elección de fabricantes.** SDN es abierto, basado en estándares y permite mezclar componentes de red de diferentes fabricantes. De esta forma, el hecho de ampliar la elección hace que se amplíe y se gane en competencia en el mercado, lo que está relacionado con una mejora en la innovación.
5. **Simplificar el aprovisionamiento de red y reducir los costes.** Ya que las redes SDN responden de manera dinámica a las políticas y carga de tráfico cambiantes, el administrador de la red se libera de tareas manuales que consumen mucho tiempo. De esta forma, se puede centrar en tareas más estratégicas que permitan reducir el coste de las operaciones de red.

La Arquitectura Nodowifi SDN debe permitir:

* Gestión de perfiles de usuarios consistentes en la red fija e inalámbrica.
* Control y configuración de los puntos de acceso inalámbricos.
* Adaptarse de forma dinámica y flexible a los servicios requeridos por la investigación y la docencia presencial/virtual.
* Mejorar la seguridad de la red WiFi y cableada.
* Facilitar la integración para uso docente/investigador de las redes cableadas e inalámbricas en los laboratorios y aulas.
* Facilitar la gestión y control de los dispositivos BYOD del personal y alumnos.
* Fijar políticas basadas en perfiles de usuarios y asegurarlas en la red como un todo (fija e inalámbrica).
* Aprovisionamiento de ancho de banda para aplicaciones clave.

Adicionalmente, como la Arquitectura propuesta se basa en sistemas abiertos y puntos de acceso multifabricante lo cual puede generar ahorros considerables en grandes despliegues mediante:

* La elimina del coste de licenciamiento.
* Mayor EOL de los equipos.
* Licitaciones y ampliaciones abiertas a más fabricantes.
* Utilización de equipos de conmutación white-box switches.

##### Migración de base de datos del modelo relacional a no relacional

En la versión actual de Nodowifi la información administrativa y de supervisión se almacena y trata de una base de datos relacional implementada en MySQL, la información de la base de datos se almacena en un esquema denominado **mngdb**, compuesto por:

* 54 tablas.
* 102 procedimientos almacenados.
* 71 funciones.

La parte administrativa de los Supranodos de la base de datos se alimenta desde el portal de gestión Nodowifi Manager, descrito anteriormente.

Los datos del estado y auditoría de las sesiones, dispositivos, equipos y usuarios, se obtiene de los distintos nodos y dispositivos que componen la red, mediante las funciones y motores de scripting diseñados para el procesado automático e inserción en las BBDD de la información recuperada en formato XML.

Para poder gestionar el gran volumen de datos generado en la parte de auditoría, se propone separar del actual sistema de BBDD relacional, toda la información de auditoría y sesiones, lo cual facilitará su utilización en procesos de mejorar de la explotación y mantenimiento de la red al poder realizar análisis más exhaustivos y técnicas de machine learning.

Para ello se requiere estudiar las distintas opciones de bases de datos no relacionales para definir un nuevo modelo de datos con los siguientes requisitos:

* Utilizar APIs para la alimentación y tratamiento de los datos.
* Esquemas flexibles.
* Escalabilidad horizontal.
* Alta disponibilidad.
* Sistema distribuido y replicable.
* Particionado.
* Código abierto.

#### Posible propuesta: uso de AI para mejorar la eficiencia energética de APs.

Con la monitorización de las conexiones de los usuarios, se puede predecir el uso de la red y los servicios, para posteriormente aplicar políticas de ahorro de energía. Por ejemplo, se pueden desconec tar APs en momentos donde el tráfico se prevé que sea bajo, y seguir dando servicio con un número más reducidos de APs. Para el caso contrario, se podrán conectar más APs en periodos de incremento de tráfico. Esta funcionalidad sería de especial interés para áreas con alta concentración de APs y flujo variable de personas, como por ejemplo el comedor**. (Ver con UVIGO)**

### Monitorización

UVIGO: ampliar/mejorar

Herramienta de monitorización de infraestructura SDN que permitirá disponer en todo momento de los KPIs de interés y un cuadro de mando (dashboard) que proporcione una visualización gráfica del estado de la SDN y la posibilidad de alertado ante eventos.

