



UNIVERSIDAD
DE MÁLAGA

REGLAMENTO 13/2023, DE 21 DE NOVIEMBRE, POR EL QUE SE REGULA EL USO DE LOS RECURSOS TIC DE LA UNIVERSIDAD DE MÁLAGA

PREÁMBULO

Las Tecnologías de la Información y la Comunicación (en adelante, TIC) proveen recursos y servicios que facilitan tanto la gestión, como la docencia y la investigación, abarcando un área muy extensa de la actividad universitaria.

La Universidad de Málaga promueve y estimula el uso de estas tecnologías, 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 compromiso de un correcto uso de las mismas por todos los miembros de la comunidad universitaria y constituye, además de un derecho, 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. Este deber se concreta, además, dentro de los valores y principios generales del Código Ético de la Universidad de Málaga prescribiendo, expresamente que se propugna la sostenibilidad y la utilización adecuada y responsable de los medios y los recursos.

Asimismo, 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 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales, y Garantía de los Derechos Digitales, establece que los responsables del tratamiento de datos deben implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales, incluyendo la protección contra el acceso no autorizado, la destrucción accidental o ilícita, la pérdida, la alteración y la divulgación indebida de los datos. Estas medidas de seguridad implican, entre otras cosas, la protección de los sistemas informáticos en los que se almacenan o procesan los datos personales.



UNIVERSIDAD
DE MÁLAGA

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, regula el uso de medios electrónicos para la tramitación de los procedimientos administrativos, y establece la obligatoriedad de garantizar la seguridad de los sistemas, comunicaciones y documentos electrónicos. Y el Esquema Nacional de Seguridad (ENS), en su artículo 6, establece que la seguridad debe entenderse como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información.

Por todo ello, son objetivos de la presente normativa:

1. Garantizar la seguridad, rendimiento y privacidad de los sistemas y comunicaciones de la Universidad de Málaga, sin perjuicio de la actividad docente e investigadora.
2. Concienciar a las personas usuarias de la necesidad de hacer un uso correcto de los recursos, y colaborar para que estos sirvan eficazmente a los fines propios de la Universidad.
3. Evitar situaciones que puedan causar a la Universidad de Málaga algún tipo de responsabilidad de naturaleza civil, administrativa o penal.
4. Proteger el prestigio y la imagen de la Universidad de Málaga.

Por último, esta norma desarrolla lo previsto en el Reglamento por el que se regula la Política de Seguridad de la Información de la Universidad de Málaga, que prevé el desarrollo de determinadas cuestiones específicas de la misma, siendo uno de los aspectos más importantes de la gestión de la información corporativa, la persona usuaria final del sistema.

De acuerdo con todo lo cual, el Consejo de Gobierno de la Universidad de Málaga, a propuesta del Equipo de Dirección, en sesión celebrada el día 21 de noviembre de 2024, aprueba el presente Reglamento.

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto y ámbito de aplicación.



UNIVERSIDAD
DE MÁLAGA

1. El presente Reglamento tiene por objeto regular el uso adecuado de los recursos y servicios TIC de la Universidad de Málaga, con el fin de garantizar que los mismos sean utilizados para el desarrollo de las funciones y competencias propias de la misma, conforme a la normativa general vigente, a la vez que proteger estos recursos frente a amenazas deliberadas o accidentales de cualquier procedencia. Esta normativa debe ser compatible con el adecuado desarrollo de las funciones de gestión docente e investigadora en la Universidad, para cuyo desempeño se requiere la utilización de recursos TIC.

2. El presente Reglamento se aplica a toda la comunidad universitaria, así como a todas aquellas personas que hacen uso de los recursos TIC proporcionados por la Universidad de Málaga, o que disponen de sistemas o redes conectadas directa o indirectamente a la red de datos de la Universidad de Málaga.

3. Esta normativa se aplica a todos los sistemas centrales, sistemas departamentales, servidores, PC, impresoras, redes internas y externas, sistemas multiusuario, servicios de comunicaciones, y demás recursos tecnológicos que sean propiedad de la Universidad de Málaga y, en general, a cualquier dispositivo que esté conectado a la red de datos de la citada Universidad.

TÍTULO II

RECURSOS TIC

Capítulo I

El Servicio Central de Informática de la UMA

Artículo 2. Objetivos.

