# NORMATIVA DE USO DE MEDIOS ELECTRÓNICOS EN LA UNIVERSIDAD DE ALCALÁ

Aprobada en Consejo de Gobierno del 17 de julio de 2025

## I. Introducción

En el mundo actual, el uso de las Tecnologías de la Información y las Comunicaciones (TIC) es un fenómeno globalizado que afecta a todos los aspectos de la sociedad. Las universidades públicas no sólo no han sido ajenas a ello, sino que se han convertido en parte activa de ese cambio, transformando sus procesos, servicios y la forma en la que se gestiona la información. Un uso adecuado de dichas tecnologías adquiere una importancia estratégica para cumplir con sus fines de investigación, docencia y administrativos.

Sin embargo, esta evolución conlleva también una mayor facilidad para el tratamiento de gran cantidad de información lo que ha generado nuevas amenazas que no deben pasar inadvertidas. En este sentido, las organizaciones se deben dotar de unas normas que les permitan protegerse adecuadamente frente a estas amenazas, limitando o denegando el acceso a aquellas personas, empresas u organismos que puedan suponer un riesgo para la información, sus infraestructuras y/o sus servicios.

La Política de Seguridad de la Universidad de Alcalá (en adelante UAH) aprobada por acuerdo del Consejo de Gobierno celebrado el 12 de diciembre de 2024 conforme a lo dispuesto en el Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad (ENS), supone un marco general sobre el tratamiento de la seguridad de la información en el ámbito de nuestra universidad que debe ser desarrollado con normas más específicas. La presente normativa desarrolla lo expuesto en la Política de Seguridad de la UAH sobre el uso correcto de las tecnologías de información y comunicaciones, así como un conjunto de buenas prácticas necesarias para la prevención, detección, respuesta y recuperación ante incidentes de seguridad.

## II. Marco legislativo

1. El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (RD ENS) establece dentro del Marco organizativo que "Se dispondrá de una serie de documentos que describan el uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido" (Normativa de seguridad [org.2]).
2. Basándose en las competencias de las Universidades y tras realizar un análisis de riesgos que contempla las vulnerabilidades y amenazas a las que éstas se ven expuestas, se ha elaborado en colaboración con la CRUE, un Perfil de Cumplimiento Específico para Universidades que permita garantizar la máxima seguridad de los sistemas de información y la implantación del ENS en las mismas. Este perfil de cumplimiento queda reflejado en la Guía de Adecuación al ENS para Universidades (CCN-STIC 881) y en el Perfil de Cumplimiento Específico Universidades (CCN-STIC 881A) y en él se ha considerado que siguiendo el procedimiento descrito en el Anexo I del RD ENS, en lo relativo las necesidades de seguridad la categoría del sistema es MEDIA.
3. La nueva política de seguridad de la información de la Universidad de Alcalá aprobada por acuerdo de 12 de diciembre de 2024, del Consejo de Gobierno de la UAH establece en su apartado 13 (Desarrollo de la Política de Seguridad de la Información):
    a. Que dicha política será complementada por medio de diversa normativa y recomendaciones de seguridad.
    b. Que esta normativa Interna del Uso de los Medios Electrónicos constituye junto con la política un primer nivel normativo y corresponde al Consejo de Gobierno su aprobación.

## III. Ámbito de aplicación

Esta normativa se aplicará:

- A la red de comunicaciones de la UAH, a todos los sistemas y servicios conectados a ella, a la información contenida en esos sistemas y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la universidad.
- A todos los dispositivos conectados a la red o con direccionamiento IP dentro del rango asignado a la UAH, tales como equipos de sobremesa, portátiles, impresoras, dispositivos móviles, servidores … etc.
- A todos aquellos dispositivos no pertenecientes a la UAH pero que se conecten a la misma por distintas vías: red WiFi, VPN, etc.
- A todas aquellas personas que tienen la consideración de usuarios de los recursos TIC de la UAH o que disponen de una cuenta de usuario en algún sistema de gestión de identidades de la UAH. A tal efecto, tienen la consideración de usuarios:
    - Los miembros de la comunidad universitaria (PDI, PTGAS y estudiantes).
    - El personal de las fundaciones y organizaciones dependientes de la UAH y entidades colaboradoras, siempre que tengan acceso a los recursos y servicios TIC de la UAH.
    - El personal de las organizaciones proveedoras de servicios en la UAH, siempre que la prestación de sus servicios requiera el acceso a los recursos y servicios TIC de la UAH.
    - Aquellas personas físicas o jurídicas que, a pesar de no formar parte de ninguno de los colectivos anteriores, sean habilitadas para el uso de los recursos TIC de la UAH, siempre que se haya establecido un acuerdo de colaboración con la UAH o una autorización explícita que así lo permita.

