Implantació de legislació internacional en matèria de protecció de dades

Javier Padilla Vázquez
Grau d'enginyeria informàtica
Administració de xarxes i sistemes operatius

Joan Ramon Esteban Grifoll
Pierre Bourdin

03/01/2018


Aquesta obra està subjecta a una llicència de Reconeixement-NoComercial-SenseObraDerivada 3.0 Espanya de Creative Commons

FITXA DEL TREBALL FINAL

Títol del treball:	*Implantació de legislació internacional en matèria de protecció de dades*
Nom de l'autor:	*Javier Padilla Vázquez*
Nom del consultor/a:	*Joan Ramon Esteban Grifoll*
Nom del PRA:	*Pierre Bourdin*
Data de lliurament (mm/aaaa):	*01/2018*
Titulació o programa:	*Grau d'enginyeria informàtica*
Àrea del Treball Final:	*Administració de xarxes i sistemes operatius*
Idioma del treball:	*Català*
Paraules clau	*LOPD, Dades, Personals*

Resum del Treball (màxim 250 paraules): *Amb la finalitat, context d'aplicació, metodologia, resultats i conclusions del treball*

La finalitat d'aquest treball és la implantació de la legislació en matèria de protecció de dades vigent en una organització amb presència en Espanya, Portugal, França, Regne Unit, Mèxic i els EUA. Aquesta organització, el grup JPV, és un conglomerat patrimonial de companyies que operen en el sector immobiliari que administren registres d'empleats i d'accés a immobles. Totes les societats són filials de l'empresa JPV Inversions S.L., que actua com a empresa matriu i en conjunt, disposa de 86 treballadors, sumant una empresa d'activitats hípiques i una Fundació.

La metodologia utilitzada consta de quatre punts: recopilació de les normatives internacionals aplicables a l'àmbit del projecte; coordinació de la comunicació per obtenir tota la informació necessària a l'organització; anàlisi de la informació per identificar els aspectes clau d'aplicació al projecte; desenvolupament un mecanisme de documentació estandarditzat i definit. El mètode de treball per tant, és personalitzat i adaptat a les particularitats d'aquest projecte, i es compon d'un seguit de tasques analítiques i de recopilació normativa, amb el seguiment d'un patró d'execució cronològic per assolir els objectius fixats.

Els resultats obtinguts són una taula de requisits globals i un document de proposta d'implantació per obtenir el principal objectiu del treball: la consecució d'una certificació en matèria de protecció de dades en l'organització abans del 31 de desembre del 2018.

El treball ha suposat un coneixement de les diferents legislacions en matèria de protecció de dades i s'han assolit els objectius plantejats seguint el pla de treball inicial i la metodologia proposada.

Abstract (in English, 250 words or less):

The purpose of this work is the implantation of the international legislation on data protection in an organization present in the following countries: Spain, Portugal, France, United Kingdom, Mexico and the USA. This organization, the JPV holding, is a conglomerate of legacy companies active in real state that manages employees and access to building records. All the companies are subsidiaries of JPV Investments S.L. the parent company that has a total of 86 workers, including a company of equestrian activities and a Foundation.

The methodology used consists of four main points: a compilation of the applicable international law; the coordination of the communication to obtain all the necessary information; the analysis of the information to identify the main aspects; the development of a standardized and well defined mechanism. The method of work adopted is personalized and adapted to the particularities of this project, and it consists of analytical tasks and a normative compilation, with the tracking of a chronological execution pattern to achieve the objectives set out.

The results achieved are a table of global requirements and a proposal to implement document to obtain the main objective of the work: the achievement of a certification in data protection before the 31 of December of the 2018.

The work has represented a knowledge of the different legislations in data protection and the objectives outlined have been achieved following the plan of initial work and the methodology proposed.

Índex

Llista de figures

Llista de taules normatives

1. Introducció

1.1 Context i justificació del Treball

Avui dia, a través de la Responsabilitat Social Corporativa (RSC), les empreses adquireixen cada vegada una major rellevància dels aspectes ètics derivats de les seves activitats en l'entorn d'una societat d'individus. Al seu torn, augmenta la preocupació d'aquesta societat per la protecció efectiva de les dades de caràcter personal i el seu possible ús fraudulent. Per tant, i davant el repte que suposa protegir la privacitat dels diferents individus que conformen una societat, la primera raó per justificar aquest treball rau precisament en els aspectes ètics adquirits per l'empresa a través d'aquesta RSC.

En segon lloc, la implantació de les normes relatives a la protecció de dades personals millora tota la seguretat informàtica de l'organització, i per tant, s'eviten perills i riscos derivats dels accessos no desitjats a la xarxa i altres amenaces que posen en perill el normal funcionament de l'organització.

En tercer lloc, l'obtenció d'una certificació en matèria de protecció de dades augmenta la credibilitat de l'organització davant dels seus clients i la imatge corporativa d'aquesta, la qual cosa es tradueix en noves oportunitats de negoci i altres beneficis.

D'altra banda, avui en dia, per a determinats contractes mercantils i negocis empresarials s'exigeix certificar l'estricte compliment d'aquesta normativa, i, per tant, la no implantació d'aquesta normativa per part de l'organització pot suposar la pèrdua de competitivitat davant d'altres companyies.

Finalment, l'incompliment de la legislació en matèria de protecció de dades pot comportar importants sancions econòmiques, amb el consegüent perjudici per a l'organització.

1.2 Objectius del Treball

L'objectiu d'aquest treball és la **consecució d'una certificació en matèria de protecció de dades en tots els països àmbit del treball abans del 31 de desembre del 2018**. A més d'aquest objectiu, es volen obtenir els següents objectius operatius:

- **Incrementar la seguretat de la informació de la companyia en un 30% durant els pròxims dos anys.**
- **Augmentar la credibilitat de l'organització davant els seus clients en més d'un 50% durant els pròxims tres anys.**

1.3 Enfocament i mètode seguit

L'enfocament d'aquest treball ha estat estructurat en quatre fases. En una primera fase es recopila la legislació actual en matèria de protecció de dades en tots els països on opera la companyia. En una segona fase, s'identifiquen les bases de dades i registres amb dades de caràcter personal administrades per l'organització. En una tercera fase es realitza un estudi analític del compliment de la legislació vigent a les bases de dades identificades, i per últim, en una quarta fase es proposa un esborrany de millora per adaptar l'organització a la legislació vigent.

El mètode de treball per tant, és personalitzat i adaptat a les particularitats d'aquest projecte, i es compon d'un seguit de tasques analítiques i de recopilació normativa, amb el seguiment d'un patró d'execució cronològic per assolir els objectius fixats.

1.4 Planificació del Treball

Desglossament de tasques del projecte

• ***Tasca 1: Recopilar i analitzar les diferents legislacions***

Descripció de la tasca

Recollir i analitzar la normativa actual en l'àmbit de la protecció de dades personals en tots els països afectats.

Objectius de la tasca

- Obtenir tot el marc legal aplicable en els països on està present l'organització.
- Realitzar un diagrama de totes les mesures aplicables.

Subtasques:

- *Tasca 1.1:* Recopilar i analitzar legislació espanyola.
- *Tasca 1.2:* Recopilar i analitzar legislació portuguesa.
- *Tasca 1.3:* Recopilar i analitzar legislació francesa.
- *Tasca 1.4:* Recopilar i analitzar legislació britànica.
- *Tasca 1.5:* Recopilar i analitzar legislació mexicana.
- *Tasca 1.6:* Recopilar i analitzar legislació americana.

• ***Tasca 2: Identificar bases de dades.***

Descripció de la tasca

Estudiar i identificar totes les bases de dades gestionades per l'organització que emmagatzemen registres de caràcter personal i definir el nivell de seguretat d'aquestes dades.

Objectius de la tasca

- Identificar totes les bases de dades gestionades per l'organització.
- Reconèixer les bases de dades amb registres de caràcter personal.
- Analitzar el nivell de seguretat d'aquestes dades.

• ***Tasca 3: Revisar el nivell de compliment.***

Descripció de la tasca

Contrastar amb el diagrama obtingut a la tasca 1 el nivell de compliment de la normativa d'aquestes bases de dades en l'organització.

Objectius de la tasca

- Identificar les mesures de seguretat aplicades a les bases de dades identificades en la tasca 2.
- Comparar les mesures aplicades amb les mesures aplicables segons normativa obtingudes a la tasca 1.

• ***Tasca 4: Documentar proposta de compliment.***

Descripció de la tasca

Documentar un esborrany de proposta de millora per adaptar els sistemes informàtics de l'organització a la legislació vigent.

Objectius de la tasca

- Realitzar un pla d'actuació amb les mesures a aplicar en l'organització per complir la normativa vigent en matèria de protecció de dades de caràcter personal.