La Universidad de Málaga dispone de un Servicio Central de Informática (SCI) que tiene como objetivo sustentar tecnológicamente la implantación y el desarrollo de las TIC en la Universidad, apoyando a la gestión, la docencia y la investigación mediante la innovación, planificación, coordinación, desarrollo y gestión de los recursos de comunicación e informáticos de carácter general que soportan técnicamente estas tareas.

Artículo 3. Recursos y servicios.



Forman parte del SCI:

- a) Todas las infraestructuras de comunicaciones de carácter general: fibra óptica, cableado estructurado, paneles de conexión, armarios de comunicaciones, electrónica de comunicaciones, etc.
- b) Las dependencias que albergan las infraestructuras de comunicaciones, con independencia del lugar donde se encuentren ubicadas, que serán gestionadas por el SCI con el fin de garantizar la seguridad y los niveles de servicio.
- c) Los Centros de Procesos de Datos de la Universidad de Málaga.
- d) Los recursos informáticos de carácter general, especialmente aquellos destinados a la gestión y los servicios universitarios.
- e) Los servicios TIC de carácter general y especialmente aquellos que soportan la gestión universitaria, la docencia o la investigación.

Artículo 4. Personal.

Además de las infraestructuras y servicios informáticos y de comunicaciones, también forma parte del SCI el personal adscrito al área TIC, o denominación con la que se le identifique en la relación de puestos de trabajo de la Universidad de Málaga.

Artículo 5. Funciones.

Son funciones del SCI:

- a) La organización, gestión y mantenimiento de los recursos informáticos y de comunicaciones generales de la Universidad de Málaga.
- b) Prestar apoyo y asistencia a los órganos de gobierno, a las unidades y servicios, y a los miembros de la comunidad universitaria en la adquisición, instalación, soporte técnico, capacitación, orientación y mantenimiento de sistemas, aplicaciones, dispositivos y soportes informáticos, en los términos previstos en el presente Reglamento y las normas que lo desarrollan.
- c) Fomentar la innovación y la utilización de las tecnologías de la información mediante el desarrollo y la implantación de sistemas, servicios y recursos que faciliten la realización de las funciones que tiene encomendada la Universidad de Málaga.
- d) Facilitar las plataformas, servicios y tecnologías que apoyen la enseñanza y el aprendizaje.



- e) Supervisar los dispositivos y redes de comunicaciones con especial atención a la seguridad, la compatibilidad y la normativa técnica aplicable.
- f) Establecer las normas reguladoras de los servicios TIC ofrecidos por la Universidad de Málaga a sus colectivos.
- g) Priorizar el despliegue y soporte de servicios en función de las directrices establecidas por los órganos de gobierno de la Universidad de Málaga.
- h) Implementar y mantener medidas de protección, detección y respuesta ante amenazas o incidentes de ciberseguridad, colaborando activamente con las autoridades y organismos de protección de datos.

Artículo 6. Principios.

El SCI se regirá por los principios de responsabilidad, integridad, respeto, eficiencia, innovación y colaboración.

Artículo 7. Seguridad de los sistemas.

El SCI podrá, de acuerdo con la normativa y planes de seguridad, comprobar en cualquier momento los niveles de seguridad de los sistemas de comunicación instalados en la Universidad de Málaga o propiedad de la misma, así como los sistemas o dispositivos informáticos que los utilizan.

Artículo 8. Dirección.

El SCI estará dirigido por un Director o Directora y estructurado en los servicios que constituyen el Área TIC según la Relación de Puestos de Trabajo vigente en cada momento.

Artículo 9. Personas usuarias.

Se consideran personas usuarias del SCI de la Universidad de Málaga, todos los miembros de la comunidad universitaria y, en general, cuantas personas, estando interesadas en la utilización de estos servicios, reciban la correspondiente autorización.



Capítulo II

Equipamiento informático

Artículo 10. Uso del equipamiento informático.

1. Los dispositivos, programas, información y servicios informáticos que la Universidad de Málaga pone a disposición de las personas usuarias deben utilizarse para el desarrollo de las funciones profesionales, académicas o investigadoras propias de su actividad.

2. Las personas usuarias deben tener en cuenta como condición inexcusable para poder usar los equipamientos informáticos de la Universidad de Málaga que, por razones de mantenimiento y seguridad, así como por obligación legal derivada del artículo 24 del Esquema Nacional de Seguridad, los Sistemas de Información y la propia información que albergan, serán objeto de inventario y monitorización por la Universidad de Málaga, que guardará los correspondientes registros informáticos durante los plazos necesarios o legalmente establecidos.

