**NORMATIVA DE LA UNIVERSIDAD PÚBLICA DE NAVARRAEN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL** (A.19/2011. Consejo de Gobierno 11-5-2011)

# NORMATIVA DE PROTECCIÓN DE DATOS

## CAPITULO I.-DISPOSICIONES GENERALES

### Artículo 1º. Objeto.

La presente normativa tiene por objeto dotar a la Universidad Pública de Navarra de las disposiciones necesarias para garantizar, en su ámbito, la aplicación y el cumplimiento de la normativa vigente en materia de protección de datos de carácter personal, constituida fundamentalmente por la Ley Orgánica 15/1999 de protección de datos de carácter personal y el reglamento que la desarrolla, aprobado por Real Decreto 1720/2007 de 21 de diciembre, y demás disposiciones que en esta materia resulten de aplicación.

### Artículo 2º. Ámbito de aplicación.

La presente disposición será de aplicación a los datos de carácter personal que figuren registrados en soportes físicos e informáticos o electrónicos de la Universidad Pública de Navarra, que los hagan susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos.

### Artículo 3º.Calidad de los datos

Los datos de carácter personal que sean recabados en los distintos procedimientos o actividades que se sigan en la Universidad Pública de Navarra, para así someterlos a su tratamiento, deberán ser adecuados, pertinentes, no excesivos en relación con la finalidad para la cual hayan sido recabados, y deberán servir a fines directamente relacionados con las competencias y funciones de la institución universitaria.

### Artículo 4º. Usos y finalidades del tratamiento

Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos fueron recogidos. No se considerará incompatible el tratamiento posterior de los datos para fines históricos, estadísticos o científicos.

**Artículo 5º.Recogida de datos**

1.-Los datos de carácter personal se recabarán a través de instancias, formularios o por aquellos medios electrónicos que en cada caso y respecto a cada procedimiento la Universidad determine.

La unidad responsable que requiera recabar datos personales deberá constatar previamente que dichos datos figuran en la relación de ficheros declarados, a tal efecto, por la Universidad. En el supuesto que dichos datos no puedan considerarse incluidos en la Resolución de creación de ficheros, publicada y comunicada a la Agencia de Protección de Datos de acuerdo con lo previsto en el artículo siguiente, no se procederá a la recogida de datos.

En cualquier caso podrá dirigir la correspondiente consulta al Servicio Jurídico.

**Artículo 6º. Procedimiento de creación, modificación y supresión de ficheros.**

La creación, modificación y supresión de ficheros de datos personales de la Universidad Pública de Navarra se realizará por Resolución del Rector, que deberá publicarse en el Boletín Oficial de Navarra y notificarse a la Agencia de Protección de Datos, de acuerdo con la normativa establecida al efecto.

Cuando una unidad de la Universidad necesite por razones de su competencia recabar datos distintos a los mencionados en los ficheros registrados de la Universidad Pública de Navarra, lo solicitará a la Secretaría General mediante escrito motivado. En caso de estimarse la solicitud, el Servicio Jurídico, llevará a cabo las actuaciones procedimentales precisas de cara a la modificación de los ficheros y su regularización ante los órganos competentes. La solicitud de creación de nuevos ficheros seguirá el mismo procedimiento.

En la Resolución de creación de ficheros se hará constar el órgano responsable del mismo, que será designado entre los Vicerrectores, Gerente, Secretario General y Directores de Centro. Asimismo, los Responsables de cada fichero deberán designar un encargado interno del tratamiento entre el personal adscrito a su unidad, que realizará el apoyo en las funciones que aquellos tienen encomendadas y supervisará la aplicación de las medidas contenidas en la presente disposición, y , en su caso, en el documento de seguridad, debiendo poner de manifiesto cuantas incidencias tenga conocimiento.