Estará basada en plataformas abiertas que eviten la dependencia con un fabricante particular.

Constará de los siguientes elementos básicos: la captación de métricas, el almacenamiento de las series de tiempo asociadas, la visualización y alertado. Deberá soportar múltiples puntos de presencia (PoPs), para lo cual se estudiará la realización de una arquitectura federada.

Se partirá de Prometheus, el principal conjunto de herramientas de monitorización de red para entornos virtualizados, para la captación de métricas, el almacenamiento y el alertado. La visualización se llevará a cabo mediante Grafana.

Se adaptarán / desarrollarán los módulos de captación (exporters) para Prometheus necesarios para recoger métricas de los elementos SDN y NFV (máquinas virtuales, contenedores, conmutadores / enrutadores virtuales) a través de sus APIs. En particular, se considerarán el API de OpenDayLight en cuanto a controladores OpenFlow y el API de OpenStack para acceder a sus componentes. También se aprovecharán protocolos estándar de monitorización de red como SNMP, sFlow y NetFlow/IPFIX.

Según las necesidades del proyecto, se incorporarán herramientas como Monasca (Monitoring-as-a-Service de Openstack). También se contemplarán otras tecnologías complementarias para cubrir aquellos aspectos que lo requieran: Telegraf, InfluxDB, etc.

Se tendrán en cuenta los avances llevados a cabo por los proyectos europeos sobre monitorización de SDN y NFV como SONATA-NFV, 5GTANGO [1] y NECOS (Novel Enablers for Cloud Slicing).

#### Requisitos

La herramienta de monitorización y visualización deberá soportar la escalabilidad requerida para la propia UNITAL. Deberá soportar múltiples PoPs, para lo cual se estudiará la realización de una arquitectura federada.

En cuanto a la captación de métricas, deberá soportar protocolos como HTTP, SNMP, sFlow, NetFlow/IPFIX, y las APIs de OpenDayLight y OpenStack.

#### Diseño/arquitectura propuesto



Figura 6.3: Diseño sistema monitorización

## Módulos

### HPaaS

ITER: ampliar/mejorar

Teide HPC

Actualmente, el ITER cuenta con el Teide HPC, un centro de computación de alto rendimiento que fue creado como parte del proyecto ALiX y que se encuentra en la lista del top 500 supercomputadores más potentes del mundo. La infraestructura cuenta con las siguientes características:

* 1000 nodos de cómputo
* Redes internas
  + Storage
  + Gestión
* Red exterior
  + Red Iris
  + Otros operadores

Sin embargo, estas capacidades se ven altamente limitadas por la falta de flexibilidad de las herramientas de compartición y gestión de recursos actualmente en uso. El datacentre requiere la configuración manual del firewall, la transferencia de ficheros mediante SFTP y el acceso a usuarios a través de VPNs y conexiones SSH.

Cambio de las condiciones de contorno

Debido a estas razones, la virtualización y containerización son necesarias en el entorno IT actual para poder competir con cloud existentes basándose en el entorno común UNITAL para la prestación de servicios entre entidades. Los usuarios potenciales serían las universidades (tanto para supercomputación como para el uso de disaster recovery sin necesidad de contar con un CPD secundario de redundancia), empresas y proveedores.

Es posible implementar este tipo de servicio desde diferentes aproximaciones. Una posibilidad es incluirlo como una capa por encima del sistema cloud en el que se desplieguen máquinas virtuales con configuración de nodos de cómputo. Otra aproximación es el desarrollar o integrar un software de acceso remoto que permita la ejecución de trabajos en un gestor de colas. Cada una de estas alternativas presenta sus ventajas e inconvenientes, así como desafíos tecnológicos para su implantación. Más adelante habría que decidir cuales se quieren afrontar y hasta qué nivel se desarrollaría el prototipo.

Módulos

Estos serían

* Planificador:
  + Centralizado
  + Independientes
* Gestión del almacenamiento
  + Movimiento de datos para ejecutar en cada infraestructura
* Catálogo de aplicaciones

### Gestión de Energía

UVIGO: ampliar/mejorar

La propuesta de gestión energética pasa por el desarrollo de mecanismos y herramientas de monitorización del uso de la nueva infraestructura de red y comunicaciones que se creará para servir al conjunto de las universidades españolas, atendiendo a parámetros de rendimiento que incorporen no sólo aspectos de QoS de las comunicaciones, sino también de consumo energético, impacto medioambiental, coste, jornada laboral, etc. Para ello, el trabajo se centrará en dos frentes:

* Diseño, implementación y validación de módulos de inteligencia artificial que procesen el caudal de medidas procedentes de cualesquiera elementos conectados a la red, a fin de caracterizar perfiles de dispositivos y usuarios, identificar correlaciones entre parámetros (e.g. actividad de envío o recepción de paquetes por parte de un conjunto variable de máquinas vs consumo energético agregado de las mismas), realizar mantenimiento proactivo, detectar anomalías (e.g. consumos anómalos o usos inadecuados de la red), optimizar configuraciones, etc.
* Diseño implementación y validación de herramientas de visualización y análisis de datos, con versiones web y móvil de todos los *front-ends* que permitan la supervisión por humanos de todos los procedimientos de monitorización, gestión y mantenimiento, al tiempo que dan soporte a todos los procesos de toma de decisiones.

Con los aportes previstos se habilitarían funcionalidades como las siguientes:

* Integración de la nueva infraestructura de comunicaciones con tecnologías de smart grid.
* Preparación para el futurible despliegue de equipos de generación de energía en los campus de todo el territorio nacional.
* Planificación y orquestación de recursos de red virtualizados con arreglo a criterios de eficiencia energética (además de los clásicos: latencias, jitter, etc.).
* Aplicación de técnicas de machine learning para detección de anomalías en tiempo real.
* Optimización de la gestión de eventos críticos por medio de IA.
* Caracterización de los umbrales que justifican el uso de elementos de red virtualizados frente a equipamiento tradicional.
* Identificación de posibles incumplimientos sistemáticos (por exceso) de la jornada laboral del personal docente o investigador.

Requisitos

La propuesta se plantea como una integración de los protocolos genéricos de Internet y específicos del Internet de las Cosas (MQTT, LoRa, BLE, …), previendo tanto escenarios en los que se puedan monitorizar parámetros de comunicaciones o consumo de manera detallada para cada dispositivo conectado, como escenarios en los que se disponga – en mayor o menor medida – de lecturas agregadas, que podrán desacoplarse a través de IA.

A efectos de la implementación de las herramientas de visualización y análisis de datos se considerarán los estándares actuales de seguridad de aplicaciones y de red, con gestión profesional de vulnerabilidades y actualizaciones. Asimismo, se perseguirán los requisitos de usabilidad/accesibilidad estipulados por las *Web Content Accessibility Guidelines* (WCAG) del consorcio W3C (estándar internacional ISO/IEC 40500) y normas afines.

### Seguridad Avanzada

UDC: ampliar/mejorar

En una infraestructura de red como la que se propone, basada en SDN, protegida de ataques externos por *firewalls* y donde el acceso a la red se controla mediante IEEE 802.1x, los riesgos frente a ataques externos son limitados. Sin embargo, todavía existen diferentes posibilidades de realizar ataques desde la red interna, debido a que los usuarios autorizados puedan llevar a cabo acciones no permitidas tanto de forma voluntaria (ataques de reconocimiento, contra la infraestructura, contra otros equipos en su subred, etc.) como accidentales (por ejemplo, los generados por *malware*).

Un usuario descontento podría lanzar un ataque deliberado contra equipos de su subred, servidores a los que se le haya autorizado el acceso o la propia infraestructura. Por otro lado, en el caso de que un equipo de la red interna se vea comprometido por *malware*, se podría aprovechar de la conexión a la red de un usuario legítimo para propagar dicho software malicioso o llevar a cabo otro tipo de acciones ilegítimas.

Para ayudar a mitigar estos riesgos se propone un sistema de detección de anomalías basado en el análisis de tráfico de la red y de la información de registro de los servidores AAA.

El sistema utilizará la interfaz *northbound* de los controladores de la SDN para obtener la información de los flujos de red que circulan por la misma, utilizando IPFIX o Netflow. De este modo se pueden modelizar los diferentes tipos de tráfico existente y detectar patrones de tráfico anormal empleando diferentes técnicas (como, por ejemplo, Random Forests o mapas autoorganizados).

Además, se dispondrá también de la información de *log* de los servidores de autenticación (usados para controlar el acceso a la infraestructura) para detectar patrones propios de comportamiento anómalo con el fin de complementar los resultados obtenidos en el análisis de flujos de tráfico.

Una vez detectadas las anomalías, el sistema podrá proporcionar información al controlador SDN para que modifique las políticas de envío, de modo que los usuarios y, por consiguiente, los dispositivos sospechosos, sean bloqueados o vean restringida su comunicación a una zona o red de cuarentena en la que los dispositivos puedan ser analizados en profundidad y tratados.

# Pruebas y validación

Todos: ampliar/mejorar una vez terminada sección 3

## Validación funcionalidad general

Demostrar que, dentro de una misma red, cada uno de los distintos sites es gestionado por un controlador local y que el conjunto de éstos es gestionado por un único punto de control, el orquestador, que aplicará de forma centralizada las diferentes políticas globales de red, traduciéndolas a instrucciones de configuración para cada uno de los puntos de control.

Estas son las distintas localidades donde los miembros del proyecto desplegarán la red:

|  |  |
| --- | --- |
| Entidad | Localidad despliegue red |
| UNEX | Escuela Politécnica - Campus de Cáceres |
| UVIGO | Vigo |
| UAH | UAH- Rellenar |
| CESGA | CPD del CESGA y campus principales de UDC y UVIGO (simular RECETGA) |
| UDC | Campus Elviña: Edificio de Servicios Centrales de Investigación, Fac. de Informática |
| ULL | Campus Central |
| ITER | Instalaciones ITER y CEDeI - Polo Sur del Parque Científico y Tecnológico de Tenerife |

*Tabla 7.1: Localidades red*

### Escalabilidad

El elevado número de sites por área de control y la latencia introducida por la lejanía entre los diferentes sites del despliegue de la red permitirá medir la escalabilidad de la red. En condiciones de funcionamiento normal, se harán mediciones de la latencia (OW and RTT), jitter y ancho de banda utilizado tanto de uplink como de downlink. Para ello, se utilizarán varios tamaños de paquetes simulando distintos tipos de conexiones y se medirán los tiempos de respuesta por parte de los controladores y orquestador a eventos de la red.

### Renumeración

Renumeración de una subred, pasando de direccionamiento público a privado en cierto departamento/site, comprobando que tanto las reglas de routing, seguridad y calidad de servicio se actualizan de acuerdo a las nuevas direcciones de red. Medición además del tiempo que tarda en converger la red desde que se aplica el cambio.

### Pruebas de carga

Para una red de 500 PoP pruebas de:

* Carga de peticiones DHCP
* Carga de nuevas conexiones IP y de los ARPs producidos por éstas
* Impacto del tráfico de control
  + DHCP
  + ARP
  + OSPF/BGP
  + DNS
  + RADIUS/Diameter

#### Pruebas de rendimiento y throughput

Impacto en el plano de datos usando de diversas combinaciones de tráfico, TCP/UDP, variando el tamaño de los paquetes, número de conexiones simultaneas.

