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

Os sistemas de protección de bens universitarios deben de apoiarse cada vez mais, en sistemas electrónicos, en particular no uso de cámaras que transmiten as imaxes a centros de control para facer a prevención de furtos, delitos ou un acceso non permitido a locais.

Estes sistemas teñen certos riscos que é necesario prevenir, mediante un uso lícito e finalista destas instalacións. Por outra banda a videovixiancia require o cumprimento de normas de protección de datos de carácter persoal.

Coa finalidade de determinar os procedementos para a instalación de cámaras, os seus requisitos e o uso, o Consello de Goberno do 7 de outubro de 2009, aprobou o seguinte

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

1.- Solicitude

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, previo informe da Unidade de Seguridade da USC.

2.- Ficheiros

As instalacións de videovixiancia, no caso de gravar os datos, formarán parte dun ficheiro de protección de datos de carácter persoal, polo que deberá darse conta a Secretaría Xeral a efectos de establecer as medidas de seguridade.

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 ou o documento legal correspondente para atribuírlle as funcións de encargados do tratamento. No documento a asinar entre as partes deberan figuran as medidas de seguridade e os requisitos de prestación do servizo, así como a obriga de cumprir o presente Protocolo.

3.- Finalidades

A Universidade de Santiago de Compostela unicamente admitirá o uso de instalacións de videovixilancia para a satisfacción de finalidades lícitas e lexítimas.

Considerarase lexítima a utilización cos fins seguintes:

a) Control de acceso aos edificios ou a parte destes.
b) Control de acceso a aparcadoiros e garaxes.
c) Seguridade interior.
d) Seguridade en instalacións deportivas.
e) Custodia de bens valiosos.

f) Seguridade no traballo e prevención de riscos laborais.
g) En ningún caso admitirase 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.
    d. Enténdese lexítima a captación de imaxes con fins docentes e de investigación, aínda que terá que notificarse con carácter previo co fin de proporcionar un soporte xurídico adecuado á actividade.

4.- Criterios de uso

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

a) Unicamente será posible para as finalidades descritas neste documento.
b) Unicamente poderán utilizarse aquelas instalacións de videovixilancia que se autorizaron adecuadamente.
c) Se as houbese, seguiranse as instrucións específicas que acompañan a autorización.
d) Sinalizaranse 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 durante un período máximo dun mes.
g) No caso de que se constate a comisión dun delito ou infracción, actuarase co que dispón o apartado sétimo deste protocolo e notificaranse os feitos á Secretaría Xeral con copia da denuncia.
h) Prohíbese:
    a. A captación intencional de imaxes na vía pública, como tamén 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.- Obrigacións de seguridade.

De acordo co que dispón o Real Decreto 1720/2007, do 21 de decembro, os ficheiros automatizados que conteñan datos de carácter persoal, os datos obtidos mediante videovixilancia cualificaranse como de nivel básico.

Os sistemas dedicados á videovixilancia poden estar automatizados ou non estar informatizados:

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.
d. Contarase cun rexistro dos usuarios que conten con chave ou calquera outro medio que permita acceder a instalacións e/ou mobiliario que conteña información protexida.
e. As gravacións se etiquetarán de maneira que se identifique con claridade o contido e vinculación ao sistema e constarán no inventario correspondente.
f. Os soportes reutilizaranse de maneira que se garanta a completa destrución da información que conteñen.
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, e en particular as relativas ás condicións ou consecuencias xurídicas do uso das videocámaras remitirase á dirección ...

