Protocolo sobre o uso de instalacións de videovixilancia na Universidade de Santiago de Compostela

A protección das persoas, bens e instalacións universitarias precisan apoiarse, cada vez mais, en sistemas electrónicos, en particular no uso de cámaras que transmiten as imaxes a centros de control para previr a comisión de infraccións, delitos ou o acceso non permitido a locais.

Estes sistemas teñen certos riscos que é necesario previr, mediante un uso lícito e finalista dos mesmos. Por outra banda, a videovixilancia require o cumprimento das normas de protección de datos de carácter persoal.

Coa finalidade de determinar os procedementos para a instalación de cámaras, os seus requisitos e o seu uso, o Consello de Goberno do 7 de outubro de 2009, aprobou o Protocolo que, ata o de agora, se ven aplicando.

Con todo, a entrada en vigor de importantes normas en materia de protección de datos, aconsella a modificación do mesmo para adaptalo á nova lexislación.

Con este obxectivo, o Consello de Goberno celebrado o día 28 de abril de 2023, aprobou unha nova versión do

PROTOCOLO SOBRE O USO DE INSTALACIÓNS DE VIDEOVIXILANCIA NA UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

1.- AUTORIZACIÓN

A instalación de videocámaras e instrumentos similares de control de acceso ou de seguridade debe ser autorizada, con carácter previo ao seu uso, pola Xerencia da Universidade de Santiago de Compostela, previa valoración do risco que implique o tratamento de datos que se levará a cabo e, de estimarse preciso, previa consulta co delegado de protección de datos.

A Secretaria Xeral da USC recibirá comunicación das novas cámaras instaladas e terá acceso ao inventario de todas as instalacións videovixiladas.

2.- REXISTRO DE ACTIVIDADES

A captación de imaxes coa finalidade de vixilancia supón un tratamento de datos de carácter persoal, tratamento que consta no rexistro de actividades de tratamento. No rexistro se incorporará toda a información esixida pola normativa aplicable e estará dispoñible na páxina web da Universidade.

Este documento é de carácter informativo e non ten valor xurídico. Está elaborado unicamente a partir das normas publicadas en Lex.gal. Consulte a información contida ao respecto na sección de preguntas frecuentes.

3.- LEXITIMACIÓN E FINALIDADE

3.1. A finalidade do establecemento dun sistema de videovixilancia por parte da USC é garantir a seguridade das persoas, bens e instalacións da mesma. Polo tanto, de conformidade co artigo 6.1.e) do Reglamento General de Protección de Datos (RGPD), o interese público lexitimaría o tratamento dos datos derivado desta actividade.

3.2. En todo caso, considerarase lexítima a utilización de videovixilancia para os seguintes fins:

a) Control de acceso aos edificios ou a parte destes.

b) Control de acceso a aparcadoiros e garaxes, tanto no interior de edificios como en espazos exteriores.

c) Seguridade interior.

d) Seguridade en instalacións deportivas.

e) Custodia de bens valiosos.

f) Seguridade no traballo e prevención de riscos laborais.

3.3. En ningún caso se admitirá o uso de instalacións de videovixilancia con fins de:

a) Control laboral.

b) Difusión externa de imaxes a través de Internet.

c) Captación de imaxes en espazos protexidos polo dereito fundamental á intimidade.

3.4. Entendese lexítima a captación de imaxes con fins docentes e de investigación da propia USC, sempre que se axuste ás esixencias da normativa de protección de datos e se poña, previamente, en coñecemento dos afectados.

4.- CRITERIOS DE USO

4.1. A utilización de videocámaras con fins de vixilancia aterase aos criterios seguintes:

a) Será posible, exclusivamente, para as finalidades descritas neste documento.

b) Unicamente se poderán utilizar aquelas instalacións de videovixilancia que se autorizaron adecuadamente.

c) Se as houbese, seguiranse as instrucións específicas que acompañen á autorización.

