

# Índice de contenido

1. OBJETIVO.....	2
2. ÁMBITO DE APLICACIÓN.....	2
2.1 Personas y colectivos.....	2
2.2 Recursos de tecnologías de información y comunicaciones.....	3
3. ASPECTOS LEGALES.....	3
4. DEFINICIÓN DE TÉRMINOS Y RESPONSABILIDADES.....	3
4.1 ATICA.....	3
4.2 Responsabilidad sobre los recursos informáticos.....	4
4.2.1 Responsables administrativos.....	4
4.2.2 Responsable usuario final.....	4
5. ACCESO Y USO DE LOS SERVICIOS.....	5
5.1 Cuentas de acceso.....	5
5.1.1 Estados de las cuentas de acceso.....	6
5.1.2 Creación de cuentas de acceso.....	7
5.1.3 Cancelación de cuentas de acceso.....	8
5.2 Carné Inteligente.....	8
5.2 Uso de recursos y servicios.....	9
5.2.1 Equipos informáticos y sistemas operativos.....	9
5.2.2 Red corporativa de la UM (UnimurNet).....	9
5.2.3 Contraseñas o claves de acceso.....	9
5.2.4 Parámetros de uso de los servicios.....	9
5.2.5 Normativas particulares de servicios.....	9
5.3 Solicitud de nuevos desarrollos.....	10
6. CONDICIONES DE PRESTACIÓN DE SERVICIOS POR PARTE DE ATICA.....	10
6.1 Limitaciones de uso.....	10
6.2 Retención de información sobre el tráfico generado y el uso de los servicios.....	10
6.3 Compromiso de confidencialidad con relación a los servicios de la UM.....	11
6.4 Exención de responsabilidad en la administración, funcionamiento y uso de los servicios.....	11
6.5 Estadísticas de uso de los servicios.....	12
6.6 Copias de seguridad.....	12
6.7 Detección y eliminación de código malicioso.....	12
6.7.1 Responsabilidades asociadas a la propagación de virus.....	12
6.8 Gestión de incidencias.....	13
7. USOS INCORRECTOS DE LOS RECURSOS.....	13
7.1 Sobre la finalidad y naturaleza del uso.....	13
7.2 Sobre confidencialidad y suplantación de identidad.....	13
7.3 Sobre la integridad, y disponibilidad de los recursos.....	14
7.4 Sobre el uso de las infraestructuras.....	14
8. MEDIDAS A APLICAR.....	14
9. PUBLICIDAD Y ACTUALIZACIÓN.....	15
10. ANEXOS.....	15

# 1. OBJETIVO

La Universidad de Murcia (UM), a través del Área de Tecnología de la Información y las Comunicaciones (ATICA) ofrece a la comunidad universitaria el acceso a los distintos recursos informáticos de su propiedad.

Este documento define con carácter general los siguientes aspectos relativos a los recursos informáticos de la UM:

- Cuáles son los derechos y obligaciones de los usuarios de dichos recursos
- Cuáles son los derechos y obligaciones de los responsables de dichos recursos
- Marco jurídico y legal en el que se desarrolla la actividad de los usuarios y de los responsables de los recursos
- El modo en el que se accede a dichos recursos y las condiciones en que se prestan a la comunidad universitaria

El objetivo último de esta Normativa de Uso de los Servicios y Recursos Informáticos es garantizar la calidad de los servicios ofertados desde ATICA y regular el uso de los mismos por parte de personas y colectivos definidos en el ámbito de aplicación de esta normativa, de acuerdo con la naturaleza y funciones de la Universidad expresadas en sus Estatutos.

## 2. ÁMBITO DE APLICACIÓN

### 2.1 Personas y colectivos

Esta normativa será de aplicación a todos los miembros de la comunidad universitaria o a cualquier persona vinculada con la UM que necesite y solicite usar los recursos informáticos de la misma bien sea de forma local o remota.

Dependiendo del tipo de vinculación con la UM, los usuarios de los recursos informáticos de la UM se organizan en colectivos. La asignación personal de recursos informáticos, así como el modo y las condiciones en que se usan pueden variar en función del colectivo al que pertenece dicha persona y en función de la naturaleza del recurso.

En la UM distinguimos los siguientes colectivos de usuarios, sin perjuicio de que en el futuro se definan otros nuevos:

- Personal Docente e Investigador (PDI)
- Alumnos
- Personal de Administración y Servicios (PAS)
- Otros usuarios (trabajadores externos, profesores invitados, becarios, etc.)

La vinculación de una determinada persona con la UM ha de registrarse convenientemente, esto es, los datos de filiación de la persona deben aparecer en las bases de datos de ATICA. Una persona que no aparezca registrada en las bases de datos de ATICA no tiene vinculación con la UM y, por tanto, no tiene derecho a usar ninguno de los recursos informáticos gestionados por ATICA.

En última instancia, es la autoridad competente de la UM la que decide qué personas tienen

acceso a qué recursos de la UM y en qué condiciones; así como la de arbitrar excepciones a la normativa recogida en este punto.