Recabar datos distintos a los contenidos en los ficheros registrados sin contar con la previa autorización de la Secretaría General, o recabarlos con anterioridad a su inclusión formal en los ficheros registrados, podrá dar lugar, en su caso, a responsabilidades disciplinarias, respondiendo frente a terceros y frente a la propia Universidad.

Los ficheros de datos de carácter personal que contengan datos a los que resulten de aplicación medidas de seguridad de nivel alto y medio deberán contar con un Responsable de seguridad de acuerdo con lo establecido en el documento de seguridad.

**Artículo 7º. Documento de Seguridad.**

La Universidad Pública de Navarra implantará un documento de seguridad que será mantenido y puesto al día por la o las unidades que la Gerencia determine y de obligado cumplimiento para todo el personal de la Universidad.

## CAPITULO II.- DERECHOS DE LOS INTERESADOS.

### Artículo 8º. Información Sobre el Tratamiento

1.-El interesado deberá ser informado de la finalidad determinada, explícita y legítima del tratamiento. Cualquiera que sea el medio o soporte de recogida de los datos personales que se utilice, deberá contener la siguiente información dirigida al interesado cuyos datos se pretenden recabar:

a)La existencia de un fichero automatizado con datos de carácter personal, la finalidad de recogida de estos y los destinatarios de la información.

b)El carácter obligatorio o facultativo de la respuesta a las preguntas que le sean planteadas.

c)Las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d)La posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

e)La identidad y dirección del responsable del tratamiento o su representante.

No será necesaria la información de los apartados b) y c) anteriores si del contenido se deduce claramente la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. La Universidad informará siempre a los interesados la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, y del órgano ante el que se ejercitan tales derechos.

2.- Cuando la captura de datos sea presencial se informará de viva voz al interesado de la información a que se refiere el apartado primero del presente artículo, en su caso, se le entregará un formulario que contenga una cláusula informativa de protección de datos, como requisito previo para continuar con el trámite correspondiente.

Cuando la captura de datos personales no sea presencial, la información, a la que se refiere el apartado primero del presente artículo, será proporcionada al interesado en función de las características del medio utilizado para su captación, debiendo articularse la fórmula adecuada a través de la que se pueda acreditar su recepción.

El texto informativo deberá incluirse, en el impreso correspondiente, siempre que se realice una recogida de datos, salvo que se hubiera informado previamente al afectado. En este sentido, se deberá asegurar la recepción de la información por el interesado. A tal efecto la nota informativa se incluirá en los impresos que vayan a ser firmados expresamente por aquel. En la misma medida tratándose de medios electrónicos se

deberá asegurar la visualización de la información por el interesado como paso previo a la tramitación electrónica correspondiente.

3.- Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por la Universidad dentro de los tres meses siguientes al momento de registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, y de la identidad y dirección del responsable del tratamiento.

4.- Corresponderá al Servicio Jurídico de la Universidad Pública de Navarra la redacción de las fórmulas o cláusulas informativas relativas al tratamiento de datos de carácter personal que necesariamente deben constar en todos los impresos, solicitudes, contratos y medios que se utilice para recabar datos personales, con independencia de que el medio utilizado sea físico o electrónico.

5**.-** Las cláusulas de protección de datos en las que el interesado haya declarado estar informado, o haya consentido, en su caso, el tratamiento de sus datos, deberán constar en los expedientes administrativos de los que traen su causa.

**Artículo 9º. Capacidad.**

Los derechos de acceso, rectificación y cancelación de datos son personalísimos y serán ejercicios únicamente por el interesado, por lo que para su ejercicio será necesario que éste acredite su identidad. Por esta razón no serán atendidas las solicitudes de ejercicio de estos derechos que se efectúen a través de tercero, o por el propio interesado por teléfono, correo electrónico o cualquier otro medio que no permita acreditar la identidad del interesado.

