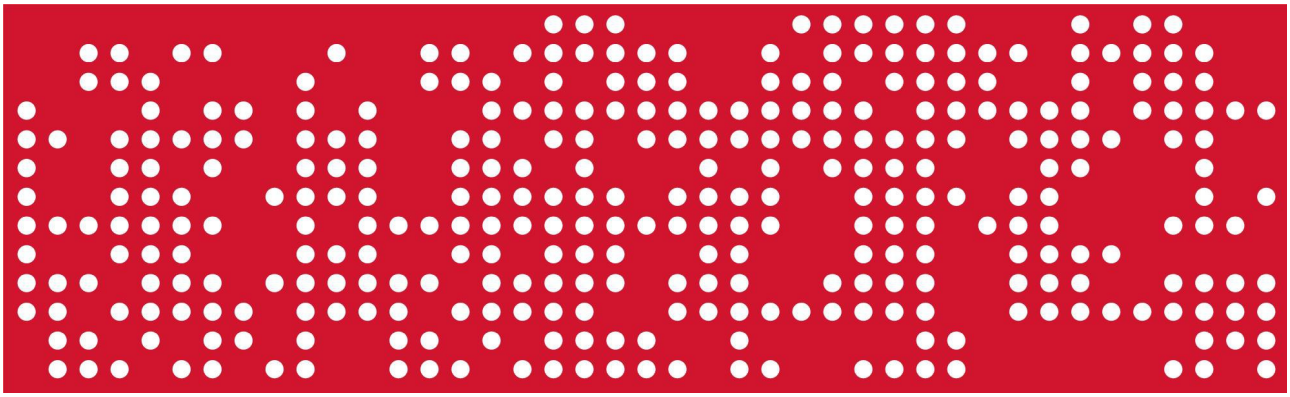
MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

Política de eduroam ES

Versión 2.0.1



1 de noviembre de 2013

red.es

Índice

1. INTRODUCCIÓN, OBJETIVO Y PRINCIPIOS

1.1. Introducción

La creación de un espacio común de movilidad entre todas las instituciones académicas y de investigación englobadas en las redes de investigación, requiere la adopción de una política común de uso de la tecnología.

La infraestructura de eduroam en España forma una federación que es operada por RedIRIS, la red académica y de investigación española, y en la que toman parte las instituciones participantes en la iniciativa. En adelante nos referiremos a la iniciativa eduroam, a nivel de España, mediante "eduroam ES". La federación está unida al mismo tiempo a la federación europea de eduroam.

Este documento pretende ser una guía de uso de la infraestructura eduroam para España, incluyendo también una relación de los requisitos técnicos y formales que han de cumplir las organizaciones participantes. El documento está basado y es compatible con la política desarrollada dentro de la actividad de servicio de eduroam en GÉANT3, que define la política a nivel europeo.

Los requisitos hacen uso de palabras en mayúsculas que definen la obligatoriedad o recomendación de cada uno de ellos, en concordancia con lo que define la RFC 2119.

1.2. Principios de la iniciativa

El proyecto eduroam ES consiste en el desarrollo de un espacio de colaboración para facilitar la movilidad en el acceso a la red entre organizaciones de la comunidad RedIRIS, de tal forma que cuando sus usuarios viajen a otras organizaciones, estos puedan disponer de una manera automática de servicios de conectividad, o autorización para utilizar otros servicios que puedan considerarse en el futuro.

Es responsabilidad del usuario del servicio respetar las políticas de uso, tanto de la institución visitada, como de su organización origen.

1.3. Objetivo de este documento

El objetivo principal de este documento es formalizar la relación entre organizaciones que están unidas a la federación eduroam ES, aportando procedimientos compatibles con la misma iniciativa a nivel europeo y mundial, así como facilitar la gestión de la movilidad entre organizaciones a nivel nacional.

2. PROVEEDOR DE SERVICIOS Y PROVEEDOR DE IDENTIDAD EN EDUROAM

Es necesario hacer una distinción entre proveedores de identidad eduroam (en adelante IdPs), y proveedores de servicio (en adelante SPs):

Una organización podrá unirse como IdP eduroam (es decir, sus propios usuarios podrán conectarse desde fuera de su organización) únicamente cuando esta se encuentre afiliada a RedIRIS, y reúna los requisitos técnicos y administrativos mencionados más adelante.

En el caso especial de una organización no afiliada a RedIRIS, esta podrá unirse **únicamente como proveedor de servicios** eduroam (ofrecer conectividad a usuarios de otras organizaciones en eduroam) bajo los siguientes supuestos:

La firma un acuerdo entre RedIRIS y la organización en el que se establezcan las condiciones bajo las cuales se ofrecerá el servicio por la organización, así como la vinculación con el mundo académico de esta. La firma de dicho acuerdo estará en cualquier caso supervisada por el comité de gestión de RedIRIS.

Exista otra organización afiliada a RedIRIS que pueda responder en nombre de la que prestará el servicio, y la relación entre ambas quede suficientemente demostrada.

El apartado 4 resume los requisitos técnicos y formales para unirse a eduroam tanto para los proveedores de servicio como para los proveedores de identidad.