5.2 Videovixilancia automatizada

a. As instalacións en que se atopen 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.
d. Contarase cun rexistro dos usuarios que contan con chave ou calquera outro medio que permita acceder a instalacións e ou mobiliario que conteña información protexida.
e. As gravacións se etiquetarán de maneira que se identifique con claridade o contido e vinculación ao sistema e constarán no inventario correspondente.
f. Os soportes reutilizaranse de maneira que se garanta a completa destrución da información que conteñen.
g. O desbote de soportes que conteñan imaxes captadas polos sistemas garantirán a absoluta inaccesibilidade ás imaxes que contiñan.
h. Os sistemas automatizados terán que contar cun control de acceso lóxico con asignación, distribución e almacenamento de contrasinais diferenciados para cada usuario. Estas almacenaranse de xeito inintelixible e cambiaranse periodicamente. Poderán articularse controis distintos cando garantan a seguridade de xeito análogo ao anterior.

i. Se se prevé un acceso ao ficheiro 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.
j. 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.
k. As incidencias que afectan aos sistemas informáticos terán que notificarse a través do procedemento común a través do Documento de Seguridade da USC.
l. 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 Obrigacións dos usuarios

Os usuarios dos sistemas haberán de:

a. Gardar o necesario segredo respecto de calquera tipo de información de carácter persoal coñecida en función do traballo desenvolvido.
b. Manter en segredo as súas claves de acceso ao sistema. Estas son persoais e intransferibles, e o usuario é o único responsable das consecuencias que puidesen derivarse do seu mal uso, divulgación ou perda, casos en que se tería que notificar a incidencia.
c. Cambiar os contrasinais a petición do sistema cando se lle indique.
d. 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.
e. Comunicar as incidencias de seguridade de que teña coñecemento.
f. 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.
g. Gardar todos os soportes físicos que conteñan información nun lugar seguro cando non se utilizan, particularmente fóra da xornada laboral.
h. Unicamente as persoas autorizadas para facelo poderán introducir ou anular os datos contidos no ficheiro obxecto de protección.
i. 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.

6. Información e dereitos

Aos titulares dos datos correspóndenlles, entre outros, os dereitos a ser informado sobre o tratamento, a consentir e/ou oporse a este, como tamén os dereitos de acceso, rectificación e cancelación. Non obstante, en materia

de videovixilancia estes dereitos teñen que modularse tendo en conta as condicións específicas de captación e tratamento.

6.1 Dereito de información na recompilación de datos

Este dereito facilitarase por medio da localización dos sinais deseñados para iso pola Universidade. 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, haberá a disposición dos usuarios folletos en que se indique:

- A existencia dun ficheiro ou tratamento de datos de carácter persoal, da finalidade da recompilación destes e dos destinatarios da información.
- A posibilidade de exercer os dereitos de acceso, rectificación, cancelación e oposición.
- A identidade e dirección do responsable do tratamento ou, no seu caso, do seu representante.

6.2. Consentimento e oposición ao tratamento

Este dereito resulta na práctica imposible de cumprir, a menos que se conte con tecnoloxía adecuada capaz de identificar a imaxe dun suxeito concreto. Entenderase que simplemente pasar por espazos suxeitos a videovixilancia e sinalizados adecuadamente supón un consentimento tácito. Por outra banda, se a Universidade establece como condición de uso dun determinado espazo o seu control por medio de videovixilancia, non resultará necesario este consentimento.
Se, así e todo, un titular dos datos invoca motivos fundados e lexítimos relativos a unha situación persoal concreta, ditarase resolución motivada.

6.3 Dereitos de acceso e cancelación

Na sinalización indicarase unha dirección web para o exercicio destes dereitos. O procedemento e prazo para o exercicio destes dereitos axustarase ás instrucións de procedemento dispoñibles no apartado da web universitaria dedicada á protección de datos http://www.usc.es/es/normativa/protecciondatos/index.html.

En materia de videovixilancia o dereito de rectificación ten unha operatividade moi limitada, xa que en ningún caso poderán alterarse ou falsearse as imaxes captadas. O dereito de acceso é persoalísimo e levarao a cabo a persoa afectada, que terá que remitir ao responsable do tratamento unha solicitude en que fará constar a súa identidade, xunto cunha fotografía actualizada e copia do DNI ou documento equivalente. O escrito dirixirase a:

- Secretaría Xeral Universidade de Santiago de Compostela Colexio de San Xerome Praza do Obradoiro 15782 Santiago de Compostela.

6.4. *Deberes de Seguridade e Secreto*.

