RESOLUCIÓN de 12 de marzo de 2013, de la Dirección General de Centros y Personal Docente, de la Conselleria de Educación, Cultura y Deporte, por la que se dictan instrucciones en materia de seguridad de los sistemas de videovigilancia de los centros educativos públicos de titularidad de la Generalitat.

La Ley Orgánica 2/2006, de 3 de mayo, de Educación determina que los responsables de la educación deben proporcionar a los centros los recursos y los medios que necesitan para desarrollar su actividad y alcanzar tal objetivo, mientras que éstos deben utilizarlos con rigor y eficiencia para cumplir su cometido del mejor modo posible. Es necesario, por tanto, que la normativa combine ambos aspectos, estableciendo las normas comunes que todos tienen que respetar, así como el espacio de autonomía que se ha de conceder a los centros docentes.

De este modo, vista la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), así como la Instrucción 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, de la Agencia Española de Protección de Datos (en adelante AEPD), la dirección general competente en materia de centros docentes, debe proporcionar un extracto de obligaciones de seguridad de los sistemas de videovigilancia aplicables a todos aquellos centros educativos públicos de titularidad de la Generalitat. Conviene, por tanto, dictar instrucciones respecto a las medidas de centros educativos públicos que instalen sistemas de videovigilancia y donde además exista un tratamiento de las imágenes (grabación, captación, transmisión, conservación, o almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real o un tratamiento que resulte de los datos personales relacionados con aquellas).

Por todo ello, y en virtud de las competencias establecidas en el Decreto 190/2012, de 21 de diciembre, del Consell, por el que se aprueba el Reglamento Orgánico y Funcional de la Conselleria de Educación, Cultura y Deporte, resuelvo:

Apartado único

1. Aprobar las instrucciones incluidas en el anexo I, a las que deberán ajustarse los centros educativos públicos de titularidad de la Generalitat que tengan instalado previamente a la publicación de esta instrucción un sistema de videovigilancia en sus instalaciones o vaya a instalarlo.
2. Establecer los modelos de información que figuran en el anexo II.
3. Aprobar las medidas de seguridad de nivel básico que se recogen en los anexos III y IV.

Valencia, 12 de marzo de 2013
El director general de Centros y Personal Docente

Santiago Martí Alepuz

GENERALITAT VALENCIANA CONSELLERIA D'EDUCACIÓ, FORMACIÓ I OCUPACIÓ

ANEXO I

Instrucciones en materia de seguridad de los sistemas de videovigilancia de los centros educativos públicos de titularidad de la Generalitat.

1. Normas generales de uso e instalación de los sistemas de videovigilancia

1.1 Deberá existir una relación de proporcionalidad entre la finalidad perseguida y el modo en el que se traten los datos según lo dispuesto en el artículo 4 de la Instrucción 1/2006 de la AEPD y de la LOPD, respectivamente.

1.2 Deberá informarse sobre la captación y/o grabación de las imágenes según establece el artículo 3 de la Instrucción 1/2006 de la AEPD y el artículo 5 de la LOPD.

1.3 Atendiendo a lo dispuesto en el artículo 4 de la Instrucción 1/2006 de la AEPD, el uso de instalaciones de cámaras o videocámaras sólo será admisible cuando no exista un medio menos invasivo.

1.4 Según este mismo artículo, la instalación de sistemas de videovigilancia sólo será legítima cuando sirva para la finalidad de vigilancia y seguridad en el centro educativo.

1.5 Del mismo modo, las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos.

1.6 Podrían tomarse imágenes parciales y limitadas de vías públicas cuando resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas, atendiendo a lo establecido en el artículo 4 de la Instrucción 1/2006 de la AEPD.

1.7 El uso de sistemas de videovigilancia deberá ser respetuoso con los derechos de las personas y el resto del Ordenamiento jurídico según establece el artículo 5 de la Instrucción 1/2006 de la AEPD, así como el artículo 15 y siguientes de la LOPD.

1.8 Las imágenes se conservarán por el tiempo imprescindible para la satisfacción de la finalidad para la que se recabaron, como así determina el artículo 6 de la Instrucción 1/2006 de la AEPD.

