



REGLAMENTO 3/2026, DE 29 DE JUNIO, DE LA UNIVERSIDAD DE MÁLAGA, PARA LA GESTIÓN, ALOJAMIENTO Y SUPERVISIÓN DE SERVIDORES EN LA UNIVERSIDAD

PREÁMBULO

La Universidad de Málaga promueve el uso de las tecnologías emergentes, respeta la privacidad de los usuarios y asume como principio que la comunidad universitaria hace un uso eficaz, ético y legal de los recursos que la institución pone a su disposición. Ahora bien, el acceso a estas tecnologías requiere un correcto uso de las mismas por todos los miembros de la comunidad universitaria y constituye, además un derecho y un deber, tal y como señala el artículo 81 de los Estatutos de la Universidad de Málaga, aprobados por Decreto 464/2019, de 14 de mayo.

De la misma forma, la Ley 3/2022, de 24 de febrero, de Convivencia Universitaria, prescribe en las letras e) y f) del artículo 3.2 que las Normas de Convivencia de las universidades públicas promoverán la utilización y conservación de los bienes y recursos de la universidad de acuerdo con su función de servicio público y el respeto de los espacios comunes, incluidos los de naturaleza digital.

Los recursos que sustentan estas TIC forman parte del patrimonio de la Universidad de Málaga y, por tanto, quedan afectos al deber de protección del mismo por parte de los órganos de gobierno y de todos los miembros de la comunidad universitaria de conformidad con lo establecido en el Capítulo Primero del Título Quinto de los citados Estatutos de la Universidad de Málaga.

La Universidad de Málaga, como se indica en el Reglamento 13/2023 de 21 de noviembre, por el que se regula el uso de los recursos TIC, promueve el uso de estas tecnologías que facilitan tanto la gestión como la docencia y la investigación.

Tales recursos deben ser gestionados y protegidos para garantizar la seguridad de los datos, a distintos niveles, mediante medidas tanto técnicas como organizativas, como se recoge en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los

CSV (Código Seguro de Verificación)	IVVH3SXSZNGM3CN26A4EGVIHCY	Fecha	02/07/2026 12:32:03
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	Validez del documento	Original
Firmado por	UNIVERSIDAD DE MALAGA		
Dirección web de verificación	https://prod-gonce-verifirma.uma.es/verifirma/code/IVVH3SXSZNGM3CN26A4EGVIHCY	Página	1/10



Derechos Digitales o en el Real Decreto 203/2021, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

En esta línea, el Reglamento 12/2024, de 21 de noviembre, por el que se regula la política de seguridad de la información de la Universidad de Málaga, recoge en su artículo 3 las directrices fundamentales de protección y seguridad que garanticen el cumplimiento básico en materia de seguridad de la información.

En la Universidad de Málaga coexisten numerosos servidores gestionados por unidades, departamentos, grupos de investigación y otros colectivos. Algunos se alojan en el centro de proceso de datos (CPD) del Servicio Central de Informática (SCI) o en otras dependencias de la Universidad, y otros fuera de ella, a veces administrados por personal propio o por terceros.

Esta diversidad, necesaria para la actividad académica e investigadora, implica riesgos de seguridad y protección de datos. Estos riesgos pueden tener procedencia variada y,

para salvaguardar la integridad de los servidores, así como su uso correcto atendiendo a su finalidad, todo ello de conformidad con las normas aplicables, se hace necesario arbitrar normas que detecten, señalen y corrijan las posibles actuaciones o usos irregulares. La competencia para la supervisión y control de estas normas se encomienda al Servicio Central de Informática como servicio especializado en la materia. Asimismo, aunque las medidas correctoras en caso de incumplimiento que se han previsto en el presente reglamento no tienen carácter sancionador –sin perjuicio de la ulterior responsabilidad disciplinaria si se diera ésta– se hace conveniente establecer unas líneas procedimentales para la materialización de dichas medidas.

