I.2.16. Acuerdo 16/CG de 13-05-22 por el que se aprueba la Normativa de Uso de la Red de Comunicaciones de la Universidad Autónoma de Madrid

NORMAS TÉCNICAS DE SEGURIDAD
NORMAS DE USO DE LA RED DE COMUNICACIONES DE LA UNIVERSIDAD AUTÓNOMA DE MADRID

Contenido

EXPOSICIÓN DE MOTIVOS

La Política de Seguridad de la Información de la Universidad Autónoma de Madrid (en adelante UAM), aprobada en Consejo de Gobierno de 16 de julio de 2015, establecía en su punto 14 que ésta debe ser objeto de desarrollo para que queden perfectamente definidas las medidas de seguridad específicas. Estas normas de desarrollo deberán respetar lo dispuesto en la política de seguridad. Dentro de este marco normativo nos encontramos en lo que el punto 14 define como normas de segundo nivel, a las que corresponde el desarrollo técnico, en este caso, del uso de la red de comunicaciones de la UAM.

La UAM ofrece a la comunidad universitaria y a instituciones vinculadas[1] el acceso a la red de comunicaciones de la universidad, a través de la cual se podrá acceder a sus distintos servicios y a Internet. La red de la UAM se conecta a Internet mediante un enlace con REDIMadrid[2], que a su vez está conectada con RedIRIS[3]. Por tanto, quienes hagan uso de la red de comunicaciones de la UAM tienen la obligación de cumplir la Política de Uso de ambas redes[4].

Las presentes normas han sido elaboradas por el Comité de Seguridad de la Información de la UAM y aprobadas por el Consejo de Gobierno de la UAM, estableciendo de esta forma las directrices generales para el uso adecuado de la red de comunicaciones de la UAM, así como las obligaciones que deben asumir quienes hagan uso de ella.

1. Objeto

El objeto de las presentes normas[5] es regular el acceso y uso de la red de comunicaciones de la UAM. Para un uso más eficiente y seguro de los Sistemas de Información de la UAM, es obligatorio el cumplimiento estricto de estas normas.
La red de comunicaciones es un servicio que la UAM proporciona como apoyo en la realización de las funciones asignadas a los diferentes colectivos de la comunidad universitaria, proporcionando acceso a todos los servicios ofrecidos en la red de la UAM y a Internet como herramienta para el mejor desempeño de estas funciones, en el ejercicio habitual de las actividades docentes y de investigación, así como en los procesos administrativos y de gestión y formación.
Dos son los principios generales que rigen estas normas:

- Definir el uso aceptable y no aceptable de la red de comunicaciones de la UAM para establecer un entorno seguro.

[1] Cualquier persona que pueda hacer uso de los recursos TIC de la UAM (Véase la definición en el apartado del "Ámbito de aplicación" de la Política de Seguridad de la Información de la UAM.)
[2] Red autonómica para la educación y la investigación de la Comunidad de Madrid. (http://www.redimadrid.es/)
[3] Red nacional para la educación y la investigación (http://www.rediris.es/)
[4] REDIMadrid https://www.redimadrid.es/files/Politica-de-uso-REDIMadrid-2019.pdf, RedIRIS https://www.rediris.es/rediris/instituciones/politica_de_uso.pdf y https://www.rediris.es/rediris/instituciones/acuerdo-afiliacion.pdf
[5] Las presentes normas se pueden encontrar en el apartado de "Normativa reguladora/Normativa de Seguridad de la Información" de la sede electrónica de la UAM (https://sede.uam.es/normativa)

- Respetar y proteger de una manera responsable, ética y legal los derechos de uso de los servicios para la comunidad universitaria.

2. Ámbito de aplicación

Estas normas y sus contenidos derivan de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la UAM. Las presentes normas serán de aplicación y de obligado cumplimiento tanto para quienes acceden directamente a la red de comunicaciones de la UAM como a quienes acceden a través de instituciones a las que la UAM proporciona el acceso a Internet.

Dichas instituciones podrán tener sus propias normas de uso de la red de comunicaciones dentro del contexto de los servicios que ofrecen. Estas normas deberán ser compatibles con las condiciones y términos expresados en el presente documento.

3. Infraestructura de red

La red institucional de comunicaciones de la UAM interconecta todos los edificios de los diferentes campus y otras sedes de la universidad. Además, proporciona el servicio de acceso a Internet a otras instituciones ubicadas en las diversas sedes de la universidad, de acuerdo con los convenios suscritos por la UAM con las mismas, y siempre cumpliendo con las condiciones que imponen las políticas de uso de las redes que nos conectan a Internet.

La Unidad de Tecnologías de la Información (en adelante TI) es la encargada de gestionar y mantener la infraestructura de red y el acceso a Internet de la UAM, así como de gestionar el espectro radioeléctrico utilizado por la red inalámbrica dentro de los edificios y espacios universitarios.