Cronograma i Diagrama de Gantt

Tasca	Subtasca	Inici	Final	Activitat	Duració
Definició del projecte		20/09/2017	27/09/2017	Definir el tema del TFG	7 dies
El·laboració del pla de treball		28/09/2017	05/10/2017	El·laborar el pla de treball del TFG	10 dies
Pla de Treball		20/09/2017	06/10/2017	Entrega del Pla de Treball	17 dies
Definició estrategia, objectius i àmbit		07/10/2017	10/10/2017	Definir la estratègia, els objectius i l'àmbit del TFG	4 dies
	Tasca 1.1	11/10/2017	13/10/2017	Recopilar i analitzar legislació Espanya	3 dies
	Tasca 1.2	14/10/2017	16/10/2017	Recopilar i analitzar legislació Portugal	3 dies
	Tasca 1.3	17/10/2017	19/10/2017	Recopilar i analitzar legislació França	3 dies
	Tasca 1.4	20/10/2017	22/10/2017	Recopilar i analitzar legislació Regne Unit	3 dies
	Tasca 1.5	23/10/2017	25/10/2017	Recopilar i analitzar legislació Mèxic	3 dies
	Tasca 1.6	26/10/2017	28/10/2017	Recopilar i analitzar legislació EUA	3 dies
Tasca 1		07/10/2017	28/10/2017	Recopilar i analitzar les diferents legislacions	18 dies
Tasca 2		29/10/2017	10/11/2017	Identificar bases de dades	13 dies
PAC2		07/10/2017	10/11/2017	Entrega de la PAC2	35 dies
Tasca 3		11/11/2017	20/11/2017	Revisar nivell de compliment	10 dies
Tasca 4		21/11/2017	30/11/2017	Documentar proposta de compliment.	10 dies
Valoració econòmica		01/12/2017	03/12/2017	Realitzar valoració econòmica	3 dies
Conclusions		04/12/2017	06/12/2017	Analitzar les conclusions del projecte	3 dies
Introducció		07/12/2017	12/12/2017	Realitzar la introducció del TFG	6 dies
Maquetació, annexos i bibliografia		13/12/2017	16/12/2017	Maquetar, corregir i afegir annexos i bibliografia	4 dies
PAC3		11/11/2017	16/12/2017	Entrega de la PAC3	36 dies
Presentació		17/12/2017	24/12/2017	Realitzar diapositives de presentació	8 dies
Video		25/12/2017	03/01/2018	Realitzar el vídeo del TFG	10 dies
Final		17/12/2017	03/01/2018	Entrega Final	18 dies

Figura 1. Cronograma del TFG (vegeu Annex I)

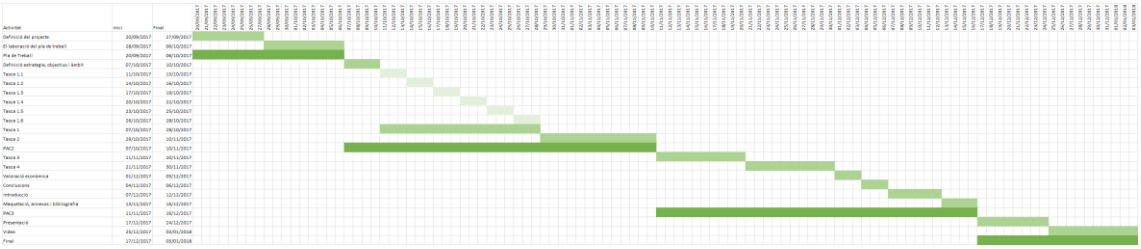

Figura 2. Diagrama de Gantt del TFG (vegeu Annex II)

1.5 Breu sumari de productes obtinguts

Els productes obtinguts a la finalització d'aquest projecte són:

- **Memòria Final**
- **Presentació de defensa**
- **Annexos**
- **Taula de requisits global**
- **Document de proposta d'implantació**

1.6 Breu descripció dels altres capítols de la memòria

Els capítols d'aquesta memòria breument resumits són aquests:

- **Contextualització: Descripció de l'organització i antecedents**

  Breu descripció de l'organització i dels antecedents per contextualitzar la finalitat del projecte.

- **Implantació del projecte**

  - **Definició de l'estratègia, objectius i àmbit d'aplicació**

    Resum de l'estratègia utilitzada, dels objectius del treball i l'àmbit d'aplicació del projecte.

  - **Anàlisi normativa**

    Recopilació i breu anàlisi de les normatives i legislacions aplicables en els països àmbit del projecte.

  - **Identificació de les bases de dades**

    Recerca i revisió de les bases de dades registrades a l'organització analitzant les seves característiques.

  - **Revisió analítica de la situació actual**

    Anàlisi de la situació actual de les bases de dades identificades en el punt anterior i elaboració de les taules de requisits en funció de la normativa aplicable.

  - **Document de proposta d'implantació**

    Resum executiu que detalla les tasques i mesures que cal dur a terme per la consecució dels objectius del projecte.

- **Valoració econòmica**

  Valoració econòmica d'acord amb les tasques identificades en el Document de Proposta d'Implantació.

- **Conclusions**

  Conclusions finals de projecte.

2. Contextualització: Descripció de l'organització i antecedents

El **grup JPV** és un conglomerat patrimonial que aglutina diferents companyies internacionals que operen en el sector immobiliari d'Espanya, Portugal, França, Regne Unit, Mèxic i els Estats Units i que actuen com a responsables de fitxers de dades de caràcter personal en comptar, entre d'altres, amb registres d'empleats i d'accés a immobles. Totes les societats immobiliàries del grup són filials de l'empresa **JPV Inversions S.L.**, que actua com a empresa matriu. Actualment, en conjunt, la part immobiliària disposa de 70 treballadors.

El grup també administra una empresa amb 10 treballadors dedicada a la gestió d'activitats hípiques anomenada **Atticus S.L.**, responsable d'un club hípic on s'organitzen diverses activitats relacionades amb l'hípica, i la **Fundació JPV**, on treballen 6 persones i que actua com a canalitzador dels projectes socials del grup:

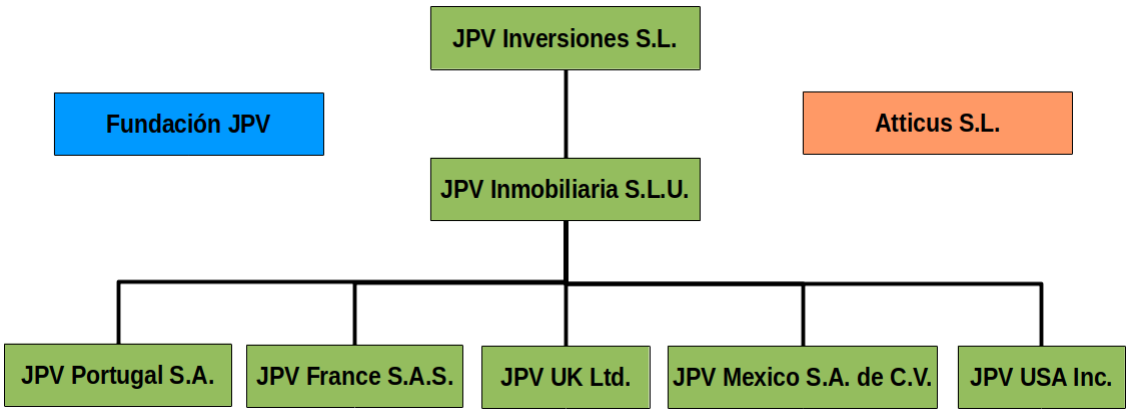

Figura 3. Organigrama del grup JPV

La gestió informàtica de la companyia està externalitzada mitjançant la consultora proveïdora de serveis informàtics **Calpurnia Consulting S.L.**, i

també disposen de consultors externs per al desenvolupament de les aplicacions **SAP** i les auditories financeres i fiscals.

La direcció del **grup JPV** està preocupat pels aspectes ètics de la protecció de dades personals en la seva organització i en la seva credibilitat davant dels seus possibles inversors i clients. A més, el grup representa els interessos patrimonials d'un conegut empresari i per tant, les actuacions del grup repercuteixen en la bona imatge d'aquest empresari.

D'altra banda, es volen evitar possibles sancions i la possibilitat de perdre contractes i altres negocis a causa de l'incompliment de les diferents legislacions vigents a cada país on opera.

Per tot això, el **grup JPV** planteja la necessitat d'adaptar la seva organització a la normativa vigent en matèria de protecció de dades personals en tots els països on opera i adaptar la seguretat informàtica de tota l'organització als requisits de seguretat i privacitat global.

En resum, les característiques principals de l'organització són les següents:

- Disposa d'una plantilla de 86 treballadors repartits arreu del món.
- Les activitats del grup són la gestió esportiva, les obres socials i un 90% de l'activitat és la gestió immobiliària.
- Disposa d'oficines repartides en els següents països: Espanya, Portugal, França, Regne Unit, Mèxic i EUA.
- L'organització disposa de treballadors externalitzats.

3. Implantació del projecte

3.1 Definició de l'estratègia, objectius i àmbit d'aplicació

Estratègia

La implantació d'una legislació internacional en matèria de protecció de dades requereix adoptar una estratègia ben definida per la consecució òptima del projecte:

- En primer lloc, cal realitzar un treball de recerca per recopilar exhaustivament totes les normatives internacionals aplicables a l'àmbit del projecte.
- Seguidament, s'ha de coordinar la comunicació amb tots els grups de treball per obtenir tota la informació necessària a l'organització.
- És també necessari una estratègia acurada d'anàlisi de la informació per identificar els aspectes clau d'aplicació al projecte.
- Finalment, s'ha de desenvolupar un mecanisme de documentació estandarditzat i definit.

Objectius

Aplicant l'estratègia esmentada, els objectius a assolir en aquest treball són:

- L'obtenció per part del **grup JPV** d'una certificació oficial en matèria de protecció de dades efectiva abans del 31 de desembre del 2018.

- Incrementar la seguretat informàtica de l'organització en un 30% abans de la fi del 2019.
- Augmentar la credibilitat de la companyia davant els seus clients en més d'un 50% durant els pròxims dos anys.

