

NORMAS DE USO DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD DE ALMERÍA

Aprobada en Consejo de Gobierno el 15/07/2024

Índice

| | | |
|-----|---|----|
| 1. | Exposición de motivos | 2 |
| 2. | Ámbito objetivo | 3 |
| 3. | Ámbito de aplicación | 3 |
| 4. | Normas generales y de uso de los dispositivos..... | 3 |
| 4.1 | De los ordenadores corporativos..... | 4 |
| 4.2 | De los dispositivos y soportes móviles corporativos | 5 |
| 5. | Uso de la red corporativa | 5 |
| 6. | Acceso a aplicaciones y servicios..... | 7 |
| 7. | Acceso y tratamiento de datos personales..... | 9 |
| 7.1 | Ficheros informáticos..... | 9 |
| 7.2 | Ficheros en papel..... | 11 |
| 8. | Sobre la Gestión de Incidentes de Seguridad | 12 |
| 9. | Incumplimientos..... | 13 |
| 10. | Disposición Adicional Primera..... | 13 |
| 11. | Disposición Adicional Segunda | 14 |
| 12. | Disposición Derogatoria..... | 14 |
| 13. | Disposición Final..... | 14 |

1. Exposición de motivos

De acuerdo con la Política de Seguridad de la Información de la Universidad de Almería, aprobada por el Consejo de Gobierno el 18 de junio de 2018, las funciones que impone el Esquema Nacional de Seguridad (en adelante, ENS) y que corresponden al «Comité de Gestión del ENS», son asumidas en la Universidad de Almería por la Comisión de Seguridad Informática y Protección de Datos (en adelante, Comisión de Seguridad).

Dentro de las funciones asignadas al citado Comité, se encuentra la de aprobar la normativa interna de seguridad de la organización, para cumplir con el ordenamiento jurídico en seguridad informática y en protección de datos, que resumidamente se encuentra formado por las siguientes normas:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDyGDD).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Documentos de la Administración en Materia de Seguridad Electrónica: Criterios de Seguridad, Normalización y Conservación.
- Instrucciones Técnicas de Seguridad de la Secretaría de Estado de Función Pública (Informe del Estado de la Seguridad, Conformidad con el Esquema Nacional de Seguridad, Auditoría de la seguridad de los sistemas de información y Notificación de incidentes de seguridad).
- Las Guías CCN-STIC de Seguridad de los Sistemas de Información y Comunicaciones.

2. **Ámbito objetivo**

Esta normativa establece las normas de uso de los equipos informáticos corporativos (ordenadores personales y portátiles) asignados o vinculados al puesto de trabajo de la red corporativa, de los servicios corporativos necesarios para el desarrollo de tareas administrativas, de aplicaciones informáticas corporativas, así como el acceso y tratamiento de datos personales, a nivel informático y en papel.

3. **Ámbito de aplicación**

Lo dispuesto en esta normativa es de obligado cumplimiento para todos los usuarios de la Universidad de Almería (en adelante, UAL) que utilizan equipamiento informático corporativo y accedan o traten información de carácter personal o no personal, para la realización de sus funciones y tareas.

La Comisión de Seguridad podrá aprobar normas de uso específicas para algunos servicios de Tecnologías de la Información y las Comunicaciones (en adelante, TIC) y promover las acciones necesarias para dar publicidad a dichas normas.

4. **Normas generales y de uso de los dispositivos**

Dentro de estas normas generales se tendrá en cuenta que en ningún caso se podrá acceder a los recursos informáticos y telemáticos con las siguientes finalidades:

- Incurrir en actividades ilícitas o ilegales de cualquier tipo y, particularmente, difundir contenidos o propaganda de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o 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.
- Difundir contenidos contrarios a los principios enunciados en los Estatutos de la UAL.
- Dañar los sistemas físicos y lógicos de la UAL, de sus proveedores o de terceras personas.
- Introducir o difundir en la red virus informáticos o cualquier sistema físico o lógico susceptible de causar daños.

- Usar cuentas de usuario sin autorización. Obtener la contraseña de acceso de una cuenta de usuario sin la autorización del propietario. Comunicar a otros la contraseña para que puedan entrar en la cuenta.
- Usar la red u ordenadores de la Universidad de Almería para conseguir acceso no autorizado a cualquier ordenador.
- Realizar con conocimiento de causa cualquier acto que interfiera en el correcto funcionamiento de los ordenadores, servicios, red de comunicaciones, etc.
- Intentar sobrepasar protecciones de datos o sistemas de seguridad informática sea cual sea la intención final.
- Violar la privacidad de los datos y el trabajo de otros usuarios.
- Apropiarse de archivos o ficheros titularidad de la Universidad de Almería, para uso particular y/o de terceros.