Este documento é de carácter informativo e non ten valor xurídico. Está elaborado unicamente a partir das normas publicadas en Lex.gal. Consulte a información contida ao respecto na sección de preguntas frecuentes.

d) Identificaranse os espazos vixiados coa sinalización homologada pola Axencia Española de Protección de Datos.

e) Os monitores ou terminais utilizados para a videovixilancia terán que instalarse de maneira que non resulten accesibles a terceiros non autorizados. Para iso, estableceranse limitacións de acceso físico ao espazo en que se sitúan.

f) As imaxes conservaranse polo período dun mes, salvo cando teñan que manterse durante un período maior para acreditar a comisión de actos que atenten contra a integridade das persoas, os bens ou as instalacións.

g) No caso de que se constate a comisión dun delito ou infracción, actuarase de acordo co disposto neste protocolo e notificaranse os feitos á Secretaría Xeral con copia da denuncia.

4.2. Non se permitirá:

a) A captación intencional de imaxes na vía publica, así como en vivendas ou espazos alleos á Universidade protexidos polos dereitos á intimidade persoal e familiar, a propia imaxe e a inviolabilidade do domicilio.

b) A captación de imaxes en espazos privados como baños, vestiarios, armarios persoais ou outros análogos.

c) A captación de sons e, en especial, de conversacións privadas.

d) A difusión por calquera medio das imaxes captadas.

5.- OBRIGAS DE SEGURIDADE

Establécense as obrigas de seguridade que deben cumprir os sistemas de videovixilancia en función do seu carácter de automatizados ou non:

5.1. Videovixilancia non automatizada.

a) As instalacións en que se atopan os monitores e sistemas de gravación disporán preferentemente dun acceso físico controlado.

b) Cando non sexa posible establecer controis de acceso físico, a disposición dos monitores impedirá o acceso á información por terceiros alleos á instalación. En todo caso, os equipos de gravación terán que disporse de maneira que resulten inaccesibles a terceiros non autorizados.

c) Os soportes que conteñan imaxes conservaranse de maneira que resulten inaccesibles a terceiros non autorizados.

Este documento é de carácter informativo e non ten valor xurídico. Está elaborado unicamente a partir das normas publicadas en Lex.gal. Consulte a información contida ao respecto na sección de preguntas frecuentes.

d) Disporase dun rexistro dos usuarios que conten con autorización e medios que permitan acceder a instalacións e/ou mobiliario que conteñan información protexida.

e) As gravacións etiquetaranse de maneira que se identifique con claridade o contido e vinculación ao sistema.

f) Os soportes reutilizaranse de maneira que se garante a completa destrución da información que conteñan.

g) O desbote de soportes que conteñan imaxes captadas polos sistemas garantirán a absoluta inaccesibilidade ás imaxes que contiñan.

h) As incidencias de natureza non técnica, en particular as relativas ás condicións ou consecuencias xurídicas do uso das videocámaras, remitirase á Secretaría Xeral.

5.2. Videovixilancia automatizada Ademais das sinaladas no epígrafe anterior, establécense as seguintes obrigas:

a) As gravacións etiquetaranse de maneira que se identifique con claridade o contido e vinculación ao sistema e constarán no inventario correspondente.

b) Os soportes reutilizaranse de maneira que se garanta a completa destrución da información que conteñen.

c) Os sistemas automatizados terán que contar cun control de acceso lóxico con asignación, distribución e almacenamento de contrasinais diferenciados para cada usuario. Estes almacenaranse de xeito inintelixible e cambiaranse periodicamente. Así mesmo, poderán articularse controis distintos cando garantan a seguridade de xeito análogo ao anterior.

d) Se se prevé un acceso aos arquivos a través de redes de comunicacións terase que protexer o contorno de comunicacións e fixarse un control de acceso lóxico nos termos do parágrafo anterior.

e) Cando resulte posible, as gravacións faranse no espazo protexido habilitado para iso pola área TIC. Se non é así, terá que garantirse a seguridade da contorna e a realización de copias de seguridade.

f) As incidencias que afectan aos sistemas informáticos terán que notificarse a través do procedemento común do Documento de Seguridade da USC.

g) Calquera outra incidencia de natureza non técnica, e en particular as relativas as condicións ou consecuencias xurídicas do uso das videocámaras remitirase á Secretaría Xeral.