3. Las personas usuarias:

- a) Evitarán comportamientos de riesgo para impedir el acceso y difusión de programas maliciosos en los equipos.
- b) Apagarán los equipos al finalizar la jornada laboral, tanto por seguridad como por eficiencia energética. Se establecerán excepciones sobre este punto en aquellos equipos que por labores de investigación o académicas no puedan ser apagados.
- c) Bloquearán la sesión, con contraseña, tras un periodo de inactividad del equipo.
- d) Facilitarán al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación, mantenimiento o seguridad.

Artículo 11. Administración e instalación de software en los servidores y equipos informáticos.

1. Es responsabilidad del SCI la instalación, administración y mantenimiento del equipamiento proporcionado por la Universidad de Málaga. Con el fin de evitar la entrada de programas maliciosos en los equipos informáticos, las personas usuarias no tendrán permisos de administración sobre los mismos. De manera excepcional, y por necesidades justificadas, se podrá solicitar la delegación de las capacidades de administración, lo que, de ser autorizada,



conllevará la aceptación, de forma explícita, de las responsabilidades que conlleva, garantizando en todo momento el cumplimiento de esta normativa. En el caso del equipamiento informático destinado al PDI para el desarrollo de su actividad, se entenderá justificada la necesidad de disponer del permiso de administración de sus equipos.

2. Los servidores adquiridos por departamentos, áreas o grupos de investigación deberán ser administrados por técnicos designados por estas unidades de forma explícita, notificando de forma oportuna tales designaciones al Responsable de Seguridad. Asimismo, deberán estar actualizados en cuanto a parches de seguridad, sistema operativo, y disponer de software antivirus y cortafuegos (firewall). Igualmente, se ubicarán en localizaciones físicas protegidas, salvo por causa justificada o acreditada por el responsable del activo.

3. Para los equipos que contengan información sensible, confidencial o protegida de la Universidad de Málaga, se establecerá por el Responsable de Seguridad su tipo de configuración y el nivel de acceso a redes internas y externas de forma que se garantice la seguridad de dicha conexión.

Artículo 12. Dispositivos portátiles.

Cuando algún miembro de la comunidad universitaria haga uso institucional de un dispositivo portátil, deberá tomar las siguientes precauciones:

- a) Vigilar adecuadamente el dispositivo portátil en los lugares públicos, con el objeto de evitar su robo.
- b) Abstenerse de almacenar información sensible, confidencial o protegida en los ordenadores u otros dispositivos portátiles, cuando no sea estrictamente necesaria para su desempeño profesional, así como eliminar periódicamente datos innecesarios.
- c) Nunca almacenar contraseñas en archivos de texto ni en los navegadores de internet.
- d) Tener actualizado y protegido convenientemente el equipo, conforme a las recomendaciones del Servicio Central de Informática.

Capítulo III Comunicaciones



Artículo 13. Uso de las comunicaciones.

1. El acceso a la red de datos de la Universidad de Málaga estará restringido a las personas a las que hace referencia el artículo 1 del presente Reglamento.
2. La red de datos de la Universidad de Málaga es para el uso exclusivo de las tareas que autorice la Universidad. Por ello, cuando así lo exija un requerimiento legal, por razones de emergencia o necesidad, la Universidad de Málaga podrá llevar a cabo actuaciones sobre la información que circula por la red de datos o los equipos donde se almacena, atendiendo siempre a los derechos y libertades de las personas usuarias, a las normativas de protección de datos de carácter personal y sin vulnerar el derecho al secreto de las comunicaciones.
3. Únicamente se permitirá la conexión a la red, tanto cableada como inalámbrica, a aquellos dispositivos que cumplan con los requisitos básicos de seguridad, salvo en las redes especialmente habilitadas para ello.
4. Se permite la conexión de dispositivos de propiedad particular a la red inalámbrica de la Universidad de Málaga, siempre que se cumpla este Reglamento y el resto de normativa que le afecte.
5. Por motivos técnicos y para garantizar la seguridad, se puede restringir o limitar la conexión de dispositivos particulares a la red.
6. El SCI es el único autorizado para acceder físicamente, administrar y manipular los sistemas de comunicaciones, el cableado, los puntos de acceso inalámbrico y cualquier otro equipamiento de la red de datos.
7. La instalación de cualquier dispositivo que modifique la topología de la red de datos (enrutadores, antenas wifi, etc.), requerirá la autorización expresa del SCI. Así mismo, queda prohibido el uso de direccionamiento IP que no haya sido asignado específicamente.
8. Siempre que se detecte un riesgo para la integridad, seguridad, o disponibilidad de la red de datos o de los recursos y servicios TIC, previa información a la persona o personas afectadas y



siguiendo el protocolo que se establezca para ello, el personal técnico del SCI podrá acceder a los equipos del puesto de trabajo para realizar cuantas intervenciones sean necesarias.