1.9 Los centros educativos que tomen la decisión de instalar sistemas de videovigilancia en las instalaciones se harán cargo del pago de la instalación a cargo de los presupuestos del centro, y se ajustarán a lo previsto en la Orden de 18 de mayo de 1995, por la que se delega en los directores de los centros educativos no universitarios determinadas facultades ordinarias en materia de contratación y se aprueban las normas que regulan la gestión económica de dichos centros (DOCV 09/06/95). Con relación a este texto legal, se recomienda la consulta de la norma cuarta referida a los gastos de adquisición de mobiliario y equipo escolar, así como el apartado 6 del anexo III, referente a mobiliario y equipo.

1.10. Estos gastos quedan condicionados a que, previamente, queden cubiertas las necesidades ordinarias para el normal funcionamiento del centro y que su cuantía no supere la cantidad fijada en los presupuestos generales de la Generalitat para el correspondiente ejercicio.

2. Principio de información

2.1 El Director o Directora del centro se responsabilizará de cumplir con el deber de información previsto en el artículo 3.a) de la Instrucción 1/2006 de la AEPD, «a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados». Para ello, se deberá colocar un cartel informativo en las zonas videovigiladas (consultar anexo II. Modelos de Información), tanto en recintos cerrados como abiertos.

2.2 Además, se dispondrá de un impreso en el cual se detalle la información prevista en el artículo 3.b) de la Instrucción 1/2006, «b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999». Dicho impreso estará disponible de manera visible en el tablón de comunicados del centro para cualquier persona de la cual se haya captado su imagen (consultar anexo II. Modelos de Información).

3. Principios de calidad, proporcionalidad y finalidad del tratamiento

3.1 La instalación de cámaras de videovigilancia en los centros educativos con el fin de controlar conductas que puedan afectar a la seguridad, ha de ser una medida proporcional en relación con la infracción que se pretenda evitar y, en ningún caso, debe suponer el medio inicial para llevar a cabo funciones de vigilancia. La utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

3.2 La instalación de cámaras de videovigilancia será una medida proporcional y justificada atendiendo a lo dispuesto en el artículo 4 de la Instrucción 1/2006 de la AEPD: «1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras. 2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal. 3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida».

3.3. Los menores son sujetos merecedores de una especial protección, por lo que el principio de proporcionalidad deberá aplicarse con un rigor extremo. Para ello, en centros educativos, esta medida sólo será legítima cuando derive de una necesidad ineludible, cuando la medida sea la más adecuada y siempre que no exista una medida alternativa. En particular:

a) La zona objeto de videovigilancia será la mínima imprescindible abarcando espacios públicos como accesos o pasillos.

b) En ningún caso podrán instalarse estos medios en espacios protegidos por el derecho a la intimidad como baños, vestuarios o aquellos en los que se desarrollen actividades cuya captación pueda afectar a la imagen o a la vida privada.

c) Salvo en circunstancias excepcionales, no resulta admisible la captación de imágenes con fines de control de asistencia escolar.

d) El uso de videocámaras con fines de seguridad en espacios de recreo, aulas y otros ámbitos en los que se desarrolla la personalidad de los menores sólo podrán ser objeto de grabación en presencia de circunstancias excepcionales, justificadas por la presencia de un riesgo objetivo y previsible para la seguridad de los menores.

4. Encargado del tratamiento

4.1 La contratación de empresas de seguridad para la instalación y mantenimiento del sistema de videovigilancia en el centro educativo público puede implicar el acceso de la empresa de seguridad a los equipos que almacenan o capturan las imágenes. Por tanto, en estos casos la empresa de seguridad adquiere la consideración de encargado del tratamiento, lo que implica la celebración de un contrato de acceso a los datos por cuenta de terceros. Por ello, según lo dispuesto en el artículo 12 de la LOPD: «1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. 2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar. 3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. 4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente».

4.2 La elaboración y firma de dicho contrato, de obligado cumplimiento, permitirá involucrar a la empresa de seguridad como encargado del tratamiento, obligándole a adoptar las medidas de seguridad técnicas y organizativas que garanticen la seguridad de los tratamientos realizados, correspondientes al nivel de seguridad básico. Dichas medidas figuran en el anexo III. Medidas de seguridad de nivel básico.

