CNS 12/2010

Dictamen en relació amb la consulta sobre el termini en el qual les entitats resten obligades a conservar la documentació relativa a les auditories

Es presenta davant l'Agència Catalana de Protecció de Dades un escrit en el que es demana que l'Agència emeti un dictamen sobre el termini en el qual les entitats resten obligades a conservar la documentació relativa a les auditories.

(....)

I

(....)

II

Tal com exposa l'entitat que formula la consulta, l'article 96 del Reglament de desplegament de la Llei orgànica de protecció de dades (RLOPD), aprovat pel Reial decret 1720/2007, de 21 de desembre, regula com a obligació dels responsables de fitxers que tinguin nivell mitjà o alt, la necessitat d'elaborar auditories internes o externes, cada dos anys o sempre que es dugui a terme modificacions substancials del sistema d'informació que puguin repercutir en les mesures de seguretat implantades. L'objectiu d'aquestes auditories, d'acord amb l'apartat primer de l'article 96 és verificar el compliment del Títol VIII del Reglament, dedicat a les mesures de seguretat:

> *"1. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoria interna o externa que verifique el cumplimiento del presente Título.*
>
> *Con carácter extraordinario deberá realizarse dicha auditoria siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoria inicia el cómputo de dos años señalado en el párrafo anterior."*

Pel que fa al contingut de l'auditoria, d'acord amb l'apartat segon d'aquest article, haurà de contenir a banda de les conclusions de l'auditor, que han de pronunciar-se clarament sobre l'adequació de les mesures de seguretat efectivament implantades al previst al RLOPD, el detall de les deficiències detectades i la proposta de les mesures correctores, així com totes aquelles dades, fets i observacions en que es recolza l'auditor per dictaminar i recomanar. En principi aquesta serà la documentació a la qual cal entendre referida la consulta, és a dir, tota aquella documentació que forma part de l'auditoria.

A banda d'aquesta informació, d'acord amb l'apartat 3 del mateix article s'ha d'elaborar, per part del responsable de seguretat, unes conclusions que han de ser elevades al responsable del fitxer o tractament, per tal que adopti les mesures adequades. Tot i que, estrictament aquestes conclusions no formen part de l'auditoria, si que en són una conseqüència directa i hi estan estretament lligades, per la qual cosa es considera que també cal conservar-les amb les mateixes condicions que els documents que integren l'auditoria.

D'acord amb aquest mateix apartat tercer de l'article 96, l'informe d'auditoria, ha de quedar a disposició de l'autoritat de control competent, en aquest cas l'Agència Catalana de Protecció de Dades.

III

Centrant-nos ja en la qüestió plantejada a la consulta, atès que l'article 96 ni cap de les altres disposicions vigents en matèria de protecció de dades, estableix de forma expressa el termini que cal conservar la documentació que integra l'auditoria, cal determinar aquest termini a partir de l'anàlisi de les obligacions del responsable del fitxer, en especial del règim de responsabilitats que li pot resultar aplicable.

Un primer criteri obvi, però vàlid com a punt de partida, pot ser que en la mesura que un informe d'auditoria no és un document aïllat sinó que forma part d'un procés continuat d'implantació i avaluació de mesures de seguretat, s'haurà de conservar, com a mínim, fins que no existeixi un ulterior informe d'auditoria, amb independència de que hagi passat el termini de 2 anys des que va ser redactat. Ara bé, com veurem a continuació, l'existència d'un informe d'auditoria posterior, ja sigui l'auditoria bianual o per modificació substancial del sistema d'informació, no implica sense més que hagi cessat l'obligació de conservar l'auditoria anterior.