9. La actuación del personal técnico del SCI se rige por los principios de profesionalidad, seguridad, secreto y pleno respeto de los derechos de las personas usuarias.

10. Será de aplicación a las personas usuarias de la red de datos, las políticas de uso de red establecidas por RedIRIS y RICA, debido a la pertenencia de la Universidad de Málaga a dichas redes.

Capítulo IV

Sistemas de Información

Artículo 14. Acceso a los sistemas de información.

1. La Universidad de Málaga reconoce expresamente la importancia de los sistemas de información que utiliza para su gestión, así como la necesidad de su protección, por constituir un activo estratégico y vital. Esta necesidad de protección está establecida en la legislación española, y se aplica en defensa de los intereses de todos y cada uno de los miembros de la comunidad universitaria y otros posibles afectados.

2. Se establecerán los medios necesarios y adecuados para la protección de datos, programas, equipos, instalaciones, documentación y otros soportes que contengan información.

3. Los datos gestionados por la Universidad de Málaga y tratados por cualquier sistema de información de ésta deben tener asignado un responsable, que será el encargado de conceder, alterar o anular la autorización de acceso a dichos datos por parte de las personas usuarias.

4. Los accesos a los sistemas de información de la Universidad de Málaga se realizarán mediante el identificador único recogido en el directorio corporativo (DUMA), de manera que aquellas operaciones realizadas por una persona serán imputadas al identificador utilizado, no



permitiéndose, por tanto, el acceso a los sistemas a través de usuarios genéricos. Las excepciones a esta norma deberán estar expresamente autorizadas.

5. Cada persona sólo podrá realizar las tareas y acceder a los datos necesarios que se requieran para cumplir su cometido, es decir, se considerará el principio del llamado "mínimo privilegio". Asimismo, usará los datos accedidos únicamente para las operaciones para las que fueron generados, sin destinarlos a otros fines o incurrir en actividades que puedan considerarse ilícitas o ilegales.

6. Se registrarán pistas de auditoría y seguimiento de actividad de los accesos. Estos rastros, en el caso de modificación de datos personales, incluyen la identificación de la persona usuaria, la fecha y hora del acceso y la operación realizada.

7. Para los equipos que contengan o tengan acceso a datos personales, se establecerá su tipo de configuración y el nivel de acceso a redes internas o externas de forma que se garantice la seguridad de dicha conexión.

8. Las empresas proveedoras con acceso a los sistemas de información, deberán cumplir con el presente Reglamento, así como con las indicaciones que se les haga por parte del SCI y, especialmente, con las contempladas para este tipo de accesos en la legislación vigente.

9. Las personas usuarias de los sistemas de información universitarios tienen el deber de guardar la confidencialidad debida respecto de toda la información que haya contenida en ellas. Este deber subsiste después de finalizar su relación con la Universidad de Málaga.

Artículo 15. Tratamiento de la información.

1. Cualquier tratamiento en los sistemas de información deberá ser conforme con la normativa vigente, especialmente con lo dispuesto en la normativa sobre Protección de Datos de Carácter Personal.



2. Sólo deberá salvaguardarse la información que se considere estrictamente necesaria, haciendo un uso razonable de la capacidad de almacenamiento disponible y siguiendo las instrucciones que sobre conservación de la información se dicten por la Universidad de Málaga.

3. No se almacenará información institucional en medios de almacenamiento ajenos a la Universidad de Málaga salvo que esté expresamente autorizado. Asimismo, se deberá evitar el uso de dispositivos extraíbles para almacenar información que contenga datos personales o información confidencial.

4. Los soportes de información que deban ser destruidos o vayan a ser reutilizados se procesarán de tal manera que no pueda revertirse la información contenida en ellos.

Artículo 16. Trabajo fuera de las instalaciones.

1. El trabajo fuera de las instalaciones de la Universidad de Málaga comprende tanto el teletrabajo, como el trabajo ocasional, usando, en ambos casos, dispositivos de computación y comunicación para conexiones remotas, ya sea desde el domicilio particular o desde congresos, alojamientos u otros.