4.1 De los ordenadores corporativos

El equipamiento informático institucional (conexión a servicios, ordenadores y red de comunicaciones), con el que los trabajadores realizan sus tareas en la Universidad de Almería, es propiedad de la Universidad y no está destinado a un uso personal. El usuario se compromete a utilizar estos recursos exclusivamente para usos relacionados con su trabajo.

El Área de Tecnologías de la Información y la Comunicación (en adelante, ATIC) será el responsable de definir la configuración básica de hardware y software de los puestos de trabajo y de administrar los accesos a la red corporativa. Cualquier necesidad de modificación del puesto será solicitada por la persona responsable de la dirección o unidad que lo solicita.

Los usuarios deben cumplir las siguientes medidas de seguridad establecidas por la Universidad de Almería para el uso de los ordenadores corporativos:

- No está permitido alterar la configuración física de los equipos ni conectar otros dispositivos a iniciativa del usuario, así como variar su ubicación.
- No está permitido alterar la configuración de software de los equipos, desinstalar o instalar programas o cualquier otro tipo de software distinto a la configuración lógica predefinida.
- La copia de seguridad periódica de los datos alojados en los servidores corporativos es responsabilidad del ATIC. Se utilizarán los espacios en sistemas de almacenamiento que

proporcionará el ATIC. Cada usuario será responsable de la integridad y copia de seguridad de la información almacenada en el ordenador que tenga asignado.

- El usuario deberá comprobar que su antivirus se actualiza con regularidad. En caso contrario, lo comunicará al ATIC para que tome medidas oportunas.
- El Usuario deberá cumplir con las instrucciones del ATIC con relación a la protección del equipo de trabajo (uso de antivirus, inclusión del equipo en el dominio, ...)
- Queda prohibida la conexión a la red corporativa de cualquier dispositivo electrónico no autorizado previamente por el ATIC.

4.2 De los dispositivos y soportes móviles corporativos

Los ordenadores portátiles de la UAL tienen la consideración de puestos de trabajo y se rigen por las normas apartado anterior. El uso al que están destinados y la posibilidad de que estos equipos se usen fuera del entorno de seguridad de la red corporativa de la UAL hacen necesarios procedimientos específicos de seguridad para actualizar los sistemas antivirus y el software instalado.

- Los equipos portátiles y los dispositivos o soportes informáticos están disponibles para permitir el desempeño de las funciones y tareas laborales encomendadas, estando prohibido el uso para otras finalidades personales.
- En caso de salida de dispositivos y soportes informáticos fuera del campus que contengan datos de carácter personal, sensibles o no, deberá el usuario de adoptar medidas técnicas de cifrado de datos para evitar sean accesibles en caso de pérdida o robo.

5. Uso de la red corporativa

La red corporativa es un recurso compartido y limitado, que sirve para el acceso de los usuarios internos de la UAL a la intranet o Internet, y para el acceso a las distintas aplicaciones informáticas corporativas.

La información que circula por la red de la UAL es de su propiedad, y como tal, es responsable del uso y protección de la misma.

El ATIC proporcionará a los empleados y estudiantes un servicio de conexión remota segura y cifrada al sistema de información de la Universidad, para cuando estos se encuentren fuera de la Universidad de Almería. Por consiguiente, no estará permitido el acceso desde el exterior a los equipos dentro de la Universidad sin esta conexión remota, segura y cifrada.

Los usuarios, además, deben cumplir una serie de normas establecidas por la UAL para el uso de la red corporativa:

- Las acciones sobre la red corporativa que intencionadamente dañen, retarden, pongan en peligro o accedan al trabajo de otros usuarios, sin autorización específica, están prohibidas.
- Está prohibido instalar o ejecutar en cualquier punto de la red informática programas que deterioren o incrementen en exceso la carga en cualquier punto de la misma, hasta el límite de llegar a perjudicar a otros usuarios o al rendimiento de la propia red. Esto incluye cualquier tipo de ensayo, experimento o actividad que, incluso pudiendo ser considerada legítima, perjudique el buen funcionamiento de la red.
- La utilización de Internet por parte de los usuarios autorizados debe limitarse a la obtención de información relacionada con el trabajo que se desempeña como personal de la UAL, debiendo por lo tanto evitarse la utilización que no tenga relación con las funciones del puesto de trabajo de usuario, y que no produzcan una mejora en la calidad del trabajo desarrollado.
- Queda prohibido cualquier uso comercial y/o privado no autorizado de la red corporativa de la Universidad de Almería.
- Está prohibido el uso de programas de compartición de contenidos en red, habitualmente utilizados para la descarga de archivos de música, vídeo, etc.
- Se prohíbe usar software de minado de criptomonedas.
- Está prohibido instalar o ejecutar en cualquier punto de la red informática programas que traten de descubrir información distinta de la del propio usuario. Esto incluye los “sniffer”, escáner de puertos, etc.
- La conexión a la red fija de comunicaciones de un nuevo equipo informático tiene que ser autorizada por el ATIC quien proporcionará a dicho equipo una dirección IP. Se prohíbe usar una dirección IP no proporcionada por el ATIC o intercambiarlas.

- Cualquier cambio de ubicación del dispositivo conectado a la red fija de comunicaciones debe ser comunicado al ATIC.
- Queda prohibida la instalación de servidores DHCP conectados a la red de comunicaciones.
- La Universidad de Almería, a través del ATIC, gestionará los rangos de direcciones IP que le han sido asignados por RedIRIS en base a criterios técnicos, de ahorro y eficacia.
- Cualquier acción sobre el cableado de la red de datos solo puede ser realizada por el ATIC, o bien por un tercero bajo su supervisión y aprobación.
- La red inalámbrica de la Universidad de Almería usa para su funcionamiento las bandas liberadas de frecuencia 2.400-2.483 Ghz y 5725-5850 Ghz. La Universidad de Almería gestionará estas bandas de frecuencias en sus instalaciones y, con el objeto de evitar interferencias con su red inalámbrica, prohíbe expresamente la instalación de cualquier punto de acceso de red inalámbrica que trabaje en las mencionadas bandas de frecuencia sin la autorización previa del ATIC.

6. Acceso a aplicaciones y servicios

La Universidad de Almería asignará a sus empleados una cuenta de usuario institucional única que permitirá identificar unívocamente al usuario.

La creación de esta cuenta institucional conlleva el alta automática y acceso a los usuarios, dependiendo del perfil correspondiente, a los siguientes servicios institucionales de gestión de la información:

- Creación de la cuenta de Campus.
- Creación de la cuenta en Microsoft 365 y Google Workspace.
- Creación de la cuenta en la aplicación portafirmas.

Los usuarios deben cumplir las siguientes medidas de seguridad establecidas por la Universidad de Almería para el uso de aplicaciones y servicios corporativos:

- Tanto el acceso al ordenador como a las distintas aplicaciones corporativas se hará identificándose y contando con la autorización del responsable correspondiente.

- La UAL podrá establecer para el acceso a determinados servicios la obligatoriedad del uso de un segundo factor de autenticación.
- La custodia de la contraseña, certificado digital u otro medio de autenticación es responsabilidad del usuario. Nunca debe utilizarse la cuenta de usuario asignada a otra persona.
- El ATIC establecerá normas de obligado cumplimiento respecto a las contraseñas: vigencia, calidad de estas, etc.
- Las contraseñas no deben anotarse, deben recordarse, o pueden almacenarse en aplicaciones específicas de gestión de contraseñas.
- Cuando se considere que la identificación de acceso se ha visto comprometida, se deberá comunicar al responsable correspondiente.
- Al abandonar el puesto de trabajo deben cerrarse las sesiones con las aplicaciones y bloquear la pantalla con contraseña.

Según el ENS (Anexo II. Medidas de Seguridad, Apartado 4. Marco operacional [op], Subapartado 4.2.1. Identificación [op.acc.1]), en relación a la identificación de los usuarios del sistema, nos indica que:

“[op.acc.1.4] Las cuentas de usuario se gestionarán de la siguiente forma:

a) Cada cuenta (de entidad, de usuario o proceso) estará asociada a un identificador único.

b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario.”

Por lo tanto, de conformidad con el apartado a) precedente, la UAL limitará el uso de cuentas de usuario genéricas (no directamente asociadas a una persona) solo a los casos y para los usos estrictamente necesarios.

Además, la UAL creará las instrucciones técnicas necesarias para garantizar el correcto flujo de información que permita el alta única de usuarios y la inhabilitación de las cuentas de usuario, cuando proceda, o modifique los permisos de acceso asociados a estas.

