

ANEXO

Normativa de uso de la red corporativa de la UM

1.- Introducción

La red corporativa de la UM (UnimurNet) debe entenderse como un servicio más puesto a disposición del colectivo universitario. Lo especial de este servicio sería la horizontalidad del mismo, ya que se trata de un servicio imprescindible para que funcionen todos los demás servicios que requieren del uso de la red.

Este servicio consiste básicamente en proporcionar acceso a la red a distintos tipos de dispositivos y por diferentes medios. El medio más común es el cable. Las conexiones cableadas se realizan a través de las rosetas RJ45 que conectan con los centros de cableado de cada edificio. El medio alternativo más extendido es la conexión inalámbrica, la cual es usada principalmente por equipos portátiles y dispositivos más ligeros tales como PDAs y teléfonos móviles.

2.- Objetivo y ámbito de aplicación

Esta norma regula el uso de los recursos de acceso a la red de la Universidad de Murcia sin perjuicio de las normas y políticas de seguridad de uso generales proporcionados por ATICA, de las normas y disposiciones de la Universidad de Murcia y de otras leyes de categoría superior que en su momento puedan aplicarse, tales como la [Política de uso de RedIRIS](#), la red académica nacional de la que formamos parte.

Las condiciones que aquí se exponen pueden ser actualizadas para adecuarlas a nuevas situaciones. Por ejemplo podrán variar las condiciones que deben darse para la denegación del servicio a equipos afectados por procesos de cuarentena. Consultar el documento de Gestión de cuarentenas para más detalles.

3.- Solicitudes de acceso a la red

Podrán disponer de acceso a la red de la Universidad de Murcia todos los usuarios que dispongan de una cuenta de correo electrónico del dominio @um.es. También podrán acceder vía WiFi los miembros de otras universidades e instituciones de la red académica española (RedIRIS) que estén dentro del proyecto EDUROAM.

Las solicitudes de acceso de personal vinculado a la UMU pero que no son PAS, PDI o alumnos, deberán seguir un procedimiento especial para su aprobación, que no está redactado aún.

4.- Acceso cableado

Las solicitudes de acceso cableado deben ser aprobadas por el responsable de la unidad para la cual se solicita el nuevo punto de red. En dicha solicitud debe especificarse la unidad a la que imputar el gasto, el código patrimonial de la dependencia donde se requiere el servicio y los detalles de ubicación de la roseta, si se estima conveniente.

Por otro lado, los ordenadores conectados a la redes de la Universidad se deben configurar mediante DHCP (direccionamiento dinámico) o mediante configuración alternativa suministrada por ATICA. En caso contrario, es posible que no se permita el acceso.

Existe la posibilidad de solicitar direccionamiento dinámico fijo para equipos que requieran tener siempre la misma IP.

5.- Acceso Inalámbrico

Para acceso inalámbrico solo es necesario disponer de una cuenta @um.es y de un equipo adecuadamente configurado para acceso a la red WiFi de la UMU.

ATICA atenderá las solicitudes de sus usuarios que demanden mejoras de cobertura WiFi en cualquier zona de sus instalaciones.

6.- Usos de la red

El usuario se compromete indirectamente a aceptar las condiciones estipuladas en los acuerdos de conexión de la Universidad a RedIRIS (<http://www.rediris.es/rediris/aup.es.html>) en las que se señala el uso de los servicios para fines puramente académicos y de investigación, lo que excluye cualquier uso comercial de la red, así como prácticas desleales o cualquier otra actividad que voluntariamente tienda a afectar a otros usuarios de la red, tanto en las prestaciones de ésta como en la privacidad de su información.

En particular quedan expresamente prohibidas las siguientes acciones:

- Tratar de causar daño a sistemas o equipos conectados a RedIRIS y otras redes a las que se proporcione acceso.
- Congestionar intencionadamente enlaces de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.
- Modificar la estructura de la red añadiendo switches o hubs departamentales para permitir la conexión de varios equipos en un solo puerto de red.
- Establecer bucles entre puertos de red.
- Cambiar el latiguillo RJ45 de roseta en caso de incidente de seguridad.
- Provocar interferencias deliberadamente en las bandas usadas para la conexión WiFi.
- Conectar dispositivos que se alimenten vía Ethernet sin autorización de ATICA.

7.- Suspensión temporal o de emergencia del servicio

Esta medida procederá en aquellos supuestos en los que la violación de los términos de este documento esté causando una degradación en los recursos de la red y/o implique a la UMU en algún tipo de responsabilidad. Esta decisión será tomada por el equipo técnico de ATICA responsable de la gestión de incidentes de seguridad. El servicio se restablecerá cuando la causa de la degradación del servicio haya desaparecido.

Existe un documento específico para la gestión de incidentes de seguridad.