Àmbit d'aplicació

Per tant, aquells conceptes no inclosos en els objectius i l'estratègia abans definits quedaran fora de l'àmbit d'aquest treball. Concretament, l'aplicació del projecte se circumscriu a l'àmbit del **grup JPV** descrit anteriorment i amb presència als següents països:

- Espanya
- Portugal
- França
- Regne Unit
- Mèxic
- EUA

La implantació del projecte tindrà en compte els diferents bases de dades i registres de caràcter personal, mantinguts i gestionats per aquesta organització.

3.2 Anàlisi normativa

Encara que existeix infinitat de normativa referent a la protecció de dades de caràcter personal, com expliquem en l'àmbit d'aplicació del treball, aquest es centra en les bases de dades i registres de caràcter personal mantinguts i gestionats per una organització, i per tant, no entrarem en matèria de comunicacions comercials (*spam*), drets dels usuaris o sectors amb regulacions especials com el transport i la salut.

3.2.1. Unió Europea

A Espanya, Portugal, França i Regne Unit (malgrat el recent referèndum, el Regne Unit segueix sent un estat membre fins al 2019), com a països membres de la UE, el dret comunitari s'integra directament en els seus ordenaments jurídics, de manera que no cal una fórmula especial per inserir-los. Dins de l'àmbit de la UE tenim la següent normativa referida a la protecció de dades de caràcter personal:

- **Reglament 2016/679 de 27 d'abril de 2016 relatiu a la protecció de les persones físiques en el tractament de dades personals i la lliure circulació d'aquestes dades. (RGPD)**

  Aquest *reglament* va entrar en vigor el 25 de maig del 2016, encara que estableix un període de dos anys per adaptar-se al nou sistema. És d'obligatori compliment i directament aplicable a tots els seus membres. Substitueix la *directiva* anterior 95/46/CE. El nou reglament s'aplica a responsables de tractament de dades establerts a la UE, i per tant, aplica a les empreses del **grup JPV** amb domicili als països membres.

  Com a principal novetat s'estableix el principi de responsabilitat activa amb l'adopció d'un seguit de mesures des del mateix moment del disseny de les dades o la realització d'avaluacions d'impacte sobre la protecció de dades.

  A més, revisa la forma d'obtenció del consentiment, amb caràcter general lliure, informat, específic i inequívoc, i explícit en el cas d'autoritzacions per al tractament de dades sensibles.

  Una altra novetat d'aquest reglament es refereix als avisos de privacitat, no obligatoris en molts casos amb l'anterior normativa.

- **Directiva 95/46/CE de 24 d'octubre de 1995 relativa a la protecció de les persones físiques en el que respecte al tractament de dades personals i a la lliure circulació de les dades.**

  Aquesta directiva estableix el marc de referència vigent en matèria de protecció de dades personals en la UE, i en Espanya es va transposar mitjançant la *llei orgànica* 15/1999 de 13 de desembre de protecció de dades de caràcter personal (LOPD). Serà substituïda amb l'entrada en vigor del reglament 2016/679 el 25 de maig de 2018.

- **Supervisor Europeu de Protecció de Dades (SEPD).**

  El SEPD és una autoritat supervisora independent que té com a objectiu principal garantir que les institucions europees compleixen la normativa en matèria de protecció de dades personals Per tant, a efectes d'aquest treball, no té cap transcendència.

La RGPD, per tant, s'estableix com la normativa general aplicable a les empreses ubicades a la UE en aquest treball. Encara que el RGPD serà d'aplicació directa en tots els estats membres de la UE, fins a la definitiva entrada en vigor, deurem analitzar les normatives particulars a cada país amb presència de l'organització, per poder donar resposta a possibles situacions no cobertes per aquesta:

1. Espanya

La normativa bàsica reguladora a Espanya en matèria de protecció de dades és la següent:

- **Llei orgànica 15/1999 de 13 de desembre de Protecció de Dades de Caràcter Personal, coneguda com LOPD.**

Aquesta llei desenvolupa la directiva 95/46/CE i té per objecte la protecció i la garantia del tractament de les dades personals, les llibertats públiques i els drets fonamentals de les persones físiques. L'àmbit d'aplicació de la LOPD són les dades de caràcter personal registrades en suport físic i susceptibles de tractament per un ús posterior en el sector públic i privat.

- **Reial Decret 1720/2007 de 21 de desembre del Reglament de desenvolupament de la LOPD, conegut com a RLOPD**

  El *Reial Decret* 1720/2007 estableix i desenvolupa les mesures de seguretat dels fitxers automatitzats que continguin dades de caràcter personal. En el títol VIII d'aquest es descriuen les mesures de seguretat en el tractament de les dades i diferència entre:

  - **Mesures de nivell bàsic**: Aplicables a qualsevol fitxer de dades de caràcter personal.
  - **Mesures de nivell mitjà**: Aplicables quan les dades abastin informació d'infraccions administratives o penals, solvència patrimonial, tributs i altres dades que permetin definir un perfil del subjecte.
  - **Mesures de nivell alt**: Aplicables a fitxers especialment protegits com els referents a ideologia, religió, vida sexual o salut.

- **Recomanacions dictades pel director de l'Agència espanyola de protecció de dades (AEPD).**

  Aquestes recomanacions tenen l'objectiu d'adequar correcte compliment de la normativa espanyola en matèria de protecció de dades. La seva elaboració respon al desenvolupament de plans sectorials referents a les administracions públiques, el comerç, les entitats financeres, els segurs, etc. Per tant, són bàsicament un seguit de pautes dictades en protecció de dades personals dirigides a un determinat sector.

- **Resolucions i instruccions dictades per l'AEPD**.

  Les resolucions de l'AEPD són ordres dictades per complir les funcions en matèria de protecció de dades, de caràcter general, obligatori i permanent que posen fi a la via administrativa.

  De caràcter normatiu, les instruccions dictades per l'Agència espanyola de protecció de dades són directrius d'actuació amb el fi d'establir criteris d'aplicació i interpretació jurídica en matèria de protecció de dades personals.

2. Portugal

A Portugal, la normativa en matèria de protecció de dades és la següent:

- **Llei nº 67/98 de 26 d'octubre de Proteccâo de dados pessoais. (LPDP)**

  A l'igual que en Espanya amb la LOPD, aquesta llei desenvolupa la directiva 95/46/CE i té per objecte la protecció i la garantia del tractament de les dades personals, i la seva lliure circulació. El seu principi general és el processament transparent de les dades personals i l'estricte respecte per la vida privada, els drets i les llibertats fonamentals.

- **Recursos de la Comissâo Nacional de Proteccâo de Dados (CNPD).**

  La CNPD és una autoritat administrativa independent que controla i fiscalitza el processament de les dades personals a Portugal. És l'autoritat de control i protecció de dades personals

3. França

França sempre ha estat un pioner a l'hora de regular la protecció de dades personals. De fet, la seva primera llei data de 1978. La normativa actual que regula a França la protecció de dades de caràcter personal és la següent:

- **Llei nº 2004-801 de 6 d'agost *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*.**

  Aquesta llei també desenvolupa la directiva 95/46/CE. Abans d'aquesta llei, França disposava d'una de les legislacions més antigues en matèria de protecció de dades (la primera llei data de 1978) i en part, la directiva 95/46/CE s'inspira en aquesta legislació. L'àmbit d'aplicació d'aquesta llei és molt ampli i cobreix la totalitat dels sectors d'activitat.

  Decret n°2005-1309 de 20 d'octubre per a l'aplicació de la llei nº 78-17 de 6 de gener *relative à l'informatique, aux fichiers et aux libertés* modificada per la llei nº 2004-801 de 6 d'agost

  Aquest decret desenvolupa les mesures de seguretat dels fitxers automatitzats que continguin dades de caràcter personal i altres aspectes tècnics de llei anterior, i estableix l'autoritat independent de la "*Commission nationale de l'informatique et des libertés*" CNIL.

- **Informacions redactades per la *Commission Nationale de l'Informatique et des Libertés (CNIL).***

  Aquestes recomanacions tenen l'objectiu d'adequar correcte compliment de la normativa francesa en matèria de protecció de dades.

4. Regne Unit

Malgrat la seva anunciada sortida de la Unió Europea, el Regne Unit segueix sent un estat membre i per tant, segueixen sent aplicables els drets i obligacions inherents a aquesta condició. Per adaptar-se a la RGPD un cop formalitzat el *Brexit,* el govern ha presentat el passat 13 de setembre de 2017 la proposta *Data Protection Bill*. Al Regne Unit, la normativa actual en matèria de protecció de dades és la següent:

- **Data Protection Act 1998 (DPA)**

  Aquesta llei també desenvolupa la directiva 95/46/CE i té per objecte la protecció i la garantia del tractament de les dades personals, i la seva lliure circulació, incloent la seva obtenció, la possessió, l'ús o revelació. La DPA va ser esmenada en el 2003 per donar a les persones individuals més control sobre les comunicacions comercials digitals.

- **Privacy and Electronic Communications (EC Directive) Regulations 2003**

  Aquesta llei es centra en el anomenat *marketing* digital i dona a les persones individuals més control sobre les comunicacions comercials digitals. Per tant, queda fóra de l'àmbit d'aquest treball.

- **Recomanacions de la Information Commissioner's Office (ICO).**

  L'Oficina del Comissionat de Informació (ICO) és l'òrgan independent del Regne Unit que defensa els drets de la informació, controla i fiscalitza el processament de les dades personals, reportant directament al parlament.