2. El trabajo fuera de las instalaciones de la Universidad de Málaga conlleva el riesgo de trabajar en lugares desprotegidos, por lo que aumentan las vulnerabilidades y la probabilidad de materialización de las amenazas, lo que hace necesario adoptar medidas adicionales.

3. La conexión con los sistemas informáticos de la Universidad de Málaga deberá llevarse a cabo a través de los sistemas que la propia Universidad determine para garantizar la accesibilidad, agilidad, seguridad y confidencialidad de las comunicaciones.

4. El SCI establecerá las medidas y los procedimientos que, en materia de ciberseguridad, deberán seguir las conexiones remotas a cualquier equipamiento conectado a la red de datos de la Universidad de Málaga.

Capítulo V

Control de acceso a los recursos



Artículo 17. Identificación y autenticación.

1. La Universidad de Málaga proporciona a las personas usuarias una cuenta de acceso consistente en un identificador y una contraseña, a través de la cual puede utilizar los recursos TIC para los cuales han sido habilitados.

2. La finalización de la relación con la Universidad de Málaga comporta la cancelación del derecho de utilizar los recursos y servicios TIC suministrados. La Universidad de Málaga se reserva el derecho de poder ampliar el periodo de utilización de los recursos TIC a las personas usuarias una vez finalizada su vinculación con la institución, atendiendo a la disponibilidad de recursos y las características de la vinculación previa de la persona con la Universidad de Málaga.

3. La cuenta proporcionada por la Universidad de Málaga es personal e intransferible, e identifica a la persona inequívocamente. Su custodia es responsabilidad de la misma. Además, la Universidad de Málaga tiene que garantizar su inviolabilidad, de forma que sólo el titular pueda acceder a los recursos asociados a su cuenta, excepto en los casos y con las garantías en que el ordenamiento jurídico lo permita.

4. Cada persona es responsable de las acciones realizadas a través de su cuenta.

5. Cada persona es responsable de la confidencialidad de su contraseña. En caso de sospecha de que pueda ser conocida, se deberá proceder a cambiarla. Si además ha podido divulgarse de forma fraudulenta, deberá informar de forma inmediata a la Unidad de Ciberseguridad (ciberseguridad@uma.es).

6. El incumplimiento del deber de custodia de la cuenta supone una vulneración grave en la seguridad de los recursos TIC, pudiendo bloquearse de forma inmediata como medida cautelar.



Capítulo VI

Acceso físico a las instalaciones

Artículo 18. Acceso físico a las instalaciones.

1. Las ubicaciones que alberguen tecnologías de la información y las comunicaciones tienen el acceso restringido.
2. Las salas de proceso de datos (CPD) deberán disponer de un sistema informatizado de registro y control de acceso que permita el acceso únicamente al personal previamente autorizado y que registre, todas las entradas y salidas incluyendo horarios e identificación de personas.
3. Los cuartos técnicos y los armarios de comunicaciones permanecerán siempre cerrados bajo llave y accesibles únicamente por el personal autorizado.
4. Las salas y despachos donde se ubiquen ordenadores personales deberán permanecer cerradas cuando no haya nadie en ellas.
5. Cada persona responsable del acceso restringido a ubicaciones TIC velará, dentro de su ámbito, por el cumplimiento de la normativa y revisará su correcta implantación o cumplimiento.

Capítulo VII

Utilidades y servicios TIC

Artículo 19. Correo electrónico.

1. La Universidad de Málaga pone un buzón personal de correo electrónico a disposición de cada uno de sus miembros que sirve como medio de comunicación básico para apoyar la realización de las actividades universitarias.
2. El correo electrónico es de carácter personal. Terceras personas no pueden acceder a los contenidos de los mensajes sin el consentimiento expreso del usuario o mediante autorización de la autoridad competente.
3. No obstante, el personal técnico puede acceder a los registros de uso de una cuenta de correo electrónico cuando este acceso sea necesario para garantizar la seguridad, la disponibilidad, la integridad y el correcto funcionamiento de los recursos TIC.