5.3. Obrigas dos usuarios.

Os usuarios dos sistemas terán que:

Este documento é de carácter informativo e non ten valor xurídico. Está elaborado unicamente a partir das normas publicadas en Lex.gal. Consulte a información contida ao respecto na sección de preguntas frecuentes.

a) Observar a debida reserva, confidencialidade e sixilo.

b) Gardar o necesario segredo respecto de calquera tipo de información de carácter persoal coñecida en función do traballo desenvolvido.

c) Manter en segredo e custodiados axeitadamente os mecanismos lóxicos e físicos que soporten os factores de identificación exixidos en función do nivel de seguridade establecido que permita o acceso ao sistema en cada momento. O usuario será o único responsable das consecuencias que puidesen derivarse do seu mal uso, divulgación ou perda, casos en que se tería que notificar a incidencia.

d) Executar as peticións do sistema relacionadas con renovación de credenciais (cambios de contrasinal periódicos, etc.), ou implantación de novos factores de identificación.

e) Nos sistemas informatizados teranse que pechar ou bloquear todas as sesións ao ausentarse temporalmente do posto de traballo e ao final da xornada laboral, co fin de evitar accesos non autorizados.

f) Comunicar as incidencias de seguridade de que teña coñecemento.

g) Non copiar a información contida en calquera tipo de soporte sen autorización expresa do responsable. Queda igualmente prohibido o traslado de calquera soporte en que se almacene información fóra dos locais da Universidade.

h) Gardar todos os soportes físicos que conteñan información nun lugar seguro cando non se utilizan, particularmente fóra da xornada laboral.

i) Unicamente as persoas autorizadas para facelo poderán introducir ou anular os datos contidos nos arquivos obxecto de protección.

l) Queda prohibido:

i. Utilizar identificadores e contrasinais doutros usuarios para acceder aos sistemas automatizados.

ii. Intentar modificar ou acceder ao rexistro de accesos.

iii. Burlar as medidas de seguridade establecidas.

iv. A ocupación da rede corporativa, sistemas informáticos e calquera medio posto ao alcance do usuario vulnerando o dereito de terceiros, os propios da organización, ou ben para a realización de actos que poidan ser considerados ilícitos.

5.4. Fendas de seguridade.

Cando se produza unha fenda de seguridade, é dicir, que teña lugar a destrución, perda ou alteración accidental ou ilícita das gravacións, ou a comunicación ou acceso non autorizado

Este documento é de carácter informativo e non ten valor xurídico. Está elaborado unicamente a partir das normas publicadas en Lex.gal. Consulte a información contida ao respecto na sección de preguntas frecuentes.

aos devanditos datos de videovixilancia, a USC, como responsable do tratamento, sempre que exista risco para os dereitos e liberdades das persoas físicas, deberá notificalo á AEPD, nun prazo máximo de 72 horas.

Calquera persoa da comunidade universitaria que coñeza a existencia dunha fenda de seguridade deberá poñela en coñecemento da USC a través do seguinte formulario https://www3.usc.es/uscincidencias. No formulario deberase marcar a opción "Notificar incidencia" e elixir "LOPD" no campo de "Tipo de incidencia".

6.- INFORMACIÓN E DEREITOS

Os artigos 15 a 22 do RGPD establecen os dereitos que os afectados poden exercitar ante os responsables e encargados:acceso, rectificación, supresión, limitación do tratamento, portabilidade, oposición e oposición a decisións individuais automatizadas.

Con todo, o exercicio destes dereitos debe ser matizado no ámbito da videovixilancia tendo en conta as condicións específicas de captación e tratamento, segundo se sinala no presente Protocolo.

As persoas interesadas poden exercer os citados dereitos a través da Sede Electrónica da USC, no seguinte enlace: https://sede.usc.es/sede/publica/catalogo/procedemento/55/ver.htm.

Tamén poden dirixirse á Axencia Española de Protección de Datos para realizar a reclamación que consideren oportuna.

6.1. Dereito de información.

Este dereito facilitarase por medio da localización dos sinais deseñados para iso pola Universidade, de acordo co modelo de cartel homologado pola Axencia Española de Protección de Datos, no que constará, en todo caso, a existencia do tratamento, a identidade do responsable e a posibilidade de exercitar os dereitos previstos no RGPD.