El interesado podrá actuar a través del representante legal cuando aquel se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los derechos en cuyo caso será necesario que el representante legal acredite tal condición. Sin perjuicio de lo anterior, los derechos antes mencionados podrán ejercerse por el interesado a través de representante apoderado específicamente para el ejercicio de los derechos mediante:

- Documento de apoderamiento original que derive directa e inequívocamente del interesado, titular del derecho, con la firma de éste último autentificada a través de medio autorizado en Derecho.
- Escritura pública de apoderamiento autorizada por un Notario Público.

**Artículo 10º.Acceso a los datos personales. Sistemas de consulta.**

1.- Los interesados tienen derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros de la Universidad Pública de Navarra. Los derechos de acceso se ejercitarán mediante escrito dirigido al Responsable del fichero, y a través del Registro General de la Universidad o por cualesquiera de los medios

previstos en el Artículo 38.4 de la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En el escrito deberán figurar las siguientes determinaciones y requisitos:

(a) Nombre, apellidos y fotocopia del documento nacional de identidad del interesado y, en los casos que se admita, de la persona que lo represente, así como el documento acreditativo de tal representación. La fotocopia del documento nacional de identidad podrá ser sustituida por copia de documento equivalente como miembro de la comunidad universitaria siempre que acredite su identidad conforme a Derecho.

(b) Petición en que se concreta la solicitud.

(c) Sistema de consulta del fichero elegido.

(d) Domicilio a efectos de notificaciones, fecha y firma del solicitante.

(e) Documentos acreditativos, en su caso, de la petición que formula.

2.-El interesado podrá optar en el escrito, por uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración o implantación material del fichero lo permita:

-Visualización en pantalla.

-Escrito, copia o fotocopia remitida por correo.

-Cualquier otro procedimiento que sea adecuado a la configuración o implantación material del fichero, ofrecido por el responsable del mismo.

No obstante, la Universidad Pública de Navarra, podrá determinar el sistema de consulta cuando el solicitado por el interesado perturbe la normal prestación de los servicios.

3.- La respuesta a la consulta del interesado, cualquiera que sea el soporte en que fuera facilitada, se dará en forma legible e inteligible, previa transcripción en claro de los datos del fichero, en su caso, y comprenderá todos los datos de base del interesado que sean accesibles, los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron.

En el caso de que los datos provengan de fuentes diversas, deberán especificarse las mismas identificando la información que proviene de cada una de ellas.

4.- El responsable del fichero deberá resolver la solicitud de acceso, en el plazo máximo de un mes desde la presentación de la misma. La obligación de resolver y contestar a las solicitudes de acceso persiste con independencia de que figuren o no datos personales del interesado en el fichero correspondiente.

Deberá dejarse siempre constancia de la respuesta de la administración al ejercicio del derecho de acceso, por parte del interesado, cualquiera que sea la fórmula o el soporte en el que fuera facilitada, y de su recepción por el interesado.

5.- El error en la identificación del responsable del fichero al que se dirija la solicitud no impedirá su tramitación, siempre y cuando del contenido de la misma puedan identificarse claramente los datos a los que se pretende acceder. A tal efecto, el receptor de la solicitud deberá remitirla a la mayor brevedad posible al responsable del fichero correspondiente.

**Artículo 11º. Rectificación y Cancelación de los datos.**

1.- Cuando el acceso a los ficheros revelare que los datos del interesado sean inexactos o incompletos, inadecuados o excesivos, éste podrá solicitar la rectificación o, en su caso, si procede, la cancelación de los mismos.

2.- Los derechos de rectificación y cancelación se harán efectivos dentro de los diez días siguientes al de la recepción de la solicitud. Si los datos rectificados o cancelados hubieran sido cedidos previamente, se deberá notificar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, a su vez, la lleve a cabo en su fichero.

3.- Los derechos de rectificación y cancelación no procederán cuando pudiesen causar un perjuicio a intereses legítimos del interesado o de tercero o cuando existiese una obligación legal de conservar los datos, cuando exista una relación contractual, cuando formen parte de un expediente administrativo, o cuando su mantenimiento sea preciso para el adecuado cumplimiento de los fines de la Universidad.