3.2.2. Mèxic

La normativa vigent en matèria de protecció de dades personals a Mèxic sorgeix de la reforma de la Constitució mexicana realitzada el 1 de juny de 2009 al paràgraf segon de l'article 16, en el qual s'estableix el dret de tota persona a la protecció de les seves dades personals, a l'accés, rectificació i cancel·lació d'aquests, així com a manifestar la seva oposició en els termes per a això establerts. Arran d'aquesta reforma es desenvolupa la normativa vigent a Mèxic:

- **Llei Federal de 27 d'abril de 2010 per a la protecció de dades personals en possessió dels particulars (LFPDPPP)**

  Aquesta llei va entrar en vigor el 6 de juliol del 2010, i té com a objectiu regular el dret a l'accés a la informació en l'àmbit particular (empreses privades i individus). Per aquest subjectes, la LFPDPPP imposa un seguit de regles, requisits, condicions i obligacions mínimes per assegurar l'ús i protecció adequats d'aquests. Els objectius de la LFPDPPP són garantir la privacitat de les persones físiques i el seu dret a la seguretat informativa, i que les seves disposicions s'aplicaran als tractaments automatitzats o no automatitzats a la informació personal que realitzin persones físiques o "morals" (a Mèxic, persones morals és sinònim de persones jurídiques).

- **Resolucions de l'Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)**

  L'INAI és la institució constitucional autònoma mexicana responsable de garantir els drets de les persones a la informació pública governamental i a la protecció de les seves dades personals, gestionades tant per l'administració pública com en empreses privades. Les seves resolucions són definitives en matèria de protecció de dades, d'acord amb la legislació federal.

3.2.3. EUA

En els Estats Units no existeix una llei nacional única i integral que reguli la protecció i l'ús de les dades personals. Més aviat, existeixen tot un seguit de lleis i reglamentacions federals, a més de pautes o *"best practices"* desenvolupades per agències governamentals. Una de les més populars, per exemple, és la **Health Insurance Portability and Accountability Act of 1996** (HIPAA), referida a la privacitat de les dades sanitàries, encara que no entra en l'àmbit d'aquest treball. Per tant, en el nostre cas particular, els principals textos a aplicar són:

- **Federal Trade Comission Act (15 U.S.C. §§41-58)**

  És una llei de 1914 de protecció al consumidor que regula i prohibeix determinades pràctiques empresarials abusives i que s'ha aplicat a les polítiques de seguretat de les dades personals dels consumidors i a la privacitat. L'última revisió d'aquesta llei data del 2006.

- **Regles de la Comissió Federal de Comerç (FTC)**

  La Comissió Federal de Comerç (FTC) és l'agència federal que protegeix als consumidors i promou la competència en els EUA. Realitza investigacions, demanda a persones i companyies i desenvolupa regles per garantir la protecció dels consumidors. Segons la seva pàgina web, la seva missió és: "*Prevenir les pràctiques comercials anticompetitives, enganyoses o deslleials cap als consumidors; millorar el nivell d'informació de les opcions disponibles per als consumidors i augmentar el grau de comprensió del procés competitiu per part del públic; i complir amb aquests objectius sense imposar una càrrega indeguda sobre l'activitat comercial legítima.*"

3.3. Identificació de les bases de dades

Per realitzar la correcta identificació de totes les bases de dades i registres referits a dades personals del **grup JPV**, analitzarem una per una les societats que formen part de l'organització.

3.3.1. JPV Inversiones S.L.

JPV Inversiones S.L. és la societat matriu del grup i la que enregistra la majoria d'aplicacions informàtiques, registres i bases de dades a les seves instal·lacions de la seu a Madrid, on treballen 32 empleats. En primer lloc, analitzarem les aplicacions que emmagatzemen informació a la companyia.

La companyia utilitza **SAP R/3 Enterprise** com a *ERP* de gestió administrativa, financera i de recursos humans. **SAP R/3** funciona utilitzant una arquitectura de client/servidor aplicada a tres nivells: Nivell de presentació (*GUI*), nivell d'aplicació i nivell de base de dades. És altament modular i s'aplica fonamentalment per mitjà del programari, de manera que els modes d'interacció entre els diversos clients i servidors puguin ser controlats. Els mòduls utilitzats a **JPV Inversiones S.L.** són:

- FI (Comptabilitat financera)
- CO (Control i pressupostos)
- HR (Recursos humans)
- RE (Gestió immobiliària)

Per a la gestió de dades referides a la selecció de personal, informació confidencial dels consellers delegats, organigrames i altra documentació sensible, utilitzen un sistema basat en el protocol de fitxers compartits *CIFS*. Aquest sistema de fitxers compartits està administrat amb **Active Directory**, la implementació de **Microsoft** del servei de directori sota una xarxa distribuïda de computadors: el domini "*Grupjpv*".

Per altra banda, la companyia fa servir **OpenKM**, un sistema de gestió documental que permet administrar el contingut empresarial i el flux de treball de l'organització. A **OpenKM** s'emmagatzema la documentació oficial de la companyia: contractes, escriptures, actes notarials, etc.

Finalment, es disposa del software **StruxureWare Data Center**, una aplicació de seguretat per al *CPD* que emmagatzema imatges obtingudes amb una videocàmera instal·lada en el mateix *CPD*.

Per tant, a **JPV Inversiones S.L.** s'identifiquen les següents bases de dades i registres amb informació:

Base de dades o registres	**Tipus d'informació**
SAP R/3	Informació de clients i proveïdors, nòmines, i altres dades personals d'empleats.
Domini "GrupJPV"	Currículums per a la selecció de personal, dades de clients i proveïdors i altra informació sensible.
OpenKM	Dades personals dels consellers delegats, documentació oficial, contractes mercantils i actes notarials.
StruxureWare Data Center	Imatges obtingudes a les instal·lacions de JPV Inversiones S.L.

3.3.2. Fundació JPV

La **Fundació JPV** és l'organització sense ànim de lucre associada al **grup JPV** i que treballa amb l'interès de crear oportunitats en dos sectors clau perquè les persones desenvolupin una vida de qualitat: l'Educació i l'Assistència Social. Concretament, en l'àmbit educatiu, aquesta institució posa a la disposició dels beneficiaris els seus programes de beques que els permeten estudiar i obtenir una formació completa a l'estranger.

La **Fundació JPV** també utilitza **SAP R/3 Enterprise** com a *ERP* de gestió administrativa, financera i de recursos humans. La base de dades utilitzada és la mateixa que per a la societat **JPV Inversiones S.L.**.

Per a la gestió de dades referides a la selecció de personal, i altra documentació sensible, també utilitzen un sistema basat en el protocol de fitxers compartits *CIFS*, sota el mateix domini "Grupjpv". Ara bé, per a la gestió dels seus projectes educatius, i concretament, per la gestió del seu programa de beques, la **Fundació JPV** administra registres i documents amb dades acadèmiques i financeres dels sol·licitants d'ajudes.

Base de dades o registres	**Tipus d'informació**
SAP R/3	Informació de clients i proveïdors, nòmines, i altres dades personals d'empleats.
Domini "GrupJPV"	Currículums per a la selecció de personal, dades de clients i proveïdors, registres i documents amb dades acadèmiques i financeres dels sol·licitants d'ajudes

3.3.3. Atticus S.L.

Atticus S.L. és la societat que administra el **Centre Hípic "Cavall Fort"**. Aquest centre hípic disposa de quadres per a cavalls propis i per als cavalls que participen en els concursos que s'organitzen al llarg de l'any. A més de classes per a nens i adults, s'organitzen altres activitats, com a campaments, gimcanes o classes d'equitació terapèutica.

Atticus S.L., a l'igual que la **Fundació JPV** i **JPV Inversiones S.L.**, utilitza **SAP R/3 Enterprise** com a *ERP* de gestió administrativa, financera i de recursos humans. La base de dades utilitzada és la mateixa que per a la resta de les societats.

Igualment, per a la gestió de dades referides a la selecció de personal, i altra documentació sensible, utilitzen el mateix domini "Grupjpv". No obstant això, per administrar les seves activitats infantils, i concretament, per la gestió de les classes d'equitació terapèutica, el **Centre Hípic "Cavall Fort"** emmagatzema informació referida a dades de tipus historial mèdic i de salut.

Base de dades o registres	**Tipus d'informació**
SAP R/3	Informació de clients i proveïdors, nòmines, i altres dades personals d'empleats.
Domini "GrupJPV"	Currículums per a la selecció de personal, dades de clients i proveïdors, informació referida a dades de tipus historial mèdic i de salut.

3.3.4. JPV Portugal S.A.

JPV Portugal S.A. és la societat immobiliària ubicada a Lisboa. Aquesta seu utilitza una *VPN* per connectar-se a la infraestructura informàtica del grup i fer ús dels seus recursos.

Per tant, **JPV Portugal S.A**., a l'igual que les altres empreses del grup, utilitza **SAP R/3 Enterprise** com a *ERP* de gestió administrativa, financera i de recursos humans. La base de dades utilitzada és la mateixa que per a la resta de les societats.

Per altra banda, **JPV Portugal S.A.** fa servir també **OpenKM**, el sistema de gestió documental per administrar el contingut empresarial i el flux de treball de l'organització. A **OpenKM** s'emmagatzema la documentació oficial de la companyia i fa servir la mateixa base de dades que **JPV Inversiones S.L.** ubicada a la seu d'Espanya.