Cuando sea necesario el uso de infraestructuras de red externas (RedIMadrid, RedIris …etc.), las políticas y recomendaciones de uso de estas instituciones serán de aplicación en nuestra red.

En el ámbito de la presente Normativa, se utiliza el término "**Recurso TIC**" para hacer referencia a cualquier dispositivo, infraestructura, instalación, sistema, servicio o aplicación informática que dé cobertura al uso de las tecnologías de la información y las comunicaciones.

Todos los usuarios de la red y de los servicios y sistemas de la UAH deberán, entre otros, respetar la integridad de los recursos basados en los sistemas de información, evitar actividades destinadas a obtener accesos no autorizados o suplantación de identidad, respetar los derechos del resto de usuarios, no acaparar los recursos compartidos con el resto de usuarios, respetar las políticas de licencias de software y colaborar en la resolución de los incidentes de seguridad por los que se vieren afectados.

El Comité de Seguridad de la Información y Seguridad TIC, el responsable de Seguridad y el Responsable de los Sistemas ejercerán las funciones y responsabilidades definidas en la Política de Seguridad de la UAH.

## IV. Aprobación

Tal y como se expone en el apartado 13 (Desarrollo de la Política de Seguridad de la Información) Corresponde al Consejo de Gobierno de la UAH la aprobación de la presente Normativa Interna del Uso de los Medios Electrónicos de la Universidad.

## V. Publicación

Esta Normativa de seguridad estará disponible en el apartado de "Normativa reguladora" dentro de la Sede Electrónica de la UAH[1].

## VI. Revisión y evaluación

La gestión de esta Normativa corresponde al Comité de Seguridad de la Información y Seguridad TIC, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Periódicamente, con el fin de garantizar una mejora continua del proceso de gestión integral de la seguridad TIC, el Comité de Seguridad TIC revisará la presente Normativa, que se someterá, de haber modificaciones, a la aprobación del Consejo de Gobierno de la Universidad, tal y como establece el punto 13 de la Política de Seguridad de la Información de la UAH.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

## VII. Normativa de uso de medios electrónicos en la UAH

1. Cuentas de usuario: Identificación y autenticación.

   1.1. Para acceder a los recursos TIC que les hayan sido habilitados, los usuarios dispondrán de una cuenta de usuario que consistirá en un identificador único y unas credenciales de acceso (contraseña, tarjeta, certificado electrónico o cualquier otro método que pueda usarse para comprobar su identidad de forma segura). La existencia de estas cuentas individualizadas permitirá que se pueda conocer a quién pertenece, con qué privilegios se accede y qué acciones se realizan.

   1.2. Los usuarios son responsables de la custodia de sus credenciales y de toda actividad relacionada con el uso de su acceso autorizado. El identificador de usuario es único para cada persona en la organización e intransferible. Si por razones del servicio fuera imprescindible crear una cuenta que no pertenezca a un usuario individual (cuenta no personal o genérica), esa cuenta estará bajo la responsabilidad de una persona identificada mediante su nombre, apellidos, identificador único y puesto o cargo en la UAH, la cual deberá tener una relación laboral de carácter fijo con la Universidad y será la responsable exclusiva de la actividad relacionada con el uso del identificador genérico. En caso de producirse algún cambio en la figura del responsable, cese o sustitución, o bien si la cuenta ya no es necesaria deberá ser notificado lo antes posible para su actualización o cancelación. En todo caso se minimizará el uso de cuentas no personales.

   1.3. Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso a otra persona, ni mantenerlas por escrito a la vista o alcance de terceros. Tampoco se deberán facilitar por otras vías (correo electrónico, teléfono).

[1] https://sede.uah.es/

1.4. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

1.5. Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona o, de forma accidental, la ha proporcionado por un medio indebido, deberá cambiarla inmediatamente y comunicar a los Servicios Informáticos el correspondiente incidente de seguridad.

1.6. El incumplimiento del deber de custodia de la cuenta supone una vulneración grave en la seguridad. La UAH puede iniciar un procedimiento administrativo para asegurar el correcto funcionamiento de los servicios prestados y adoptar las medidas correctoras y disciplinarias necesarias, entre las cuales está el bloqueo inmediato de la cuenta de usuario como medida cautelar.