4. Acceso a la red

La red de comunicaciones de la UAM permite conectarse en función del medio disponible y de la ubicación de quienes hagan uso de ella.

Es competencia de TI organizar las redes, desde un punto de vista lógico, atendiendo a criterios de eficiencia, escalabilidad y seguridad.

Las solicitudes de ampliación de la red deben cursarse a través del Centro de Atención a Usuarios (en adelante CAU) de TI, indicando la ubicación donde se requiere el servicio.

Todos los equipos que se conecten a la red de comunicaciones deben estar configurados siguiendo las directrices definidas por TI.

Existen tres tipos de acceso a la de red que se detallan en los siguientes puntos.

4.1. Acceso mediante red cableada

La conexión a la red cableada es el método tradicional para acceder a la red de comunicaciones de la UAM, mediante la utilización de un cable conectado a una roseta. Estas rosetas ya se encuentran instaladas en muchas ubicaciones en previsión de futuras necesidades. Para utilizarlas, basta con que se solicite al CAU su activación.

Si la roseta no existe, o no hay roseta cercana disponible, es preciso desarrollar un proyecto de cableado. Esta solicitud será tramitada a través del contacto con el CAU.

El coste del proyecto deberá ser asumido por la persona solicitante con cargo a un departamento, proyecto de investigación, etc. En el caso de obra nueva, TI participará en el proyecto inicial de infraestructura de red. Cuando se trate de remodelaciones, será necesario contactar con TI para solicitar un presupuesto de la obra de cableado necesaria, que se presentará quien lo haya solicitado. Excepcionalmente, en el caso de solicitudes aisladas de puntos dispersos de hasta dos rosetas, el coste será asumido por TI. En todos los casos, TI se encargará de la gestión, supervisión y control de los trabajos de instalación de las infraestructuras de red.

Para optimización de los recursos, TI desactivará todas aquellas rosetas que hayan estado inactivas durante un periodo superior a un año.

Además de la roseta, se ha de asignar a cada equipo conectado una dirección IP que le permita la utilización de la red. Esta asignación puede ocurrir de dos formas:

1. Rosetas sin autenticación de usuaria o usuario:
    - Se asigna una IP al equipo mediante un registro inicial del equipo, y se configurará siguiendo las indicaciones técnicas de TI.
2. Rosetas con autenticación:
    - El equipo que vaya a ser conectado debe estar configurado para soportar el acceso autenticado a la red.
    - El usuario o usuaria debe proporcionar sus credenciales corporativas[6] y en caso de ser válidas, se asigna una IP asociada individual durante el tiempo que dure la conexión a la red cableada.

La forma de asignación más adecuada es la segunda, porque permite la configuración automática del equipo conectado.

4.2. Acceso inalámbrico (Wifi)

La red inalámbrica (en adelante WiFi[7]) complementa a la red cableada, añadiendo movilidad y permitiendo el acceso desde cualquier ubicación dentro del área de cobertura. No pretende ser nunca un sustituto a la red cableada, y no se debe utilizar para puestos de trabajo permanentes, pues no se puede garantizar la misma disponibilidad que ofrece la red cableada.

[6] https://www.uam.es/uam/tecnologias-informacion/servicios/id-uam-gestion-cuentas/
[7] https://www.uam.es/wifi

El acceso a la WiFi siempre será autenticado, mediante las credenciales corporativas de cada usuaria o usuario. No está permitido el uso de credenciales genéricas. Dado que la UAM pertenece a la iniciativa internacional eduroam[8], la conexión puede hacerse utilizando la misma configuración del equipo, tanto a la WiFi de la UAM como a las del resto de instituciones afiliadas.

Quienes no dispongan de credenciales pueden conectarse a la Wifi empleando la red inalámbrica para visitantes (UAM_Visitantes).

4.3. Acceso desde internet a servicios de la UAM

Sólo serán accesibles desde Internet aquellos servicios que sean considerados como públicos. Tendrán esta consideración, tanto los sistemas de información institucionales que ofrezcan información o servicios a la ciudadanía, como los servicios que por necesidades de las usuarias y usuarios de la UAM deban ser accesibles desde Internet.

Se considera servicio interno de la UAM aquel que sólo se ofrece a la propia comunidad universitaria.

Los y las usuarias de la UAM accederán desde Internet a los servicios internos de la UAM mediante el servicio de acceso remoto que se define en las “Normas para el acceso remoto a los servicios de información internos de la UAM”.

5. Uso de la red de comunicaciones

5.1. Uso aceptable

Por lo que respecta al uso de la red, se aplica lo dispuesto en la Normativa general de uso de recursos TIC y sistemas de información de la UAM (Acuerdo 5/CG 14-07-16).