Per a la gestió de dades referides a la selecció de personal, i altra documentació sensible, utilitzen el mateix domini "Grupjpv". No obstant això, les dades i els registres s'ubiquen a Lisboa, emmagatzemats en un petit servidor a les mateixes instal·lacions de **JPV Portugal S.A..**

Base de dades o registres	**Tipus d'informació**
SAP R/3	Informació de clients i proveïdors, nòmines, i altres dades personals d'empleats.
OpenKM	Dades personals dels consellers delegats, documentació oficial, contractes mercantils i actes notarials.

Domini “GrupJPV”	Currículums per a la selecció de personal, dades de clients i proveïdors.

3.3.5. JPV France S.A.S.

JPV France S.A.S. és la societat immobiliària del **grup JPV** ubicada a Paris. Al igual que **JPV Portugal S.A.**, aquesta seu utilitza una connexió *VPN* per connectar-se a la infraestructura informàtica del grup i fer ús dels seus recursos.

Aleshores, **JPV France S.A.S.,** a l’igual que les altres empreses del grup, utilitza **SAP R/3 Enterprise** com a *ERP* de gestió administrativa, financera i de recursos humans. La base de dades utilitzada és la mateixa que per a la resta de les societats.

JPV France S.A.S. fa servir també **OpenKM**, el sistema de gestió documental per administrar el contingut empresarial i el flux de treball de l’organització. A **OpenKM** s’emmagatzema la documentació oficial de la companyia i fa servir la mateixa base de dades que **JPV Inversiones S.L.** ubicada a la seu d’Espanya.

Finalment, per a la gestió de dades referides a la selecció de personal, i altra documentació sensible, utilitzen el mateix domini “Grupjpv”. No obstant això, les dades i els registres s’ubiquen a Paris, i s’emmagatzemen en un petit servidor ubicat a les mateixes instal·lacions de **JPV France S.A.S.**.

Base de dades o registres	Tipus d'informació
SAP R/3	Informació de clients i proveïdors, nòmines, i altres dades personals d'empleats.
OpenKM	Dades personals dels consellers delegats, documentació oficial, contractes mercantils i actes notarials.
Domini "GrupJPV"	Currículums per a la selecció de personal, dades de clients i proveïdors.

3.3.6. JPV UK Ltd.

La societat immobiliària del **grup JPV** ubicada a Londres és **JPV UK Ltd**. Al igual que les altres societats a l'estranger, aquesta seu utilitza una connexió VPN per connectar-se a la infraestructura informàtica del grup i fer ús dels seus recursos.

Per tant, **JPV UK Ltd**., a l'igual que les altres empreses del grup, utilitza **SAP R/3 Enterprise** com a *ERP* de gestió administrativa, financera i de recursos humans. La base de dades utilitzada és la mateixa que per a la resta de les societats.

JPV UK Ltd. fa servir també **OpenKM**, el sistema de gestió documental per administrar el contingut empresarial i el flux de treball de l'organització. A **OpenKM** s'emmagatzema la documentació oficial de la companyia i fa servir la mateixa base de dades que **JPV Inversiones S.L.** ubicada a la seu d'Espanya.

Per últim, per a la gestió de dades referides a la selecció de personal, i altra documentació sensible, utilitzen el mateix domini “Grupjpv”. No obstant això, les dades i els registres s’ubiquen a Londres, i s’emmagatzemen en un petit servidor ubicat a les mateixes instal·lacions de **JPV UK Ltd.**.

Base de dades o registres	Tipus d’informació
SAP R/3	Informació de clients i proveïdors, nòmines, i altres dades personals d’empleats.
OpenKM	Dades personals dels consellers delegats, documentació oficial, contractes mercantils i actes notarials.
Domini “GrupJPV”	Currículums per a la selecció de personal, dades de clients i proveïdors.

3.3.7. JPV Mexico S.A. de C.V.

JPV Mexico S.A de C.V. és la societat immobiliària del **grup JPV** ubicada a la Ciutat de Mèxic. A l’igual que altres societats estrangeres del grup, utilitza una connexió *VPN* per connectar-se las sistemes informàtics del grup i fer ús dels seus recursos.

JPV Mexico S.A de C.V., al igual que les altres empreses del grup, utilitza **SAP R/3 Enterprise** com a *ERP* de gestió administrativa, financera i de recursos humans. La base de dades utilitzada és la mateixa que per a la resta de les societats ubicada a la seu de Madrid.

JPV Mexico S.A de C.V. fa servir també **OpenKM**, el sistema de gestió documental per administrar el contingut empresarial i el flux de treball de l'organització. A **OpenKM** s'emmagatzema la documentació oficial de la companyia i fa servir la mateixa base de dades que **JPV Inversiones S.L.** ubicada a la seu d'Espanya.

Per últim, per a la gestió de dades referides a la selecció de personal, i altra documentació sensible, utilitzen el mateix domini "Grupjpv". No obstant això, les dades i els registres s'ubiquen a la Ciutat de Mèxic, i s'emmagatzemen en un petit servidor ubicat a les mateixes instal·lacions de **JPV Mexico S.A de C.V..**

Base de dades o registres	Tipus d'informació
SAP R/3	Informació de clients i proveïdors, nòmines, i altres dades personals d'empleats.
OpenKM	Dades personals dels consellers delegats, documentació oficial, contractes mercantils i actes notarials.
Domini "GrupJPV"	Currículums per a la selecció de personal, dades de clients i proveïdors.

3.3.8. JPV USA Inc.

JPV USA Inc. és la societat immobiliària del **grup JPV** ubicada a Miami. Al igual que altres societats estrangeres del grup, utilitza una connexió *VPN* per connectar-se las sistemes informàtics del grup i fer ús dels seus recursos.

JPV USA Inc., a l'igual que les altres empreses del grup, utilitza **SAP R/3 Enterprise** com a *ERP* de gestió administrativa, financera i de recursos humans. La base de dades utilitzada és la mateixa que per a la resta de les societats ubicada a la seu de Madrid.

JPV USA Inc. fa servir també **OpenKM**, el sistema de gestió documental per administrar el contingut empresarial i el flux de treball de l'organització. A **OpenKM** s'emmagatzema la documentació oficial de la companyia i fa servir la mateixa base de dades que **JPV Inversiones S.L.** ubicada a la seu d'Espanya.

Per últim, per a la gestió de dades referides a la selecció de personal, i altra documentació sensible, utilitzen el mateix domini "Grupjpv". No obstant això, les dades i els registres s'ubiquen a Miami, i s'emmagatzemen en un petit servidor ubicat a les mateixes instal·lacions de **JPV USA Inc.**.

Base de dades o registres	**Tipus d'informació**
SAP R/3	Informació de clients i proveïdors, nòmines, i altres dades personals d'empleats.
OpenKM	Dades personals dels consellers delegats, documentació oficial, contractes mercantils i actes notarials.
Domini "GrupJPV"	Currículums per a la selecció de personal, dades de clients i proveïdors.

3.4. Revisió analítica de la situació actual

Un cop revisada la legislació internacional vigent en matèria de protecció de dades personals i identificades totes les bases de dades del grup susceptibles de registrar dades sensibles, és el moment d'estudiar la situació actual i fer una anàlisi comparativa amb els requisits normatius d'obligat compliment a cada societat.

3.4.1. Situació actual

El primer pas abans de fer la revisió analítica és obtenir una foto acurada de la situació actual en totes les societats del grup país a país.

1. Espanya

En el cas de les societats espanyoles, la situació actual data de l'última revisió de l'adaptació a la LOPD que es va realitzar l'any 2015. A partir dels documents obtinguts en aquesta revisió, analitzarem les diferents bases de dades i la seva situació actual:

JPV Inversiones S.L.

Base de dades	SAP R/3
Tipus	Bàsic
País	Espanya
Normativa reguladora	L.O.P.D. i RGPD a partir del 25 maig 2018
Situació actual	Document de seguretat LOPD bàsic (Annex III. Document de seguretat de JPV Inversiones S.L.)

	Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
		Historial de 5 últimes contrasenyes
		Bloqueig de contrasenya al 3 intent
		Caducitat contrasenyes en 45 dies
		Identificació inequívoca dels usuaris
		Confidencialitat de les contrasenyes
		Tallafocs de xarxa
		Sistema antivirus
		Copies de seguretat periòdiques
		Actualitzacions periòdiques
	Inscrita al Registre General de Protecció de Dades	

Base de dades	Domini 'GrupJPV'
Tipus	Bàsic
País	Espanya
Normativa reguladora	L.O.P.D. i RGPD a partir del 25 maig 2018
Situació actual	Document de seguretat LOPD bàsic **(**Annex III. Document de seguretat de JPV Inversiones S.L.**)**

	Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
		Historial de 5 últimes contrasenyes
		Bloqueig de contrasenya al 3 intent
		Caducitat contrasenyes en 45 dies
		Identificació inequívoca dels usuaris
		Confidencialitat de les contrasenyes
		Tallafocs de xarxa
		Sistema antivirus
		Copies de seguretat periòdiques
		Actualitzacions periòdiques
	Inscrita al Registre General de Protecció de dades	

Base de dades	OpenKM
Tipus	Bàsic
País	Espanya
Normativa reguladora	L.O.P.D. i RGPD a partir del 25 maig 2018
Situació actual	Document de seguretat LOPD bàsic **(**Annex III. Document de seguretat de JPV Inversiones S.L.**)**

	Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
		Historial de 5 últimes contrasenyes
		Bloqueig de contrasenya al 3 intent
		Caducitat contrasenyes en 45 dies
		Identificació inequívoca dels usuaris
		Confidencialitat de les contrasenyes
		Tallafocs de xarxa
		Sistema antivirus
		Copies de seguretat periòdiques
		Actualitzacions periòdiques
	Inscrita al Registre General de Protecció de dades	

Base de dades	Struxuware Data Center
Tipus	Bàsic
País	Espanya
Normativa reguladora	L.O.P.D. i RGPD a partir del 25 maig 2018
Situació actual	Document de seguretat LOPD bàsic **(**Annex III. Document de seguretat de JPV Inversiones S.L.**)**

	Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
		Historial de 5 últimes contrasenyes
		Bloqueig de contrasenya al 3 intent
		Caducitat contrasenyes en 45 dies
		Identificació inequívoca dels usuaris
		Confidencialitat de les contrasenyes
		Tallafocs de xarxa
		Sistema antivirus
		Copies de seguretat periòdiques
		Actualitzacions periòdiques
	Inscrita al Registre General de Protecció de dades	

Fundació JPV

Base de dades	SAP R/3
Tipus	Bàsic
País	Espanya
Normativa reguladora	L.O.P.D. i RGPD a partir del 25 maig 2018
Situació actual	Document de seguretat LOPD bàsic **(Annex IV.**

	Document de seguretat de la Fundació JPV)	
	Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
		Historial de 5 últimes contrasenyes
		Bloqueig de contrasenya al 3 intent
		Caducitat contrasenyes en 45 dies
		Identificació inequívoca dels usuaris
		Confidencialitat de les contrasenyes
		Tallafocs de xarxa
		Sistema antivirus
		Copies de seguretat periòdiques
		Actualitzacions periòdiques
	Inscrita al Registre General de Protecció de dades	

Base de dades	Domini 'GrupJPV'
Tipus	Mitjà
País	Espanya
Normativa reguladora	L.O.P.D. i RGPD a partir del 25 maig 2018

Situació actual	Document de seguretat LOPD mitjà (**Annex IV. Document de seguretat de la Fundació JPV**)	
	Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
		Historial de 5 últimes contrasenyes
		Bloqueig de contrasenya al 3 intent
		Caducitat contrasenyes en 45 dies
		Identificació inequívoca dels usuaris
		Confidencialitat de les contrasenyes
		Tallafocs de xarxa
		Sistema antivirus
		Copies de seguretat periòdiques
		Actualitzacions periòdiques
	Inscrita al Registre General de Protecció de dades	

Atticus S.L.

Base de dades	SAP R/3
Tipus	Bàsic
País	Espanya

Normativa reguladora	L.O.P.D. i RGPD a partir del 25 maig 2018	
Situació actual	Document de seguretat LOPD bàsic (Annex V. Document de seguretat d'Atticus S.L.)	
	Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
		Historial de 5 últimes contrasenyes
		Bloqueig de contrasenya al 3 intent
		Caducitat contrasenyes en 45 dies
		Identificació inequívoca dels usuaris
		Confidencialitat de les contrasenyes
		Tallafocs de xarxa
		Sistema antivirus
		Copies de seguretat periòdiques
		Actualitzacions periòdiques
	Inscrita al Registre General de Protecció de dades	

Base de dades	Domini 'GrupJPV'
Tipus	Alt
País	Espanya

<table>
<tr><td>Normativa reguladora</td><td colspan="2">L.O.P.D. i RGPD a partir del 25 maig 2018</td></tr>
<tr><td rowspan="11">Situació actual</td><td colspan="2">Document de seguretat LOPD alt (Annex V. Document de seguretat d’Atticus S.L.)</td></tr>
<tr><td rowspan="9">Mesures de seguretat</td><td>Contrasenyes alfanumèriques de 8 caràcters de longitud</td></tr>
<tr><td>Historial de 5 últimes contrasenyes</td></tr>
<tr><td>Bloqueig de contrasenya al 3 intent</td></tr>
<tr><td>Caducitat contrasenyes en 45 dies</td></tr>
<tr><td>Identificació inequívoca dels usuaris</td></tr>
<tr><td>Confidencialitat de les contrasenyes</td></tr>
<tr><td>Tallafocs de xarxa</td></tr>
<tr><td>Sistema antivirus</td></tr>
<tr><td>Copies de seguretat periòdiques</td></tr>
<tr><td>Actualitzacions periòdiques</td></tr>
<tr><td colspan="2">Inscrita al Registre General de Protecció de dades</td></tr>
</table>

2. Portugal

Al dia d'avui, no s’ha realitzat cap revisió d’adaptació a la legislació vigent portuguesa en la societat situada a Portugal. No obstant això, les mesures de

seguretat generals de l'organització són aplicables també a les bases de dades i registres ubicats a Portugal, ja que pertanyen a la mateixa xarxa informàtica.

JPV Portugal S.A.

Base de dades	SAP R/3
Tipus	Bàsic
País	Portugal
Normativa reguladora	L.P.D.P. i RGPD a partir del 25 maig 2018
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

Base de dades	OpenKM
Tipus	Bàsic
País	Portugal
Normativa reguladora	L.P.D.P. i RGPD a partir del 25 maig 2018
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

Base de dades	Domini GrupJPV
Tipus	Bàsic

País	Portugal
Normativa reguladora	L.P.D.P. i RGPD a partir del 25 maig 2018
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

3. França

Igual que Portugal, al dia d'avui, no s'ha realitzat cap revisió d'adaptació a la legislació vigent francesa en la societat situada a França. Ara bé, les mesures de seguretat generals de l'organització són aplicables també a les bases de dades i registres ubicats a França, ja que pertanyen a la mateixa xarxa informàtica.

JPV France S.A.S.

Base de dades	SAP R/3
Tipus	Bàsic
País	França
Normativa reguladora	Llei nº 2004-801 de 6 d'agost. i RGPD a partir del 25 maig 2018
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

Base de dades	OpenKM

Tipus	Bàsic
País	França
Normativa reguladora	Llei nº 2004-801 de 6 d'agost. i RGPD a partir del 25 maig 2018
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

Base de dades	Domini GrupJPV
Tipus	Bàsic
País	França

Normativa reguladora	Llei nº 2004-801 de 6 d'agost. i RGPD a partir del 25 maig 2018
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

4. Regne Unit

Tampoc s'ha realitzat cap revisió d'adaptació a la legislació vigent britànica en la societat situada al Regne Unit. No obstant això, les mesures de seguretat generals de l'organització són aplicables també a les bases de dades i registres ubicats al Regne Unit, ja que pertanyen a la mateixa xarxa informàtica.

JPV UK Ltd.

Base de dades	SAP R/3
Tipus	Bàsic
País	Regne Unit
Normativa reguladora	Data Protection Act (DPA) i Data Protection Bill (DPB) o RGPD a partir del 25 maig 2018
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

Base de dades	OpenKM

Tipus	Bàsic
País	Regne Unit
Normativa reguladora	Data Protection Act (DPA) i Data Protection Bill (DPB) o RGPD a partir del 25 maig 2018
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

Base de dades	Domini GrupJPV
Tipus	Bàsic
País	Regne Unit

Normativa reguladora	Data Protection Act (DPA) i Data Protection Bill (DPB) o RGPD a partir del 25 maig 2018
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

5. Mèxic

Com a la resta de societats fora d'Espanya, no s'ha realitzat cap revisió d'adaptació a la legislació vigent mexicana en la societat situada a Mèxic. Ara bé, les mesures de seguretat generals de l'organització són aplicables també a les bases de dades i registres ubicats a Mèxic, ja que pertanyen a la mateixa xarxa informàtica.

JPV Mexico S.A. de C.V.

Base de dades	SAP R/3
Tipus	Bàsic
País	Mèxic
Normativa reguladora	Llei Federal de 27 d'abril de 2010 per a la protecció de dades personals en possessió dels particulars (LFPDPPP)
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

Base de dades	OpenKM
Tipus	Bàsic
País	Mèxic
Normativa reguladora	Llei Federal de 27 d'abril de 2010 per a la protecció de dades personals en possessió dels particulars (LFPDPPP)
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

Base de dades	Domini GrupJPV

Tipus	Bàsic
País	Mèxic
Normativa reguladora	Llei Federal de 27 d'abril de 2010 per a la protecció de dades personals en possessió dels particulars (LFPDPPP)
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

6. EUA

Al dia d'avui, no s'ha realitzat cap revisió d'adaptació a la legislació vigent nord-americana en la societat situada als EUA. No obstant això, les mesures de

seguretat generals de l'organització són aplicables també a les bases de dades i registres ubicats als EUA, ja que pertanyen a la mateixa xarxa informàtica.

JPV USA Inc.