Al marge del que direm a continuació, des d'un punt de vista estricte d'auditoria, resulta coherent mantenir tota la documentació de l'auditoria mentre es mantingui un determinat sistema d'informació. Disposar d'aquesta documentació pot aportar informació valuosa a processos d'auditoria posteriors per tal de seguir l'evolució de mesures de seguretat aplicades. I encara resulta més recomanable, quan es tracta d'àmbits, com el sanitari, en que l'ordenament vigent obliga a la conservació de determinada informació, en concret la informació que forma part de la història clínica durant períodes molt llargs de temps.

Però més enllà d'això, a l'hora de determinar el termini de conservació cal atenir-se al règim de responsabilitats establert a la LOPD i a la resta de l'ordenament jurídic. És en aquest sentit que l'apartat tercer de l'article 96 requereix que la documentació que forma part de l'auditoria estigui a disposició de l'autoritat de control. I no només com a mitjà que permeti aportar informació sobre determinats incompliments, sinó també des del punt de vista de l'entitat responsable del fitxer, com a mitjà per acreditar el compliment de la normativa vigent.

Des del punt de vista del règim sancionador previst a la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD), l'obligació de dur a terme les auditories és una mesura de seguretat i per tant la manca de la seva realització pot ser sancionada com a falta greu, a tenor del que disposa l'article 44.3.h de la LOPD. D'acord amb l'article 47.1 de la mateixa LOPD el termini de prescripció per a les infraccions greus és de dos anys. Termini de dos anys que caldria comptar des de la data en que es realitza l'auditoria. Per tant aquest seria un primer termini a tenir en compte des del punt de vista de les responsabilitats. Ara bé, no es pot descartar que l'auditoria, igual que ho pot ser, per altres motius, el registre d'incidències, pot ser un valuós element probatori en la investigació d'altres tipus d'infraccions que tenen atribuït un termini de prescripció més llarg, com és el cas de la infracció molt greu prevista l'article 44.4.f) de la LOPD, que tindria un termini de prescripció de tres anys.

Cal fer però un aclariment, perquè el termini de conservació, en aquests casos no abastaria només el termini de prescripció, sinó també el termini necessari per a la conclusió dels procediments sancionadors que s'hagin pogut incoar abans que transcorri aquest termini.

Però el règim de responsabilitats previst a la LOPD no s'esgota amb el règim sancionador, sinó que l'article 19 de la LOPD preveu també la responsabilitat pels danys o lesions que les persones afectades pateixin en els seus béns o drets, ja sigui mitjançant la reclamació de la responsabilitat de l'administració, quan el dany sigui imputable a una administració pública, o mitjançant el sistema de responsabilitat extracontractual previst al dret civil. En aquest sentit, disposar de la documentació relativa a les auditories pot ser un element probatori important per a l'acreditació de la diligència del responsable en el compliment de les mesures de seguretat exigibles. Al respecte cal recordar que la lletra d) de l'article 121-21 del Llibre primer del Codi civil de Catalunya estableix que prescriuen al cap de tres anys les pretensions derivades de responsabilitat extracontractual i la resta de pretensions al cap de 10 anys, llevat de la recuperació de la possessió (arts. 121-20 i 121-22)

D'acord amb les consideracions fetes en aquests fonaments jurídics en relació amb la consulta plantejada en relació amb el termini en el qual les entitats resten obligades a conservar la documentació relativa a les auditories, es fan les següents,

Conclusions

D'acord amb la normativa de protecció de dades, la documentació que forma part de les auditories de seguretat requerides per aquesta normativa, ha de conservar-se per un període mínim de tres anys, o fins que es realitzi l'auditoria de seguretat següent si aquesta no s'ha realitzat dins el termini de dos anys exigible.

Al marge d'això, la conservació d'aquesta documentació pot resultar convenient per un termini més ampli als efectes de disposar d'una informació completa que permeti avaluar l'evolució de les mesures de seguretat aplicades, i també als efectes de disposar d'elements probatoris del compliment de la normativa vigent en matèria de protecció de dades, mentre no hagin prescrit les responsabilitats pels danys que s'hagi pogut ocasionar amb el tractament de dades.