Por todo lo expuesto, con el fin de garantizar la seguridad, la trazabilidad, la protección de datos y la coherencia institucional, y bajo el amparo de las potestades que establecen los artículos 3 y 46 de la Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario; los artículos 6 y 89 de la Ley 1/2026, de 20 de febrero, Universitaria para Andalucía y 14 de los Estatutos de la Universidad de Málaga, se dicta el presente reglamento aprobado en el Consejo de Gobierno en su sesión celebrada el día 29 de junio de 2026.

CSV (Código Seguro de Verificación)	IVVH3SXSZNGM3CN26A4EGVIHCY	Fecha	02/07/2026 12:32:03
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	Validez del documento	Original
Firmado por	UNIVERSIDAD DE MÁLAGA		
Dirección web de verificación	https://prod-gonce-verifirma.uma.es/verifirma/code/IVVH3SXSZNGM3CN26A4EGVIHCY	Página	2/10





TÍTULO I DISPOSICIONES GENERALES

Artículo 1. Objeto

El presente Reglamento tiene por objeto regular la gestión, administración, alojamiento, registro y supervisión de los servidores pertenecientes o vinculados a la Universidad de Málaga, asegurando su adecuación a las políticas institucionales de seguridad, protección de datos y buen uso de los recursos tecnológicos.

Artículo 2. Ámbito de aplicación

1. Este Reglamento será de aplicación a todas las unidades, departamentos, grupos de investigación, servicios, proyectos y cualesquiera otras estructuras vinculadas a la Universidad de Málaga, y sus miembros.
2. Y, en particular, será de aplicación a todos los servidores que:
 - a) se encuentren virtualizados o alojados en el CPD del Servicio Central de Informática,
 - b) estén virtualizados o alojados en instalaciones externas o por terceros y utilicen dominios, subdominios o recursos de red institucionales, con independencia de su ubicación física.

Artículo 3. Definiciones

A efectos del presente Reglamento, se adoptan las siguientes definiciones:

1. Servidor. Cualquier sistema informático, físico o virtual, que utilice un subdominio de la UMA, destinado a ofrecer servicios, aplicaciones, almacenamiento, procesamiento de información o cualquier tipo de recurso accesible por otros usuarios o sistemas a través de la red universitaria o de Internet.

CSV (Código Seguro de Verificación)	IVVH3SXSZNGM3CN26A4EGVIHCY	Fecha	02/07/2026 12:32:03
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	Validez del documento	Original
Firmado por	UNIVERSIDAD DE MALAGA		
Dirección web de verificación	https://prod-gonce-verifirma.uma.es/verifirma/code/IVVH3SXSZNGM3CN26A4EGVIHCY	Página	3/10





2. Servidor externo. Todo servidor cuyo alojamiento físico, virtual o en la nube se encuentre fuera de la infraestructura tecnológica de la Universidad.
3. Responsable administrativo del servidor. Es la persona perteneciente a la unidad, departamento, grupo de investigación o servicio universitario con autoridad sobre la actividad para la que se utiliza el servidor, que asume la responsabilidad institucional del sistema.

Sus funciones incluyen:

- a) Definir la finalidad y legitimidad del servidor.
 - b) Garantizar el cumplimiento del Reglamento, de la normativa de la Universidad y, en su caso, de la legislación sobre protección de datos.
 - c) Ser interlocutor oficial ante el SCI y ante otros órganos de la Universidad.
 - d) Asegurar la existencia de recursos humanos y materiales para su mantenimiento.
4. Responsable técnico del servidor. Es la persona encargada de su administración, mantenimiento y seguridad operativa. Sus funciones incluyen:
 - a) Configurar, actualizar y mantener el sistema.
 - b) Aplicar las medidas de seguridad requeridas por el SCI y por la normativa de protección de datos.
 - c) Resolver incidencias técnicas y coordinarse con el SCI cuando sea necesario.
 - d) Garantizar la continuidad del servicio y la correcta gestión de accesos.

El responsable técnico puede ser personal propio de la Universidad o un tercero autorizado, siempre bajo supervisión del responsable administrativo.