Base de dades	SAP R/3
Tipus	Bàsic
País	EUA
Normativa reguladora	Federal Trade Comission Act (15 U.S.C. §§41-58) i regles de la FTC
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

Base de dades	OpenKM
Tipus	Bàsic
País	EUA
Normativa reguladora	Federal Trade Comission Act (15 U.S.C. §§41-58) i regles de la FTC
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

Base de dades	Domini GrupJPV

Tipus	Bàsic
País	EUA
Normativa reguladora	Federal Trade Comission Act (15 U.S.C. §§41-58) i regles de la FTC
Mesures de seguretat	Contrasenyes alfanumèriques de 8 caràcters de longitud
	Historial de 5 últimes contrasenyes
	Bloqueig de contrasenya al 3 intent
	Caducitat contrasenyes en 45 dies
	Identificació inequívoca dels usuaris
	Confidencialitat de les contrasenyes
	Tallafocs de xarxa
	Sistema antivirus
	Copies de seguretat periòdiques
	Actualitzacions periòdiques

3.4.2. Taules de requisits

Continuant amb l'estructura utilitzada en els apartats anteriors, s'analitzaran els requeriments d'obligat compliment a cada país per poder elaborar les taules de requisits corresponents a cada societat.

Per abordar amb èxit aquesta feina, cal traslladar la normativa recopilada anteriorment a les diferents bases de dades i registres identificats. Per tant, per cada zona d'aplicació normativa de l'organització realitzarem una taula de requisits analitzant el seu compliment.

1. Unió Europea i Regne Unit

Com es va veure a l'anàlisi normativa, a partir del pròxim 28 de maig del 2018 entrarà en vigor la nova normativa europea que regula la protecció de dades de caràcter personal, la RGPD. En el Regne Unit, independentment de la seva sortida de la UE, adoptaran aquesta legislació traslladada al seu àmbit jurídic mitjançant la *Data Protection Bill*. Per tant, realitzarem la taula de requisits conjuntament a totes les societats ubicades a la UE i el Regne Unit.

La principal normativa en matèria de protecció de dades actualment vigent a la Unió Europea, com es va veure a l'anàlisi normativa, és la Directiva 95/46/CE de 24 d'octubre de 1995, desenvolupada als països membres per les seves respectives lleis, com la LOPD a Espanya. Ara bé, a partir del pròxim 28 de maig del 2018 entrarà en vigor la RGPD, la nova legislació europea en matèria de protecció de dades. No és competència d'aquest treball realitzar una anàlisi comparatiu i exhaustiu de les dues normes, però si és imprescindible analitzar breument les principals característiques de la RGPD i les diferències amb la Directiva anterior.

El RGPD té com a principi la prevenció per part de les organitzacions que tracten dades mitjançant el concepte de responsabilitat activa. És a dir, les empreses estan obligades a adoptar mesures que assegurin el compliment dels principis, drets i garanties que estableix el Reglament. Adoptar una estratègia d'actuació davant d'una infracció és insuficient, ja que els danys infringits als individus poden ser irreparables. Per això, la RGPD estableix tota una bateria de mesures:

- Protecció de dades des del disseny
- Protecció de dades per defecte

- Mesures de seguretat
- Manteniment d'un registre de tractaments
- Realització d'avaluacions d'impacte sobre la protecció de dades
- Elecció d'un delegat de protecció de dades
- Notificació de violacions de la seguretat de les dades
- Promoció de normes de conducta i esquemes de certificació

Per tant, l'adaptació a la RGPD requereix d'adoptar les següents mesures:

- Elaboració d'una valoració dels riscos de les dades registrades
- Determinar mesures de responsabilitat activa adequades al risc
- Establir un registre d'activitats de tractament
- Revisar les mesures de seguretat
- Establir mecanismes per identificar violacions de seguretat de les dades
- Preveure mesures de reacció enfront a violacions de seguretat
- Notificar de violacions de la seguretat de les dades
- Adaptar les clàusules informatives a incloure en els formularis de sol·licitud d'informació:
- Elaborar document d'informació al personal amb accés a les dades
- Establir un conjunt de mesures tècniques de seguretat.

A continuació, s'analitzarà en més detall els elements descrits anteriorment:

Valoració de riscos

Els responsables en el tractament de dades hauran de realitzar una valoració del risc de les dades gestionades per establir les mesures a aplicar i com aplicar-les. Aquesta anàlisi dependrà del tipus de tractament, la naturalesa de les dades, el nombre d'interessats afectats i la quantitat i varietat de tractaments que l'organització realitzi. Aquesta anàlisi haurà de realitzar-se mitjançant una de les metodologies existents en anàlisi de riscos, com MAGERIT v3, OCTAVE o CRAMM.

Registre d'activitats

A diferència de l'anterior normativa, desenvolupada a Espanya per la LOPD, la RGPD no estableix l'obligatorietat d'inscripció de les bases de dades en el Registre General de Protecció de Dades. En el seu lloc, estableix l'obligatorietat d'establir una sèrie de procediments i mecanismes enfocats en els tipus d'operacions de tractament. Aquesta és la funció principal del Registre d'Activats de Tractament.

El Registre d'Activitats és obligatori per organitzacions amb més de 250 treballadors, i recomanat en la resta de situacions, i aquest haurà d'estar mantingut pel responsable o l'encarregat del tractament de les dades. El contingut d'aquest registre d'activitats serà:

- Identificació i dades de contacte del responsable, representant i delegat de protecció de dades.
- Fins del tractament.
- Descripció de categories d'interessats i dades.
- Categories de destinataris existents o previstos (inclusives en tercers països u organitzacions internacionals).
- Transferències internacionals de dades i documentació de garanties per transferències de dades internacionals.

Informar de la violació de les dades

La RGPD estableix l'obligatorietat de que el responsable notifiqui a l'autoritat de protecció de dades competent quan es produeixi una violació de la seguretat de les dades, tret que sigui improbable que la violació suposi un risc per als drets i llibertats dels afectats. La notificació de la fallida a les autoritats ha de produir-se sense dilació indeguda i, si pot ser, dins de les 72 hores següents al fet que el responsable tingui constància d'ella. La notificació ha d'incloure:

- La naturalesa de la violació.

- Categories de dades i d'interessats afectats.
- Mesures adoptades pel responsable per solucionar la fallida.
- Si escau, les mesures aplicades per pal·liar els possibles efectes negatius sobre els interessats.

Clàusules informatives

La RGPD, igual que la Directiva anterior, estableix el deure d'informar a les persones interessades sobre les dades personals registrades en poder d'una organització. La Directiva 95/46/CE de 24 d'octubre de 1995 anomenava les següents obligacions respecte a la informació a facilitar:

- Existència del fitxer, finalitat i destinataris.
- Caràcter obligatori o no de la resposta.
- La possibilitat d'exercir el dret d'accés, rectificació, cancel·lació i oposició.
- La identitat i les dades de contacte del Responsable del Tractament.

Per la seva banda, la RGPD amplia aquests requisits afegint les següents obligacions a l'hora d'informar:

- La identitat i les dades de contacte del Delegat de Protecció de Dades.
- La base jurídica o legitimació del tractament.
- Criteri i termini per la conservació de les dades.
- Existència d'automatització de les dades.
- Previsió de transferència a tercers països.
- Dret a presentar una reclamació davant les autoritats de control.
- L'origen de les dades, en el cas que no s'obtinguin directament del mateix interessat.
- La categoria de les dades.

Document d'informació al personal

La RGPD determina la necessitat d'establir garanties de seguretat adequades contra el tractament no autoritzat o il·lícit, contra la pèrdua de les dades personals, la destrucció o el dany accidental. A més de mesures tècniques, això implica l'adopció de mesures organitzatives encaminades a assegurar la integritat i confidencialitat de les dades personals i la possibilitat de demostrar que aquestes mesures s'han portat a la pràctica (responsabilitat proactiva).

La principal mesura organitzativa és l'elaboració i distribució de la informació d'obligat coneixement pel personal de l'organització amb accés a les dades de caràcter personal. Aquest document enregistrarà el deure de confidencialitat i secret, els drets dels titulars de les dades, les violacions de seguretat de dades de caràcter personal i la captació d'imatges amb càmeres de seguretat.

Mesures tècniques de seguretat

A més de les mesures organitzatives, la RGPD determina la necessitat d'establir garanties de seguretat tècniques, i per tant, això implica l'adopció de mesures tècniques encaminades a assegurar la integritat i confidencialitat de les dades personals. Aquestes mesures tècniques són les següents:

- Creació de diferents perfils en els ordinadors que accedeixen a les dades amb usuaris sense privilegis d'administració.
- Garantia d'accés a les dades mitjançant contrasenyes d'almenys 8 caràcters alfanumèrics.
- Identificació d'usuaris inequívoca.
- Confidencialitat de les contrasenyes.
- Actualitzacions periòdiques d'ordinadors i dispositius.
- Adopció d'un sistema antivirus i *malware* en els ordinadors amb accés a les dades.
- Implantació d'un sistema de tallafocs per evitar accessos remots.

- Xifrat de les dades per a la seva extracció fora del recinte de l'organització.
- Elaboració periòdica de còpies de seguretat en un suport distint i emmagatzemat en un lloc segur.

Taula de requisits

En resum, la taula simplificada de requisits a complir per adaptar les bases de dades a la legislació europea i britànica són les següents:

Valoració de riscos	Elaborar un informe de valoració de riscos utilitzant alguna de les metodologies d'anàlisis de riscos existents.
Registre d'activitats	Creació d'un registre d'activitat de tractament per part del responsable o encarregat.
Circular de vulneració seguretat	Creació d'una circular model amb les informacions requerides en cas de vulneració de la seguretat.
Clàusules de seguretat	Adició de les clàusules de seguretat obligatòries en formularis i sol·licituds.
Document d'informació al personal	Elaboració i distribució d'un document dirigit al personal amb accés a les dades.
Mesures tècniques de seguretat	Perfils usuaris

	Contrasenyes 8 alfanumèrica
	Identificació inequívoca
	Confidencialitat de les contrasenyes
	Actualitzacions periòdiques
	Antivirus
	Tallafocs
	Xifrat dispositius externs
	Còpies de seguretat periòdiques

Taula 1. Normativa UE i UK

2. Mèxic

A Mèxic, la principal normativa en matèria de protecció de dades actualment vigent és la Llei Federal de 27 d'abril de 2010 per a la protecció de dades personals en possessió dels particulars (LFPDPPP), com es va veure a l'anàlisi normativa. Per tant, cal analitzar breument les principals característiques de la LFPDPPP per establir la taula de requisits.

