

I.2.7. Acuerdo 7/ CG 14-07-16 por el que se aprueba Normativa de gestión de accesos físicos a las áreas seguras TIC de la Universidad Autónoma de Madrid.

1 Introducción

La presente normativa establece las condiciones y acciones a realizar para la gestión del acceso físico a las áreas seguras TIC de la Universidad Autónoma de Madrid (en adelante UAM), estableciendo tanto el control de autorización como los protocolos de acceso para cada caso.

Las áreas seguras TIC son sectores concretos de las infraestructuras de la universidad que dan servicio a los sistemas de información de la UAM, y que exigen medidas específicas de seguridad. Por su especial criticidad, son espacios delimitados por barreras físicas y con acceso restringido a personas y equipamiento. Estas áreas incluyen tanto aquellas en las que se alojan los recursos TIC de la UAM (CPD's, Almacén, Racks de comunicaciones, salas...) como las infraestructuras eléctricas que les dan servicio.

2 Objetivo

El objeto del presente documento es la definición de la normativa aplicable a la Gestión de los accesos físicos a las áreas seguras TIC de la UAM, dentro del alcance señalado en el Esquema Nacional de Seguridad (ENS) en el ámbito de la administración electrónica. Esta normativa contempla las autorizaciones para los accesos físicos a dichas áreas.

3 Ámbito de aplicación

Esta normativa es de aplicación a todo el ámbito de actuación de la UAM, y sus contenidos derivan de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la UAM. Será de aplicación y de obligado cumplimiento para todas las personas que accedan a las áreas seguras TIC de la UAM.

La presente normativa ha sido elaborada por el Comité de Seguridad de la Información de la UAM y aprobada por su Consejo de Gobierno, estableciendo de esta forma las directrices generales para la gestión de accesos físicos a las áreas seguras TIC.

4 Normas Técnicas

4.1 Áreas Seguras TIC

Las áreas seguras TIC de la UAM son las siguientes:

- **Centro de Proceso de Datos (CPD) de Tecnologías de la Información:** Está ubicado en la planta baja de las dependencias de Tecnologías de la Información (en adelante TI) en el edificio Ada Lovelace de la Escuela Politécnica Superior. Su acceso estará restringido a:
 - Personal de TI responsable de algún equipo ubicado en el CPD.
 - Otro personal debidamente autorizado por el responsable de esta área segura TIC.
 - Personal ajeno a TI acompañado por alguna persona autorizada.

En esta área segura, por su especial criticidad, no se alojará ningún equipamiento ajeno a TI.

- **Área de alojamiento de copias respaldo de los Sistema de Información de la UAM:** La universidad dispone de copias de respaldo distribuidas en diferentes ubicaciones. Su acceso estará restringido a:
 - Personal de TI responsable de los sistemas de copia de respaldo de TI.
 - Otro personal debidamente autorizado por el responsable de esta área segura TIC.
 - Personal ajeno a TI acompañado por alguna persona autorizada.
- **Racks y cuartos de comunicaciones:** Están distribuidos por todos los edificios de los diferentes campus y ubicaciones de la UAM. Serán manipulados exclusivamente por el personal de TI, o por el personal ajeno debidamente autorizado por el responsable de esta área segura. Estas instalaciones no contendrán ningún tipo de electrónica ni equipamiento no dedicado a este fin salvo expresa autorización por TI. También están sujetos a las mismas restricciones de manipulación los Puntos de Acceso (APs) que dan servicio a la red inalámbrica corporativa y las rosetas y cableado de la red de comunicaciones de la universidad.
- **Almacenes de Tecnologías de la Información:** TI dispone de algunos espacios en el campus donde se almacena diverso material. Su acceso estará restringido a parte del personal de TI, o al personal ajeno debidamente autorizado por el responsable de esta área segura.
- **Despachos de Tecnologías de la Información:** Debido a la información sensible presente en estos despachos y a los accesos privilegiados a los sistemas de información, el acceso a estas instalaciones está restringido al personal de TI, o al personal ajeno debidamente autorizado por el responsable de esta área segura.
- **Infraestructura eléctrica que da servicio a los sistemas de información de la UAM:** Está distribuida por todos los edificios de los diferentes campus y ubicaciones de la UAM. Será exclusivamente manipulada por el personal del Servicio de Mantenimiento, o por el personal ajeno debidamente autorizado por el responsable de esta área segura.

