INFORME D' AUDITORIA GLOBAL SOBRE EL COMPLIMENT DE LA LLEI ORGÀNICA 15/1999 DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL (L.O.P.D.)

PETICIONARI:
CONSORICI BIBLIOTEQUES DE BARCELONA
La Rambla 99, 1º
08019 Barcelona

RESULTATS: RESUM EXECUTIU

El CONSORCi DE BIBLIOTEQUES DE BARCELONA s'ha sotmès a una auditoria externa sobre el compliment de la Llei Orgànica 15/1999 de protecció de dades de caràcter personal i l'aplicació de les mesures de seguretat que estableix el seu Reglament de desenvolupament 1720/2007.

Els resultats obtinguts per l'equip auditor és el d'una entitat que està plenament conscienciada en complir amb la citada normativa i que ha fet millores respecte de l'anterior auditoria del 2014, posant en marxa les accions correctores proposades.

Es disposa d'un Responsable de Seguretat degudament nomenat que vetlla per l'aplicació i compliment de la normativa tant a les oficines centrals ubicades a la Rambla 88 com a totes les biblioteques que en formen part.

Per tant el compliment actual del CONSORCI es valora com a ALT:

Registre de fitxers: La situació actual de fitxers inscrits al registre de l'APDCAT respon a la realitat de tractament de dades dut a terme pel CONSORCI. Per tant no s'han detectac nous fitxers a serveis centrals ni s'ha detectat la necessitat de suprimir-ne'n cap. Tant les finalitats com els nivells de seguretat assignats s'ajusten a l'actualitat.

No obstant, com a resultat de la revisió duta a terme a algunes de les biblioteques, s'han detectat alguns fitxers que actualment no estan declarats. S'haurà de determinar quin d'aquests registres decideix mantindre el Consorci, amb totes les conseqüencies tant legals com tècniques que això implicaría (declaració dels nous fitxers davant l'APDCAT, avisos legals, mesures de seguretat).

Revisió de protocols: Tots els responsables dels fitxers han signat degudament el seu nomenament formal assumint les funcions i obligacions que en materia de protecció de dades els hi corresponen tenint en compte totes les accions establertes en el seu protocol: avisos legals, contractes amb tercers i períodes de retenció de la informació, així com els procediments establerts per atendre els drets dels afectats (accés, rectificació, cancel·lació i oposició)

El compliment és elevat, no obstant es proposen una serie d'accions que resumim a continuació:

FITXER ACTIVITATS I ESDEVENIMENTS CULTURALS:

- Formulari gravacions de tercers: es proposa canviar el camp "domicili" pel camp "telf", doncs s'ajusta més al principi de qualitat de les dades establert a l'art. 4 de la LOPD.

FITXER RRRHH

- Està previst l'ús d'una nova aplicació informàtica en SAP per l'elaboració de nòmines, pel que serà necessari subscriure l'oportú contracte d'encarregat del tractament.
- En quan al fitxer de "treballs per la comunitat" es recomana l'elaboració d'un EXCEL de control per procedir a la eliminació definitiva de l'expedient passat l'any en curs.

- Certificats de delinqüents sexuals: (Llei 26/2015, de 28 de juliol que modifica el sistema de protecció a la infancia i a l'adolescencia): el fet d'emmagatzemar aquest tipus de certificat implica tenir en compte les mesures de seguretat de nivell mig que en aquest cas serien les següents:

    - Auditar el citat fixter cada dos anys
    - Si es guarden en format electrònic: habilitar mecanismes per identificar els diferents intents fallits als sistemes d'informació per part d'un mateix usuari.
    - Si es guarden en format paper: Tancat amb clau i d'accés restringit al personal autoritzat.

  Pel que fa a la resta de mesures, no cal la declaració d'un fitxer a part, doncs s'emmarcaria dins el fitxer de RRHH (Que ja està declarat de nivell alt) i en quan a l'avís legal son dades necessàries per dur a terme la contractació per tant es disposaría d'habiliatació legal per poder incorporar-la a l'expedient del treballador, sense èsser necessari el consentiment exprés del mateix.

- Candidats (CV): Es proposa afegir a l'avís legal que actualment consta a l'instància, el període de retenció de 5 anys que aplica el Consorci. A més es recomana incloure l'avís legal complert a les bases de contractació per cobrir possibles casos en que el candidat no utlitizi el model d'instància de l'entitat.

FITXER VOLUNTARIS

- Degut a la publicació de la nova Llei del voluntariat deixarà d´ èsser competència pel Consorci la gestió de voluntaris passant a dependre del Consell de l'Associacionisme i el Voluntariat de Catalunya, òrgan consultiu i d'assessorament en la matèria. Per tant s'haurà de donar de baixa el fitxer al registre de l'APDCAT.