La aplicación de los contenidos de esta normativa se hará de forma individual (personal docente e investigador, alumnos y personal de administración y servicios) o colectiva (centros, departamentos, grupos de investigación, institutos universitarios, asociaciones estudiantiles, servicios universitarios, etc.)

## **2.2 Recursos de tecnologías de información y comunicaciones**

Quedan sujetos a las normas y condiciones contenidas en este documento todos los equipos y sistemas de información y comunicaciones de la UM, ya sean personales o compartidos y estén o no conectados a la red.

Aquellos equipos que no sean propiedad de la UM, pero que se conecten a la red de la UM o usen los servicios y recursos de la misma, también deberán cumplir con esta normativa de uso.

Se incluyen, por tanto, en el ámbito de esta normativa, cualquier equipo informático, así como el software (aplicaciones informáticas) instaladas en los mismos.

Los servicios y recursos ofrecidos por la UM a sus usuarios, serán utilizados en las condiciones previstas en cada caso. Estas condiciones estarán recogidas en normativas específicas, cuando no exista normativa específica para un servicio o recurso, éste estará regulado por la normativa que con carácter general define el presente documento.

## **3. ASPECTOS LEGALES**

Son de aplicación las leyes y normativas españolas, así como las que dimanen de la Unión Europea y de la Comunidad Autónoma de la Región de Murcia en relación con protección de datos personales, propiedad intelectual y uso de herramientas telemáticas, así como las que puedan aparecer, en un futuro, a este respecto.

Esta normativa se sitúa dentro del marco jurídico definido por las leyes y reales decretos siguientes:

- Ley Orgánica 15/1999, de Protección de Datos.
- Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la intimidad Personal y Familiar y a la Propia Imagen.
- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- Ley 34/2002, de 11 de julio, de Servicios de Sociedad de la Información (LSSI)
- Real Decreto 994/1999: Reglamento de medidas de seguridad de los ficheros automatizados que contienen datos de carácter personal.
- Real Decreto 263/1996: Utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del estado.

## **4. DEFINICIÓN DE TÉRMINOS Y RESPONSABILIDADES**

## **4.1 ATICA**

ATICA es la unidad responsable de la gestión de la red corporativa de comunicaciones de la UM (UnimurNet) así como de todos los servicios informáticos y recursos corporativos dedicados a la gestión, docencia e investigación. Al mismo tiempo será el responsable de la gestión, coordinación y administración del espacio radioeléctrico dentro de los ámbitos físicos de la UM.

Se entiende que ATICA actúa siempre en última instancia bajo la dependencia orgánica de la Gerencia, y funcional del Vicerrectorado correspondiente. En adelante, en el presente documento, cuando se detalle que ATICA otorga tal o cual responsabilidad, o presta y/o deniega tal o cual servicio, se entiende siempre que es salvo superior criterio.

Entre las atribuciones asignadas a ATICA se incluyen:

- Asegurar la conectividad de red a los usuarios de la UM
- Asegurar el acceso a las distintas aplicaciones y servicios corporativos de la UM
- Proporcionar los mecanismos necesarios para garantizar la autenticidad, privacidad e integridad de las comunicaciones en el uso sus aplicaciones y servicios
- Facilitar la comunicación y resolución de problemas relativos al uso de sus servicios y aplicaciones

## **4.2 Responsabilidad sobre los recursos informáticos**

Para cada recurso informático existirá un responsable administrativo así como un responsable usuario final del mismo. Tanto el responsable administrativo como el usuario final están obligados a aceptar las condiciones de esta normativa de uso y aplicarla a los recursos que gestiona y utiliza así como a los servicios a los que accede.

### **4.2.1 Responsables administrativos**

El responsable administrativo debe en todo momento conocer, controlar el acceso, velar por el buen uso y funcionamiento de los recursos objeto de su responsabilidad así como atender a los usuarios de los mismos.

Los responsables administrativos serán:

- ATICA es responsable de los recursos de la red y de todos los sistemas destinados a dar servicios corporativos, tanto a nivel ofimático como telemático, de aplicaciones etc. así como de los ordenadores personales de uso general no adscrito a unidades concretas.
- Los Decanos y Directores de Centro son responsables de los recursos informáticos de uso general dentro del centro.
- Los Directores de Departamento, de Institutos Universitarios y grupos de investigación son los responsables de los recursos informáticos de los miembros de su Dpto., Instituto o grupo bajo su tutela, destinados a la docencia o investigación.
- Los Jefes de Servicio, Área o Sección de las unidades de Administración y Servicios son responsables administrativos de los recursos de su unidad.

### **4.2.2 Responsable usuario final**

Usuario final es cualquier persona vinculada con la UM en los términos recogidos en el punto 2.1 del presente documento, que accede y usa un determinado recurso informático de la UM.