7. Acceso y tratamiento de datos personales

Las instrucciones descritas en este documento lo son en aplicación y en la observancia del cumplimiento del *Esquema Nacional de Seguridad, el Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales*.

Consiguientemente, dado que esta legislación trata de salvaguardar un derecho fundamental mediante la adopción de diferentes medidas de seguridad, técnicas y organizativas, el usuario que accede y trata información de carácter personal en el desempeño de las funciones y tareas universitarias, deberá atender a las siguientes obligaciones:

- Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal, conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la Universidad de Almería.
- Adoptar las medidas de seguridad adecuadas a los tipos de tratamientos que realice, de acuerdo con los principios de responsabilidad que las normas en protección de datos han establecido.

Y, además, debe conocer la definición de qué es un dato de carácter personal y en qué consiste un tratamiento de datos:

Dato personal: Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

7.1 Ficheros informáticos

De acuerdo con lo expuesto anteriormente deberá tenerse en cuenta:

- Claves de acceso al sistema informático. Las contraseñas de acceso al sistema informático son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. Queda prohibido, asimismo, emplear identificadores y contraseñas de otros usuarios para acceder al sistema informático.
- Bloqueo o apagado del equipo informático. Bloquear la sesión del usuario en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos de otras personas al equipo informático. Esto, sobre todo, deberá tenerse en cuenta, por parte del personal que esté en atención al público.
- Almacenamiento de archivos o ficheros en la red informática. Guardar todos los ficheros de carácter personal empleados por el usuario, en el servicio de almacenamiento institucional habilitado por la Universidad de Almería, en concreto por el ATIC, a fin de facilitar la realización de las copias de seguridad o respaldo y proteger el acceso frente a personas no autorizadas.
- Manipulación de los archivos o ficheros informáticos. Únicamente las personas autorizadas podrán introducir, modificar o anular los datos personales contenidos en los ficheros.
- No deberá usarse el correo electrónico para envíos de información de datos de carácter personal sensible. Se prohíbe usar correo electrónico (incluso el corporativo) para enviar información personal sensible (esto es, salud, ideología, religión, creencias, origen racial o étnico). Excepcionalmente, este tipo de envíos únicamente podrán realizarse si se adoptan los mecanismos necesarios para que la información no sea inteligible ni manipulada por terceros.
- Comunicación de incidencias y en su caso, violaciones de seguridad. Comunicar qué incidencias puedan afectar a la seguridad de los datos o los sistemas, dirigiéndose a la Comisión de Seguridad e informando de lo sucedido, cuando se tenga conocimiento de lo ocurrido.
- Desechado y destrucción de soportes de almacenamiento. No podrán tirarse soportes de almacenamiento (pendrive, disco duro o cualquier otro dispositivo que guarde información institucional) a papeleras o contenedores, de modo que pueda ser legible o fácilmente recuperable la información. A estos efectos, el dispositivo deberá ser siempre destruido mediante cualquier medio de destrucción que no permita la recuperación de la información. El ATIC dispone de una destructora de discos duros.

7.2 Ficheros en papel

En relación con los ficheros o cualquier otro dispositivo o soporte que permita almacenaje en papel, deberán cumplir con las siguientes diligencias:

- Custodia de llaves de acceso a archivadores o dependencias. Mantener debidamente custodiadas las llaves de acceso a locales o dependencias, despachos, armarios, archivadores u otros elementos con soportes o documentos en papel con datos personales.
- Cierre de despachos o dependencias. Cerrar con llave la puerta al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
- Almacenamiento de soportes o documentos en papel. Guardar los soportes o documentos con información personal en un lugar seguro cuando estos no sean usados, en particular, fuera de la jornada laboral. Cuando estos soportes o documentos no se encuentren almacenados, por revisarse o tramitarse, será la persona que deba custodiar e impedir que un tercero no autorizado pueda acceder.
- No dejar en fotocopiadoras, faxes o impresoras papeles con datos de carácter personal. Asegurarse de que no quedan documentos impresos que contengan datos personales, en la bandeja de salida de fotocopiadoras, impresoras o faxes.
- Documentos no visibles en los escritorios, mostradores u otro mobiliario. Se mantendrá la confidencialidad de los datos personales de los documentos depositados o almacenados en los escritorios, mostradores u otros muebles; especialmente en las zonas de atención al público, guardando así una adecuada política de prevención de mesas limpias.
- Desechado y destrucción de soportes o documentos en papel con datos personales. No tirar soportes o documentos en papel, que contengan datos personales, a papeleras o contenedores, de modo que pueda ser legible o fácilmente recuperable la información. A estos efectos, deberá ser siempre desechada o destruida mediante las destructoras de papel de las que dispone la Universidad de Almería. Se prohíbe terminantemente echar en papeleras, contenedores de cartón o papel, soportes o documentos, que contengan datos personales sin destruir.
- Archivo de soportes o documentos. Los soportes o documentos en papel se almacenarán según el criterio de archivo de la Universidad de Almería. Dichos criterios