4.3. En aquellos casos en los cuales exista una prestación de servicios sin acceso a datos personales, deberá figurar expresamente en el contrato de prestación de servicios la prohibición de acceso a datos personales.

5. Medidas de seguridad

5.1 Según establece el artículo 9 de la Instrucción 1/2006 de la AEPD: « el responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado».

Por tanto, el centro educativo público deberá adoptar las medidas de seguridad de nivel básico para el fichero de videovigilancia, de manera que se garantice también el cumplimiento del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley 15/1999 (en adelante RLOPD).

5.2. En general, los sistemas de videovigilancia son tratamientos automatizados, por lo que deberán adoptarse las medidas de nivel básico que figuran en el RLOPD, y que figuran en el Anexo III. Medidas de seguridad de nivel básico y Anexo IV. Medidas técnicas de seguridad.

6. Cancelación de las imágenes

6.1 Las imágenes deberán ser canceladas una vez transcurrido el plazo de un mes desde su grabación, de acuerdo con el artículo 6 de la Instrucción 1/2006 de la AEPD, según la cual «los datos serán cancelados en el plazo máximo de un mes desde su captación».

6.2. 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, y la denunciase, deberá conservar las imágenes a disposición de la citada autoridad.

7. Inscripción de ficheros

7.1 Según el artículo 7 de la Instrucción 1/2006 de la AEPD: «1. La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma. Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. 2. A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real».

7.2 La Conselleria competente en materia de educación es la encargada del registro del fichero de videovigilancia en el Registro General de la AEPD, previa publicación de la ORDEN 14/2011, de 7 de octubre, de la Conselleria de Educación, Formación y Empleo, por la que se crea el fichero con datos de carácter personal de videovigilancia.

7.3 La Conselleria competente en materia de educación dispondrá de un inventario de aquellos centros que instalen sistemas de videovigilancia.

7.4 El centro educativo deberá solicitar la autorización/regularización para la instalación del sistema de videovigilancia, tal y como se describe en el procedimiento del punto 8 del presente anexo.

7.5. En aquellos casos en los cuales las videocámaras que se vayan a instalar reproduzcan las imágenes en tiempo real (sin grabación ni almacenamiento de imágenes), únicamente estarán sujetas a informar a los afectados a través de carteles informativos (ver Anexo II. Modelos de Información), no siendo obligatoria ni necesaria la inscripción del fichero.

8. Procedimiento

8.1. El procedimiento que debe seguir un centro educativo que tenga instalado previamente a la publicación de esta instrucción un sistema de videovigilancia en sus instalaciones o vaya a instalarlo, es el siguiente:

8.1.1 Deberá dirigir una solicitud a la dirección territorial competente en materia de educación correspondiente, y podrán presentarse utilizando los medios telemáticos facilitados por los

servidores de información de la Conselleria competente en materia de educación. El formulario de solicitud se encuentra disponible en la Oficina Virtual (https://oficinavirtual.edu.gva.es/oficina_edu/)

8.1.2 Las solicitudes deberán de ir acompañadas de la documentación siguiente:

- Proyecto de instalación del sistema de videovigilancia previsto, inidcando si se trata o no de una regularización de instalación previa.
- Acuerdo favorable del consejo escolar.
- Presupuestos de ejecución.
- Informe de la Unidad Técnica, que supervisará asimismo la ejecución de las instalaciones.
- Informe de necesidad, proporcionalidad e idoneidad elaborado por la Inspección Educativa en el que se valorará la existencia de una necesidad ineludible por no existir una medida alternativa y el cumplimiento del punto 3 de la presente Instrucción.
- Informe técnico de la Dirección General de Tecnologías de la Información de la Conselleria de Hacienda y Administración Pública.

8.1.3 Toda la documentación deberá adjuntarse al expediente tramitado telemáticamente. La documentación que no cumpla estos requisitos no será tenida en cuenta a la hora de tramitar la solicitud.

8.1.4 Si la solicitud no reúne los requisitos y documentos que se señalan en estas bases se requerirá al centro educativo para que, en un plazo de quince días hábiles, subsane la falta o acompañe los documentos preceptivos, con indicación de que, si así no lo hiciera, se tendrá en cuenta a la hora de dictar la resolución y se considerará que desiste de la solicitud.

