CODI TIPUS INFORMA **78/14**

Sobre el control d'accessos indeguts

La normativa de protecció de dades determina la necessitat de disposar d'un registre d'accessos per a tots aquells sistemes informàtics i documentació que tractin dades de nivell alt. Concretament aquest aspecte queda regulat a l'article 103 del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

L'establiment del registre d'accessos no es limita a la seva mera existència, sinó que per a tots aquells fitxers o tractaments informatitzats, a més, serà necessari fer una revisió de la informació registrada.

Com bé diu l'apartat 5 del precepte 103 ja citat, "*el responsable de Seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados*".

De manera que no només s'ha de disposar d'un registre dels accessos esdevinguts a les dades de nivell alt sinó que també serà necessari revisar-los mensualment, a fi de detectar possibles accessos no autoritzats.

El Codi Tipus ha considerat interessant l'elaboració del present document per tal de donar unes pautes d'actuació a les entitats sobre com desenvolupar aquest control d'accessos a les dades emmagatzemades als sistemes d'informació de les entitats.

Com moltes entitats han manifestat, la verificació de tots els accessos és molt complicada pel volum de moviments i accessos que es generen mensualment. És per això, que des del Codi Tipus recomanem fer una revisió mensual d'una mostra dels expedients o HC (aconsellem que no sigui inferior a 20 expedients/HC) de manera aleatòria, procedint llavors a elaborar un informe tot indicant els fitxers revisats, els resultats obtinguts i les anomalies detectades, en el seu cas.

Existeix també la possibilitat de fer la revisió sobre els accessos efectuats per un treballador concret, si es té la sospita que aquest ha accedit a dades que, d'acord amb el seu perfil, no li corresponien.

Tornant a la opció d'efectuar revisió dels expedients/HC, el criteri de selecció de la mostra és un aspecte important, pel que, sota el nostre criteri, s'haurien de revisar les HC o expedients que siguin més susceptibles de ser accedits de manera il·legítima, com ara les HC dels propis treballadors de l'entitat, pacients que no hagin estat visitats en un període llarg de temps, HC de pacients VIP's o notòries, etc.

Determinades les HC que s'examinaran, serà necessari analitzar una per una, fent la revisió dels accessos esdevinguts i comprovant que la persona que ha accedit disposa d'autorització per fer-ho. Des del Codi Tipus, aconsellem que la verificació d'aquests accessos es dugui a terme de manera conjunta per personal tècnic (sistemes d'informació) i personal assistencial o de RRHH per tal de determinar de manera fefaent la procedència o improcedència de l'accés.

Posteriorment, un cop analitzades les HC, si es detecta alguna anomalia en els accessos, identificant accessos no autoritzats, cal que es citi a l'usuari afectat per tal que es justifiqui en la seva actuació. Si, malgrat la seva justificació es considera que l'accés no es troba autoritzat, l'entitat haurà d'adoptar les mesures disciplinàries que corresponguin d'acord amb el conveni laboral aplicable, modulant-les tenint en compte les circumstàncies concretes de cada cas.

En aquest punt, considerem molt important comentar que el manual de bones pràctiques haurà d'informar sobre aquest aspecte, detallant l'existència de perfils d'usuaris per tal d'acotar els tipus d'accés i informant als usuaris que s'han de limitar a accedir a la informació que els hi correspon d'acord amb el seu perfil. Així mateix, s'hauria d'informar de la possibilitat de que es revisin els accessos a les HC i finalment, establir les conseqüències de l'incompliment de les funcions encomanades als treballadors.

Barcelona, 27 de novembre de 2014