4. El uso principal de las cuentas de correo electrónico proporcionadas por la Universidad de Málaga se tiene que relacionar con las finalidades de esta.
5. Se permite la utilización privada de la cuenta de correo electrónico, siempre que este uso sea proporcionado y no impida la realización de su finalidad principal.
6. Cada persona es responsable de las acciones realizadas a través de su cuenta de correo electrónico de la Universidad de Málaga.
7. Es ilegal y estará penalizada la falsificación de cabeceras del correo electrónico.
8. No está permitida la utilización de las cuentas de correo personales de la Universidad de Málaga para el envío de publicidad ni para el envío de correo a personas que han expresado su deseo de no recibirlo.
9. No puede enviarse mensajes a través de la estafeta de la Universidad de Málaga con direcciones de origen que no sea "uma.es".
10. En ningún caso se podrá utilizar el servicio de correo electrónico de forma que interfiera con el rendimiento del servicio o con las labores propias de los gestores del servicio. Este apartado engloba la prohibición explícita de prácticas englobadas en los tipos definidos de Abuso de Correo Electrónico (ACE).
11. Las personas usuarias deben ser conscientes de que la dirección de correo electrónico @uma.es informa de su relación con la institución universitaria a diferencia de las direcciones ofrecidas por cualquier proveedor de Internet.
12. Las direcciones de correo electrónico de contacto del personal de la Universidad de Málaga son públicas y, salvo excepciones justificadas, pueden ser difundidas en los directorios universitarios.
13. La Universidad de Málaga puede configurar el sistema de correo para que detecte de manera automática acciones que se puedan considerar SPAM, y bloquee preventivamente una cuenta. Para las personas que legítimamente requieran el envío masivo de correos, se pone a su disposición servicios específicos a este fin, como las listas de distribución de correo.

Artículo 20. Internet.

1. El acceso a Internet es un recurso centralizado que la Universidad de Málaga pone a disposición de las personas usuarias como herramienta necesaria para el acceso a contenidos y recursos y como apoyo al desempeño de su actividad.



2. La Universidad de Málaga velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad, como de los riesgos asociados a su uso.
3. El acceso a Internet para fines personales debe limitarse y, de ser absolutamente necesario, solo debe utilizarse un tiempo razonable, que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.
4. Deberá notificarse cualquier anomalía detectada en el uso de acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.
5. Por motivos de seguridad, el SCI mantendrá un listado de puertos autorizados. En caso de que alguna persona usuaria requiera otros puertos, deberá solicitarlo para su estudio y, en su caso, posible autorización.

Artículo 21. Recursos web bajo dominios titularidad de la Universidad de Málaga.

1. La Universidad de Málaga tiene asociado el dominio uma.es como dominio corporativo.
2. La Universidad de Málaga puede habilitar, para uso de la comunidad universitaria, espacios para la prestación de servicios consistentes en la creación de recursos web dentro de los dominios pertenecientes a la misma.
3. La creación de recursos web institucionales de carácter público la autoriza el Responsable de Información de la Universidad y su desarrollo deberá cumplir con los protocolos de actuación que se establezcan.
4. En la cesión de espacios web, la Universidad de Málaga actúa de buena fe y no garantiza ni es responsable, directamente o subsidiariamente, de cualquier reclamación que se pueda derivar de su calidad, fiabilidad o exactitud, ni de los contenidos presentes a los sitios web a que eventualmente puedan conducir los enlaces incluidos en los recursos web, lo que será responsabilidad exclusiva del cesionario del espacio.
5. Los recursos web bajo dominio de la Universidad de Málaga deberán respetar las guías, manuales, protocolos o reglamentos que se establezcan en cuanto a contenidos, estilo e identidad visual.
6. El alojamiento de dominios distintos a uma.es en ordenadores de la Universidad de Málaga necesitará de autorización expresa.

Artículo 22. Recursos web y servicios en nube que no son titularidad de la Universidad de Málaga.



1. Los miembros de la Universidad de Málaga que, para el desarrollo sus tareas en el ámbito universitario usen servicios externos, tienen la obligación de leer y comprender las condiciones legales de estos servicios, sabiendo en todo momento a qué se comprometen y qué responsabilidades tiene el prestador de servicios, y asegurándose que éstas se ajustan al ámbito normativo vigente. En cualquier caso, son los únicos responsables de su uso.
2. Se prohíbe alojar información confidencial o restringida propia de la Universidad de Málaga en servidores externos que no haya ofrecido la institución, en particular cuando se trate de datos de carácter personal contenidos en los sistemas de información.
3. La Universidad de Málaga no tiene control sobre los servicios externos a la institución. Por ello, no es responsable del acceso de terceros a la información ni de las incidencias, pérdidas o daños que se puedan producir en el uso de estas aplicaciones.

Artículo 23. Redes sociales.