8.1.5 Los datos personales de los representantes de los centros educativos, recogidos en el transcurso del procedimiento, serán incluidos en un fichero, en los términos y condiciones que se recogen en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la referida ley orgánica.

8.1.6 La instrucción del procedimiento corresponderá a la dirección territorial competente en materia de educación correspondiente, la cual realizará de oficio cuantas actuaciones estime necesarias para la determinación, conocimiento y comprobación de los datos en virtud de los cuales debe formularse la propuesta de resolución.

8.1.7 Una vez valorado el expediente, el director territorial correspondiente resolverá la autorización de las instalaciones. El plazo máximo para dictar y notificar la resolución correspondiente será de seis meses a contar desde la fecha de la presentación de la solicitud en la Dirección Territorial correspondiente, de conformidad con lo establecido en el artículo 42 de la LRJAP.

8.2. Los centros educativos que hubieran realizado la instalación de sistemas de videovigilancia de manera previa a la publicación de la presente disposición, deberán presentar la solicitud de autorización en el plazo máximo de 6 meses a partir de la publicación de la presente disposición.

8.3. Con posterioridad a la instalación del sistema de videovigilancia en el centro educativo, se podrán ejercer funciones de inspección o control, con el fin de supervisar el cumplimiento o no de las medidas de seguridad implantadas en el centro educativo y establecidas en la presente disposición.

9. Modificación de la instalación de sistemas de videovigilancia en centros educativos
Los centros educativos que realicen modificaciones en los sistemas de videovigilancia instalados en sus instalaciones deberán notificarlo a la Conselleria competente en materia de educación, la cual podrá ejercer funciones de inspección o control, con el fin de supervisar las modificaciones realizadas y su correspondiente cumplimiento o no de las medidas de seguridad establecidas en la presente disposición.

10. Derecho de acceso
10.1 Mediante el derecho de acceso, la persona titular de la imagen o su representante legal tiene derecho a que la persona responsable del tratamiento le informe sobre si su imagen ha sido captada a través de sistemas de videovigilancia, la finalidad de la captación, si la imagen es registrada en un fichero, si es objeto de algún otro tratamiento, si se ha realizado o se ha previsto alguna comunicación y cuál es el periodo de conservación de las imágenes.

10.2 Cuando la persona interesada así lo pida, también tiene derecho a acceder a las imágenes y a obtener copia, como también de las elaboraciones posteriores que se hayan hecho.

10.3 En caso de que el ejercicio del derecho afecte también imágenes de terceras personas, salvo que se cuente con su consentimiento, el acceso requiere la disociación previa de las imágenes con cualquier medio que impida la identificación. Cuando la disociación exija esfuerzos desproporcionados en atención al lapso temporal registrado o al elevado número de terceras personas afectadas, la persona responsable puede solicitar que se reduzca el periodo de grabación al que se pretenda tener acceso.

11. Derecho de rectificación
11.1 Sólo procede el ejercicio del derecho de rectificación de las imágenes captadas con sistemas de videovigilancia cuando la imagen haya sido distorsionada o alterada con posterioridad a su captación.

11.2 Con el fin de dar cumplimiento a lo que prevé este artículo, cuando se alteren o distorsionen las imágenes se debe guardar copia de la grabación original o disponer de un mecanismo de recuperación de la información original. La alteración o distorsión debe quedar reflejada en el registro de incidencias, indicando el periodo afectado y el motivo.

12. Derecho de cancelación
Mediante el derecho de cancelación la persona titular de la imagen o su representante legal puede pedir la supresión, previo bloqueo, de sus imágenes o voz cuyo tratamiento sea inadecuado, excesivo o contrario al ordenamiento jurídico.

13. Derecho de oposición
Mediante el derecho de oposición, a menos que una norma con rango de Ley o norma de derecho comunitario de aplicación directa disponga lo contrario, la persona titular de la imagen o su representante legal puede pedir la exclusión del tratamiento de su imagen en aquellos supuestos en que no sea necesario su consentimiento. La solicitud de ejercicio de este derecho debe justificarse en motivos fundamentados y legítimos relativos a una situación personal concreta.