El usuario final está obligado a:

- Cumplir la normativa general aquí expuesta así como la específica del recurso al que accede
- Comunicar al responsable administrativo pertinente cualquier anomalía detectada en el uso o en el funcionamiento del recurso
- Comunicar, por los medios oportunos y establecidos al efecto, al responsable administrativo pertinente cualquier cambio en la titularidad del recurso informático que tenga asignado; mientras esta notificación no se produzca, continuará siendo el único responsable a todos los efectos de los actos derivados del uso del recurso

## **5. ACCESO Y USO DE LOS RECURSOS**

El acceso a los recursos informáticos de la UM puede efectuarse de distintos modos:

- Por tener acceso al espacio físico (despacho, sala de ordenadores, zona de cobertura inalámbrica) en donde se encuentra el recurso (ordenador personal, servidor, punto de red, punto de acceso inalámbrico)
- A través de una cuenta de acceso de la UM
- A través de un carnet inteligente de la UM

La UM se reserva el derecho de decidir la modalidad de acceso a cada uno de sus recursos, así como la posibilidad de adoptar nuevas modalidades de acceso o suprimir otras. El modo en que se accede a un recurso concreto de la UM está recogido en su normativa específica de uso.

### **5.1 Acceso al espacio físico**

Para acceder a determinados recursos de la UM (ordenadores personales, servidores, puntos de red) hay que tener acceso al espacio físico en el que se encuentran. El acceso a este espacio físico puede ser restringido o abierto. En cualquier caso, es tarea del responsable administrativo pertinente (ver punto 4.2.1) controlar quién accede al espacio. Del m

### **5.2 Cuentas de acceso**

Para acceder a determinados recursos de la UM (servicios y aplicaciones corporativas) es preciso disponer de una cuenta de acceso. Una cuenta de acceso consta de un identificativo de acceso (en adelante login) y de una clave de acceso (en adelante clave o contraseña). Una cuenta de acceso permite:

- autenticar (identificar) a cualquier persona o entidad que pretenda acceder a cualquiera de los recursos informáticos corporativos de la UM
- decidir cuáles de esos recursos puede usar esa persona o entidad

Una misma cuenta de acceso puede tener asociados uno o más recursos, de manera que el usuario de la cuenta puede acceder mediante el mismo login y contraseña a todos los recursos asociados a esa cuenta.

Las cuentas de acceso pueden ser personales o no personales. Las cuentas de acceso personales son para uso exclusivo del titular de la misma. Las cuentas de acceso no personales pueden ser usadas por más de una persona y están destinadas a permitir el acceso y compartir el uso de los recursos informáticos asociados a esa cuenta a un grupo de personas. El titular de una cuenta de acceso no personal es la persona responsable del grupo o unidad que hace uso de la

misma.

Normativa que, con carácter general, se aplican a las cuentas de acceso:

- Siempre debe haber una persona que responda del uso de una cuenta de acceso
- El responsable de una cuenta de acceso personal es el titular (usuario) de la misma
- El responsable de una cuenta de acceso no personal es, en primer lugar, el titular de la misma y en segundo lugar los usuarios que comparten su uso
- Solo el titular de una cuenta de acceso no personal puede cambiar su clave
- Es responsabilidad del titular de la cuenta no personal el otorgar o revocar el uso de la misma a los usuarios que la comparten; el acto de otorgación o revocación se efectuará mediante el cambio de clave de la cuenta de acceso no personal y la posterior comunicación de la clave a aquellos usuarios que el titular estime conveniente
- Es responsabilidad del titular de la cuenta no personal el registrar y documentar la otorgación o revocación sobre el uso de la cuenta a sus usuarios
- Cualquier cuenta de acceso debe tener vinculado el DNI (o similar) del titular de la cuenta. Esta vinculación se registrará en las bases de datos corporativas de la UM
- La obtención de una cuenta de acceso compromete a su titular (y al resto de usuarios en el caso de cuentas no personales) a cumplir y hacer cumplir la normativa de uso general del presente documento así como la particular de los servicios a los que esa cuenta tenga acceso
- Cualquier cambio en la titularidad de una cuenta de acceso debe ser comunicado inmediatamente al responsable administrativo correspondiente
- Salvo cuentas de acceso no personales, no está permitido el uso de cuentas por personas ajenas a su titular (con conocimiento o no del mismo). Tampoco está permitido revelar la clave de una cuenta de acceso (salvo en el caso de cuentas de acceso no personales)
- No está permitido el uso de cuentas personales por otra persona que no sea el titular de la cuenta (con conocimiento o no del titular)
- No está permitido revelar la clave de una cuenta de acceso (salvo en el proceso de otorgación de uso de una cuenta de correo no personal)

El usuario debe notificar inmediatamente a la UM cualquier uso no autorizado de una cuenta de acceso o de cualquier otro fallo de seguridad, usando los medios habilitados a tal efecto (Sistema Atención usuarios: DUMBO).

Asimismo, el usuario debe asegurarse de que su cuenta queda cerrada al final de cada sesión, con el fin de que no pueda ser usado por terceras personas. Si se produjera un mal uso de la misma bajo estas circunstancias, la responsabilidad es del citado usuario.

La Universidad se reserva el derecho de aceptar o no la creación de cuentas. Asimismo, la Universidad podrá suspender o cancelar cuentas por uso indebido, sin perjuicio de imponer las sanciones correspondientes.