**Artículo 12º. Bloqueo de los Datos.**

En los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización. Se exceptúa, no obstante, el supuesto en el que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.

**Artículo 13º.Procedimiento.**

Las solicitudes de acceso, cancelación o rectificación, dirigidas a los Responsables del fichero, de acuerdo con lo previsto en el artículo décimo**,** serán tramitadas a través de la Secretaría General de la Universidad. Recibida la petición, por el Servicio Jurídico se comprobará el cumplimiento de los requisitos formales indicados.

Seguidamente se remitirá solicitud al Responsable del Fichero, quien bien directamente o a través del Encargado Interno del Tratamiento correspondiente recabará la información solicitada y la remitirá, en el caso del derecho de acceso en el plazo

máximo de diez días hábiles, y de cinco días hábiles en el caso de los derechos de rectificación y cancelación, al Servicio Jurídico.

La Secretaría General mantendrá un Registro de accesos, rectificaciones y cancelaciones.

La desestimación de la petición de acceso rectificación o cancelación deberá ser motivada y notificarse al interesado dentro del mismo plazo correspondiente para su resolución.

La resolución será adoptada por el Secretario General de la Universidad y se comunicará al interesado remitiéndose al domicilio que éste hubiere señalado al efecto.

**Artículo 14º.Cesión de Datos**.

1.- La Universidad Pública de Navarra no realizará otras cesiones de datos personales que las previstas en las leyes y otras normas de obligado cumplimiento, las que impliquen el desarrollo de las relaciones jurídicas que tenga establecidas con los afectados y las necesarias para el cumplimiento de las finalidades que tiene encomendadas, así como las cesiones necesarias a otras administraciones públicas para el ejercicio de las competencias propias de éstas sobre las mismas materias, que según lo previsto en la normativa vigente están excluidas de tratamiento.

2.- La cesión de datos de carácter personal se efectuará en la forma y con las limitaciones y derechos que otorga la LOPD. En particular:

– No se cederán datos a terceros salvo que se cuente con el consentimiento del interesado o éste no sea preciso.
– En cualquier caso, los datos sólo podrán ser cedidos para fines relacionados con el ejercicio de funciones legítimas del cedente y del cesionario.

Las cesiones de datos previstas para cada fichero figurarán en su documento de seguridad.

3.- La cesión o el acceso a datos personales para la prestación de servicios a la Universidad Pública de Navarra deberá ser previamente autorizada por el Gerente de la Universidad. Cualquier cesión de estas características, realizada por una unidad, sin autorización previa del Gerente, será responsabilidad exclusiva de quien la realice, frente a terceros y frente a la Universidad.

La revelación de datos en estos supuestos requiere la celebración de un contrato entre el titular del fichero y el prestador del servicio en el que se acuerde la confidencialidad de la información, la finalidad exclusiva de tratamiento de datos para la prestación del servicio, la obligación de destrucción de los datos y/o devolución de los soportes una vez prestado el servicio, la declaración del cesionario de cumplir con las medidas de

seguridad exigidas por la ley, así como la prohibición de cesión sucesiva salvo autorización expresa del cedente, todo ello de acuerdo con lo establecido en el artículo 12 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

La realización de estas cesiones deberá ser reflejada en el Registro de Incidencias de la Universidad Pública de Navarra.

**Artículo 15º. Privacidad y Confidencialidad.**

Con carácter general en todos los contratos que se formalicen con empresas para la prestación de servicios a la institución universitaria que entrañe el acceso o conocimiento directa o indirectamente de datos personales, deberán contener las correspondientes cláusulas de confidencialidad y deber de secreto. Específicamente en aquellos contratos que se formalicen con empresas cuyo objeto consista o implique necesariamente el acceso o tratamiento de datos personales además deberán reflejar las obligaciones establecidas en la normativa de protección de datos.