3. TÉRMINOS DE PRESTACIÓN DEL SERVICIO

El servicio deberá ser prestado por las organizaciones participantes bajo los siguientes términos:

- El servicio eduroam DEBE ser para uso único de usuarios que pertenezcan a organizaciones afiliadas a redes de investigación que se encuentren unidas al proyecto eduroam a nivel internacional.
- Los usuarios en itinerancia DEBEN autenticarse en su propia organización (IdP), con el fin de obtener servicios de acceso en la organización visitada (SP).
- Todos los usuarios en itinerancia DEBEN ser responsables de sus credenciales, y DEBEN respetar tanto la política de uso de su organización como la de las organizaciones que visiten.
- Los SP DEBERÍAN hacer publicidad del servicio de acceso eduroam para que los usuarios visitantes tengan constancia y puedan hacer uso del mismo.
- La organización visitada DEBE garantizar la transmisión segura de las credenciales de los usuarios móviles. Los estándares a utilizar para el cumplimiento de este requisito se explican en el siguiente apartado.
- El SP PUEDE bloquear el acceso a cualquier usuario visitante si estima que no cumple con la política de uso de la organización visitada. Cualquier abuso DEBE reportarse a RedIRIS.
- Las organizaciones visitadas DEBEN establecer en cualquier caso la autorización de cara al acceso a los servicios prestados a los usuarios de otras instituciones.

La organización origen del usuario DEBE ser la responsable para dar soporte a sus propios usuarios, incluyendo formación en tecnologías de acceso a la red, así como de la aceptación de políticas de uso.

4. REQUISITOS A CUMPLIR POR LAS ORGANIZACIONES EN eduroam

Los términos de servicio expresados en el párrafo anterior se concretan en los siguientes requisitos a cumplir.

1. Los IdPs DEBEN responsabilizarse de formar a sus usuarios en el respeto a las políticas de uso de las organizaciones visitadas, así como ayudar en cualquier aspecto relacionado con sus usuarios cuando estos estuvieran en itinerancia en otras organizaciones.

2. Como SP, las organizaciones participantes DEBEN poseer un servidor de autenticación (NAS) que pueda, de un modo seguro, procesar y transmitir las credenciales de usuario solicitadas, utilizando para ello paquetes `Access-Accept` de RADIUS, en conformidad con la sección 3.16 de la RFC3580.

3. Los SPs DEBERÍAN disponer de mecanismos para informar a los usuarios sobre las peculiaridades de la oferta del servicio, así como las ubicaciones en las que están disponibles.

4. Los SPs DEBEN usar siempre el SSID "eduroam". Sólo en aquellos casos en los que exista un solapamiento de puntos de acceso de distintas organizaciones físicamente muy cercanas, se recomienda además (nunca como sustitución) el uso de SSIDs de la forma "eduroam-[INST]", donde [INST] es una sigla descriptiva de la institución a la que pertenece cada uno de los puntos de acceso en cuestión.

5. Los SPs DEBEN disponer de mecanismos para informar a sus usuarios visitantes de los niveles de seguridad ofrecidos en la transmisión de credenciales.

6. En el despliegue de redes inalámbricas nuevas DEBE usarse siempre cifrado WPA2/AES. Aquellas organizaciones unidas a la iniciativa antes del 1 de enero de 2012 PUEDEN usar WPA/TKIP como único método de cifrado hasta el 1 de enero de 2013, a partir de esta fecha todas las instituciones DEBEN soportar WPA2/AES.

7. Los IdPs DEBEN informar convenientemente a sus usuarios del servicio de movilidad, aclarando que el soporte técnico recae sobre

su organización origen. Cuando la organización origen determine que existe un problema que puede ser responsabilidad de la organización visitada, DEBERÍA notificarlo a RedIRIS para la depuración del mismo, implicándose a la organización visitada si fuera necesario.

8. Las organizaciones participantes DEBEN guardar información relativa a sesiones de autenticación y acceso a la red. Asimismo DEBEN ser capaces de realizar un seguimiento de un usuario por razones de seguridad. En concreto, DEBERÁN mantener la CORRELACIÓN de direcciones MAC y direcciones IP dadas a los visitantes mediante DHCP, junto con la hora, establecida a partir de una fuente fiable de tiempo, en la que se produjo la asignación. Las organizaciones participantes deben comunicar problemas de seguridad o uso fraudulento tanto a los responsables de la iniciativa eduroam ES, como a los responsables de seguridad de RedIRIS (IRIS-CERT), para solucionarlo de manera coordinada.

9. Las organizaciones participantes deben disponer de mecanismos de monitorización y seguimiento que permitan conocer el estado de los servidores de autenticación, para poder analizar problemas de conexión.

10. De acuerdo con la política establecida para el servicio a nivel europeo, sólo podrá usarse el nombre "eduroam" para mecanismos de control de acceso basados en el estándar IEEE 802.1x (tanto en redes cableadas como inalámbricas, protegidas con el nivel de cifrado citado anteriormente). Cualquier otro uso del nombre eduroam o de la infraestructura de eduroam fuera de este cometido queda terminantemente prohibido.