

## **REGLAMENT DE VIDEOVIGILÀNCIA DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA**

*(Aprovat pel Consell de Govern en la sessió de 17 de desembre de 2009)*

Les instal·lacions de sistemes de videovigilància en l'àmbit de la Universitat Politècnica de València generen múltiples responsabilitats, pel que fa a la protecció de les dades de caràcter personal, derivades del tractament d'imatges que realitzen aquests sistemes.

La seguretat i vigilància de les instal·lacions i el mobiliari de la UPV no és incompatible amb el dret fonamental a la protecció de la imatge com a dada personal, sempre que es respecte la normativa existent en matèria de protecció de dades.

La captació i gravació d'imatges amb fins de vigilància i control, com és el cas que ens ocupa, es troba plenament sotmesa al que disposa la LOPD, sobretot quan els afectats resulten perfectament identificables, dins de l'àmbit on es realitza la captació d'imatges.

## **REGLAMENTO DE VIDEOVIGILANCIA DE LA UNIVERSIDAD POLITÉCNICA DE VALENCIA**

*(Aprobado por el Consejo de Gobierno en su sesión de 17 de diciembre de 2009)*

Las instalaciones de sistemas de videovigilancia en el ámbito de la Universidad Politécnica de Valencia generan múltiples responsabilidades en lo relativo a la protección de los datos de carácter personal, derivadas del tratamiento de imágenes que realizan estos sistemas.

La seguridad y vigilancia de las instalaciones y mobiliario de la UPV no es incompatible con el derecho fundamental a la protección de la imagen como dato personal, siempre que se respete la normativa existente en materia de protección de datos.

La captación y grabación de imágenes con fines de vigilancia y control, como es el caso que nos ocupa, se encuentra plenamente sometida a lo dispuesto en la LOPD, máxime cuando los afectados resultan perfectamente identificables, dentro del ámbito donde se realiza la captación de imágenes.

La Instrucció 1/2006, de 8 de novembre, de l'Agència Espanyola de Protecció de Dades, sobre el tractament de dades personals amb fins de vigilància a través de sistemes de càmeres o videocàmeres, en l'article 1 assenyala que "aquesta instrucció s'aplica al tractament de dades personals d'imatges de persones físiques identificades o identificables, amb fins de vigilància a través de sistemes de càmeres i videocàmeres".

## **CAPÍTOL I. Finalitats de la videovigilància**

### **Article 1. Labors de videovigilància**

Els sistemes de seguretat han de tenir com a finalitat protegir únicament i exclusivament les instal·lacions, els equips i els materials propietat de la Universitat Politècnica de València. Per a complir aquesta finalitat es permet gravar imatges dels treballadors o persones que estiguen en contacte amb els equips i instal·lacions. La gravació de la imatge d'una persona, ja siga treballador o no de la Universitat, es considera dada personal, segons el criteri de l'AEPD expressat en la Instrucció 1/2006.

### **Article 2. Finalitats**

Les imatges s'han de tractar de manera lleial i lícita, i s'han de destinar a fins determinats, explícits i legítims. S'han d'utilitzar de conformitat amb el principi segons el qual les dades han de ser adequades, pertinents i no excessives. No s'han de tractar posteriorment de manera incompatible amb els dits fins i s'han de conservar durant el període que estableix el present reglament.

La Universitat Politècnica de València únicament admet la instal·lació de càmeres de videovigilància per a satisfer finalitats lícites i legítimes. Es considera legítima utilitzar aquestes amb els fins següents:

1. Control de l'accés als edificis o a part d'aquests
2. Control de l'accés als aparcaments i garatges
3. Seguretat interior
4. Seguretat de les instal·lacions esportives
5. Custòdia de béns valuosos
6. Seguretat en el treball i prevenció de riscos laborals

En cap cas s'admet la instal·lació de càmeres de videovigilància amb fins de:

1. Control laboral
2. Difusió externa d'imatges a través d'Internet
3. Captació d'imatges en espais protegits pel dret fonamental a la intimitat, com ara banys o vestidors
4. Gravació de converses
5. Captació d'imatges amb fins docents i d'investigació sense la notificació de caràcter previ d'aquesta intenció

La Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, en su artículo 1 señala que "la presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras".

## **CAPÍTULO I. Finalidades de la videovigilancia**

### **Artículo 1. Labores de videovigilancia**

Los sistemas de seguridad tendrán como finalidad proteger única y exclusivamente las instalaciones, equipos y materiales propiedad de la Universidad Politécnica de Valencia. Para el cumplimiento de esta finalidad se permitirá grabar imágenes de los trabajadores o personas que estén en contacto con los equipos e instalaciones. La grabación de la imagen de una persona ya sea trabajador o no de la universidad es considerada dato personal, según el criterio de la AEPD expresado en la Instrucción 1/2006.

### **Artículo 2. Finalidades**

Las imágenes deberán ser tratadas de manera leal y lícita, y se destinarán a fines determinados, explícitos y legítimos. Se utilizarán de conformidad con el principio según el cual los datos deben ser adecuados, pertinentes y no excesivos. No serán tratadas posteriormente de manera incompatible con dichos fines y se conservarán durante el periodo que se establezca en el presente Reglamento.