## CAPÍTULO III.

## MEDIDAS DIRIGIDAS A GARANTIZAR LA APLICACIÓN DE LOS PRINCIPIOS EN MATERIA DE PROTECCIÓN DE DATOS

**Artículo 16. Disposición General.**

Los distintos órganos de gobierno, áreas, servicios y unidades de la Universidad Pública de Navarra, y sus empleados, podrán hacer uso de los datos personales contenidos en los ficheros de la Universidad, dentro del ámbito de las competencias y funciones que tienen atribuidas, y siempre que los datos a los que se acceda se utilicen para la misma finalidad que motivó su recogida y tratamiento.

**Artículo 17º. Medidas Generales de Actuación**

1.-Todo empleado de la Universidad Pública de Navarra con acceso a los datos de carácter personal, ya sea a los contenidos en soportes físicos, ya sea a los contenidos en sistemas de información, tiene el deber de guardar secreto y de confidencialidad de los datos personales de los que tenga conocimiento y, la obligación de garantizar, en la medida de sus posibilidades, la intimidad, integridad y confidencialidad de la información que maneja. Obligaciones que subsistirán aún después de finalizar sus relaciones con la institución universitaria.

2.-Asimismo, deberán cumplir las normas de seguridad establecidas reglamentariamente y las contenidas en el documento de seguridad, y que persiguen evitar la alteración pérdida y acceso y tratamiento no autorizado, a los datos de carácter personal que constan en los archivos automatizados o no de la Universidad.

Y a modo enunciativo vendrán obligados a cumplir las siguientes reglas de actuación:

a) Respetar, en todo momento, los derechos de información, acceso, rectificación y cancelación de los afectados por ficheros de datos de carácter personal.

b) No realizar copias, no autorizadas, de datos de carácter personal.

c)La atención al público se realizará teniendo en cuenta que no deberá depositarse en la mesa o mostrador documentación visible en la que se pueda identificar datos personales de personas distintas a las que se les está dirigiendo la atención.

d) En la gestión de procedimientos administrativos se utilizarán exclusivamente los programas que facilite la Universidad. Dentro de lo posible, el usuario mantendrá limpio de programas dañinos su puesto de trabajo.

e) Está prohibida la cesión de identificaciones y de contraseñas. Cada identificación y contraseña es de uso individual y confidencial, será responsabilidad del titular la utilización que de ellas se haga.

f) Es obligatorio informar al responsable de su unidad de cualquier acceso no autorizado, anomalía, amenaza, acceso con riesgo para la seguridad observado o cuando se conozca, lo más rápidamente posible.

g) Siempre que se utilicen ficheros temporales creados a partir de ficheros a los cuales tenga acceso, mantendrá las medidas de seguridad adecuadas para evitar el acceso no autorizado a ellos y eliminará el fichero temporal en cuanto termine de utilizarlo.

h) Asimismo se deberá procurar que las pantallas de los ordenadores que tengan abiertas aplicaciones en la que figuren datos personales no sean visibles por las personas que acuden o demandan información en las distintas oficinas y dependencias de la universidad respectivamente.

i)Al finalizar la jornada laboral no deberá quedar encima de la mesa, ni en lugar visible o accesible, ninguna documentación, expediente administrativo, informe, etc. en la que figuren datos personales, siendo responsable el empleado público correspondiente de asegurar que dicha documentación quede guardada en los armarios o archivadores que deberán disponer de cerradura adecuada.

j) Asimismo, se deberá proceder a apagar los ordenadores de uso personal a la finalización de la jornada laboral. Las claves de acceso deberán de ser conservadas por el Jefe de la Sección, Director de Servicio o responsable de la unidad de que se trate.

**Artículo 18º.Publicación en Espacios Físicos.**

1.- La publicación de cualesquiera actos administrativos que contenga datos personales en los tablones de anuncios físicos de la Universidad deberá ser temporal, por el tiempo indispensable para servir de notificación. Transcurrido dicho plazo deberán ser retirados

de los tablones de anuncios, siendo responsable el servicio que gestione el procedimiento de que se trate.