1. Con el objetivo de compartir experiencias, conocimientos e información, la Universidad de Málaga está presente de diversas formas en las denominadas redes sociales en un intento de acercar sus actuaciones y competencias a la ciudadanía y a sus colectivos.
2. Ninguna persona que preste sus servicios en la Universidad de Málaga podrá darse de alta en ninguna red social, en nombre o en representación de la Universidad de Málaga, salvo autorización expresa de la misma.
3. Las cuentas de redes sociales se crearán desde correos electrónicos corporativos, delegándose la gestión de las mismas en las unidades organizativas designadas para cada una de ellas.
4. La información contenida en el perfil de la red social no deberá considerarse nunca como información oficial en relación con las funciones y competencias de la Universidad de Málaga en los términos que puedan estar reservados a las funciones de la sede electrónica, según dispone el artículo 38 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
5. La Universidad de Málaga velará en todo momento por preservar el buen uso del perfil y, por ello, se reserva el derecho a eliminar cualquier aportación que considere ilegal, irrespetuosa, discriminatoria, o que, de alguna forma, pueda ocasionar daños y perjuicios materiales o morales o vulnerar el Código Ético de la Universidad de Málaga.



Capítulo VIII

Seguridad y Auditoría

Artículo 24. Gestión de incidentes de seguridad.

1. Un ciberincidente es cualquier situación o eventualidad en la que pueda verse amenazada la información almacenada en un sistema informático, ya sea de manera intencionada, o como consecuencia de negligencias, desconocimientos o fallos. La Universidad de Málaga dispondrá de un procedimiento de registro o gestión de ciberincidentes que incluirá, al menos: roles, mecanismos de detección, de notificación, de clasificación, de registro, y de comunicación a las partes interesadas.

2. En caso de que cualquier miembro de la comunidad universitaria, tenga conocimiento de un incidente de seguridad, deberá comunicarlo a la Unidad de Ciberseguridad (ciberseguridad@uma.es) desde donde se reportará, en su caso, al responsable del sistema afectado por el incidente.

3. Se realizarán acciones de concienciación entre el personal de la Universidad de Málaga acerca de la normativa en materia de seguridad.

Artículo 25. Registros de acceso y auditoría.

1. La Universidad de Málaga, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

- a) Revisará periódicamente el estado de los equipos, el software instalado y los dispositivos y redes de comunicaciones de su responsabilidad.
- b) Monitorizará los accesos a la información contenida en sus sistemas.
- c) Auditará la seguridad de las credenciales y aplicaciones.
- d) Monitorizará los servicios de Internet, correo electrónico y otras herramientas de colaboración.

2. Para su verificación, los datos de conexión y tráfico se guardarán en un registro durante el tiempo que se establezca. En ningún caso esta retención de datos afectará al secreto de las comunicaciones.



TÍTULO III RESPONSABILIDADES Y CONDICIONES DE USO

Artículo 26. Compromisos de las personas usuarias.

1. El uso de los equipos y recursos informáticos se hará de acuerdo con las políticas establecidas en este Reglamento y en las directivas, procedimientos y normativa que lo desarrolle.
2. Las personas usuarias deberán cuidar los equipos informáticos que les sean facilitados. Con carácter general, no podrán alterarlos ni modificar sus configuraciones hardware ni software.
3. Queda prohibida expresamente la instalación de programas para los cuales la Universidad de Málaga no tenga licencia de uso, ni ejecutar o guardar archivos no confiables.
4. Las personas usuarias serán responsables de la información extraída fuera de la organización a través de dispositivos o mensajes.
5. Todas las personas usuarias de la red de datos de la Universidad de Málaga tendrán la obligación de cooperar:
 - a) En las tareas de mantenimiento del inventario de los recursos, en su disposición y uso.
 - b) En las tareas de diagnóstico, que faciliten la resolución de las incidencias técnicas que se puedan producir.

Artículo 27. Usos específicamente prohibidos.

En ningún caso, los recursos TIC se pueden usar para alguna de las finalidades siguientes:

- a) Incurrir en actividades ilícitas o ilegales de cualquier tipo y, particularmente, difundir contenidos de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo, que atenten contra los derechos humanos, o que actúen en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.
- b) Congestionar intencionadamente la red de la Universidad de Málaga o interferir en su funcionamiento.