### 5.1.1 Estados de las cuentas de acceso

Dada una cuenta de acceso y un recurso asociado a esa cuenta (por ejemplo el servicio de correo electrónico), se definen, con carácter general, los siguientes estados para la cuenta:

- **cuenta activa.** Todas las funciones del recurso asociado a esa cuenta están disponibles (por ejemplo, recibir, enviar, leer o eliminar mensajes)
- **cuenta bloqueada.** El recurso asociado a esa cuenta tiene limitadas todas o parte de sus funcionalidades (por ejemplo no puede recibir mensajes, no puede enviar mensajes, si puede leer y borrar los ya existentes en su buzón)
- **cuenta cancelada.** El recurso asociado a esa cuenta ya no está disponible para el usuario de la cuenta (el usuario no puede usar el correo). Los datos del recurso asociados a esa

cuenta pueden ser eliminados o movidos a un espacio de almacenamiento offline (por ejemplo, el buzón del usuario puede ser suprimido o movido a otro sitio)

Las cuentas de acceso se crean inicialmente en el estado activa para todos sus recursos asociados.

Una cuenta de acceso puede ser bloqueada para todos o alguno de sus recursos asociados en alguno de los siguientes casos:

- por decisión de la autoridad competente de la UM, al cometer el usuario de la cuenta una infracción lo suficientemente grave en el uso del recurso
- por motivos técnicos que aconsejen su bloqueo en situaciones de emergencia
- mientras duren procesos de mantenimiento del recurso o recursos asociados a la cuenta
- mientras se rebasen los parámetros de funcionamiento del recurso por parte del usuario de la cuenta (por ejemplo se llena el buzón de correo)

Una cuenta de acceso puede ser cancelada en los casos contemplados en el punto 5.1.3 del presente documento.

Finalmente, una cuenta de acceso se **elimina**, desapareciendo todo rastro de la cuenta y de los datos de los recursos asociados si y sólo si lleva cancelada un periodo de tiempo determinado y específico para cada uno de los recursos asociados. El login de una cuenta de acceso eliminada puede ser rehusado (puede ser asignado a otra cuenta de acceso nueva).

Cada normativa específica de un recurso o servicio puede definir otros estados para las cuentas de acceso, así como modificar su significado.

## **5.1.2 Creación de cuentas de acceso**

### Cuentas de acceso personales

Para crear una cuenta de acceso personal el titular de la cuenta debe tener una relación formal y vigente con la UMU, apareciendo sus datos de filiación en las bases de datos de ATICA. Esto es, la persona en cuestión pertenece al colectivo PDI, PAS o alumno o bien a otro colectivo conocido de la UMU (becario, trabajador externo, profesor invitado, etc.).

En el caso del PAS, PDI o alumnos de la UM se generará una cuenta de acceso de manera automática en el momento de establecer su relación con la UM (formalización del contrato o matriculación). Esta cuenta dará acceso a los recursos informáticos básicos que la autoridad competente de la UM estime convenientes (como, por ejemplo, el servicio de correo electrónico).

Si, por el motivo que fuese, un miembro del PAS, PDI o un alumno de la UM no tuviese cuenta de acceso para acceder a los recursos informáticos básicos de la UM, podrá solicitarla en cualquier momento mediante los procedimientos habilitados al efecto.

Las personas que no pertenezcan a ninguno de los colectivos arriba mencionados y necesiten obtener una cuenta de acceso, podrán hacerlo mediante solicitud efectuada por el responsable de la unidad organizativa de la que dependen.

### Cuentas de acceso no personales

Para crear una cuenta de acceso no personal, ésta deberá ser solicitada por el responsable del grupo o unidad organizativa que va a usarla. El responsable del grupo debe pertenecer al PAS o PDI de la UM o estar debidamente autorizado por la autoridad competente de la UM. Una vez creada la cuenta de acceso el responsable que la solicitó pasa a ser el titular de la cuenta.

## Procedimiento de creación de las cuentas de acceso y asignación de recursos

Siempre que sea posible, la solicitud de creación de una cuenta de acceso se efectuará por medios informáticos, para ello el solicitante de la cuenta deberá acreditar su identidad mediante certificado digital personal.

Cuando el solicitante no disponga de certificado digital y no pueda solicitar la cuenta por medios informáticos, la solicitud podrá efectuarse mediante formulario dirigido a ATICA y debidamente sellado por el jefe de la unidad organizativa de la UM interesado en la creación de la cuenta. En este caso es responsabilidad del jefe de la unidad organizativa el comprobar la identidad del usuario de la cuenta cuando se trate de cuentas personales.

El modelo del formulario de solicitud será establecido por ATICA, podrá obtenerse desde la página web del Área.

Una vez comprobada la identidad del solicitante y el derecho a obtener la cuenta de acceso, se procederá a la creación de la cuenta. La creación de la cuenta puede postergarse por motivos técnicos justificados, en cualquier caso ATICA informará al solicitante por los medios que considere más oportunos de:

- cuándo ha sido o será creada la cuenta
- la clave de acceso a la misma
- documentación relativa al uso de los servicios informáticos a los que la cuenta permite acceder: normativa específica de cada servicio, parámetros de configuración de cada servicio, etc.
- cualquier otra información que se estime relevante

En el caso de que la solicitud sea rechazada se informará al solicitante de los motivos del rechazo.