Artículo 4. Competencias y funciones

CSV (Código Seguro de Verificación)	IVVH3SXSZNGM3CN26A4EGVIHCY	Fecha	02/07/2026 12:32:03
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	Validez del documento	Original
Firmado por	UNIVERSIDAD DE MÁLAGA		
Dirección web de verificación	https://prod-gonce-verifirma.uma.es/verifirma/code/IVVH3SXSZNGM3CN26A4EGVIHCY	Página	4/10





1. La supervisión y control del cumplimiento de este Reglamento corresponde al SCI de la Universidad de Málaga.
2. Serán funciones del SCI:
 - a) Mantener un registro actualizado de servidores autorizados.
 - b) Publicar en su página web el formulario oficial de solicitud de alta y renovación de servidores.
 - c) Definir las políticas técnicas de seguridad, procedimientos de conexión y requisitos mínimos para servidores alojados en la red universitaria.
 - d) Realizar auditorías técnicas o de seguridad cuando lo considere necesario.
 - e) Adoptar medidas correctivas en caso de incumplimiento.

TÍTULO II PROCEDIMIENTOS

Artículo 5. Procedimiento de alta y renovación de datos de servidores

1. Toda unidad, grupo o servicio que desee alojar o mantener un servidor, tanto dentro como fuera del CPD, deberá solicitar su alta mediante el formulario disponible en la web del SCI. El formulario incluirá, al menos, la siguiente información
 - a) Identificación del responsable administrativo del servidor.
 - b) Identificación del responsable técnico.
 - c) Descripción de los objetivos, contenidos y finalidad del servidor.
 - d) Dominio propuesto.
 - e) Indicación sobre si existe tratamiento de datos personales y las medidas aplicadas al respecto.
 - f) Otros detalles de interés.

CSV (Código Seguro de Verificación)	IVVH3SXSZNGM3CN26A4EGVIHCY	Fecha	02/07/2026 12:32:03
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	Validez del documento	Original
Firmado por	UNIVERSIDAD DE MALAGA		
Dirección web de verificación	https://prod-gonce-verifirma.uma.es/verifirma/code/IVVH3SXSZNGM3CN26A4EGVIHCY	Página	5/10





2. El SCI realizará la revisión técnica y de seguridad de todas las solicitudes de alta de servidores, pudiendo requerir a la unidad solicitante las aclaraciones o modificaciones que considere necesarias para garantizar el cumplimiento de las políticas institucionales. En ningún caso se aceptarán solicitudes para alojamiento de páginas o contenidos personales.
3. Cuando el servidor esté alojado fuera de la Universidad, o cuando se detecte que la naturaleza, finalidad o contenido del servicio pudiera requerir una validación adicional, el SCI emitirá un informe preceptivo y vinculante y lo remitirá a la Secretaría General para su valoración y, en su caso, aprobación.
4. En caso de denegación, se comunicará a la unidad, grupo o servicio solicitante, quedando la solicitud sin efecto.
5. Cualquier cambio en los responsables administrativos o técnicos deberá ser comunicado al SCI. No se atenderán solicitudes de intervención o modificación que no procedan de los responsables declarados en el registro. La omisión de comunicación de los cambios reseñados en este apartado constituirá un incumplimiento con las posibles responsabilidades establecidas en el artículo 9 del presente Reglamento.
6. El registro tendrá validez anual. La renovación deberá realizarse cada año. La falta de renovación podrá conllevar la baja automática del servidor y su desconexión de la red universitaria.

Artículo 6. Alojamiento en el CPD de la Universidad de Málaga

1. El alojamiento en el CPD se realizará, como norma general, mediante el uso de los recursos de virtualización gestionados por el SCI, que constituyen la modalidad prioritaria y recomendada.
2. El SCI procederá a realizar copias de seguridad periódicas de los servidores virtualizados en base a sus recursos, garantizando al menos cuatro copias, durante el último mes, con periodicidad semanal.