La Universidad Politécnica de Valencia únicamente admitirá la instalación de cámaras de videovigilancia 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
6. Seguridad en el trabajo y prevención de riesgos laborales

En ningún caso se admitirá la instalación de cámaras de videovigilancia con fines de:

1. Control laboral
2. Difusión externa de imágenes a través de Internet
3. Captación de imágenes en espacios protegidos por el derecho fundamental a la intimidad, como baños o vestuarios
4. Grabación de conversaciones
5. Captación de imágenes con fines docentes y de investigación sin la notificación de carácter previo de tal intención

## CAPÍTOL II. Instal·lació dels sistemes de videovigilància

### Article 3. Instal·lació de càmeres de videovigilància

La instal·lació de sistemes de videovigilància amb fins de seguretat privada comporta necessàriament contractar serveis d'empreses de seguretat degudament autoritzades pel Ministeri de l'Interior, que segons l'article 5 de la Llei 23/1992 de Seguretat Privada puguen prestar el servei de vigilància i protecció de béns i instal·lació i manteniment d'aparells, dispositius i sistemes de seguretat.

Per tant, la utilització de sistemes per a captar i/o tractar imatges amb fins de videovigilància i seguretat a la Universitat Politècnica de València està subjecta al que preveu aquesta llei i el seu reglament de desplegament, de manera que solament poden prestar aquests serveis empreses degudament autoritzades en virtut de les seues condicions i qualificació.

D'altra banda, les condicions tècniques de les instal·lacions i de la configuració de la xarxa de dades a través de què s'han de tractar les imatges són les definides a aquest fi per l'Àrea de Sistemes d'Informació i Comunicacions.

### Article 4. Responsables de la instal·lació de sistemes de videovigilància

Són els caps de servei, directors dels departaments, directors o degans dels centres i directors dels instituts els que per a complir els fins anteriorment especificats sol·liciten la instal·lació de càmeres de videovigilància. Així mateix, són els que han de vetlar perquè el tractament de les imatges captades s'ajuste en tot moment al que preveu la declaració del fitxer i les mesures de seguretat que l'afecten.

### Article 5. Autorització prèvia

La instal·lació, manteniment i visionament de sistemes de vigilància requereix l'autorització prèvia del Vicerectorat dels Campus i Infraestructures (o l'òrgan que eventualment el substituïska en aquestes funcions). Una vegada obtinguda aquesta autorització, el responsable de la instal·lació ha d'instal·lar les càmeres a través d'una empresa de seguretat privada autoritzada per a això segons el que preveu la Llei 23/1992 de Seguretat Privada. La petició d'autorització s'ha de formalitzar a través de la sol·licitud d'instal·lació (ANNEX I).

S'ha de presentar la sol·licitud al Servei d'Assumptes Generals de la UPV, que és l'encarregat de comprovar si la finalitat de la videocàmera a instal·lar s'ajusta a les finalitats recollides en el present reglament. Altrament, s'ha d'informar al sol·licitant sobre la impossibilitat d'instal·lar la videocàmera.

## CAPÍTULO II. Instalación de los sistemas de videovigilancia

### Artículo 3. Instalación de cámaras de videovigilancia

La instalación de sistemas de videovigilancia con fines de seguridad privada comporta necesariamente la contratación de los servicios de empresas de seguridad debidamente autorizadas por el Ministerio del Interior, que conforme al artículo 5 de la Ley 23/1992 de Seguridad Privada puedan prestar el servicio de vigilancia y protección de bienes e instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad.

Por lo tanto la utilización de sistemas para la captación y/o tratamiento de imágenes con fines de videovigilancia y seguridad en la Universidad Politécnica de Valencia estará sujeta a lo previsto en esta ley y en su Reglamento de desarrollo, de modo que solamente podrán prestar estos servicios empresas debidamente autorizadas en virtud de sus condiciones y cualificación.

Por su parte, las condiciones técnicas de las instalaciones y de la configuración de la red de datos a través de la que se tratarán las imágenes serán las definidas a tal fin por el Área de Sistemas de Información y Comunicaciones.

### Artículo 4. Responsables de la instalación de sistemas de videovigilancia

Serán los Jefes de Servicio, Directores de los Departamentos, Directores o Decanos de los Centros y Directores de los Institutos los que para el cumplimiento de los fines anteriormente especificados, soliciten la instalación de cámaras de videovigilancia. Siendo así mismo los que deberán velar porque 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 5. Autorización previa

La instalación, mantenimiento y visionado de sistemas de vigilancia requerirá la autorización previa del Vicerectorado de los Campus e Infraestructuras (o el órgano que eventualmente lo sustituya en estas funciones). Una vez obtenida esta autorización, el responsable de la instalación procederá a la instalación de las cámaras a través de una empresa de seguridad privada autorizada para ello según lo previsto en la ley 23/1992 de Seguridad Privada. La petición de autorización se formalizará a través de la solicitud de instalación (ANEXO I).

La solicitud deberá ser presentada en el Servicio de Asuntos Generales de la UPV que será el encargado de comprobar si la finalidad de la videocámara a instalar se ajusta a las finalidades recogidas en el presente Reglamento. En caso contrario se informará al solicitante de la imposibilidad de instalación de la videocámara.

Després de valorar la finalitat de la instal·lació, s'ha de traslladar la petició al Servei d'Infraestructures, el qual ha d'emetre un informe de viabilitat tècnica de la instal·lació, i a l'Àrea de Sistemes d'Informació i Comunicacions (o l'òrgan que eventualment el substituïska en les funcions de control de la protecció de dades), per a l'adequació d'aquesta als requisits de protecció de dades personals que inclou aconseguir del sol·licitant el compromís de tractament de dades personals (ANNEX II) necessari per a començar a tractar imatges una vegada instal·lada la videocàmera. A la vista de l'informe de viabilitat tècnica i del compromís de tractament de dades personals, l'Àrea de Sistemes d'Informació i Comunicacions trameta l'autorització d'instal·lació al sol·licitant.