Los recursos y servicios informáticos básicos asignados a una cuenta de acceso pueden variar en función del colectivo al que pertenece el usuario (PAS, PDI, alumnos, otros) o del tipo de cuenta (personal, no personal). En cualquier caso, es la autoridad competente de la UM la que decide los recursos asociados a una cuenta de acceso en función del tipo de cuenta y del colectivo al que va destinada.

### **5.1.3 Cancelación de cuentas de acceso**

Con carácter general, se procederá a cancelar una cuenta de acceso cuando:

- En el caso de cuentas personales, la relación de la persona con la UM deja de estar vigente. O sea, la persona deja de ser alumno, miembro del PAS, PDI u otro colectivo conocido de la UM
- El responsable de la cuenta solicita la cancelación de la misma
- Por decisión de la autoridad competente de la UM por comisión de infracciones que lleven pareja la cancelación de la cuenta de correo
- Cuando no se detecte actividad en el uso de la cuenta (cuentas de acceso abandonadas)

En cualquier caso será la autoridad competente de la UM la que decida en qué casos, cuándo y cómo se cancela una cuenta de acceso, así como la de arbitrar excepciones a las normas de carácter general arriba expuestas.

Salvo indicación expresa de la autoridad competente de la UM, o causas de fuerza mayor, la cancelación de una cuenta de acceso será avisada con tiempo suficiente para que el responsable de la misma efectúe las acciones oportunas sobre cualquier dato almacenado en el recurso o recursos asociados a la cuenta de acceso. El aviso se efectuará mediante mensaje de correo

electrónico o por cualquier otro medio que se estime oportuno.

ATICA no se responsabiliza de los perjuicios ocasionados por la cancelación de cuentas de acceso en las condiciones arriba expuestas.

## **5.2 Carné Inteligente**

Tanto al personal de la UM (PDI y PAS) como a los alumnos, se les hará entrega de un Carné Inteligente personalizado, provisto de chip, y de datos identificativos: DNI, apellidos y nombre y fotografía.

La solicitud del carné se podrá realizar en el momento de la formalización del contrato del trabajador (PAS o PDI), en el momento de la formalización de la matrícula (caso de alumnos) o cuando cualquiera de ellos lo solicite.

La vigencia del carné será indefinida en el caso de personal con contrato indefinido, hasta la finalización del contrato en caso de contrataciones temporales y de un curso académico (1 de octubre a 30 de septiembre) en el caso de los alumnos, renovándose automáticamente cada año en el caso de que la relación de la persona con la universidad continúe.

El carné inteligente permite el acceso a los recursos y aplicaciones que la UM pone a disposición de su colectivo, sirviendo como medio de autenticación física y electrónica y como soporte para el certificado electrónico personal y monedero electrónico.

El procedimiento de creación y cancelación de un carnet inteligente, así como la asignación de servicios y recursos al mismo se rige por las mismas normas aplicadas a las cuentas de acceso, salvo en la clave, que en el caso del carne es el PIN (Personal Identification Number).

## **5.2 Uso de recursos y servicios**

### **5.2.1 Equipos informaticos y sistemas operativos**

Los usuarios tendrán máximo cuidado en la manipulación y el uso de los equipos informáticos y de toda la infraestructura complementaria.

Los equipos no deben presentar configuraciones ni operar con software o dispositivos que causen problemas en la red o a otros equipos conectados a ella.

Los responsables de los equipos conectados a la red UnimurNet deben asegurarse de tener instalados los parches de seguridad, antivirus y actualizaciones de sistemas operativos y software recomendados por ATICA.

### **5.2.2 Red corporativa de la UM (UnimurNet)**

La red corporativa de la UM (UnimurNet) debe entenderse como un servicio más puesto a disposición del colectivo universitario. Como tal servicio dispone de un anexo específico que regula su uso y funcionamiento.

### **5.2.3 Contraseñas o claves de acceso**

Cualquier cuenta de acceso de la UM tiene asociada una clave o contraseña que permite acceder a los servicios asignados a la cuenta. El usuario se compromete a aceptar la normativa específica sobre uso y gestión de claves expuesta en el correspondiente anexo.

### **5.2.4 Parámetros de uso de los servicios**

El funcionamiento de cualquier servicio corporativo de la UM está regulado por distintos parámetros. Estos parámetros se definen en la normativa específica del servicio y tienen como objetivo limitar el uso de los recursos del servicio (espacio en disco, uso de la red, etc.), regulando el funcionamiento del servicio y garantizando un funcionamiento correcto del mismo. El usuario se compromete a aceptar los parámetros establecidos para cada servicio; en particular se compromete a aceptar que su cuenta de acceso al servicio pueda ser bloqueada si se efectúa un "mal uso" del servicio o recurso, provocando que se alcancen o rebasen los límites impuestos por dichos parámetros para dicho servicio.