14. Procedimiento de ejercicio de derechos
14.1 Para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, hay que formular una solicitud dirigida al director del centro docente responsable del fichero, indicando el lugar, la fecha y la hora aproximada, en franjas no superiores a dos horas, en que su imagen pudo ser captada. La solicitud debe acompañarse de una imagen de la persona solicitante que corresponda al periodo en que se captó, de manera que permita identificarla. Con el fin de comprobar la coincidencia entre la imagen aportada y las imágenes registradas, se pueden utilizar herramientas de reconocimiento de imágenes.

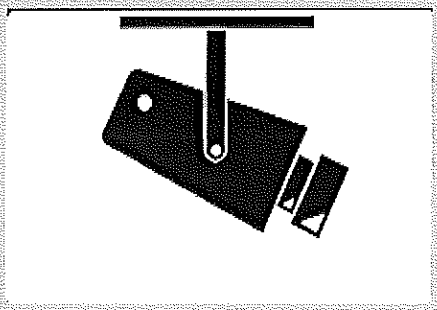
14.2 La tramitación y la resolución de la solicitud se rige por lo que establecen la normativa de protección de datos de carácter personal y por la presente Instrucción. La obligación de resolver persiste, con independencia de que las imágenes no hayan sido registradas o que ya hayan sido canceladas en el momento en que se ejerce el derecho. En este último caso, la resolución puede limitarse a exponer esta circunstancia y a informar de la imposibilidad material de dar satisfacción al derecho ejercido.

14.3. Puede denegarse la solicitud de ejercicio de los derechos de acceso, rectificación, cancelación u oposición cuando no concurran los requisitos exigibles, o cuando el nivel de coincidencia entre la imagen aportada con la solicitud y las que hayan sido objeto de tratamiento no permita asegurar que ésta última corresponde a la persona interesada. También puede denegarse cuando no hayan sido registradas o ya hayan sido canceladas.

ANEXO II

Modelos de información

ZONA VIDEOVIGILADA



LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS

PUEDE EJERCITAR SUS DERECHOS ANTE:

□Insertar el nombre del centro docente□

□Insertar la dirección del centro docente□

<Insertar el logo del centro>

CLÁUSULA INFORMATIVA DEL SISTEMA DE VIDEOVIGILANCIA

De conformidad con lo dispuesto en el artículo 5.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos, se informa:

1. Que sus datos personales se incorporarán al fichero denominado VIDEOVIGILANCIA del que es responsable ese organismo, creado por ORDEN 14/2011, de 7 de octubre, de la Conselleria de Educación, Formación y Empleo, por la que se crea el fichero con datos de carácter personal de videovigilancia y/o serán tratados con la finalidad de seguridad a través de un sistema de videovigilancia.

2. Que el destinatario de sus datos personales es la empresa de seguridad <Indicar el nombre de la empresa de seguridad, si procede>

3. Que puede ejercitar sus derechos de acceso, cancelación y oposición ante el responsable del fichero.

4. Que el responsable del fichero tratamiento es <Indicar nombre o razón social del centro educativo> ubicado en <Indicar dirección del centro educativo>

ANEXO III

Medidas de Seguridad de Nivel Básico

1. Funciones y obligaciones del personal

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.
También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.
2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

2. Registro de incidencias

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

3. Control de acceso

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

4. Gestión de soportes y documentos

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.
Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.
2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

5. Identificación y autenticación
1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

6. Copias de respaldo y recuperación
1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.
3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.
Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

ANEXO IV

Medidas técnicas de seguridad

1. Cumplimiento de medidas técnicas de seguridad adicionales

1. La transmisión de datos de carácter personal a través de redes cableadas o redes inalámbricas de comunicación electrónicas se realizará cifrando dichos datos, o bien, utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

2. Para el cifrado de las comunicaciones se utilizarán protocolos criptográficos que proporcionen la seguridad de la información que viaja a través de ellas, empleando algoritmos de cifrado actuales.

3. El acceso a la sala donde se hallen los equipos físicos en los cuales se almacenen las imágenes deberán disponer de mecanismos de seguridad que impidan el acceso no autorizado de personas ajenas o no autorizadas.

4. Las redes de comunicación electrónicas para la transmisión de imágenes de los dispositivos de videovigilancia, en ningún caso podrán ser las redes de comunicaciones de datos corporativas de los centros educativos; siendo responsabilidad de la empresa instaladora el uso de una red propia independiente de las existentes en el centro.