2.-La publicación de los resultados de los procesos de evaluación académica de los estudiantes de la Universidad podrá realizarse, en los tablones de anuncios físicos del Aulario de Arrosadía, o Tudela, o en la Escuela de Estudios Sanitarios, o en los ubicados en los Centros o Departamentos correspondientes, cualquiera que sea el tipo de evaluación y con independencia de que se trate de calificaciones parciales, globales, provisionales o definitivas.

Los listados únicamente contendrán la identificación del estudiante, mencionando los apellidos y el nombre del estudiante, o simplemente el DNI o el NIA y la calificación obtenida. Los tablones de anuncios en los que se publiquen dichos listados, deberán estar cerrados, con llave o por cualquier otro medio adecuado, en aras a evitar su sustracción, y copia.

La publicación de las calificaciones será temporal por el tiempo indispensable para servir de notificación a los estudiantes.

**Artículo 19º. Publicación en el sitio WEB de la Universidad.**

1.- La publicación de documentación, en el sitio web de la Universidad se realizará teniendo en cuenta que la publicación de datos personales se deberá ajustar a la normativa sobre protección de datos, y en este sentido se deberá atender las reglas contenidas en los apartados siguientes.

2.- La publicación de datos personales relativos a miembros de un servicio, sección departamento o centro se realizará únicamente respecto al nombre y apellidos y al puesto que ocupan en la institución universitaria, el teléfono de la unidad y la dirección de correo electrónico. El sistema de búsqueda será el inverso.

La publicación de cualquier dato personal distinto de los anteriores requerirá el consentimiento del interesado, salvo que se trate de actos, acuerdos o documentos, adoptados por los órganos de la Universidad en ejercicio de sus funciones que exijan su publicidad, debiendo asegurarse el acceso restringido a los miembros de la comunidad universitaria.

3.- La publicación en las distintas páginas del sitio web de la Universidad, de actos administrativos conteniendo datos de carácter personal, correspondientes a la tramitación de procedimientos, de concurrencia competitiva u otros cuya convocatoria o disposición así lo establezca, es responsabilidad del servicio gestor de dicho procedimiento administrativo. Dicha publicación no podrá extenderse más allá de los plazos previstos para la tramitación del procedimiento correspondiente.

4.-La tramitación de cualquier procedimiento a través de la web se realizará con sujeción a lo dispuesto en la normativa de protección de datos y a lo establecido en la presente disposición, debiendo asegurarse en el diseño del procedimiento telemático que el interesado queda perfectamente informado de las obligaciones contenidas en el artículo 5 de la Ley Orgánica de Protección de Datos y correspondiente reglamento.

## CAPÍTULO IV.- FICHEROS DE VIDEOVIGILANCIA

### Artículo 20º. Disposición General.

La Universidad Pública de Navarra implantará cámaras de video-vigilancia en las dependencias e instalaciones cuando resulten necesarias para la satisfacción de finalidades lícitas y legítimas. Se considerará legítima la utilización de las mismas con los fines siguientes:

1. Control del acceso a los edificios o a parte de estos.
2. Control del acceso a los aparcamientos y garajes.
3. Seguridad interior.
4. Seguridad de las instalaciones deportivas.
5. Custodia de bienes valiosos.

La utilización de sistemas para la captación y/o tratamiento de imágenes con fines de video-vigilancia y seguridad en la Universidad Pública de Navarra se llevará a cabo de acuerdo con lo previsto en la normativa vigente en la materia.

Cuando la Universidad acuda a la contratación de una empresa de servicios para la gestión de las cámaras de video-vigilancia, la empresa contratada deberá estar debidamente autorizada por el Ministerio del Interior, que conforme al artículo 5 de la Ley 23/1992, de Seguridad Privada, pueda prestar el servicio de vigilancia y protección de bienes e instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad. En el contrato de servicios de seguridad que se formalice se designará a la empresa de seguridad como encargada del tratamiento de las imágenes, siendo esta última la responsable del Documento de Seguridad en el caso de que se trate de un sistema de grabación de imágenes.