### Pruebas alta disponibilidad

* Simular la caída de alguno de los controladores de la red, comprobando cómo el orquestador detecta su baja, ejecuta una nueva instancia y resume el control de la red, midiendo además el tiempo de respuesta y de resolución.
* Simular la caída del orquestador, causando que la instancia que se estaba ejecutando en segundo plano como esclavo se convierta en máster, conservando el estado y configuración del anterior y resumiendo el control sin bajas en la red. Se probará también como las caídas en dichas funciones afectan a las funcionalidades del sistema, en términos de latencia, QoE de los usuarios…etc
* Comparación de los resultados obtenidos con otros protocolos legacy para obtener alta disponibilidad en el plano de datos como Hot Standby Router Protocol (HSRP) o Gateway Load Balancing Protocol (GLBP).

## Validación arquitectura y módulos

### Validación Arquitectura

#### Slicing con federación

Implantación en la UDC de un piloto con 2 entornos de pruebas con los equipos del proyecto en los 2 centros seleccionados en la propuesta. Se prestará servicio a usuarios concretos para validar las funcionalidades solicitadas.

#### Seguridad

#### Red inalámbrica

Migración al nuevo sistema y electrónica de red 300APs distribuidos en las 3 ubicaciones de UEX propuestas en el proyecto, probando con tráfico y usuarios reales.

#### Monitorización

### Validación Módulos

#### HPaaS

#### Gestión de Energía

La validación se plantea por separado para los módulos de IA y las herramientas de visualización y análisis:

* Por una parte, los distintos módulos de IA se desarrollarán inicialmente en entorno controlado de laboratorio, alimentados por datos generados sintéticamente o recuperados de *datasets* de acceso abierto. A medida que se avance en la construcción y despliegue de la nueva infraestructura, se irán integrando en la misma y se lanzarán experimentos de complejidad creciente, empezando por subredes aisladas y abriéndose progresivamente a la totalidad de los recursos conectados.
* Por otra parte, las herramientas se validarán contando con la participación de administradores de sistemas expertos, que participarán en sucesivas rondas de diseño y prueba para avanzar en la identificación de requisitos, necesidades y expectativas a propósito de los distintos *front-ends* y sus versiones web y móvil.

#### Seguridad Avanzada

# Presupuesto del proyecto y división de tareas

## Presupuesto

Telcaria: actualizar una vez terminada la sección 3 y 4

Presupuesto preliminar por tareas y CCAA

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Comunidad | Sitios | Desarrollo Arquitectura | Desarrollo Módulos | Desarrollo Subcont. | Capacitación | Implantación y Soporte | Switches | TOTAL |
| Andalucía | 4 | 887.000 | 793.000 | 161.000 | 56.000 | 296.490 | 306.000 | 2.499.490 |
| Canarias | 3 | 887.000 | 656.000 | 144.000 | 42.000 | 238.680 | 229.500 | 2.197.180 |
| Castilla La Mancha |  |  |  |  |  |  |  |  |
| Extremadura | 4 | 887.000 | 793.000 | 161.000 | 56.000 | 296.490 | 306.000 | 2.499.490 |
| Galicia | 4 | 887.000 | 793.000 | 161.000 | 56.000 | 296.490 | 306.000 | 2.499.490 |
| TOTAL | 15 | 3.548.000 | 3.035.000 | 627.000 | 210.000 | 1.128.150 | 1.147.500 | 9.695.650 |
| Porcentaje |  | 37% | 31% | 6% | 2% | 12% | 12% | 100% |

*Tabla 8.1: Presupuesto*

## Presupuesto por Paquetes de Trabajo

Telcaria: rellenar una vez terminada la sección 3 y 4 (junto con el resto de subcontratados)

En la realización del proyecto se identifican dos fases principales que son:

1.- Creación de una infraestructura base que permita la creación y administración de slices con federación, la creación de reglas de acceso y de seguridad básicas entre éstas, la integración con la red inalámbrica y un sistema de monitorización.