4.2 Responsable de área segura TIC

El responsable del área segura TIC será la persona encargada de autorizar los accesos al área segura TIC de su competencia.

Los responsables de cada área segura se definen en el Anexo I.

Sus responsabilidades son:

- Autorizar el acceso al área segura TIC bajo su responsabilidad.
- Delegar la autorización de acceso al área segura TIC bajo su responsabilidad.

4.3 Autorización de acceso a las áreas seguras TIC

El acceso a las áreas seguras TIC de la UAM sólo debe ser realizado por personal debidamente autorizado para garantizar en todo momento la disponibilidad e integridad de los sistemas de información de la UAM.

El responsable de cada una de las áreas seguras TIC definidas en el Anexo I, será el encargado de autorizar o delegar la autorización de acceso físico a las mismas, tal y como se establece en los procedimientos de gestión de accesos físicos a dichas áreas.

5 Responsabilidades e incumplimientos

Todos los usuarios tienen la obligación de colaborar con TI para corregir, cesar y, en su caso, rectificar el ejercicio de acciones que incumplan esta normativa.

Aquellas personas que de forma reiterada, deliberada o por negligencia ignoren o infrinjan la presente normativa, podrán verse sujetas a las actuaciones técnicas (para minimizar los efectos de la incidencia) que se estimen oportunas.

Constatado un incumplimiento de las obligaciones derivadas de esta normativa, el Comité de Seguridad de la Información podrá instar la depuración de las responsabilidades disciplinarias a las que hubiera lugar.

El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de estudiantes, del personal al servicio de las Administraciones Públicas o de la propia UAM.

6 Disposición final

En el presente documento se utiliza el masculino gramatical como genérico, según los usos lingüísticos, para referirse a personas de ambos sexos.

Anexo I: Áreas seguras TIC

Área segura TIC	Tipo	Responsable	Procedimiento	Ubicación
Centro de Proceso de Datos (CPD) de TI	CPD	Jefe de Unidad Técnica de Infraestructura de Equipos Centrales de TI.	Procedimiento de gestión de acceso físico al CPD de TI.	Planta baja de las dependencias de TI en el edificio Ada Lovelace de la Escuela Politécnica Superior.
Áreas de alojamiento de copias respaldo de los Sistema de Información de la UAM	CPD	Jefe de Unidad Técnica de Infraestructura de Equipos Centrales de TI.	Procedimiento de gestión de acceso físico a las áreas de alojamiento de copias respaldo	Diversas ubicaciones en la universidad.
Racks y cuartos de comunicaciones	Cuarto técnico	Jefe de Unidad Técnica de Comunicaciones de TI.	Procedimiento de gestión de acceso físico a los Racks y cuartos de comunicaciones.	Distribuidos por todos los edificios de los diferentes campus y ubicaciones de la UAM.
Almacenes de TI	Almacén	Dirección de TI.	Procedimiento de gestión de acceso físico a los Almacenes de TI	Espacios distribuidos por el campus donde TI almacena diverso material.
Despachos de TI	Zona de trabajo	Dirección de TI.	Procedimiento de gestión de acceso físico a los Despachos de TI	Dependencias de TI en la universidad.
Infraestructura eléctrica que da servicio a los sistemas de información de la UAM	Cuadros eléctricos	Dirección de infraestructuras	No existe	Distribuida por todos los edificios de los diferentes campus y ubicaciones de la UAM.