Os sinais situaranse de maneira que se informe ao usuario do inicio dun espazo vixiado e poida evitalo, se quere. Todos os accesos a espazos vixiados teranse que sinalizar, sen excepción.

Así mesmo, incluirase no dispositivo informativo a dirección de internet ou un código QR a través do cal se poderá consultar a información relativa ao tratamento de datos.

6.2. Dereitos de acceso, rectificación, supresión e limitación do tratamento.

Respecto do exercicio dos dereitos dos afectados, en materia de videovixilancia, deben facerse unha serie de precisións:

Este documento é de carácter informativo e non ten valor xurídico. Está elaborado unicamente a partir das normas publicadas en Lex.gal. Consulte a información contida ao respecto na sección de preguntas frecuentes.

a) Non resulta posible o exercicio do dereito de rectificación, xa que pola natureza dos datos - imaxes tomadas da realidade que reflicten un feito obxectivo-, trataríase do exercicio dun dereito de contido imposible.

b) Tampouco sería aplicable o dereito de portabilidade, xa que, aínda que se leve a cabo un tratamento automatizado, a lexitimación non se basea nin no consentimento nin na execución dun contrato.

c) Non se aplica parte do contido do dereito á limitación do tratamento, no seu aspecto de "cancelación cautelar", que está vinculado ao exercicio dos dereitos de rectificación e oposición.

Con todo, si serían aplicables os seguintes dereitos:

a) O dereito de acceso, aínda que reviste características singulares, xa que require achegar como documentación complementaria unha imaxe actualizada que permita ao responsable verificar e contrastar a presenza do afectado nos seus rexistros. Resulta practicamente imposible acceder a imaxes sen que poida verse comprometida a imaxe dun terceiro. Por iso, de acordo co criterio manifestado pola AEPD, podería facilitarse o acceso que se solicite mediante o formulario establecido na Sede Electrónica da USC no que, coa maior precisión posible, e sen afectar a dereitos de terceiros, se especifiquen os datos que foron obxecto de tratamento.

b) O dereito de supresión das imaxes no prazo máximo dun mes, sen prexuízo da excepción referida anteriormente.

c) O dereito á limitación do tratamento si resultaría aplicable na súa outra vertente, é dicir, mediante a solicitude formulada a través da Sede Electrónica da USC para que se conserven as imaxes cando:

i. O tratamento de datos sexa ilícito e o interesado se opoña á supresión dos seus datos e solicite no seu lugar a limitación do seu uso.

ii. O responsable xa non necesite os datos para os fins do tratamento pero si os necesite para a formulación, exercicio ou defensa de reclamacións.

7.- DENUNCIA DE INFRACCIÓNS E DELITOS

Ante a constatación da comisión dun delito ou infracción aplicaranse as regras de actuación seguintes:

a) Denunciarase o feito ante a autoridade competente dentro das 72 horas seguintes á constatación. Na denuncia farase constar de xeito expreso a existencia dun sistema de videovixilancia na Universidade de Santiago de Compostela, que consta no Rexistro de Actividades de tratamento de datos persoais, así como a identificación do soporte no que se atopan as gravacións.

Este documento é de carácter informativo e non ten valor xurídico. Está elaborado unicamente a partir das normas publicadas en Lex.gal. Consulte a información contida ao respecto na sección de preguntas frecuentes.

b) As imaxes poranse inmediatamente a disposición desta autoridade.

c) Se o soporte que contén as imaxes queda en poder da autoridade competente, procurarase facer unha copia que se arquivará coa comunicación ou denuncia e se documentará debidamente.

d) Cando a natureza do soporte que conteña as imaxes obrigue á entrega dunha copia, mentres que as imaxes se conserven en sistemas da Universidade, estas non se borrarán nin se suprimirán transcorrido o prazo dos 30 días fixados neste protocolo. Manteranse mentres continúe a necesidade conservalas.

e) Notificaranse os feitos presuntamente delictivos á Secretaría Xeral, con copia da denuncia.