2.- Desarrollo de una serie de verticales que cubran las necesidades más específicas y avanzadas dentro del entorno universitario: HPaaS (incluyendo cloud privada), gestión de energía y seguridad avanzada (uso de IA para la detección de anomalías).

Las tareas de alto nivel a desarrollar en cada una de las fases son las descritas en los siguientes paquetes de trabajo:

### PT 1: Gestión y dirección

Se realizarán todas las tareas necesarias para llevar a cabo el proyecto con éxito, es decir, en el plazo determinado, con el alcance definido y los recursos planificados. En concreto, se realizará el establecimiento de las metodologías para el inicio, planificación, ejecución, seguimiento, control y cierre del proyecto, así como las actividades necesarias para realizar todas estas tareas.

1. Inicio: En esta etapa se hace la redacción de la propuesta (objeto, objetivos, alcance, calidad y riesgos del proyecto), y describe cómo se llevará a cabo. Incluye también estimaciones de coste y tiempo, y efectúa la Integración de todo lo anterior con lo que sigue.

2. Planificación: Se realiza la planificación de todas las actividades necesarias para llevar a cabo el proyecto, considerando las prioridades del proyecto, los recursos necesarios, los tiempos esperados para ejecutar cada una de las tareas. 3. Ejecución: Se refiere a la implementación o puesta en marcha del proyecto, consiste en poner en práctica la planificación llevada a cabo previamente. Durante la ejecución del proyecto, se debe poner énfasis en la comunicación para tomar decisiones lo más rápido posible en caso de que surjan problemas.

4. Seguimiento y Control: El fin de las actividades de control es asegurar que los objetivos sean alcanzados en el tiempo y calidad planificada, realizando una buena supervisión y medición del rendimiento de los resultados, con el objetivo de que se puedan tomar acciones correctivas.

5. Cierre: Cierre es la etapa final de un proyecto en la que éste es revisado, y se llevan a cabo las valoraciones pertinentes sobre lo planeado y lo ejecutado, así como sus resultados, en consideración al logro de los objetivos planteados. Se realizan las pruebas finales de corrección de la solución y la verificación.

### PT 2: Desarrollo Arquitectura

En este paquete se desarrollará la primera fase identificada en 8.2 para la creación de la infraestructura base.

#### Slicing con federación

#### Seguridad

#### Red inalámbrica

#### Monitorización

### PT3: Desarrollo Módulos

#### HPaaS

#### Gestión de Energía

#### Seguridad Avanzada

### PT4: Capacitación

### PT4: Implantación

# Bibliografía

|  |  |
| --- | --- |
| [1] | C.Parada, J.Bonnet, E.Fotopoulou, A. Zaferopoulos, E.Kapassa, M. Toulopou, D.Kyriazis, R.Vilalta, R. Muñoz, R. Casellas, R. Martinez and G. K. Xilouris, "5GTANGO: A Beyond-MANO Service Platform," in *IEEE European Conference on Networks and Communications (EuCNC)*, 2018. |
| [2] | Open Netoworking Foundation, "OpenFlow Switch Specification," 2015. [Online]. Available: https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf. |

[Cisco\_VNI] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper (https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html)

[INTEF\_TIC] Indicadores del uso de las TIC en España y Europa 2016. Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF) Dep. de Proyectos Europeos. 2016.

1. <https://www.srgresearch.com/articles/switch-router-revenues-set-new-record-cisco-market-share-still-over-50> [↑](#footnote-ref-2)
2. <https://www.idc.com/tracker/showproductinfo.jsp?prod_id=1002> [↑](#footnote-ref-3)
3. <https://www.idc.com/tracker/showproductinfo.jsp?prod_id=1001> [↑](#footnote-ref-4)