### **5.2.5 Normativas particulares de servicios**

Independientemente de esta normativa de carácter general, la utilización de los servicios corporativos lleva asociada unas condiciones específicas asociadas a las características particulares de cada servicio. Estas condiciones de uso se encuentran en los siguientes documentos anexos a esta normativa general:

- Normativa de uso de la red corporativa de la UM (UnimurNet)
- Normativa de uso del servicio de correo electrónico.
- Normativa de uso del servicio de hospedaje web (para publicación de contenidos web).
- Normativa de uso del servicio de videoconferencia.
- Normativa de uso de ALAs.
- Normativa sobre uso y gestión de claves

## **5.3 Solicitud de nuevos desarrollos**

Los responsables de las distintas unidades administrativas podrán solicitar nuevos proyectos o servicios informáticos así como el mantenimiento y/o ampliación de los existentes a través del sistema PAPYS (Proyectos y Aplicaciones: Presupuesto y Seguimiento).

Asimismo, los responsables antedichos podrán solicitar modificaciones o desarrollos puntuales de los proyectos y servicios existentes mediante el sistema DUMBO.

El Vicerrector con competencias en materia de TIC, a la vista de las solicitudes propondrá al equipo de gobierno la aprobación de la ejecución de los nuevos proyectos o servicios, así como la prioridad con la que ÁTICA deberá abordarlo.

ÁTICA, con el fin de aumentar la calidad de los servicios prestados y optimizar la asignación de sus recursos, sólo vendrá obligada a atender las solicitudes que se realicen mediante los mecanismos anteriormente especificados en este epígrafe.

## **6. CONDICIONES DE PRESTACIÓN DE SERVICIOS POR PARTE DE ATICA**

### **6.1 Limitaciones de uso**

La UM, a través del Vicerrectorado con competencias en materia de TICs o a través de ATICA, en su caso, podrá establecer limitaciones en el acceso o uso de sus servicios y recursos por alguna de las siguientes causas:

- mantener la operatividad y disponibilidad de los servicios y recursos
- garantizar el cumplimiento de la ley en, por ejemplo, materia de propiedad intelectual
- evitar perjuicios a sus usuarios, por ejemplo, limitando la recepción de mensajes con virus, spam, etc.

ATICA podrá limitar o denegar el acceso a un determinado servicio o recurso (incluida la desactivación del punto de red) cuando se detecte un uso incorrecto o no aceptable del mismo, ya se trate de un uso intencionado o provocado por alguna otra causa: avería, código malicioso (virus, gusanos, etc.).

### **6.2 Retención de información sobre el tráfico generado y el uso de los servicios**

Por razones de seguridad y operatividad de los servicios informáticos ofrecidos por la UM y con el objetivo de velar por la correcta utilización de los recursos informáticos de la misma así como cumplir con la legalidad vigente, ATICA podrá, con carácter ordinario, realizar un seguimiento del uso de los servicios y recursos por parte de los usuarios, quedando registrados en archivos específicos la actividad de los mismos.

Del mismo modo, la UM, a través de ATICA, podrá monitorizar, intervenir y examinar el contenido de las cuentas de los usuarios en alguna de las siguientes circunstancias:

- Cuando el responsable de la cuenta lo pida, para detectar y corregir posibles problemas que afecten a su normal funcionamiento.
- Cuando sucedan eventos que afecten al funcionamiento general del servicio, para detectar el origen y las causas del problema.
- Por requerimiento legal.

ATICA deberá registrar e informar a la autoridad competente de la UM de los datos obtenidos de cualquier tipo de seguimiento realizado, sea éste de carácter ordinario o extraordinario.

La UM, en cumplimiento de lo dispuesto por la Ley Orgánica de Protección de Datos de Carácter Personal, efectuará el seguimiento de todos los accesos que sus usuarios realicen o intenten realizar a los ficheros con datos personales cuya titularidad corresponda a la Universidad, para poder determinar en caso de un mal uso de los mismos las posibles responsabilidades de sus usuarios.

ATICA está obligada a poner en conocimiento de la autoridad universitaria competente la existencia de ficheros que no se adecúen a lo dispuesto en la normativa sobre protección de datos personales, proponiendo la adopción de las medidas adecuadas para poner fin a tal situación.

## **6.3 Compromiso de confidencialidad con relación a los servicios de la UM**

Todo el personal vinculado a la UM, independientemente del tipo de contrato e incluyendo aquel perteneciente a empresas externas con las que se ha establecido alguna relación contractual, asume un “compromiso explícito de confidencialidad” por el que debe cumplir con la obligación de secreto y confidencialidad respecto a los archivos y los contenidos a los que por su trabajo tenga acceso.

La confidencialidad de contenidos y contraseñas a las que se refiere este apartado no excluye la posibilidad de que, en estricto cumplimiento de los pertinentes requerimientos judiciales o, en su caso, autoridad legalmente autorizada, deban revelarse los contenidos así como la identidad de los autores.

## **6.4 Exención de responsabilidad en la administración, funcionamiento y uso de los servicios**

El usuario acepta que la UM no tiene responsabilidad u obligación legal por pérdidas de datos, errores en las comunicaciones, o cualquier otro daño o perjuicio, cuando éstos se deriven de acciones efectuadas durante las tareas de mantenimiento normal de los servicios o durante situaciones especiales o de emergencia.

La UM queda eximida de cualquier responsabilidad derivada del mal funcionamiento de los servicios que tenga su origen en una circunstancia accidental, fuerza mayor, trabajos necesarios de mantenimiento o cualquier otra causa no imputable a la misma.

La utilización de estos servicios está sometida a la exclusiva responsabilidad del usuario de los mismos, quienes conocen esta circunstancia y la aceptan.

## **6.5 Estadísticas de uso de los servicios**

ATICA podrá generar estadísticas del uso de servicios o recursos con el fin de medir y optimizar el rendimiento, la utilización que se hace de los mismos y detectar posibles comportamientos anómalos que pudieran producirse.

En función de la legalidad vigente, queda a criterio de ATICA y de las unidades de quienes depende, cuáles de las estadísticas generadas podrán hacerse públicas para información y mejora del servicio de la comunidad universitaria.

## **6.6 Copias de seguridad**

ATICA se compromete a realizar copia de seguridad de los siguientes aspectos relativos a los servicios corporativos por ella gestionados:

1. programas y archivos de configuración del propio servicio
2. archivos de registro de eventos o “logs”
3. datos de usuario vinculados al servicio
4. archivos de configuración personales de los usuarios depositados en el servidor

La frecuencia y número de copias de seguridad efectuadas podrán variar en función de la disponibilidad y características de los datos a almacenar. En cualquier caso, ATICA no asegura la recuperación de datos y archivos de configuración. Es responsabilidad del usuario del servicio el efectuar copia de los datos que considere importantes en un medio local y personal: disco duro, disquete, cdrom, etc.

## **6.7 Detección y eliminación de código malicioso**

Por código malicioso entendemos cualquier programa de ordenador que pueda ocasionar perjuicios en cualquiera de los recursos informáticos de la UM o fuera de la UM. En este sentido entran en esta definición los virus, gusanos y troyanos, pero también cualquier otro programa cuya ejecución provoque un mal funcionamiento de la red o de los servicios.

ATICA se compromete a mantener en funcionamiento y actualizados programas específicos de detección y eliminación de virus en sus servidores corporativos, así como a proporcionar a los usuarios programas específicos para ser usados en sus equipos personales.

No es responsabilidad de ATICA la detección y eliminación de código malicioso en equipos personales y servidores y aplicaciones ajenos a su administración. En estos casos es el responsable administrativo o el usuario de dichos recursos informáticos el que debe asegurarse de la tarea de detección y eliminación; para efectuar esta tarea podrá contar con la colaboración de personal de ATICA.

### **6.7.1 Responsabilidades asociadas a la propagación de virus**

La UM declina cualquier responsabilidad derivada de la propagación de código malicioso. Es responsabilidad del usuario el tomar las medidas necesarias para evitar la infección y sus consecuencias; entre las medidas se incluyen:

- no abrir ficheros adjuntos en mensajes de correo no solicitados aunque procedan de remitentes conocidos
- usar un antivirus en el ordenador personal y mantenerlo actualizado
- efectuar copias de seguridad periódicas de los programas, datos y configuraciones de su equipo

## **6.8 Gestión de incidencias**

Cualquier usuario está obligado a informar a ATICA, a través de los cauces habilitados a tal efecto, sobre posibles incidencias detectadas en el funcionamiento de los servicios ofertados o uso indebido de los recursos..

Las incidencias que afecten a un usuario concreto deben gestionarse a través del sistema DUMBO ([www.um.es/atica/dumbo](http://www.um.es/atica/dumbo), [dumbo@um.es](mailto:dumbo@um.es) o a través del sistema de recepción telefónica de incidencias extensión 4222).

Las incidencias que supongan quejas o consultas de personas o entidades ajenas a la UM se encauzarán a través de alguna de las siguientes direcciones de correo:

- [postmaster@um.es](mailto:postmaster@um.es): Administrador del servicio de correo de la UM (ATICA).
- [abuse@um.es](mailto:abuse@um.es): Consultas y quejas sobre abusos (barrido de puertos, spam, ...) originados en la UM.
- [antivirus@um.es](mailto:antivirus@um.es): Consultas y quejas sobre virus propagados por correo electrónico o por

cualquier otro medio.

- [cert@um.es](mailto:cert@um.es): Cualquier otra consulta o queja relativa a seguridad.
- [noc@um.es](mailto:noc@um.es): Consultas relativas a la gestión de red y DNS

El compromiso de ATICA es atender cualquier incidencia con prontitud y a darle solución en el plazo más breve posible.

## **7. USOS INCORRECTOS DE LOS RECURSOS.**

El uso de los recursos informáticos de la UM debe circunscribirse principalmente a actividades docentes e investigadoras o a actividades necesarias para el desempeño de la función administrativa.