8.- COMUNICACIÓN DE IMAXES A TERCEIROS

8.1. En relación coa investigación e axuizamento de infraccións penais ou para a execución das penas.

O artigo 7.1 da Lei Orgánica 7/2021, do 26 de maio, de protección de datos persoais tratados para fins de prevención, detección, investigación e axuizamento de infraccións penais e de execución de sancións penais impón, tanto para as Administracións como para as persoas físicas ou xurídicas, un deber xeral de colaboración coas autoridades xudiciais, o Ministerio Fiscal e a Policía Xudicial.

Nestes supostos, a comunicación destes datos estaría lexitimada polo cumprimento dunha obriga legal e non sería preciso o consentimento do interesado (artigo 236 ter da Lei Orgánica 6/1985, de 1 de xullo, do Poder Xudicial).

8.2. En relación coa prevención, detección e investigación de infraccións penais e para a prevención e protección fronte a un perigo real e grave para a seguridade pública.

O artigo 7.2. da mencionada Lei Orgánica 7/2021, establece, nestes supostos, un deber xeral de colaboración coas autoridades competentes.

Deberán, por tanto, cederse as imaxes que se soliciten, en cumprimento dunha obriga legal. En todo caso, deberá existir unha petición formal da autoridade competente que terá que:

a) ser concreta e específica.

b) conter a motivación que acredite a súa relación cos indicados supostos.

c) facer referencia ao número do procedemento penal do que trae causa.

Todas as solicitudes deberán remitirse á Secretaría Xeral da USC, que será o órgano que analice a súa procedencia e entregue a información, de ser o caso.

8.3. Imaxes solicitadas por particulares.

Este documento é de carácter informativo e non ten valor xurídico. Está elaborado unicamente a partir das normas publicadas en Lex.gal. Consulte a información contida ao respecto na sección de preguntas frecuentes.

Ademais dos supostos mencionados nos apartados precedentes, podería darse o caso de que un particular solicitase acceder a determinadas imaxes gravadas polas cámaras de videovixilancia da USC, para coñecer a identidade dun terceiro, aos efectos de poder exercitar determinadas accións xudiciais e/ou contractuais.

Nestes supostos, de acordo cos criterios establecidos pola AEPD coa fin axustarse á normativa de protección de datos, deberán cumprirse as seguintes condicións:

a) O interese lexítimo invocado deberá referirse ao exercicio do dereito fundamental á tutela xudicial efectiva, na medida que as imaxes serán utilizadas para a obtención de probas para formular unha posterior denuncia por delito ou reclamación por responsabilidade contractual, ou extracontractual a una compañía de seguros.

b) A comunicación de datos non pode perseguir unha finalidade diferente a aquela coa que se recolleron os datos, entrando dentro do termo amplo de "seguridade", aos efectos descritos no parágrafo anterior.

c) A cesión ou comunicación das imaxes de terceiros deberá limitarse ao mínimo necesario para a finalidade pretendida, na medida que o solicitante poida determinar exclusivamente o relacionado co incidente concreto e específico a que se refira a súa petición.

Con todo, deberá analizarse en cada caso se concorren os anteditos requisitos. Así mesmo, de acordo co exposto, esixirase un compromiso por escrito do solicitante de que a única finalidade do uso dos datos persoais comunicados será a descrita anteriormente, advertíndolle das responsabilidades en materia de protección de datos que poden derivarse en caso de empregar os devanditos datos para calquera outro uso.

Todas as solicitudes deberán remitirse á Secretaría Xeral da USC, que será o órgano que analice a súa procedencia e entregue a información, de ser o caso.

9.- AS EMPRESAS DE SEGURIDADE COMO ENCARGADAS DO TRATAMENTO

No caso de que os controis de acceso e seguridade sexan realizados por unha empresa de seguridade allea á USC deberá subscribirse o oportuno contrato para atribuírlle as funcións de encargados do tratamento, de conformidade coa normativa de protección de datos.