5.2. Uso no aceptable

Además de lo dispuesto en la Normativa general de uso de recursos TIC y sistemas de información de la UAM, se consideran usos específicamente prohibidos de la red de comunicaciones, los siguientes:

- Interferir, dentro del campus de la UAM, los rangos de frecuencia que utiliza la red inalámbrica de la universidad y que causen un mal funcionamiento de ésta.
- Conectar a la red de comunicaciones cualquier equipamiento de red activo (hubs, switches, routers, firewalls, puntos de acceso inalámbricos, etc.), salvo expresa autorización de la dirección de TI.
- Alojar dominios en la red de la universidad distintos a los dominios corporativos de la UAM, salvo expresa autorización de la dirección de TI.
- Alojar los dominios corporativos de la UAM en redes ajenas a las de la propia universidad, salvo expresa autorización de la dirección de TI.

[8] https://www.eduroam.es y https://www.eduroam.org

6. Medidas de seguridad

6.1. Confidencialidad

En la actividad ordinaria del personal técnico de TI, los datos que circulan por la red de comunicaciones se tratarán de forma anónima y confidencial. Sin embargo, el acceso a estos datos podrá producirse en cualquiera de estos casos:

- Con autorización de quien haya generado la información, según se contempla en la legislación vigente.
- Cuando sea requerido por las autoridades judiciales.

6.2. Registro de actividad

Para garantizar el correcto funcionamiento de la red de comunicaciones de la universidad, así como el cumplimiento de estas normas, existen elementos de gestión, control y monitorización permanente del tráfico de la red institucional de la UAM y su conexión con Internet. Estas actuaciones se llevarán a cabo siguiendo lo dispuesto en el artículo 24 del Esquema Nacional de Seguridad. Se garantizará el derecho al honor, a la intimidad personal y familiar y a la propia imagen de las personas afectadas, y las normas sobre protección de datos de carácter personal, y de función pública o laboral, y demás disposiciones que resulten de aplicación.

TI podrá hacer uso de los datos registrados por estos elementos exclusivamente para el seguimiento y control del correcto funcionamiento de la red y de su rendimiento, así como para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa, tal como dispone el Esquema Nacional de Seguridad.

6.3. Detección de ataques y código dañino

En cumplimiento del artículo 24 del Esquema Nacional de Seguridad y al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones Públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, TI podrá, en la medida estrictamente necesaria y proporcional, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

La red de la universidad cuenta con elementos de seguridad cuyo objetivo es proteger, tanto a la red en sí misma como a los diferentes recursos TIC conectados, de los riesgos y amenazas que supone estar conectado a Internet. Estos elementos de seguridad son, por ejemplo, sistemas de cortafuegos, sistema de detección de intrusiones, soluciones de detección de código dañino, etc.

7. Responsabilidades e incumplimientos

Todas las personas que accedan a la red tienen la obligación de colaborar con TI para el uso correcto de la red de comunicaciones de la UAM siguiendo en todo momento las indicaciones que se les trasladen desde TI.

Quienes ignoren o infrinjan las presentes normas, podrán sufrir las actuaciones técnicas que se estimen oportunas de manera que se minimicen lo antes posible los efectos de la incidencia. Estas actuaciones técnicas serán: suspensión temporal del servicio por razones de emergencia y suspensión indefinida del servicio.

Todas estas medidas sólo se adoptarán, bajo criterios de necesidad, eficacia, proporcionalidad y transparencia, cuando se esté poniendo en riesgo el adecuado funcionamiento de la red de la universidad.

Constatado un incumplimiento de las obligaciones derivadas de estas normas, si procede, el Comité de Seguridad de la Información trasladará al Servicio de Inspección de la UAM el incumplimiento detectado a los efectos que correspondan.

7.1. Suspensión temporal del servicio

Procederá suspender temporalmente el servicio de acceso a la red de datos de la universidad cuando:

- se produzca un uso no aceptable de la red en los términos establecidos en el punto 5.2 de las presentes normas.
- se esté causando un mal funcionamiento de la red.

En cualquier caso, procederá la suspensión temporal del servicio cuando las consecuencias de las actuaciones derivadas de los incumplimientos anteriormente descritos puedan implicar a la UAM en algún tipo de responsabilidad.

La suspensión temporal cesará cuando se resuelva la causa que ha llevado a tomar esta medida.

7.2. Suspensión indefinida del servicio

Procederá la suspensión indefinida del servicio cuando de forma reiterada:

- se produzca un uso no aceptable de la red en los términos establecidos en el artículo 5.2 de las presentes normas.
- se esté causando un mal funcionamiento de la red.

En cualquier caso, se suspenderá el servicio de red cuando las consecuencias de las actuaciones derivadas de los incumplimientos anteriormente descritos puedan implicar a la UAM en algún tipo de responsabilidad.

Para restablecer el servicio, será necesario acreditar que se han adoptado las medidas indicadas por el o la Responsable de Seguridad a fin de garantizar un uso aceptable de la red.

8. Entrada en vigor

Las presentes normas técnicas, una vez aprobadas por el Consejo de Gobierno, entrarán en vigor al día siguiente de su publicación en el Boletín Oficial de la Universidad Autónoma de Madrid.