### Artículo 21º. Responsables de la instalación de sistemas de video-vigilancia.

La instalación, mantenimiento y visionado de sistemas de video-vigilancia requerirá la autorización previa del Gerente de la Universidad.

El Gerente de la Universidad será el Responsable del Tratamiento de los datos personales del fichero de video vigilancia tal y como consta en la correspondiente resolución de creación del fichero. Asimismo, designará un encargado interno del tratamiento respecto a cada una de las unidades en las que se ubiquen las cámaras de video-vigilancia, que realizará la supervisión del cumplimiento de los fines anteriormente especificados, y velará para que el tratamiento de las imágenes captadas se ajuste, en todo momento, a lo previsto en la declaración del fichero y a las medidas de seguridad que le afectan.

### Artículo 22º. Criterios de Uso.

Las imágenes captadas por los sistemas de video-vigilancia instalados únicamente podrán ser visionadas y grabadas por quien en cada caso se designe a tal efecto y en los locales habilitados para ello.

La utilización de videocámaras con fines de vigilancia se atendrá a los siguientes criterios:

1. Se señalizarán los espacios vigilados con la identificación establecida por la Agencia Española de Protección de Datos.

2. Los monitores o terminales utilizados para la video-vigilancia habrán de instalarse de forma que no resulten accesibles a terceros no autorizados. Se establecerán las limitaciones adecuadas para impedir el acceso físico a los espacios donde se ubiquen.

3. En el caso de que se trate de sistemas de grabación de imágenes, éstas se conservarán durante un periodo máximo de un mes.

4. Si se constatase la comisión de un delito o infracción, se notificarán los hechos a la Secretaría General.

5. Queda expresamente prohibida:

a) La captación intencional de imágenes de la vía pública, así como edificios o espacios ajenos a la Universidad, fuera de aquellas que resulten inevitables en función de la finalidad perseguida.

b) La captación de imágenes en espacios privados como son baños, vestuarios, taquillas personales y otros análogos.

c) La captación de sonidos y en especial de conversaciones privadas.

d) La difusión por cualquier medio de las imágenes captadas.

**Artículo 23º.Sistemas de Grabación de Imágenes.**

1.-Serán sistemas de grabación de imágenes los que realicen grabaciones en una unidad de disco de las imágenes obtenidas.

2.- Las instalaciones en las que se encuentren los monitores y sistemas de grabación dispondrán preferentemente de un acceso físico controlado.

Cuando no sea posible establecer controles de acceso físico, la disposición de los monitores impedirá el acceso a la información por terceros ajenos a la instalación. En todo caso, los equipos de grabación habrán de disponerse de forma que resulten inaccesibles a terceros no autorizados.

Se contará con un registro de los usuarios que cuenten con una clave o cualquier otro medio que permita acceder a las instalaciones o mobiliario que contenga información protegida.

Los sistemas habrán de contar con un control de acceso lógico con asignación distribución y almacenamiento de contraseñas diferenciadas para cada usuario. Estas se almacenarán de forma ininteligible y se cambiarán periódicamente. Podrán articularse controles distintos que garanticen la seguridad de manera análoga a la anterior.

3.-Los soportes que contengan imágenes se conservarán de manera que resulten inaccesibles a terceros no autorizados.

Las grabaciones se etiquetarán de manera que se garantice la completa destrucción de la información que contienen.

El desechado de los soportes que contengan imágenes captadas por los sistemas garantizará la absoluta inaccesibilidad a las imágenes que contienen.

Si se prevé el acceso al fichero a través de redes de comunicaciones se habrá de proteger el entorno de comunicación y fijar un control de acceso lógico en los términos establecidos en el apartado anterior.