A USC, como responsable, debe elixir un encargado do tratamento que ofreza garantías suficientes respecto á implantación e ao mantemento das medidas técnicas e organizativas apropiadas, de acordo co establecido no RGPD, e que garanta a protección dos dereitos das persoas afectadas. Deberase asinar con el un contrato que cumpra coas esixencias contidas na normativa aplicable. O mesmo sucederá se hai acceso aos soportes e medios de gravación por parte de empresas externas que prestan servizos de mantemento.

En todo caso, constarán os seguintes aspectos no referido contrato:

a) As instrucións do responsable do tratamento.

Este documento é de carácter informativo e non ten valor xurídico. Está elaborado unicamente a partir das normas publicadas en Lex.gal. Consulte a información contida ao respecto na sección de preguntas frecuentes.

b) O deber de confidencialidade.

c) As medidas de seguridade adoptadas e os requisitos de prestación do servizo.

d) O réxime da subcontratación.

e) A forma en que o encargado asistirá ao responsable no exercicio dos dereitos dos afectados.

f) A colaboración no cumprimento das obrigas do responsable.

g) O destino dos datos ao finalizar a prestación do servizo.

h) A obriga de cumprir o presente Protocolo.

Por outra banda, debe terse en conta que aqueles sistemas de videovixilancia que vaian estar conectados cunha central receptora de alarmas ou cun centro de control, deberán cumprir o previsto na Lei de Seguridade Privada e demais normativa aplicable.

En todo caso, tenderase a que o encargado do tratamento sexa común para todas as instalacións de videovixilancia da USC. As empresas de seguridade encargadas do tratamento deberán cumprir o presente protocolo e realizar a súa tarefa conforme aos requisitos aquí establecidos, que deberán figurar no correspondente prego de contratación.

10.- SOFTWARE

Os produtos de software destinados ao tratamento automatizado de datos de carácter persoal deberán incluír na súa descrición técnica o nivel de seguridade que teñan implantado.

ANEXO - INFORMACIÓN A DISPOSICIÓN DOS USUARIOS

O texto mínimo que debe figurar como información a disposición dos usuarios será o seguinte:

"Informáselle de que estas instalacións, por motivos de seguridade, contan con sistemas de videogravación de imaxes. As imaxes obtidas por estes sistemas de seguridade serán tratadas conforme ao RGPD e á Lei Orgánica 3/2018, de 5 de decembro, de Protección de Datos Persoais e garantía dos dereitos dixitais.

O responsable do tratamento destas imaxes é a Universidade de Santiago de Compostela, Colexio de San Xerome, Praza do Obradoiro s/n de Santiago de Compostela (A Coruña).

Infórmase ás persoas usuarias que poderán exercitar os dereitos recoñecidos nos artigos 15 a 22 del RGPD, na Sede Electrónica da USC a través do seguinte enlace: https://sede.usc.es/sede/publica/catalogo/procedemento/55/ver.htm.

Direccións de interese:

Este documento é de carácter informativo e non ten valor xurídico. Está elaborado unicamente a partir das normas publicadas en Lex.gal. Consulte a información contida ao respecto na sección de preguntas frecuentes.

• A información sobre protección de datos na USC figura na Web http://www.usc.es/es /normativa/protecciondatos/index.html

• Páxina da Axencia Protección de Datos, https://www.agpd.es

Tratamento dos datos:

a. Tratarase, salvo que resulte imprescindible para a finalidade de vixilancia pretendida ou imposible por razón da localización das cámaras, de non obter imaxes de espazos públicos.

b. Suprimiranse os datos que se obteñan a través da gravación de imaxes obtidas a través dos sistemas de seguridade no prazo máximo dun mes desde a súa obtención (borrado das imaxes obtidas), salvo que deban de ser conservados para acreditar a comisión de actos que atenten contra a integridade das persoas, dos bens ou das instalacións.

c. Adoptaranse as medidas de seguridade técnicas e organizativas para evitar a perda, alteración ou acceso non autorizado ás gravacións.

d. Calquera persoa que por razón do exercicio das súas funcións teña acceso aos datos deberá de observar a debida reserva, confidencialidade e sixilo".

Este documento é de carácter informativo e non ten valor xurídico. Está elaborado unicamente a partir das normas publicadas en Lex.gal. Consulte a información contida ao respecto na sección de preguntas frecuentes.