BOLETÍN OFICIAL DE LA UNIVERSIDAD CARLOS III DE MADRID

uc3m | Universidad Carlos III de Madrid

**BOEL de 16 de marzo de 2026**

# Resolución de la Vicerrectora de Infraestructuras, Estrategia y Transformación Digital por la que se publica la Instrucción Técnica para acceso a servidores internos, aprobada por la Comisión de Seguridad de la Información en su sesión del día 7 de octubre de 2025.

**Preámbulo**

En cumplimiento de lo establecido por el Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo), en los apartados op.acc.5, op.acc.6, mp.com.2 y mp.com.3, así como mp.com.4 (Refuerzo 2), que hacen referencia al control de credenciales de acceso, y protección de la confidencialidad, así como a la segmentación lógica de la red. Se establece la siguiente instrucción técnica referente al despliegue de servidores que deben ser accedidos desde el exterior sin el empleo de conexión mediante Red Privada Virtual (VPN).

**Contexto**

Las organizaciones habitualmente establecen medidas de seguridad más restrictivas para aquellos accesos que se realizan desde el exterior de la red corporativa, exponiendo sólo aquellos servicios e información que debe ser pública. Por ello, los atacantes suelen dirigir sus esfuerzos a conseguir el acceso a sistemas menos vigilados, que al estar conectados a la red de datos interna, gozan de menores restricciones de seguridad para acceder a los sistemas críticos.

Es por ello que se hace necesario establecer unos criterios y requisitos que deben cumplir todos aquellos sistemas que puedan ser accesibles desde el exterior de la red corporativa sin requerir el establecimiento de la conexión mediante Red Privada Virtual (VPN).

**Ámbito de aplicación de la presente instrucción técnica**

Esta instrucción técnica aplica a aquellos sistemas TIC que tengan permitido el acceso desde fuera de la red corporativa sin necesidad de establecer la conexión VPN previamente.

**Requisitos para la autorización de acceso desde el exterior**

**Requisitos generales de configuración del sistema TIC**

1. Se creará un registro de autorizaciones gestionado por el Área de Seguridad del Servicio de Informática y Comunicaciones de la Universidad (SDIC).

2. En la solicitud de autorización, que se deberá dirigir al Área de Seguridad del SDIC, se incluirá información de contacto, indicando Nombre y Apellidos, dirección de correo electrónico, número de teléfono fijo y móvil, tanto del responsable de servicio como de los administradores. Cualquier cambio de responsable y/o administrador deberá ser notificado al Área de Seguridad a la mayor brevedad posible.

3. El responsable del sistema TIC deberá tener relación contractual con la universidad.

4. El sistema tendrá automatizada la instalación de las actualizaciones del sistema y del software base.

5. El sistema tendrá instalados aquellos componentes que establezca el Área de Seguridad con objeto de tener información sobre los procesos, usuarios y actividad del sistema para la detección temprana de posibles incidentes de seguridad.

6. Los logs de acceso se entregarán en tiempo real al SdIC para su supervisión y además se guardará copia de los mismos durante al menos 2 meses.

7. En caso de que se requiera autenticación de usuarios, el Área de Seguridad determinará los requisitos necesarios para implementar dicha acción.

8. Se podrá suspender el servicio en los siguientes casos:

a) Descubrimiento de alguna vulnerabilidad en el sistema que suponga un riesgo para la integridad de los sistemas de TIC de la UC3M.
b) Incumplimiento de los procedimientos de alta/autorización o baja de usuarios en el sistema.
c) Activación de mecanismos alternativos de acceso a recursos no autorizados.
d) Suspensión del envío de logs de acceso del servicio.
e) Utilización para acceso a recursos no autorizados.
f) No acreditación de los conocimientos necesarios para la administración del sistema.

g) Carencia de notificación de cambios en los titulares de los roles de administración y/o responsable.

9. En caso de suspensión del servicio será preceptivo informar al cargo institucional con responsabilidad sobre el sistema TIC corporativo, en el plazo máximo de 48 horas a partir del momento de la suspensión. También se informará, al responsable que designe el departamento afectado o en su defecto al director del mismo.

**Requisitos generales de los administradores del sistema TIC**

Los administradores de los sistemas TIC deberán cumplir los siguientes requisitos:

1. Deberán contar con relación contractual con la Universidad, preferiblemente de duración indefinida.

2. Tendrán conocimientos técnicos de seguridad y protección de la información del sistema administrado o experiencia acreditada en materia de seguridad de la información. El Área de Seguridad, establecerá con periodicidad anual, los requisitos mínimos admisibles para acreditar dichos conocimientos en las plataformas y sistemas más habituales.

**Requisitos específicos para servicios Web**

El Servicio de Informática y Comunicaciones ofrece la posibilidad de disponer de espacios Web en los que alojar la información correspondiente a servicios, departamentos y grupos de investigación, por lo que deberá emplearse este servicio si sólo se pretende publicitar la actividad corporativa.

En el caso de que se requiera la puesta en marcha de un servicio Web, como norma general el acceso a dichos servicios se realizará a través de un servicio de Web Application Firewall o proxy inverso corporativo.

Será decisión del Área de Seguridad permitir acceso directo a un servidor web interno desde el exterior.

**Requisitos específicos para servicios VPN, Escritorio Remoto y similares**

Este tipo de servidores permiten la ejecución de programas y el acceso a otros sistemas, por lo que además de los requisitos generales deberán cumplir los expuestos a continuación.

**Requisitos generales de configuración del sistema TIC**

1. Por defecto los usuarios de la UC3M deberán usar la VPN corporativa ofrecida por el Servicio de Informática y Comunicaciones.

2. Caso de que un departamento docente desee utilizar un servicio de vpn propio, este deberá cumplir los siguientes requisitos:

a) Deberá autenticar a los usuarios autorizados mediante un mecanismo de doble factor de autenticación.
b) Los usuarios autorizados deberán tener algún tipo de vínculo con la universidad: ser personal de la UC3M (docente o de administración), tener matrícula en vigor, disfrutar de algún tipo de beca de la UC3M o de programas internacionales.
c) Deberá existir un procedimiento escrito de altas y bajas de usuarios en el sistema, en el cual se contemplen explícitamente períodos de carencia la hora de dar de baja a usuarios. Superado este tiempo se anularán las credenciales del usuario que causa baja. Las carencias nunca podrán superar los 7 días naturales.
d) Esa VPN ofrecerá acceso sólo a los recursos del departamento que sean autorizados, para lo cual debe aceptar la existencia de mecanismos de control interpuestos entre su servidor VPN y los recursos a los que se quiera acceder.
e) Deberá existir algún mecanismo que compruebe la robustez de las credenciales de los usuarios del sistema.

**Formación requerida por los responsables y administradores**

La formación requerida por los responsables y los administradores, se recoge en un documento elaborado por el Área de Seguridad de la Información, disponible en https://docs.google.com/spreadsheets/d/1vq_j6HbqpB3QyHmu5HnD3XnsYFZrr0lqizDZDSBQo2I que será actualizado anualmente.

**Régimen transitorio**

Se establece un plazo de seis meses a partir de la entrada en vigor de la presente instrucción técnica para que aquellos sistemas que se encuentran accesibles se ajusten a la misma, presentando la correspondiente solicitud para su inscripción en el registro de autorizaciones.

**Entrada en vigor**

La presente instrucción técnica entrará en vigor al día siguiente de su publicación en el Boletín Electrónico de la Universidad Carlos III de Madrid.

En Getafe, a fecha de firma electrónica

Fdo. Beatriz López Boada

Vicerrectora de Infraestructuras, Estrategia y Transformación Digital