1.7. Las contraseñas de todas las cuentas (individuales o genéricas) en la Universidad de Alcalá deberán cumplir los requisitos definidos en la Política de contraseñas en lo relacionado, entre otras cosas, con: longitud, formato, restricciones y periodo de caducidad. Todas las contraseñas deberán cumplir los requisitos mínimos establecidos.

1.8. Para sistemas de nivel Medio[1], el acceso con contraseña se debe reforzar con un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es».

1.9. La finalización de la relación con la Universidad de Alcalá comporta el cese del derecho a utilizar los recursos y servicios TIC suministrados por la institución. Cuando los usuarios dejen la entidad, hayan sido cesados en su función o se les hayan revocado los permisos, se inhabilitarán sus cuentas, manteniendo los registros de actividad asociados durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denomina «periodo de retención».

1.10. Una vez finalizada la relación con la Universidad de Alcalá, el usuario dispondrá de un periodo de tiempo para el acceso a sus datos con el fin de obtener copia antes de la cancelación total de su cuenta. Este periodo de tiempo se fija en un año. Del mismo modo, la UAH se reserva el derecho de poder ampliar el periodo de utilización de los recursos TIC a los usuarios una vez finalizada su vinculación con la institución.

2. Normativa sobre uso de equipos informáticos

2.1. La UAH facilita a los usuarios que así lo precisen, los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Los datos, dispositivos, programas y servicios informáticos que la Universidad pone a disposición de los usuarios deben utilizarse exclusivamente con la actividad docente, investigadora o corporativa de la Universidad de Alcalá y bajo ningún concepto se debe utilizar para realizar acciones que no estén relacionadas con dichas actividades.

2.2. Se permite la conexión de equipos informáticos de propiedad particular a la red inalámbrica de la universidad (red eduroam). Los equipos conectados estarán sujetos a ésta y cuantas normativas de seguridad le sean aplicables en el seno de la UAH.

2.3. La conexión de equipos informáticos no inventariados o de propiedad particular mediante cable a la red de la UAH no está permitida. De forma excepcional se podrá permitir dicha conexión,

[1] El Anexo II (Plan de Adecuación al ENS para Universidades) de la Guía 881 (Adecuación al ENS para Universidades) determina para los sistemas universitarios una categoría de nivel Medio.

con una duración limitada en el tiempo, siempre que esté debidamente justificada; la autorización corresponderá al Responsable de Seguridad de la UAH y/o del Responsable del Sistema.

2.4. Como norma general, los equipos informáticos propiedad de la UAH se instalan y configuran bajo la supervisión y/o directrices del personal técnico de los Servicios Informáticos de la UAH, por lo cual ningún usuario deberá realizar cambios en su configuración.

2.5. La configuración de los equipos se realizará en base a los principios de "funcionalidad mínima" y "mínimo privilegio" de forma que los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones. Por este motivo, como norma general, los usuarios no tendrán privilegio de administrador sobre los recursos TIC, salvo autorización expresa del responsable de Seguridad o de aquel en quien delegue tal competencia. Cuando por razones justificadas un usuario tenga dichos permisos se compromete a usarlo de conformidad con lo dispuesto en esta normativa, asumiendo la responsabilidad correspondiente en caso de incumplimiento. Así, entre otras actividades se compromete a:

a) Mantener actualizada la seguridad de los sistemas operativos, antivirus y cortafuegos (firewalls) de sus equipos de trabajo mediante actualizaciones automáticas y, en todo caso, de acuerdo con los procedimientos establecidos o con la asistencia del Centro de Atención al Usuario de la Universidad (CAU).
b) Instalar únicamente programas para los cuales la UAH tiene licencia de uso. No se permite instalar software para el cual no se disponga de licencia, ni ejecutar o guardar archivos no confiables.
c) En el caso de servidores, será responsabilidad del administrador designado para el equipo aplicar y mantener las medidas de seguridad oportunas, siguiendo las normas, procedimientos, instrucciones, guías y recomendaciones específicas que sean de aplicación.

2.6. Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Si el personal de soporte técnico detecta cualquier anomalía que alerta de una utilización de los recursos contraria a la presente norma, lo pondrá en conocimiento del Responsable de Seguridad y/o del Responsable del Sistema, quienes podrán tomar las oportunas medidas correctoras.