En matèria de **formació** s'han dut a terme varies accions durant el 2016 que garanteixen un alt grau de coneixement per part dels treballadors de les biblioteques.

Finalment en el tema de les **mesures de seguretat** hem de destacar el següent:

Els fitxers del CONSORCI resideixen majoritàriament, en els servidors de l'IMI que presta els serveis informàtics i de hosting al CONSORCI, per tant l'encarregat de vetllar per l'aplicació de les mesures de seguretat que estableix el Reglament de la LOPD. En el moment de l'auditoria s'ha pogut verificar de l'existència d'un contracte. En relació a les altres empreses externes que ofereixen serveis de hosting per determinats fitxers, també s'han subscrit correctament. El fet de que aquest contracte amb l'IMI s'hagi signat, eleva substancialment el compliment per part del Consorci respecte de l'anterior auditoria, on les principals deficiències es centraven es aspectes purament tècnics que depeníen, en la gran majoría, de l'IMI.

Per altra banda en quan al **Document de Seguretat** de l'entitat cal assenyalar que es manté complert i plenament actualitzat. Alguns dels annexos (purament tècnics) depenen directament de l'IMI (com encarregats del tractament en temes de serveis informàtics i de hosting) i s'ha fet una bona feina recabant tota aquesta informació tècnica al Document de Seguretat del Consorci.

Com a annexes desactualitzats únicament s'ha detectat l'annex C (on ja no hi hauria de constar el fitxer BAC).

En relació a l'aplicació de les **mesures de seguretat tècniques e informàtiques** el CONSORCI està aplicant les mesures establertes per l'IMI. S'han pogut comprovar les següents evidències:

- Identificació i autenticació: Usuari i contrasenya personal. No obstant les contrasenyes no caduquen tal i com estableix la normativa (com a mínim un cop l'any) ni l'usuari es bloqueja després de varis intents d'accés fallit al sistema.
- Control d'accessos: Les aplicacions informàtiques amb les que treballa el personal del consorci tenen un control d'accés restringit segons usuaris autoritzats. La part d'ofimàtica que en l'anterior auditoría estava oberta, i permetia a qualsevol usuari tenir accés a qualsevol departament, ara ja ha quedat solventat tècnicament, de tal manera que cada usuari només accedirà al que li correspongui segons les seves competències. S'han establert, doncs, polítiques d'accés segons estableix la normativa.

Hem detectat no obstant l´existència de documents escanejats (informes de PRL) que contenen dades de nivell alt i per tant s´han de protegir amb les mesures de seguretat que preveu el Reglament per aquest nivell si es volen seguir conservant en aquest format.

En relació a l'aplicació de les **mesures de seguretat als fitxers no automatitzats (paper)** les mesures son elevades. S'ha verificat que la documentació està tancada dins armaris degudament tancats amb clau i d'accès restringit al personal autoritzat. L'entitat disposa de màquines destructores de paper. Les dades en paper de nivell alt estan degudament tancades en armaris amb clau, no existeix un registre d´accés però existeix només un responsable per la seva gestió.

Per acabar es presenta una avaluació in situ duta a terme a dues biblioteques escollides com a mostra per tal de comprovar les accions aplicades actualment:

Hem pogut comprovar que en general la normativa de protecció de dades es compleix adequadament, existeix una elevada conscienciació per part dels seus responsables sobre la importància de dur a terme les mesures previstes per la legislació vigent.

Hem detectat no obstant, algunes irregularitats relacionades amb les captacions d'imatges i les gravacions a les sales d'actes que no reuneixen els requisitis d'informació i consentiment establerts a la normativa.
Per aixo s'haurà d'elaborar un protocol d'actuació on es reuneixen els diferents supòsits i situacions que es poden donar a les biblioteques i que sigui difòs a tot el personal que hi treballa per evitar possibles conflictes i les corresponents denuncies d'algun afectat.

Conclusions finals

El resultat del present informe i el pla d'acció que se'n derivi hauràn d'èsser elevats als responsables delegats de cada fitxer així com als responsables de cada biblioteca per tal de tenir coneixement del resultat de la present auditoria i poder aplicar les mesures correctores que en aquest es proposen.

Així mateix amb l'entrada en vigor del nou Reglament europeu de protecció de dades el passat 25 de maig de 2016 (Reglamento 2016/679 del parlamento europeo y del consejo del 27 de abril del 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos) es deixa de marge dos anys perquè les organitzacions puguin adaptar-se i per tant no començarà a ésser aplicable fins al proper maig del 2018.

Recomanem per tant, anar preparant des de ja, l'aplicació d'aquestes mesures, així com d'altres modificacions pràctiques derivades del propi Reglament.