deberán garantizar la correcta conservación de los documentos, su localización y consulta de la información. No podrá acceder o utilizar los archivos pertenecientes a otros departamentos, que compartan la sala o dependencia habilitada a archivo.

- Traslado de soportes o documentos en papel con datos de carácter personal. En los procesos de traslado de soportes o documentos se adoptarán medidas dirigidas a impedir el acceso o manipulación por terceros y, de manera que no se vea el contenido, sobre todo, si hay datos personales.
- Traslado de dependencias. En caso de cambiar de dependencia, en el proceso de traslado de los soportes o documentos en papel, se deberá realizar con el debido orden. Asimismo, se mantendrá fuera de la vista de cualquier personal de la entidad, documentos o soportes en papel con datos personales.
- Envío de datos personales sensibles en sobre cerrado. Si se envían a terceros ajenos a la Universidad de Almería, datos especialmente sensibles (esto es, salud, ideología, religión, creencias, origen racial o étnico) contenidos en soporte o documento papel, se debe realizar en sobre cerrado y, en cualquier caso, tener presente que haya de efectuarse por medio de correo certificado o a través de una forma de correo ordinario que permita su completa confidencialidad.
- Comunicación de incidencias y, en su caso, violaciones de seguridad que afecten a la seguridad de datos de carácter personal. Comunicar las incidencias de las que tenga conocimiento y que puedan afectar a la seguridad de los datos personales a la Comisión de Seguridad.

8. Sobre la Gestión de Incidentes de Seguridad

La Universidad de Almería cuenta con un Procedimiento de gestión de incidentes y notificación de brechas de seguridad en datos de carácter personal, que define y establece los procedimientos mediante los cuales se deben identificar, catalogar, resolver y/o escalar todas aquellas entradas con eventos de seguridad.

De conformidad con el art. 4.12 RGPD, se entiende por violación de seguridad de los datos personales, aquel incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Por tanto, toda violación de seguridad tendrá la

consideración de incidente, pero no todo incidente supondrá una violación de seguridad, sino únicamente aquellos que afecten a datos de carácter personal.

Teniendo en cuenta los aspectos destacados a los que aluden los apartados anteriores, 7.1 Ficheros Informáticos y 7.2 Ficheros en Papel, relacionados como brechas de seguridad en los que se vean implicados “datos personales”, será de obligado cumplimiento para todo el personal de la UAL, informar a la mayor brevedad posible a la Comisión de Seguridad, sobre cualquier hecho detectado para que se evalúe y se revise de la forma adecuada.

Vía de comunicación de incidencias con la Comisión de Seguridad:

- a través del email consulta.comision.seguridad@ual.es
- a través del Formulario de notificación de incidencias de protección de datos, de la página web de la Comisión de Seguridad <http://seguridad.ual.es>

Cualquier otro tipo de incidencia de seguridad TIC se comunicará al ATIC a través de su Centro de Atención a Usuarios:

- Teléfono 950 015999
- <http://caustic.ual.es>

9. Incumplimientos

Ante el incumplimiento de estas normas y de manera independiente de las actuaciones investigadoras y/o sancionadoras que la UAL realice para determinar responsabilidades, el ATIC podrá adoptar las medidas técnicas necesarias para garantizar el restablecimiento de los servicios.

10. Disposición Adicional Primera

La Comisión de Seguridad revisará anualmente estas normas.

11. Disposición Adicional Segunda

Estas normas han sido redactadas con género masculino como género gramatical no marcado. Cuando proceda, se entenderá en género femenino, dependiendo de las personas o cargos afectados por las denominaciones.

12. Disposición Derogatoria

Quedan derogadas las “Normas de uso de los sistemas de información de la UAL”, aprobadas por el Consejo de Gobierno en fecha 11 de junio de 2019.

13. Disposición Final

Estas Normas de uso de los sistemas de información de la UAL serán de aplicación para toda la Comunidad Universitaria desde el día siguiente a su aprobación por el Consejo de Gobierno.