- c) Realizar actividades que pongan en peligro la integridad o seguridad de la Información disponible en la red.
- d) Dañar los sistemas físicos y lógicos de la Universidad de Málaga, introducir o difundir en la red virus informáticos y realizar cualquier otro tipo de actividad que sea susceptible de provocar daños en la Universidad de Málaga, a sus miembros, proveedores o terceras personas.
- e) Facilitar el acceso a los recursos de red a personas no autorizadas.
- f) Proporcionar acceso externo desde la propia red de comunicaciones, mediante la instalación de dispositivos de acceso remoto, salvo autorización expresa.
- g) Realizar tratamientos de datos personales que no estén expresamente autorizados por la Universidad de Málaga.
- h) Extraer información sensible, confidencial o protegida fuera de la organización por cualquier medio, salvo que las funciones propias del puesto de trabajo lo requieran.
- i) Publicar o difundir datos, documentos y/o archivos que estén sujetos a derechos de propiedad intelectual o cualesquiera otros derechos o intereses legítimos, sin el consentimiento expreso de las personas afectadas y/o del titular de los derechos.
- j) Hacer uso de los recursos TIC con fines comerciales, excepto los casos que se hayan autorizado expresamente.
- k) Usar o manipular la imagen corporativa de la Universidad de Málaga para la publicación, la difusión o el almacenamiento de contenidos de carácter no institucional que puedan inducir a considerar la existencia de relación o apoyo de la Universidad de Málaga con los contenidos. Esta prohibición se extiende no solamente a los recursos TIC de la Universidad de Málaga, sino a cualquier entorno que permita esta utilización y en particular a recursos en Internet propiedad de terceros ajenos a la Universidad.

Artículo 28. Inobservancia de las normas.

1. En el supuesto de que una persona usuaria no observe alguno de los preceptos señalados en el presente Reglamento, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, de las responsabilidades legales correspondientes, se podrá acordar la suspensión del uso de los recursos informáticos asignados. En concreto:

- a) Cuando se hayan llevado a cabo actividades contrarias al ordenamiento jurídico.



- b) Cuando se incumpla este Reglamento o cualquier otra normativa aprobada por la Universidad de Málaga.
- c) Cuando haya un requerimiento judicial que determine la adopción de medidas cautelares o de protección de cualquier tipo.
- d) Cuando sea necesario para el mantenimiento y el correcto funcionamiento de los recursos de la Universidad de Málaga.
- e) Cuando sea necesario para garantizar la seguridad de los recursos y sistemas.

2. La Universidad de Málaga pondrá en conocimiento de la autoridad judicial, el Ministerio Fiscal o las Fuerzas y Cuerpos de Seguridad del Estado aquellas infracciones que pueden ser constitutivas de delito.

Artículo 29. Responsabilidad de la Universidad de Málaga.

1. La Universidad de Málaga no es responsable, ni directa ni subsidiariamente:

- a) De las opiniones expresadas por los miembros de la comunidad universitaria, ni de las expresiones manifestadas por estos, ni de los contenidos publicados a través de los recursos TIC ofertados.
- b) De la información que los usuarios transmiten a través de la red de datos de la Universidad de Málaga, salvo que ésta se haya generado o difundido en el marco de las gestiones administrativas y las comunicaciones institucionales.
- c) De la información almacenada o de los enlaces a contenidos mantenidos por los usuarios de los recursos TIC, siempre que no se tenga conocimiento efectivo que la actividad o la información es ilícita o que lesiona bienes o derechos de un tercero.

2. En todo caso, la Universidad de Málaga actúa de buena fe cuando pone al alcance de sus usuarios sus recursos TIC y no es responsable, directa o subsidiariamente, de cualquier reclamación que se pueda derivar de su calidad, fiabilidad o exactitud.

Disposición adicional

El Esquema Nacional de Seguridad impone un proceso de mejora continua que nos obliga a ir aplicando las medidas de seguridad que se vayan incorporando a la normativa nacional. Para



UNIVERSIDAD
DE MÁLAGA

ello, la Universidad de Málaga realizará las comunicaciones y campañas de información que sean necesarias para ir adaptándonos a esas mejoras de seguridad que se vayan incorporando.

Disposición derogatoria

Queda derogado el Reglamento de Seguridad de las Tecnologías de la Información de la Universidad de Málaga, aprobado en Consejo de Gobierno de 19 de julio de 2013, así como cualquier otra disposición de igual o inferior rango que se oponga a lo dispuesto en el presente Reglamento.

Disposición final.

El presente Reglamento entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de la Universidad de Málaga.