2.7. La responsabilidad del uso adecuado de las herramientas informáticas, ordenador personal, periféricos y programas instalados es del propio usuario, el cual debe procurarse los conocimientos imprescindibles para el manejo de sus programas y aplicaciones. La UAH pondrá a disposición de los usuarios herramientas que les facilitarán la realización de copias de seguridad de los datos que se consideren relevantes. La UAH sólo realiza copias de seguridad de los datos y ficheros almacenados en los espacios de almacenamiento corporativos.

3. Aspectos mínimos de seguridad

3.1. Todos los recursos TIC deben estar al día en cuanto a las actualizaciones del Sistema Operativo; la única excepción será para los casos de no compatibilidad con aplicaciones necesarias para el trabajo del usuario con autorización del Responsable de Seguridad de la UAH y/o del Responsable del Sistema.

3.2. Todos los equipos conectados deben tener activos y actualizados mecanismos de protección y reacción frente a código dañino, (antivirus, EDR, XDR …) los cuales deberán estar configurados de forma adecuada e implementarán protección en tiempo real. Todo el sistema se escaneará regularmente para detectar código dañino.

3.3. Con el fin de disponer de una forma centralizada de administrar, gestionar y aplicar políticas de seguridad corporativas, así como de garantizar una distribución ágil y eficiente de los mecanismos de protección descritos en los apartados anteriores, todos los equipos propiedad de la Universidad deberán estar unidos al dominio "uah.es" salvo incompatibilidad del sistema o autorización expresa del responsable de Seguridad o de aquel en quien delegue tal competencia.

3.4. Cortafuegos personales: Es recomendable que todos los dispositivos móviles que se conecten a la red tengan activo un cortafuegos, basado en un software instalado en la propia máquina y debidamente configurado.

3.5. Protección física del equipo (protección de escritorio y acceso local): El equipo o puesto de trabajo se deberá configurar para que se bloquee al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso. Se recomienda un tiempo de 10 minutos.

3.6. Servicios o aplicaciones no necesarias: Si una aplicación no es necesaria para el trabajo del usuario del equipo, no debe estar instalada y desde los Servicios Informáticos se podrá requerir al usuario su desinstalación.

3.7. El acceso remoto (desde Internet) a ordenadores y servidores conectados a la red de la UAH se hará exclusivamente utilizando mecanismos seguros de conexión y permitidos por el Responsable del Sistema y/o Seguridad.

3.8. El uso del software instalado en equipos informáticos de la Universidad debe ajustarse en todo momento a la normativa legal vigente. En consecuencia, los usuarios deben asegurarse de que disponen de las licencias adecuadas al uso que hagan de dicho software, ya sea utilizando licencias adquiridas de forma centralizada por la UAH (software de uso común), mediante la adquisición individual de las correspondientes licencias, o bien mediante el uso de software libre. De no ser así la responsabilidad recaerá totalmente sobre el usuario. Queda terminantemente prohibido la instalación de programas o aplicaciones de los cuales no se disponga de licencia.

3.9. Los puestos de trabajo permanecerán despejados, sin que exista material distinto del necesario en cada momento. Una vez usado, y siempre que sea factible, el material se almacenará en lugar cerrado.

4. Gestión y acceso a la Red de la UAH

4.1. Los Servicios Informáticos de la UAH, a través de personal propio o de proveedores de servicios, son los responsables únicos de la administración y gestión de la Red de la Universidad.

- La instalación (o cambios) de nuevos puntos de red conectados a la Red de la UAH se hará de conformidad con los criterios aprobados (según la norma técnica de aplicación) y será competencia exclusiva de los Servicios Informáticos.
- No se permitirá la instalación de electrónica de red (conmutadores, concentradores, equipos de enrutamiento …etc.) y de puntos de acceso de redes inalámbricas con conexión a la Red de la UAH sin la debida información y autorización de los Servicios Informáticos. En caso de detección de algún equipo no autorizado se procederá a su inmediata desconexión.
- Los equipos electrónicos de gestión e infraestructura de la red de la UAH serán instalados, configurados y mantenidos exclusivamente por los Servicios Informáticos.
- No se permite el empleo de mecanismos para la manipulación de direcciones de red o cualquier otro uso que pueda afectar a la topología o a la estructura lógica de la red.

4.2. Todos los equipos que se conectan a la red deben recibir una dirección IP y un nombre de red asignados por los Servicios Informáticos, además de ser incluidos en el registro correspondiente, junto con la identidad y los datos de contacto del responsable del equipo. No está permitida la conexión de equipos con direcciones no registradas.