Una vegada obtinguda l'autorització per a la instal·lació, el responsable d'aquesta ha de realitzar-la en un termini màxim de sis mesos. En el cas que aquest termini no es complisca, l'autorització perdrà la vigència i s'ha d'iniciar un nou procés de petició, tal com estableix aquest mateix article.

#### **Article 6. Registre del contracte d'instal·lació**

El sol·licitant és l'encarregat de trametre al Vicerectorat dels Campus i Infraestructura el model de contracte d'instal·lació de dispositius de videovigilància (ANNEX III). El dit contracte, l'ha d'emplenar l'empresa instal·ladora (incorporant la seua capçalera) per a l'enviament posterior a l'òrgan corresponent del Ministeri de l'Interior. Una vegada dipositat el contracte, l'empresa instal·ladora n'ha de trametre a l'Àrea de Sistemes d'Informació i Comunicacions el número de registre.

### **CAPÍTOL III. Requisits i criteris d'ús dels sistemes**

#### **Article 7. Contracte d'encarregat de tractament de les imatges**

Les imatges captades pels sistemes de videovigilància instal·lats únicament poden ser visionades i gravades per l'empresa de seguretat contractada per la UPV als locals habilitats a aquest efecte. El responsable de cada instal·lació autoritzada, per tant, ha de subscriure l'annex al contracte de serveis de seguretat de la UPV en què es designa l'empresa de seguretat com a encarregat del tractament de les imatges, i aquesta última és la responsable del document de seguretat en el cas que es tracte d'un sistema de gravació d'imatges.

#### **Article 8. Criteris d'ús**

La instal·lació i l'ús de sistemes de videovigilància a la Universitat Politècnica de València únicament és possible per a les finalitats descrites en aquest document, i sempre que l'ús d'aquests s'han autoritzat degudament.

Tras ser valorada la finalidad de la instalación se dará traslado de la petición al Servicio de Infraestructuras que emitirá un informe de Viabilidad Técnica de la instalación y al Área de Sistemas de Información y Comunicaciones (o el órgano que eventualmente lo sustituya en las funciones de control de la protección de datos) para la adecuación de la misma a los requisitos de protección de datos personales que incluye recabar del solicitante el Compromiso de Tratamiento de Datos Personales (ANEXO II) necesario para comenzar a tratar imágenes una vez instalada la videocámara. A la vista del informe de viabilidad técnica y del Compromiso de Tratamiento de datos personales, será el Área de Sistemas de Información y Comunicaciones la que remitirá la autorización de instalación al solicitante.

Una vez obtenida la autorización para la instalación, el responsable de la misma deberá proceder a realizarla en un plazo máximo de seis meses, en el caso de que este plazo no se cumpliera la autorización perderá su vigencia y deberá iniciarse un nuevo proceso de petición tal y como se establece en este mismo artículo.

#### **Artículo 6. Registro del contrato de instalación**

Será el Solicitante el encargado de remitir al Vicerrectorado de los Campus e Infraestructura el modelo de Contrato de instalación de dispositivos de videovigilancia (ANEXO III), dicho contrato deberá ser cumplimentado por la empresa instaladora (incorporando su membrete) para su posterior envío al órgano correspondiente del Ministerio del Interior. Una vez depositado el contrato, la empresa instaladora deberá remitir al Área de Sistemas de Información y Comunicaciones el número de registro del mismo.

### **CAPÍTULO III. Requisitos y criterios de uso de los sistemas**

#### **Artículo 7. Contrato de encargado de tratamiento de las imágenes**

Las imágenes captadas por los sistemas de videovigilancia instalados únicamente podrán ser visionadas y grabadas por la empresa de seguridad contratada por la UPV en los locales habilitados al efecto. El responsable de cada instalación autorizada deberá por tanto suscribir el anexo al contrato de servicios de seguridad de la UPV en el que se designará a la empresa de seguridad como encargado 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 8. Criterios de uso**

La instalación y uso de sistemas de videovigilancia en la Universidad Politècnica de Valencia únicamente será posible para las finalidades descritas en este documento, y siempre y cuando el uso de estos hayan sido debidamente autorizado.

La utilització de videocàmeres amb fins de vigilància s'ha d'atendre als criteris següents:

1. S'han de senyalitzar els espais vigilats amb la senyalítica establida per l'Agència Espanyola de Protecció de Dades.
2. Els monitors o les terminals utilitzats per a la videovigilància han d'instal·lar-se de manera que no resulten accessibles a tercers no autoritzats. S'han d'establir les limitacions adequades per a impedir l'accés físic als espais on s'ubiquen.
3. En el cas que es tracte de sistemes de gravació d'imatges, aquestes s'han de conservar durant un període màxim d'un mes.
4. Si es constata la comissió d'un delictes o infracció, s'actuarà com disposa l'apartat 11 d'aquest reglament i s'han de notificar els fets a la Secretaria General, amb còpia de la denúncia.

Queda expressament prohibida:

1. La captació intencional d'imatges de la via pública, així com edificis o espais aliens a la Universitat protegits pels drets a la intimitat personal i familiar, la pròpia imatge i la inviolabilitat del domicili.
2. La captació d'imatges en espais privats, com són banys, vestidors, taquilles personals i altres anàlegs.
3. La captació de sons i en especial de converses privades.
4. La difusió per qualsevol mitjà de les imatges captades.