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

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 do ficheiro "Videovixilancia" da Universidade de Santiago de Compostela e a identificación do soporte que o contén no inventario correspondente.
b. As imaxes poranse inmediatamente á disposición desta autoridade.
c. Se o soporte que contén as imaxes queda en poder da autoridade competente, procurarase facer copia que se arquivará coa denuncia e documentarase no inventario correspondente.
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 cancelarán transcorrido o prazo dos 30 días fixados neste protocolo. Manteranse mentres continúe a necesidade conservalas.
e. Notificaranse os feitos delictivos á Secretaría Xeral con copia da denuncia.

8. Encargados do tratamento. Empresas de seguridade

Cando o uso das instalacións de videovixilancia se encomende a unha empresa de seguridade, aínda no caso que capte e grave as imaxes con medios propios, terá a condición de encargada do tratamento. Unicamente poderíase considerar responsable do tratamento cando preste servizos exclusivamente de control de acceso aos edificios. Neste caso poderá aplicarse a Instrución 1/1996, de 1 de marzo, da Axencia de Protección de Datos, sobre ficheiros automatizados establecidos coa finalidade de controlar o acceso aos edificios, a norma segunda da cal dispón:
«Terá a consideración de responsable do ficheiro a persoa física ou xurídica, de natureza pública ou privada, ou órgano administrativo por conta da cal se efectúe a realización do servizo de seguridade. No entanto o anterior, por medio do correspondente contrato de prestación de servizos de seguridade, poderá ter a consideración de responsable do ficheiro a empresa que preste os servizos daquela natureza. O responsable do ficheiro asumirá o cumprimento de todas as obrigacións establecidas na Lei Orgánica 5/1992 e, entre elas, a da inscrición do ficheiro no Rexistro Xeral de Protección de Datos».
Polo tanto, cando a empresa de seguridade teña a condición de encargada do tratamento terá que formalizarse, en aplicación do art. 12 LOPD, o contrato adecuado de acceso aos datos por conta de terceiros. O mesmo sucederá se hai acceso aos soportes e medios de gravación por parte de empresas externas que prestan servizos de mantemento.

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 os requisitos aquí establecidos, que deberán figurar no correspondente prego.

9.- Software

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

ANEXO II
INFORMACIÓN A DISPOSICIÓN DOS USUARIOS

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

"Infórmaselle que estas instalacións e por motivos de seguridade contan con sistemas de videogravación de imaxes. As imaxes obtidas por estes sistemas de seguridade serán tratadas conforme á Lei Orgánica 15/1999, de Protección de Datos.

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).

Os datos obtidos a partir das imaxes gravadas, incorporaranse ao ficheiro automatizado de titularidade da Universidade de Santiago de Compostela sendo o responsable do ficheiro a Xerencia da Universidade de Santiago de Compostela (Rúa Nova 6. CP:15782. Santiago de Compostela. A Coruña).

Infórmase aos usuarios que poderán exercitar os seus dereitos de acceso, rectificación e oposición ante a Secretaría Xeral da Universidade de Santiago Colexio de San Xerome, Praza do Obradoiro s/n.15782. Santiago de Compostela. A Coruña. A información para o exercicio destes dereitos figura na web http://www.usc.es/es/normativa/protecciondatos/index.html

***Direccións de interese**:*

- *Páxina da Axencia Protección de Datos, https://www.agpd.es*
- *Protocolo de Videovixiancia da USC e Normativa sobre protección de datos de carácter persoal da USC. http://www.usc.es/es/normativa/protecciondatos/index.html*

***Tratamento dos datos**:*

a. Trataranse, salvo que resulte imprescindible para a finalidade de vixilancia pretendida ou resultar imposible por razón de localización das cámaras, de non obter imaxes de espazos públicos.
b. Cancelaranse 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).
c. Deberes de Seguridade e Secreto. Adoptaranse as medidas de seguridade técnicas e organizativas para evitar a perda, alteración ou acceso non autorizado ás gravacións. Calquera persoa que por razón do exercicio das súas funcións teña acceso aos datos deberá de observar a debida reserva, confidencialidade e sixilo.
d. O prazo para a arquivar as imaxes será dun mes, pasado o cal serán destruídas."

ANEXO I I
Modelo de sinalización: