I.2.17. Acuerdo 17/CG de 13-05-22 por el que se aprueba la Normativa para el Acceso Remoto a los Servicios de Información Internos de la Universidad Autónoma de Madrid

NORMAS TÉCNICAS DE SEGURIDAD

NORMAS PARA EL ACCESO REMOTO A LOS SERVICIOS DE INFORMACIÓN INTERNOS 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 específicas de seguridad. 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 cuales les corresponde el desarrollo técnico, en este caso, del acceso remoto a los servicios de información internos de la UAM.

Los recursos TIC de la Universidad Autónoma de Madrid son, con frecuencia, fuente de riesgos y objeto de amenazas provenientes de Internet. Por tanto, y con el fin de proteger estos recursos, sólo son accesibles desde el exterior de la red de la UAM, aquellos servicios considerados como públicos.

Cuando la conexión a la red de la UAM[1] se realice desde el exterior, y con el fin de poder proporcionar todo acceso a los servicios y recursos TIC[2] internos de la UAM, tal como si se realizara físicamente a través de la conexión a la red interna, se proporciona el servicio de acceso remoto.
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 acceso remoto a los servicios de información internos de la UAM, así como las obligaciones que deben asumir quienes utilicen estos servicios.

1. Objeto

El objeto de las presentes normas[3] es definir el servicio de acceso remoto a la red de la UAM, cuando sea necesario conectarse a los servicios y recursos TIC internos de la UAM desde el exterior de la red de la UAM.

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

[1] Podrá realizar esta conexión toda persona que haga uso de los recursos TIC de la UAM (Véase la descripción de quiénes disfrutan de este derecho en el apartado del "Ámbito de aplicación" de la Política de Seguridad de la Información de la UAM).
[2] Tal y como se define en el apartado del "Ámbito de aplicación" de la Política de Seguridad de la Información de la UAM, los recursos TIC son "…todos los sistemas centrales y departamentales, estaciones de trabajo, ordenadores de puesto, impresoras y otros periféricos y dispositivos de salida, sistemas de localización, redes internas y externas, sistemas multiusuario y servicios de comunicaciones (transmisión telemática de voz, imagen, datos o documentos) y sistemas de almacenamiento que sean de su propiedad."
[3] 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)

obligado cumplimiento para quienes accedan a los servicios y recursos TIC internos de la UAM desde el exterior de la red de la UAM.

3. Servicio de acceso remoto

El servicio de acceso remoto permite acceder de forma autenticada y segura a los servicios y recursos TIC internos de la universidad, tal como si la conexión se realizara a través de la propia red de la universidad, independientemente de la ubicación desde la que se establezca. Para ello se establece una conexión segura mediante VPN[4], utilizando las credenciales corporativas para autenticarse y un factor de autenticación adicional (MFA)[5].

Se utiliza el factor de autenticación adicional (MFA) como complemento a la seguridad de las credenciales corporativas. Será posible elegir el factor adicional entre el conjunto facilitado por la Unidad de Tecnologías de la Información (en adelante TI) y que será un elemento diferente del usuario o usuaria y contraseña de las credenciales corporativas, como, por ejemplo, autenticación mediante aplicación en el móvil, código de un sólo uso, envío de SMS, etc.

Por lo que respecta al uso de la red, se aplica lo dispuesto en las Normas de uso de la red de comunicaciones de la UAM.

El Servicio de acceso remoto tiene las siguientes características y requisitos:

- Para utilizar el servicio, es necesaria la instalación previa de un software específico (cliente VPN) en el equipo desde el que se va a realizar la conexión.
- Puesto que el servicio requiere que se proporcionen las credenciales corporativas (identificador de usuaria o usuario y contraseña) para conectarse, no se debe utilizar desde ordenadores públicos o desde aquellos en los que no se confíe en su seguridad.
- A quienes tengan vinculación con empresas externas que, por motivos de servicio, necesiten utilizar el servicio de acceso remoto, se les suministrarán credenciales para el acceso al servicio.
- Cuando se utiliza el servicio de acceso remoto, el equipo se conecta virtualmente a la red de la universidad, por lo tanto:
    - serán de aplicación las políticas de acceso a Internet de la UAM y no las de la red a la que se encuentre físicamente conectado,
    - serán de aplicación las mismas condiciones de uso que si el equipo estuviera físicamente ubicado en la UAM[6]. En concreto, si se dejara el equipo informático desatendido, será necesario bloquear la sesión de usuario.

[4] Una red privada virtual (en inglés Virtual Private Network, VPN), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. https://es.wikipedia.org/wiki/Red_privada_virtual

[5] https://es.wikipedia.org/wiki/Autenticación_de_múltiples_factores

[6] Normativa general utilización recursos TIC y sistemas de información"

Ante cualquier incidencia con el servicio, será obligatorio comunicarlo al Centro de Atención a Usuarios (CAU) de TI.

4. Servicios según su accesibilidad

No requieren del uso del servicio de acceso remoto:

- Servicios públicos:

Se consideran servicios públicos, tanto los sistemas de información institucionales que ofrezcan información o servicios a la ciudadanía, como los que, por necesidades de la UAM y de quienes utilizan sus servicios de red, deban ser accesibles desde Internet.

La solicitud para que un servicio sea accesible desde Internet se realizará a través del CAU.
Requieren del uso del servicio de acceso remoto:

- Servicios y Recursos TIC internos:

La protección de estos servicios y recursos requiere que su acceso sólo sea posible desde la red de la universidad, y no desde cualquier otra parte de Internet (incluyendo la red de otra universidad o el acceso desde el propio domicilio).

Se distinguen dos tipos:

- Servicios internos:

Aquellas aplicaciones y servicios de red sólo disponibles para la comunidad universitaria (por ejemplo: sistemas de gestión, acceso a recursos del servicio de bibliotecas, portal del empleado, etc.).

- Recursos TIC internos:

Además de los servicios públicos e internos, existen otro tipo de recursos TIC conectados a la red de la universidad, a los que puede ser necesario acceder (por ejemplo: PCs de usuario, aparatos de medida y control de experimentos, servidores departamentales internos, etc.).

5. Responsabilidades e incumplimientos

Quienes utilicen estos servicios 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 consecuencias de las actuaciones técnicas que se estimen oportunas de manera que se minimicen lo antes posible los efectos de la incidencia.

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

6. 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.