#### **CAPÍTOL IV. Tipus de sistemes de videovigilància**

##### **Article 9. Sistemes de circuit tancat**

Els sistemes dedicats a la videovigilància es cataloguen de circuit tancat quan no realitzen gravacions en una unitat de disc de les imatges obtingudes, a diferència dels que efectivament ho fan.

Les instal·lacions en què es troben els monitors han de disposar preferentment d'un accés físic controlat.

Quan no és possible establir controls d'accés físic, la disposició dels monitors ha d'impedir l'accés a la informació per tercers aliens a la instal·lació. En tot cas, els equips han de disposar-se de manera que resulten inaccessibles a tercers no autoritzats.

Aquests sistemes han de disposar d'un control d'accés lògic amb assignació, distribució i emmagatzematge de contrasenyes diferenciades per a cada usuari. Aquestes s'han d'emmagatzemar de manera intel·ligible i s'han de canviar periòdicament. Poden articular-se controls distints que garantisquen la seguretat de manera anàloga a l'anterior.

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

1. Se señalarán los espacios vigilados con la señalética establecida por la Agencia Española de Protección de Datos.
2. Los monitores o terminales utilizados para la videovigilancia 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 período máximo de un mes.
4. Si se constatase la comisión de un delito o infracción, se actuará como se dispone en el apartado 11 de este Reglamento y se notificarán los hechos a la Secretaría General con copia de la denuncia.

Queda expresamente prohibida:

1. La captación intencional de imágenes de la vía pública, así como edificios o espacios ajenos a la Universidad protegidos por los derechos a la intimidad personal y familiar, la propia imagen y la inviolabilidad del domicilio.
2. La captación de imágenes en espacios privados como son baños, vestuarios, taquillas personales y otros análogos.
3. La captación de sonidos y en especial de conversaciones privadas.
4. La difusión por cualquier medio de las imágenes captadas.

#### **CAPÍTULO IV. Tipos de sistemas de videovigilancia**

##### **Artículo 9. Sistemas de circuito cerrado**

Los sistemas dedicados a la videovigilancia se catalogarán como de circuito cerrado cuando no realicen grabaciones en una unidad de disco de las imágenes obtenidas, a diferencia de aquellos que efectivamente lo hagan.

Las instalaciones en las que se encuentren los monitores 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 habrán de disponerse de forma que resulten inaccessibles a terceros no autorizados.

Estos 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 intel·ligible y se cambiarán periódicamente. Podrán articularse controles distintos que garanticen la seguridad de manera análoga a la anterior.

S'ha de disposar d'un registre dels usuaris que tinguen una clau o qualsevol altre mitjà que permeta accedir a les instal·lacions o al mobiliari que continga informació protegida.

La utilització de sistemes de circuit tancat no dóna lloc a la creació d'un fitxer de dades personals; per tant, no n'és exigible la declaració prèvia per a tractar les imatges, tot i que sí és obligatori complir els requisits d'informació recollits en l'article 5 del present Reglament.

#### **Article 10. Sistemes de gravació d'imatges**

Són sistemes de gravació d'imatges els que realitzen gravacions en una unitat de disc de les imatges obtingudes.

Les instal·lacions en què es troben els monitors i sistemes de gravació han de disposar preferentment d'un accés físic controlat.

Quan no és possible establir controls d'accés físic, la disposició dels monitors ha d'impedir l'accés a la informació per tercers aliens a la instal·lació. En tot cas, els equips de gravació han de disposar-se de manera que resulten inaccessibles a tercers no autoritzats.

Els suports que continguem imatges s'han de conservar de manera que resulten inaccessibles a tercers no autoritzats.

S'ha de disposar d'un registre dels usuaris que tinguen una clau o qualsevol altre mitjà que permeta accedir a les instal·lacions o al mobiliari que continga informació protegida.

Les gravacions s'han d'etiquetar de manera que es garanteixca la destrucció completa de la informació que contenen.

El rebuig dels suports que continguem imatges captades pels sistemes ha de garantir la inaccessibilitat absoluta a les imatges que contenen.

Els sistemes han de disposar d'un control d'accés lògic amb assignació, distribució i emmagatzematge de contrasenyes diferenciades per a cada usuari. Aquestes s'han d'emmagatzemar de manera intel·ligible i s'han de canviar periòdicament. Poden articular-se controls distints que garantisquen la seguretat de manera anàloga a l'anterior.

Si es preveu l'accés al fitxer a través de xarxes de comunicacions, s'haurà de protegir l'entorn de comunicació i fixar un control d'accés lògic en els termes establits en el paràgraf anterior.

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.

La utilización de sistemas de circuito cerrado no da lugar a la creación de un fichero de datos personales, por lo tanto no será exigible la previa declaración del mismo para el tratamiento de las imágenes, aunque sí será obligatorio cumplir con los requisitos de información recogidos en el artículo 5 del presente Reglamento.

#### **Artículo 10. Sistemas de grabación de imágenes**

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

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.

Los soportes que contengan imágenes se conservarán de manera 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.

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 inaccessibilidad a las imágenes que contienen.

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 inteligible y se cambiarán periódicamente. Podrán articularse controles distintos que garanticen la seguridad de manera análoga a la anterior.

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 párrafo anterior.

L'ús de sistemes de gravació d'imatges dona lloc a la creació d'un fitxer de dades personals; per tant, n'és exigible la declaració prèvia per a tractar les imatges.

Atenent al que disposa el Reial Decret 1720/2007, de 21 de desembre, les dades obtingudes mitjançant videovigilància es qualifiquen de nivell bàsic.