4.3. En el caso de los servidores departamentales, o sea, aquéllos instalados en un departamento y administrados por personal de éste para dar un determinado servicio propio del departamento, debe quedar claramente definida la persona que actúa como responsable del mismo y quién se encarga de su mantenimiento, además de la información técnica oportuna según se indique en la normativa específica que se desarrolle al efecto. Esta persona deberá tener relación contractual permanente con la Universidad y responderá ante incidencias e incumplimiento de esta Normativa por parte del sistema local.

4.4. La red de la UAH tendrá un enlace con Internet (a través de la infraestructura proporcionada por RediMadrid) cuya administración y correcto funcionamiento es responsabilidad de los Servicios Informáticos.

4.5. Los usuarios de la red no deben utilizar esta infraestructura y servicios para otros usos que no sean los permitidos en la Política de uso de RedIRIS, RedIMadrid o los propios necesarios para el desempeño de su actividad.

4.6. No está permitido que los usuarios utilicen su conexión a red para proporcionar tráfico a terceras personas o entidades.

4.7. Ningún usuario está autorizado a utilizar analizadores del tráfico que circula por la red de la UAH. Igualmente está prohibido utilizar herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. El uso de estas herramientas sólo está permitido a los administradores de la red previa autorización por parte del Responsable de Seguridad.

4.8. La actuación del personal técnico de los Servicios Informáticos se rige por los principios de profesionalidad, seguridad, secreto y pleno respeto de los derechos de los usuarios.

5. Uso de servicios en la Nube, no titularidad de la UAH

5.1. Excepto en aquello casos expresamente autorizados, se prohíbe alojar información propia de la UAH en servidores externos en "la nube" con los cuales no haya una relación contractual establecida y que no hayan sido ofrecidos por la institución.

6. Gestión del personal

6.1. Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos, en particular sobre:

- ✓ El buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
- ✓ La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
- ✓ El procedimiento para informar sobre incidentes de seguridad.

6.2. Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a:

- ✓ Configuración de sistemas.
- ✓ Detección y reacción ante incidentes.
- ✓ Gestión de la información.

7. Uso abusivo o indebido de los Sistemas de información

7.1. En el uso de los recursos y servicios TIC de la UAH, los usuarios tienen que respetar los derechos y deberes reconocidos en la Constitución española, el ordenamiento jurídico, los Estatutos de la Universidad y cuantas normas de ámbito interno, propias de la UAH le sean de aplicación.

7.2. Además de lo antes indicado, se considera un mal uso o uso inaceptable a aquella actuación del usuario que puede afectar a la disponibilidad de un servicio, al trabajo del resto de usuarios, o que, en general, ponga en riesgo cualquiera de las dimensiones de seguridad (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) de la información y/o los servicios.

7.3. A modo de ejemplo y sin ánimo de exhaustividad, se consideran malos usos:

- Incurrir en actividades ilícitas o ilegales de cualquier tipo, especialmente aquellas que puedan suponer perjuicio para los derechos, libertades e imagen de las personas.
- Uso de Internet para propósitos que puedan influir negativamente en la imagen de la UAH, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.
- El uso de una cuenta de usuario para la que no se tiene autorización o bien el robo de credenciales.
- El uso de la Red de la UAH para conseguir el acceso no autorizado a cualquier ordenador, servidor o aplicación.
- Realizar alguna actuación de forma intencionada que interfiera en el funcionamiento normal de otros ordenadores, impresoras, dispositivos o redes.
- Instalar y ejecutar de forma intencionada en cualquier ordenador o subred cualquier tipo de software que provoque el mal funcionamiento o la sobrecarga en dicho equipo o subred (malware). También se incluye aquí la distribución de este malware a otros usuarios.
- El abuso deliberado de los recursos puestos a disposición del usuario.
- Los intentos de saltarse medidas de protección de la información o de explotar posibles fallos de seguridad de los sistemas.
- El no cumplimiento de las condiciones de las licencias del software o de sus derechos de autor.
- Cualquier actividad que pueda suponer una vulneración de derechos de propiedad intelectual.
- El envío de mensajes de correo de forma masiva (spam) o con contenido fraudulento, ofensivo, obsceno o amenazante.
- Ocultar o falsificar la identidad de una cuenta de usuario o de una máquina.
- El uso de los servicios de difusión de información para fines que no tengan relación con las propias del desempeño laboral o que no sean de interés para la comunidad universitaria.
- Los intentos de monitorización y rastreo de las comunicaciones de los usuarios.
- La lectura, copia, modificación o borrado de los ficheros de otros usuarios sin la autorización explícita del propietario.

7.4. Las acciones realizadas desde una cuenta de usuario o desde una cuenta de correo electrónico de usuario son responsabilidad de su titular.

7.5. Los sistemas se pueden configurar para prevenir acciones que puedan ser consideradas contrarias a la Política de Seguridad de la UAH, a esta normativa o a cuantas otras normativas específicas se desarrollen. Estos sistemas pueden adoptar las medidas preventivas y de detección correspondientes.

7.6. Si algún Área o Departamento de la UAH lleva a cabo actividades de docencia o investigación que requieran de un tratamiento especial en materia de seguridad, deberá ponerlo en conocimiento del Comité de Seguridad de la Información y Seguridad TIC o del Responsable de Seguridad.

## VIII. Monitorización y aplicación de esta normativa

El artículo 24 (Registro de actividad y detección de código dañino) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad establece que "con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa", así, "al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información".

La UAH, 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) Podrá revisar periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones bajo su responsabilidad.
b) Podrá monitorizar los accesos a la información contenida en sus sistemas.
c) Podrá auditar y analizar periódicamente los recursos corporativos compartidos bajo su responsabilidad.
d) Auditará la seguridad de las credenciales y aplicaciones.
e) Podrá monitorizar los servicios de internet, correo electrónico y otras herramientas de colaboración.
f) Se mantendrá un registro de actividad, mediante el establecimiento de un registro de auditoría que contendrá al menos el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito).

Estos registros se revisarán de forma periódica en busca de patrones anormales, documentándose los eventos de seguridad. El acceso a estos registros se realizará sólo por personal autorizado.

La UAH llevará a cabo esta actividad de monitorización de manera proporcional al riesgo, con las cautelas legales pertinentes y las señaladas en la jurisprudencia y con observancia de los derechos de los usuarios.

La actuación del personal técnico se regirá por los principios de profesionalidad, seguridad, secreto, confidencialidad y respeto a los derechos del usuario.

Los servicios, sistemas o recursos (cuentas de usuario) en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca. Los Servicios Informáticos, con la colaboración de las restantes unidades de la UAH, velarán por el cumplimiento de la presente Normativa e informarán al Comité de Seguridad de la Información y Seguridad TIC sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa.

El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar a los administradores sobre usos prolongados e indebidos del servicio.

Los recursos corporativos compartidos serán analizados periódicamente buscando contenido malicioso o inapropiado que no cumpla con los fines propios de la actividad académica, investigadora o administrativa. En caso de detectarse dicho contenido, en función del riesgo, podrá ser puesto en cuarentena o directamente eliminado, informando de la acción al propietario, al Responsable de Seguridad y al Responsable del Sistema.

**IX. Suspensión del uso de los recursos**

La Universidad de Alcalá podrá suspender el uso de los recursos y servicios TIC a los usuarios, temporal o definitivamente, en los casos siguientes:

a) Cuando se hayan llevado a cabo actividades contrarias al ordenamiento jurídico.
b) Cuando se incumpla esta normativa y aquellas disposiciones adoptadas por la UAH en su desarrollo y aplicación.
c) Cuando haya un requerimiento judicial que determine la adopción de medidas cautelares.
d) Cuando haya problemas en la disponibilidad de los recursos.
e) Cuando sea necesario para el mantenimiento y el correcto funcionamiento de los sistemas de la UAH.
f) Cuando sea necesario para garantizar la seguridad de los recursos y sistemas.

La suspensión definitiva en el uso de los recursos y servicios requiere una resolución del Comité de Seguridad de la Información y Seguridad TIC. La suspensión temporal podrá ser acordada por el Responsable de Seguridad.

En todo caso, la suspensión definitiva se podrá acordar directamente en aquellos casos en que una resolución judicial firme haya declarado probados los hechos.

El procedimiento y las sanciones aplicables serán las establecidas en la legislación vigente sobre régimen disciplinario del personal al servicio de las administraciones públicas, régimen disciplinario de estudiantes y cuantas otras sean aplicables en el entorno de la UAH.

**X. Desarrollo Normativo**

La presente normativa se desarrollará en procedimientos, instrucciones técnicas y guías específicas entre las que se podrán encontrar:

a) Utilización del correo electrónico
b) Acceso a Internet
c) Gestión de Incidentes de Seguridad
d) Acceso remoto a recursos corporativos
e) Despliegue de aplicaciones y sistemas
f) Uso de dispositivos móviles
g) Teletrabajo