**Artículo 24º.Cancelación de las Imágenes.**

El plazo de cancelación de las imágenes grabadas será de un mes desde su captación, una vez trascurrido este plazo, éstas se bloquearán, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión de las imágenes.

**Artículo 25º. Obligaciones de los Usuarios de los Sistemas de Video-vigilancia.**

1. Los usuarios de los sistemas habrán de guardar el necesario secreto respecto a cualquier tipo de información de carácter personal que se conozca en función del trabajo desarrollado.

2. Mantendrán en secreto sus claves de acceso al sistema, ya que estas son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que se pudiesen derivar de su mal uso, divulgación o pérdida, casos en los que se deberá notificar la incidencia.

3. Cambiarán las contraseñas a petición del sistema cuando se le indique. Se comunicarán las incidencias de seguridad de las que tenga conocimiento.

4. No se copiará la información contenida en cualquier soporte sin autorización expresa del responsable. Queda igualmente prohibido el traslado de cualquier soporte en el que se almacene información fuera de los locales de la Universidad.

5. Guardarán todos los soportes físicos que contengan información en un lugar seguro cuando no se utilicen, particularmente fuera de la jornada laboral.

6. Únicamente las personas autorizadas podrán introducir o anular los datos contenidos en el fichero objeto de protección.

Queda expresamente prohibido:

1. Utilizar identificaciones o contraseñas de otros usuarios para acceder a los sistemas automatizados.

2. Intentar modificar o acceder al registro de accesos.

3. Burlar las medidas de seguridad establecidas.

4. El uso de la red de la Universidad, los sistemas informáticos y cualquier otro medio puesto a disposición del usuario para vulnerar derechos de terceros, los propios de la organización o bien para la realización de actos que pudiesen ser considerados ilícitos.

**Artículo 26º.Derecho de información en la recogida de datos.**

La información de la utilización de un sistema de video-vigilancia se realizará mediante la colocación del distintivo informativo establecido por la Agencia Española de Protección de Datos en su instrucción 1/2006, que se ubicará en los accesos a las zonas vigiladas, sean estos exteriores o interiores. Si el lugar vigilado dispone de varios accesos se deberán colocar en todos ellos al objeto de que la información sea visible con independencia de la vía de acceso.

Además, en el interior de los locales, se dispondrá de un impreso en el que se informará, en el caso de sistemas de grabación, de:

1. La existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información.

2. La posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.

3. La identidad y dirección del responsable del tratamiento o, si es el caso, de su representante.

## DISPOSICIONES ADICIONALES

**Primera.**

La Universidad, incluirá en sus planes de formación de los empleados públicos, cursos sobre la normativa vigente en materia de protección de datos y aplicable a la institución universitaria, y más concretamente, sobre las funciones y obligaciones que les incumben en materia de confidencialidad, deber de secreto, y tratamiento de datos personales.

**Segunda.**

Todos los plazos previstos en esta normativa se computarán conforme a lo dispuesto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

**Tercera.**

El Servicio Jurídico de la Universidad elaborará los modelos normalizados de información y de solicitudes que sean necesarios para el ejercicio de los derechos correspondientes en materia de protección de datos y prestará el apoyo y asesoramiento que resulte necesario para la aplicación de las presentes disposiciones.

## DISPOSICIONES TRANSITORIAS

**Primera.**

En el plazo de seis meses desde la entrada en vigor de la presente normativa se revisarán los ficheros existentes en la Universidad y el Documento de seguridad, debiendo instarse su modificación o adaptación, en su caso, a la misma.

**Segunda.**

En el plazo de un mes siguiente a la aprobación de la presente normativa se procederá al nombramiento de los Encargados Internos de los distintos ficheros vigentes en la actualidad.

## DISPOSICIÓN FINAL

La presente normativa entrará en vigor al día siguiente de su publicación en el Boletín Oficial de Navarra.