#### **CAPÍTOL V. Règim d'ús de les imatges**

##### **Article 11. Cancel·lació de les imatges**

El termini de cancel·lació de les imatges gravades és d'un mes des de la captació. Una vegada transcorregut aquest termini, aquestes s'han de bloquejar, i s'han de conservar únicament a disposició de les administracions públiques, jutges i tribunals, per a atendre les possibles responsabilitats nascudes del tractament, durant el termini de prescripció d'aquestes. Complert el termini esmentat, s'han de suprimir les imatges.

En els casos que el responsable constata la gravació d'un delicte o infracció administrativa que s'ha de posar en coneixement d'una autoritat, la denunciarà i conservarà les imatges a disposició d'aquesta.

Atesa la constatació de la comissió d'un delicte o infracció, s'han d'aplicar les regles d'actuació següents:

1. S'ha de denunciar el fet a l'autoritat competent i fer-se constar en la denúncia, de manera expressa, l'existència d'un fitxer que conté les imatges i la identificació del suport tal com conste en l'inventari corresponent.
2. Les imatges s'han de posar immediatament a disposició de l'autoritat competent.
3. Si el suport en què es contenen les imatges obliga a lliurar-ne una còpia, mentre que les imatges es conserven en els sistemes de la Universitat, aquestes no s'esborraran, ni es cancel·laran transcorregut el termini de 30 dies fixat en aquest reglament.

##### **Article 12. Obligacions dels usuaris dels sistemes de videovigilància**

1. Els usuaris dels sistemes han de guardar el secret necessari respecte a qualsevol tipus d'informació de caràcter personal que es conega en funció del treball desenvolupat.
2. Han de mantenir-ne en secret les claus d'accés al sistema, ja que aquestes són personals i intransferibles, i l'usuari és l'únic responsable de les conseqüències que se'n puguin derivar del mal ús, divulgació o pèrdua, casos en què s'hauria de notificar la incidència.
3. Canviaran les contrasenyes a petició del sistema quan se li indique.

El uso de sistemas de grabación de imágenes dará lugar a la creación de un fichero de datos personales, por lo tanto será exigible la previa declaración del mismo para el tratamiento de las imágenes.

Atendiendo a lo dispuesto por el Real Decreto 1720/2007, de 21 de diciembre, los datos obtenidos mediante videovigilancia se calificarán como de nivel básico.

#### **CAPÍTULO V. Régimen de uso de las imágenes**

##### **Artículo 11. Cancelación de las imágenes**

El plazo de cancelación de las imágenes grabadas será de un mes desde su captación, una vez transcurrido 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.

En aquellos casos en los que el responsable constatase la grabación de un delito o infracción administrativa que deba ser puesta en conocimiento de una autoridad, procederá a su denuncia y conservará las imágenes a disposición de ésta.

Ante la constatación de la comisión de un delito o infracción se aplicarán las reglas de actuación siguientes:

1. Se denunciará el hecho ante la autoridad competente haciéndose constar en la denuncia, de manera expresa, la existencia de fichero que contiene las imágenes y la identificación del soporte tal y como conste en el inventario correspondiente.
2. Las imágenes se pondrán inmediatamente a la disposición de la autoridad competente.
3. Si el soporte donde se encuentran contenidas las imágenes obliga a la entrega de una copia, mientras que las imágenes se conserven en los sistemas de la Universidad, estas no se borrarán, ni se cancelarán transcurrido el plazo de 30 días fijado en este Reglamento.

##### **Artículo 12. Obligaciones de los usuarios de los sistemas de videovigilancia**

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 habría de notificar la incidencia.
3. Cambiarán las contraseñas a petición del sistema cuando se le indique.

4. En els sistemes de circuit tancat s'han de tancar o bloquejar totes les sessions quan han d'absentar-se temporalment del lloc de treball i al final de la jornada laboral per tal d'evitar accessos no autoritzats.
5. S'han de comunicar les incidències de seguretat de què tinga coneixement.
6. No s'ha de copiar la informació continguda en qualsevol suport sense autorització expressa del responsable. Queda igualment prohibit traslladar qualsevol suport en què s'emmagatzeme informació fora dels locals de la Universitat.
7. S'han de guardar tots els suports físics que contenen informació en un lloc segur quan no s'utilitzen, particularment fora de la jornada laboral.
8. Únicament les persones autoritzades poden introduir o anul·lar les dades contingudes en el fitxer objecte de protecció.

Queda expressament prohibit:

1. Utilitzar identificacions o contrasenyes d'altres usuaris per a accedir als sistemes automatitzats.
2. Intentar modificar o accedir al registre d'accessos.
3. Eludir les mesures de seguretat establides.
4. Ús de la xarxa de la Universitat, els sistemes informàtics i qualsevol altre mitjà posat a disposició de l'usuari per a vulnerar drets de tercers, els propis de l'organització o bé per a realitzar actes que es puguen considerar il·lícits.

#### **Article 13. Dret d'informació en la recollida de dades**

El procediment per a informar a les persones les imatges de les quals es capten s'ha de portar a cap a través de la col·locació del distintiu informatiu establert per l'Agència Espanyola de Protecció de Dades en la Instrucció 1/2006 que s'ha d'ubicar com a mínim en els accessos a les zones vigilades, siguen aquests exteriors o interiors. Si el lloc vigilat disposa de diversos accessos, s'han de col·locar en tots aquests amb l'objecte que la informació siga visible amb independència de la via d'accés.

A més, s'ha de disposar d'un imprès en què s'ha d'informar, en el cas de sistemes de grabació, de:

1. L'existència d'un fitxer o tractament de dades de caràcter personal, de la finalitat de la recollida d'aquestes i dels destinataris de la informació.
2. La possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició.
3. La identitat i direcció del responsable del tractament o, si és el cas, del seu representant.