CSV (Código Seguro de Verificación)	IVVH3SXSZNGM3CN26A4EGVIHCY	Fecha	02/07/2026 12:32:03
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	Validez del documento	Original
Firmado por	UNIVERSIDAD DE MÁLAGA		
Dirección web de verificación	https://prod-gonce-verifirma.uma.es/verifirma/code/IVVH3SXSZNGM3CN26A4EGVIHCY	Página	6/10





3. Dado que los recursos de computación del SCI son limitados, este podrá denegar solicitudes de máquinas virtuales cuyas necesidades de procesamiento (CPU y RAM) o almacenamiento se consideren desproporcionadas, inviables o incompatibles con la capacidad disponible.
4. Solo en casos excepcionales y debidamente justificados, el SCI podrá autorizar el alojamiento de servidores físicos pertenecientes a las unidades o grupos solicitantes. Para ello deberá acreditarse la imposibilidad técnica de utilizar los recursos virtualizados ofrecidos por el SCI.
5. En estos casos excepcionales:
 - a) El SCI evaluará la idoneidad técnica, energética y de seguridad del equipamiento.
 - b) El solicitante asumirá íntegramente la responsabilidad del mantenimiento, soporte y actualizaciones del equipo.
 - c) Los accesos físicos al servidor serán los mínimos imprescindibles, deberán realizarse previo acuerdo con los responsables del CPD y únicamente dentro del horario laboral, salvo emergencia justificada.
 - d) El SCI podrá revocar la autorización si el equipo compromete la seguridad o el funcionamiento del CPD.

Artículo 7. Obligaciones de seguridad y protección de datos

1. Todos los servidores que empleen dominios institucionales tienen la obligación de asegurar la seguridad y protección de datos, y a tal fin deberán:
 - a) Mantenerse actualizados, protegidos y configurados conforme a las normas técnicas del SCI.
 - b) Disponer de copias de seguridad propias y controles de acceso adecuados.
 - c) Aplicar cifrado en comunicaciones y almacenamiento cuando sea necesario.

CSV (Código Seguro de Verificación)	IVVH3SXSZNGM3CN26A4EGVIHCY	Fecha	02/07/2026 12:32:03
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	Validez del documento	Original
Firmado por	UNIVERSIDAD DE MÁLAGA		
Dirección web de verificación	https://prod-gonce-verifirma.uma.es/verifirma/code/IVVH3SXSZNGM3CN26A4EGVIHCY	Página	7/10





- d) Designar responsables administrativo y técnico.
 - e) Permitir al personal del Servicio de Ciberseguridad realizar las actuaciones, verificaciones o pruebas que considere necesarias para garantizar los mínimos de seguridad.
 - f) En caso de tratamiento de datos personales, cumplir estrictamente la normativa aplicable y quedar sometidos a la supervisión del Delegado de Protección de Datos (DPO).
 - g) Ningún servidor podrá alojar contenidos bajo un dominio distinto a uma.es, salvo en casos excepcionales debidamente solicitados, justificados y autorizados expresamente por la Universidad de Málaga a través de la Secretaría General.
2. El incumplimiento de cualquiera de las obligaciones establecidas en el apartado anterior podrá conllevar la aplicación de las medidas establecidas en el artículo 9.

TÍTULO III

RÉGIMEN DE USOS Y MEDIDAS CORRECTORAS

Artículo 8 Usos prohibidos y limitaciones

1. La infraestructura de red y los servidores vinculados a la Universidad de Málaga se destinarán únicamente a fines académicos, investigadores o de gestión administrativa, conforme a las normas de uso de las redes académicas CICA y RedIRIS.
2. Queda expresamente prohibido el uso de servidores para la realización de actividades comerciales, empresariales o económicas de cualquier índole. Esto incluye, de forma no taxativa, la realización de transacciones financieras, la venta de servicios, la inclusión de publicidad con ánimo de lucro o la monetización de contenidos.
3. No se autorizará, en ningún caso, el alojamiento de páginas, servicios o contenidos de carácter estrictamente personal.