### **7.1 Sobre la finalidad y naturaleza del uso**

- La transmisión de información o acto que viole la legislación vigente en el Estado Español, Unión Europea, la Comunidad Autónoma de la Región de Murcia y los Estatutos de la UM.
- El uso de los recursos para fines privados, personales o lúdicos o no estrictamente relacionados con las actividades propias de la UM.
- El uso con fines comerciales no relacionado con las actividades propias de la UM.
- La transmisión de información difamatoria o de contenido fraudulento, ofensivo, obsceno o amenazante.
- Almacenar, anunciar, enviar por correo electrónico o de cualquier otra forma transmitir contenido ilegal de cualquier tipo y, particularmente, difundir contenidos de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo, peligroso, amenazador, difamatorio, obsceno, atentatorio contra los derechos humanos o actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas
- La distribución y uso de material que viole los derechos de propiedad intelectual, particularmente el uso de software no licenciado

### **7.2 Sobre confidencialidad y suplantación de identidad**

- Acceder a ordenadores, aplicaciones, datos o información o redes para las que no estén debidamente autorizados. Tampoco deberán permitir de forma intencionada que otros lo hagan.
- Realizar de forma intencionada acciones cuyo fin sea la obtención de contraseñas de otros usuarios sin el consentimiento de éstos.
- En el uso de cuentas mediante el sistema de login y palabra de paso, no aplicar las recomendaciones del documento sobre “Normativa de uso y gestión de claves” de la UM.
- Compartir recursos (ficheros, directorios, etc.) sin los mecanismos de seguridad necesarios y disponibles en cada sistema operativo y/o aplicaciones que garanticen la seguridad de su equipo y la red.
- La destrucción, manipulación o apropiación indebida de la información que circula por la red o pertenece a otros usuarios.

### **7.3 Sobre la integridad, y disponibilidad de los recursos**

- El intento de causar cualquier tipo de daño físico o lógico a los recursos informáticos de la UM: equipos, aplicaciones, programas, documentación, etc.
- El desarrollo o uso de programas que puedan provocar caídas o falta de disponibilidad en

- servidores, equipos de red o cualquier otro recurso (ataques de denegación de servicio).
- El desarrollo, uso o distribución intencionada de programas cuyo objetivo es dañar otros sistemas o acceder a recursos restringidos (malware, virus, troyanos, puertas traseras, etc.) o que pueda resultar nocivo para el correcto funcionamiento de los sistemas informáticos de la UM.
- La modificación no autorizada de permisos o privilegios en sistemas informáticos

## 7.4 Sobre el uso de las infraestructuras

- La conexión de equipos de red activos (hubs, conmutadores, routers) que perturbe el correcto funcionamiento de la red de la UM o comprometa la seguridad, salvo expresa autorización de ATICA.
- Proporcionar acceso externo desde la propia red de comunicaciones, mediante la instalación de dispositivos de acceso remoto.
- El alojamiento de dominios distintos a um.es, salvo expresa autorización del Vicerrectorado competente en esta materia.
- La instalación de servidores telemáticos o de otro tipo (web, correo, etc.), sin las medidas de seguridad adecuadas.
- La conexión, desconexión o reubicación de equipos ajenos, sin la expresa autorización de los responsables de los mismos.
- Facilitar el acceso a los recursos de red a personas no autorizadas.
- No hacer un uso racional, eficiente y considerado de los recursos disponibles, tales como: el espacio en disco, la memoria, las líneas telefónicas, terminales, canales de comunicación, etc.
- Por último, también se considera hacer uso incorrecto, actuar de forma contraria a las condiciones y normas de uso de todos los documentos complementarios de normativa de utilización de los servicios y recursos informáticos proporcionados por la UM, referenciados en este documento.

## 8. MEDIDAS A APLICAR

El incumplimiento de las presentes Normas y Condiciones de Uso o de cualesquiera otras establecidas por la Universidad, comportará de forma preventiva la inmediata suspensión del servicio prestado y/o bloqueo temporal de sistemas, cuentas o acceso a la red, con el fin de garantizar el buen funcionamiento de los servicios TICs de la UM.

Los órganos competentes de la UM decidirán las acciones a tomar en el caso de incumplimiento de la presente Normativa de uso de los servicios y recursos informáticos de la UM y de la normativa complementaria asociada a cada servicio. Todo ello sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales que en su caso correspondan, a las personas presuntamente implicadas en dicho incumplimiento.

## 9. PUBLICIDAD Y ACTUALIZACIÓN

Las condiciones de uso expuestas en el presente documento pueden ser actualizadas por la UM tras aprobación del Consejo de Gobierno.

La versión más reciente de las mismas puede consultarse en la siguiente página web:  
<http://www.um.es/atika/acceso-y-uso-servicios>

## 10. ANEXOS

1. Normativa de uso de la red corporativa de la UM (UnimurNet)
2. Normativa de uso del servicio de correo electrónico..
3. Normativa de uso del servicio de hospedaje web.
4. Normativa de uso del servicio de videoconferencia
5. Normativa de uso de las Aulas informáticas.
6. Normativa de uso y gestion de claves
7. Parámetros de uso de los servicios de ATICA