#### **Article 14. Drets d'accés i cancel·lació**

L'exercici del dret de rectificació no resulta possible en matèria de videovigilància, ja que per la naturalesa de les dades

4. En los sistemas de circuito cerrado se cerrarán o bloquearán todas las sesiones cuando deban ausentarse temporalmente del puesto de trabajo y al final de la jornada laboral al fin de evitar accesos no autorizados.
5. Se comunicarán las incidencias de seguridad de las que tenga conocimiento.
6. 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.
7. Guardarán todos los soportes físicos que contengan información en un lugar seguro cuando no se utilicen, particularmente fuera de la jornada laboral.
8. 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 13. Derecho de información en la recogida de datos**

El procedimiento para informar a las personas cuyas imágenes se capten se llevará a cabo a través de la colocación del distintivo informativo establecido por la Agencia Española de Protección de Datos en su instrucción 1/2006 que se ubicará como mínimo 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 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.

#### **Artículo 14. Derechos de acceso y cancelación**

El ejercicio del derecho de rectificación no resulta posible en materia de videovigilancia, ya que por la naturaleza de los



(imatges preses de la realitat que reflecteixen un fet objectiu) es tractaria d'un dret de contingut impossible.

Per altra banda, el dret d'accés és personalíssim i l'ha de portar a cap l'afectat/ada que ha de trametre al responsable del tractament una sol·licitud en què n'ha de fer constar la identitat, juntament amb una imatge actualitzada i còpia de DNI o document equivalent.

Atès que és pràcticament impossible accedir a imatges sense que pugua veure's compromesa la imatge d'un tercer, pot facilitar-se l'accés mitjançant un escrit certificat en què, amb la major precisió possible i sense afectar drets de tercers, s'especifiquen les dades objecte de tractament.

El dit escrit pot tenir la formulació següent: "La vostra imatge es va registrar en els nostres sistemes el dia \_\_\_ de \_\_\_\_\_ de \_\_\_\_\_ entre les \_\_ hores i les \_\_ hores. En concret, en el sistema que registra (accessos, corredors, aules, etc.)."

#### **Disposició final. Entrada en vigor**

El present reglament entra en vigor el mateix dia de l'aprovació pel Consell de Govern.

datos (imágenes tomadas de la realidad que reflejan hecho objetivo) se trataría de un derecho de contenido imposible.

Por su parte el derecho de acceso es personalísimo y lo llevará a término el afectado/a que habrá de remitir al responsable del tratamiento una solicitud en la que hará constar su identidad, juntamente con una imagen actualizada y copia de DNI o documento equivalente.

Puesto que es prácticamente imposible acceder a imágenes sin que pueda verse comprometida la imagen de un tercero, podrá facilitarse el acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros se especifiquen los datos que han sido objeto de tratamiento.

Dicho escrito podrá tener la siguiente formulación: "Su imagen fue registrada en nuestros sistemas el día \_\_\_ del \_\_\_\_\_ de \_\_\_\_\_ entre las \_\_ horas y las \_\_ horas. En concreto en el sistema que registra (accesos, pasillos, aulas, etc.)."

#### **Disposición final. Entrada en vigor**

El presente Reglamento entrará en vigor el mismo día de su aprobación por el Consejo de Gobierno.

### **ANNEX I / ANEXO I**

#### **FORMULARI DE SOL·LICITUD D'INSTAL·LACIÓ DE CÀMERES DE VIDEOVIGILÀNCIA A LA UPV FORMULARIO DE SOLICITUD DE INSTALACIÓN DE CÁMARAS DE VIDEOVIGILANCIA EN LA UPV**

<b>DATA</b> <b>FECHA</b>	
<b>SOL·LICITANT (Nom, càrrec i entitat)</b> <b>SOLICITANTE (Nombre, cargo y entidad)</b>	
<b>EDIFICI/S DE LA INSTAL·LACIÓ</b> <b>EDIFICIO/S DE LA INSTALACIÓN</b>	
<b>FINALITAT DE LES CÀMERES</b> <b>FINALIDAD DE LAS CÁMARAS</b>	
<b>TECNOLOGIA, MARCA I MODEL DE LES CÀMERES</b> <b>(inclòs el gravador, si n'hi ha)</b> <b>TECNOLOGÍA, MARCA Y MODELO DE LAS CÁMARAS</b> <b>(incluido el grabador si existe)</b>	
<b>NÚMERO I LOCALITZACIÓ DE LES CÀMERES</b> <b>(adjunteu plànol)</b> <b>NÚMERO Y LOCALIZACIÓN DE LAS CÁMARAS</b> <b>(adjuntar plano)</b>	

<b>GRAVACIÓ _ SÍ _ NO</b> <b>En cas de gravació, descriuiu el mètode d'esborrament d'imatges</b> <b>GRABACIÓN _ SÍ _ NO</b> <b>En caso de grabación describa el método de borrado de imágenes</b>	
<b>MÈTODES DE TRACTAMENT DE LES IMATGES</b> <b>Tipus de connexió (IP/Altres)</b> <b>En cas de no ser IP, especifiqueu connector</b> <b>Format d'imatge (jpg, altres)</b> <b>MÉTODOS DE TRATAMIENTO DE LAS IMÁGENES</b> <b>Tipo de Conexión (IP/Otras)</b> <b>En caso de no ser IP, especificar conector</b> <b>Formato imagen (jpg, otros)</b>	
<b>EMPRESA ENCARREGADA DE LA INSTAL·LACIÓ I</b> <b>Núm. DE REGISTRE AL MINISTERI</b> <b>EMPRESA ENCARGADA DE LA INSTALACIÓN Y N° DE</b> <b>REGISTRO EN EL MINISTERIO</b>	
<b>CENTRE DE COST</b> <b>CENTRO DE COSTE</b>	
<b>SIGNATURA DEL SOL·LICITANT</b> <b>FIRMA DEL SOLICITANTE</b>	