CSV (Código Seguro de Verificación)	IVVH3SXSZNGM3CN26A4EGVIHCY	Fecha	02/07/2026 12:32:03
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	Validez del documento	Original
Firmado por	UNIVERSIDAD DE MALAGA		
Dirección web de verificación	https://prod-gonce-verifirma.uma.es/verifirma/code/IVVH3SXSZNGM3CN26A4EGVIHCY	Página	8/10





Artículo 9. Medidas correctoras y de restablecimiento de la legalidad

1. El incumplimiento de las obligaciones dispuestas en este Reglamento podrá conllevar la adopción, por parte de la Universidad de Málaga, a través del SCI, de las siguientes medidas según la naturaleza del incumplimiento:
 - a) La ausencia de renovación anual de los datos del servidor dará lugar a su baja automática del registro y a su desconexión de la red universitaria.
 - b) En los casos en que un servidor comprometa la seguridad, la integridad o el correcto funcionamiento de la red institucional, se podrá revocar su autorización y proceder a su desconexión inmediata.
 - c) La detección de actividades comerciales conllevará:
 1. La suspensión del acceso del servidor a la red universitaria.
 2. La retirada del dominio institucional asignado.
 - d) En casos de incumplimientos que no comprometan de forma grave la seguridad, el SCI podrá emitir un requerimiento de corrección otorgando un plazo determinado al responsable técnico y administrativo. El incumplimiento de este requerimiento facultará al SCI para la suspensión del servicio.
 - e) En cualquier supuesto de incumplimiento que afecte al tratamiento de datos de carácter personal, se realizará una notificación al Delegado de Protección de Datos (DPO) para que supervise las actuaciones correspondientes.
2. Las medidas previstas en el apartado anterior no tendrán carácter sancionador o disciplinario, sin perjuicio de que las infracciones cometidas, por su naturaleza y tipificación, puedan ser susceptibles, asimismo, de responsabilidad disciplinaria en cuyo caso se derivará al órgano competente.

Artículo 10. Procedimiento para la adopción de medidas correctoras

CSV (Código Seguro de Verificación)	IVVH3SXSZNGM3CN26A4EGVIHCY	Fecha	02/07/2026 12:32:03
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	Validez del documento	Original
Firmado por	UNIVERSIDAD DE MALAGA		
Dirección web de verificación	https://prod-gonce-verifirma.uma.es/verifirma/code/IVVH3SXSZNGM3CN26A4EGVIHCY	Página	9/10





1. En el momento en que, por cualquier medio, el SCI detecte el incumplimiento de cualquier obligación, uso prohibido, limitación o cualquier acción u omisión recogidas en la normativa general, en el presente reglamento o en las disposiciones dictadas en desarrollo del mismo, lo pondrá en conocimiento de quien haya incurrido en las mismas.
2. En los supuestos descritos en los apartados a), b) y c) del apartado 1 del artículo anterior, se adoptarán las medidas concretas y se comunicará la causa por la que se han adoptado. Sin perjuicio del mantenimiento de las medidas, se otorgará un plazo de diez días para que se puedan presentar alegaciones al respecto.
3. En los supuestos descritos en los apartados d) del apartado 1 del artículo anterior se emitirá el requerimiento pertinente otorgándose un plazo no superior a diez días para la corrección.
4. En los supuestos descritos en el apartado e) del apartado 1 del artículo anterior se remitirá el asunto al DPO para que, de conformidad con sus plazos y procedimientos, determine las medidas a adoptar.

Disposición transitoria

Aquellas las unidades, departamentos, grupos de investigación, servicios, proyectos y cualesquiera otras estructuras vinculadas a la Universidad de Málaga y sus miembros que, a la fecha de entrada en vigor del presente reglamento estuvieran haciendo usos de los servidores incluidos en su ámbito de aplicación, dispondrán de un plazo no superior a un mes para solicitar la renovación de la autorización de conformidad con el artículo 5.

Disposición final

El presente Reglamento entrará en vigor al día siguiente a su publicación en el Boletín Oficial de la Universidad de Málaga y será de aplicación inmediata a todos los servidores existentes y futuros.

CSV (Código Seguro de Verificación)	IVVH3SXSZNGM3CN26A4EGVIHCY	Fecha	02/07/2026 12:32:03
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	Validez del documento	Original
Firmado por	UNIVERSIDAD DE MÁLAGA		
Dirección web de verificación	https://prod-gonce-verifirma.uma.es/verifirma/code/IVVH3SXSZNGM3CN26A4EGVIHCY	Página	10/10