**ANNEX II / ANEXO II**  
**COMPROMÍS DE TRACTAMENT DE DADES PERSONALS**  
**COMPROMISO DE TRATAMIENTO DE DATOS PERSONALES**

Sr./Sra. ....com  
a responsable del sistema de videovigilància instal·lat a  
.....  
es compromet a:

1. Utilitzar el dit sistema de videovigilància únicament amb la finalitat d'assegurar els edificis i béns que pertanyen al centre del qual és responsable.
2. Col·locar als espais vigilats la senyalística establida per l'Agència Espanyola de Protecció de Dades.
3. Instal·lar els monitors o les terminals utilitzats per a la videovigilància de manera que no resulten accessibles a tercers no autoritzats, i establir les limitacions adequades per a impedir l'accés físic als espais on s'ubiquen.
4. Mantenir la ubicació de les càmeres de videovigilància tal com va autoritzar la Universitat Politècnica de València.

Don/Doña .....como  
responsable del sistema de videovigilancia instalado en  
.....  
se compromete a:

1. Utilizar dicho sistema de videovigilancia únicamente con la finalidad de asegurar los edificios y bienes pertenecientes al centro del cual es responsable.
2. Colocar en los espacios vigilados la señalética establecida por la Agencia Española de Protección de Datos.
3. Instalar los monitores o terminales utilizados para la videovigilancia de forma que no resulten accesibles a terceros no autorizados. Estableciendo las limitaciones adecuadas para impedir el acceso físico a los espacios donde se ubiquen.
4. Mantener la ubicación de las cámaras de videovigilancia tal y como fueron autorizadas por la Universidad Politècnica de Valencia.

5. En el cas que es tracte de sistemes de gravació d'imatges, conservar-les durant un període màxim d'un mes.
6. Informar sobre la comesa d'un delictes o infracció, si els capta el sistema de videovigilància.
7. Signar l'annex al contracte de serveis de seguretat de la UPV amb l'empresa que tractarà les imatges captades pel sistema de videovigilància com a contracte d'encarregat de tractament.
8. Impedir la captació intencional d'imatges de la via pública, així com edificis o espais aliens al centre protegits pels drets a la intimitat personal i familiar, la pròpia imatge i la inviolabilitat del domicili.
9. Prescindir de la captació d'imatges en espais privats, com són banys, vestidors, taquilles personals i altres anàlegs.
10. Captar sons i en especial de converses privades.
11. Impedir la difusió per qualsevol mitjà de les imatges captades.
12. Informar al Servei d'Assumptes Generals de la UPV sobre qualsevol modificació substancial del sistema de videovigilància.

I, perquè conste, se signa a València, .... de.....  
de .....

5. En el caso de que se trate de sistemas de grabación de imágenes, conservarlas durante un periodo máximo de un mes.
6. Informar de la comisión de un delito o infracción, si fuesen captados por el sistema de videovigilancia.
7. Firmar el anexo al contrato de servicios de seguridad de la UPV con la empresa que va a tratar las imágenes captadas por el sistema de videovigilancia como contrato de encargado de tratamiento.
8. Impedir la captación intencional de imágenes de la vía pública, así como edificios o espacios ajenos al centro protegidos por los derechos a la intimidad personal y familiar, la propia imagen y la inviolabilidad del domicilio.
9. Prescindir de la captación de imágenes en espacios privados como son baños, vestuarios, taquillas personales y otros análogos.
10. La captación de sonidos y en especial de conversaciones privadas.
11. Impedir la difusión por cualquier medio de las imágenes captadas.
12. Informar al Servicio de Asuntos Generales de la UPV de cualquier modificación sustancial del sistema de videovigilancia.

Y para que conste lo firma en Valencia a .... de .....  
de .....

### ANNEX III / ANEXO III

#### CONTRACTE D'INSTAL·LACIÓ DE DISPOSITIUS DE VIDEOVIGILÀNCIA CONTRATO DE INSTALACIÓN DE DISPOSITIVOS DE VIDEOVIGILANCIA

CONTRACTE Número: .....

#### REUNITS

D'una banda, la UNIVERSITAT POLITÈCNICA DE VALÈNCIA (en endavant la UPV), amb CIF Q4618002B, creada amb rang d'universitat en virtut del Decret 495/1971, d'11 de març (BOE de 26 de març de 1971), amb seu al camí de Vera, s/n, de VALÈNCIA (Espanya), i en nom i representació seu el Sr. Salvador López Galarza, vicerector dels Campus i Infraestructures, per delegació de signatura atorgada per Resolució del rector de 27 d'octubre de 2009 per a signar els contractes d'instal·lació d'aparells, dispositius i sistemes de seguretat per a la vigilància dels campus de la Universitat Politècnica de València.

I, de l'altra, ..... (en endavant "l'empresa") amb seu a ....., amb CIF ....., i en nom i representació seu, el Sr. o la Sra. ...., amb DNI

CONTRATO Número: .....

#### REUNIDOS

De una parte la UNIVERSIDAD POLITÈCNICA DE VALENCIA (En adelante la UPV), con CIF Q4618002B, creada con rango de universidad en virtud del Decreto 495/1971, de 11 de marzo (BOE de 26 de marzo de 1971), con sede en el Camino de Vera, s/n de VALENCIA (España), y en su nombre y representación el Sr. Salvador López Galarza, Vicerrector de los Campus e Infraestructuras, por delegación de firma otorgada por Resolución del Rector de 27 de octubre de 2009 para la firma de los contratos de instalación de aparatos, dispositivos y sistemas de seguridad para la vigilancia de los campus de la Universidad Politécnica de Valencia.

Y de otra parte, ..... (en adelante "la Empresa") con sede en ....., con CIF ....., y en su nombre y representación Don/Doña ....., con DNI

núm. .... que actua en virtut d'escriptura de poder que té atorgada davant del notari o notària de ..... Sr./Sra. ...., el dia ... de ..... de ....., amb número de protocol.....

### MANIFESTEN

Que és desig de la UPV instal·lar un sistema de videovigilància a les seues dependències per a protegir únicament i exclusivament les instal·lacions, els equips i els materials de propietat seua.

Que la dita instal·lació s'ha de realitzar d'acord amb la normativa de protecció de dades de caràcter personal i més concretament amb el Reglament de Videovigilància que a aquest efecte ha dictat la mateixa UPV.

Que l'empresa declara que es troba inscrita al Registre d'Empreses de Seguretat de la Direcció General de la Policia amb el número ....., el dia ..... de ..... de ....., per a les activitats d'instal·lacions i manteniment d'aparells, dispositius i sistemes de seguretat, amb àmbit estatal/autonòmic. *(Elegiu el que calga.)*

En virtut de l'assenyalat anteriorment, l'empresa i la UPV subscriuen de mutu acord el present contracte que s'ha de regir per les següents:

### CLÀUSULES

#### Primera: Objecte del contracte

L'objecte d'aquest contracte és la prestació, per l'empresa, d'un servei d'INSTAL·LACIÓ DE SISTEMA DE VIDEOVIGILÀNCIA/VIDEOGRAVACIÓ. *(Elegiu el que calga.)*

#### Segona: Durada del contracte

La durada del present contracte és el del curs de les obres més una garantia d'un any des de la data de finalització d'aquestes.

#### Tercera: Inici de la prestació

El servei s'inicia al tercer dia de la presentació a la comissaria de Policia.

#### Quarta: Ubicació de la instal·lació

El servei objecte del present contracte s'ha de realitzar a .....  
.....  
.....  
..... *(Definiu la ubicació de la instal·lació a les dependències de la UPV.)*

#### Cinquena: Mitjans de prestació del servei

Els mitjans a utilitzar en la prestació d'aquest servei són els relacionats en l'annex.

nº ..... que actúa en virtud de escritura de poder que tiene otorgada ante el Notario/a de ..... Don/Doña ....., el día ... de ..... de ....., con número de protocolo.....

### MANIFIESTAN

Que es deseo de la UPV instalar un sistema de videovigilancia en sus dependencias para proteger única y exclusivamente las instalaciones, equipos y materiales de su propiedad.

Que dicha instalación se realizará conforme a la normativa de protección de datos de carácter personal y más concretamente al Reglamento de Videovigilancia que a tal efecto ha dictado la propia UPV.

Que la Empresa declara hallarse inscrita en el Registro de Empresas de Seguridad de la Dirección General de la Policía con el número ....., en fecha ..... de ..... de ....., para las actividades de instalaciones y mantenimiento de aparatos, dispositivos y sistemas de seguridad, con ámbito estatal/autonómico. *(Elegir lo que proceda.)*

En virtud de lo señalado anteriormente, la Empresa y la UPV, suscriben de mutuo acuerdo el presente Contrato que se regirá por las siguientes:

### CLÁUSULAS

#### Primera: Objeto del Contrato

El objeto de este contrato es la prestación por parte de la Empresa de un servicio de: INSTALACIÓN DE SISTEMA DE VIDEOVIGILANCIA/VIDEOGRABACIÓN. *(Elegir lo que proceda.)*

#### Segunda: Duración del Contrato

La duración del presente contrato será el del curso de las obras más una garantía de un año desde la fecha de finalización de las mismas.

#### Tercera: Inicio prestación

El servicio se iniciará al tercer día de su presentación en la Comisaría de Policía.

#### Cuarta: Ubicación de la instalación

El servicio objeto del presente contrato se realizará en .....  
.....  
.....  
..... *(Definir la ubicación de la instalación en las dependencias de la UPV.)*

#### Quinta: Medios de prestación del servicio

Los medios a utilizar en la prestación de este servicio serán los relacionados en el Anexo.

**Sisena: Normativa reguladora**

El present contracte i les activitats derivades d'aquest, sense perjudici del compliment de les normes generals que s'han d'aplicar, es regeix igualment per la normativa reguladora de la seguretat privada.

I com a prova de conformitat, ambdues parts subscriuen el present contracte en la data i lloc indicats.

PER / POR.....

(Signatura/ Fdo.)

València, ..... de..... de 20.....

**Sexta: Normativa reguladora**

El presente contrato y las actividades derivadas del mismo, sin perjuicio del cumplimiento de las normas generales que le sean de aplicación, se regirá igualmente por la normativa reguladora de la seguridad privada.

Y en prueba de conformidad, ambas partes suscriben el presente Contrato en la fecha y lugar indicados.

PER / POR LA UPV

(Signatura / Fdo.)

Valencia, ..... de..... de 20.....