La LFPDPPP té com a principis rectors la licitud, el consentiment, la informació, la qualitat, la finalitat, la lleialtat, la proporcionalitat i la responsabilitat, a més d'uns deures: la confidencialitat i la seguretat. Per això, la LFPDPPP estableix la recomanació de l'adopció d'un sistema de gestió de la seguretat de les dades personals (SGSDP) basat en el cicle PFVA (Planejar, Fer, Verificar i Actuar). Per tant, la LFPDPPP estableix tota una bateria de mesures basades en aquests 4 conceptes:

- Planejar
    - Definir la política de seguretat amb el seu àmbit, objectius i responsables
    - Inventariar les bases de dades
    - Anàlisi de riscos
- Fer
    - Implementació de mesures de seguretat tècniques
- Verificar
    - Realitzar una auditoria
- Actuar
    - Adopció de mesures correctives en funció dels resultats de l'auditoria
    - Capacitar al personal que efectuí el tractament de les dades
    - Informar i analitzar les vulneracions de les dades personals

Per tant, l'adaptació a la LFPDPPP requereix d'adoptar les següents mesures:

- Elaborar document de política de seguretat.
- Inventariar les bases de dades.
- Elaboració d'una valoració dels riscos de les dades registrades.
- Establir un conjunt de mesures tècniques de seguretat.
- Auditar les mesures de seguretat i establir mecanismes correctors.
- Capacitar al personal amb accés a les dades.
- Informar de la vulneració de les dades.

A continuació, s'analitzarà en més detall els elements descrits anteriorment:

Document de política de seguretat

L'art. 57 de la LFPDPPP estableix que "*el responsable i, si escau, l'encarregat hauran d'establir i mantenir les mesures de seguretat administratives, físiques i, si escau, tècniques per a la protecció de les dades personals*". Per tant, la

primera mesura a adoptar és l'elaboració del document de política de seguretat definint l'àmbit, els objectius i els responsables del tractament de les dades de caràcter principal. Aquesta és la funció principal del Document de Política de Seguretat.

Inventariar les bases de dades

Segons l'art. 61, Fracció I de la LFPDPPP, el responsable deurà considerar l'elaboració d'un inventari de dades personals i dels seus sistemes de tractament. Per tant, és necessari realitzar un inventari de les bases de dades utilitzades a l'organització.

Valoració de riscos

L'art. 60 de la LFPDPPP estableix que el responsable en el tractament de dades hauran de realitzar una valoració del risc de les dades gestionades per establir les mesures a aplicar i com aplicar-les. Aquesta anàlisi dependrà del tipus de tractament, la naturalesa de les dades, les conseqüències de la vulneració de les dades i la tecnologia existent. No estableix cap metodologia per a la seva realització. Com podem veure, aquest requisit és pràcticament el mateix que a la RGPD.

Mesures tècniques de seguretat

La LFPDPPP, igual que la RGPD, determina la necessitat d'establir garanties de seguretat tècniques, i per tant, això implica l'adopció de mesures tècniques encaminades a assegurar la integritat i confidencialitat de les dades personals. El legislador, de totes maneres, dona total llibertat a les empreses a establir les seves mesures de seguretat sense cap tipus de directiva ni recomanació. En aquest cas suposarem que les mesures tècniques establertes a la RGPD són suficients.

Realització d'una auditoria

D'altra banda, la LFPDPPP si recomana en els seus art. 61 i 62 la realització d'auditories de seguretat i revisions. Aquestes auditories de seguretat no estan definides en el reglament, ni les seves metodologies. També assenyala l'obligatorietat d'establir mecanismes de correcció de seguretat en funció dels resultats d'aquestes auditories.

Capacitació del personal que efectua el tractament

La fracció VIII de l'art. 61 de la LFPDPPP estableix l'obligatorietat de capacitar al personal que efectuí el tractament de les dades personals a fi d'establir i mantenir la seguretat d'aquestes dades. No desenvolupa més aquest punt, deixant a criteri del responsable de les dades aquesta capacitació. Per tant, es considera que amb un document d'informació al personal amb accés a les dades, com l'exigit a la RGPD es compleix aquest requisit.

Informar de la vulneració de les dades

Per últim, l'art. 64 de la LFPDPPP diu que '*el responsable haurà d'informar el titular les vulneracions que afectin de forma significativa els seus drets patrimonials o morals, quan confirmi que va ocórrer la vulneració i hagi pres les accions encaminades a detonar un procés de revisió exhaustiva de la magnitud de l'afectació, i sense cap dilació, a fi que els titulars afectats puguin prendre les mesures corresponents.*' Aquesta informació es desenvolupa en l'art. 65 de la llei, establint els següents elements que ha de tenir aquesta informació:

- La naturalesa de l'incident.
- Les dades personals compromeses.
- Les recomanacions al titular sobre les mesures que aquest pugui adoptar per protegir els seus interessos.
- Les accions correctives realitzades de forma immediata.
- Els mitjans on pot obtenir més informació sobre aquest tema.

Com es pot comprovar, aquest requisit amplia l'obligatorietat imposta per la RGPD al deure d'informar de les violacions de seguretat de les dades.

Taula de requisits

En resum, la taula simplificada de requisits a complir per adaptar les bases de dades a la legislació mexicana són les següents:

Document de política de seguretat	Creació d'un document descrivint la política de seguretat de l'organització, l'àmbit, els objectius i els responsables del tractament de les dades
Inventari de les Bases de Dades	Elaboració d'un inventari de dades personals i dels seus sistemes de tractament.
Valoració de riscos	Elaborar un informe de valoració de riscos utilitzant alguna de les metodologies d'anàlisis de riscos existents.
Auditoria de seguretat	Realització d'auditories de seguretat i revisions, i establir mecanismes de correcció de seguretat.
Circular de vulneració seguretat	Creació d'una circular model amb les informacions requerides en cas de vulneració de la seguretat.
Document d'informació al personal	Elaboració i distribució d'un

	document dirigit al personal amb accés a les dades.
Mesures tècniques de seguretat	Perfils usuaris
	Contrasenyes 8 alfanumèrica
	Identificació inequívoca
	Confidencialitat de les contrasenyes
	Actualitzacions periòdiques
	Antivirus
	Tallafocs
	Xifrat dispositius externs
	Còpies de seguretat periòdiques

Taula 2. Normativa Mèxic

3. EUA

Com s'ha vist a l'anàlisi normativa, en el cas dels EUA no existeix una normativa general en matèria de protecció de dades. En canvi, existeixen tot un seguit de lleis i reglamentacions federals, a més de pautes o "*best practices*" desenvolupades per agències governamentals com la FTC (Comissió Federal de Comerç).

Analitzar totes aquestes lleis federals, sentències jurídiques (val recordar al lector que el model legislatiu dels EUA es basa en jurisprudència) i pautes queda completament fora de l'àmbit d'aquest treball, però si val la pena

enumerar algunes recomanacions realitzades a la web de la FTC per transposar aquestes amb els requisits anteriorment mencionats.

La FTC disposa d'un breu manual amb cinc consells bàsics a aplicar respecte al tractament de les dades personals per part dels negocis. Aquests cinc consells es basen en cinc principis bàsics:

- Inventariar les dades
- Reduir dels arxius
- Tancar amb clau
- Eliminar l'innecessari
- Planificar amb anticipació

Inventariar les dades

Segons la web de la FTC, '*el punt essencial a considerar en l'avaluació de les vulnerabilitats de seguretat és entendre bé com la informació ingressa, es processa i surt del seu negoci i qui tenen o podrien tenir accés a les dades. Solament després d'identificar aquest procés podrà determinar els millors mecanismes per protegir la informació.*' Per tant, la FTC dona una sèrie de pautes per identificar les dades de caràcter personal i realitzar un inventari. Aquest requisit està cobert mitjançant el requisit establert a la LFPDPPP mexicana.

Reduir els arxius

Aquest principi es basa en la legitimació de la informació, concepte que ja contempla la RGPD i que estableix la necessitat de justificar la conservació de les dades de caràcter personal, és a dir, la base jurídica de la informació. Per exemple, és necessari per a un concessionari de cotxes documentar dades relatives a la salut dels seus clients? Per tant, aquest requisit es considera cobert amb els requisits de la RGPD amb el registre d'activitats.

Tancar amb clau

El concepte de tancar amb clau fa referència a l'establiment de mesures de seguretat tant físiques com electròniques per assegurar la informació registrada a l'organització. Respecte al que s'ha vist anteriorment, podem identificar una novetat respecte a la normativa europea i mexicana, i és que enumera tot un seguit de mesures de seguretat físiques, que encara que implícites, no estan regulades per aquestes. Aquestes mesures de seguretat són:

- Assegurar amb clau els suports electrònics que emmagatzemen la informació.
- Emmagatzemar la informació en suport paper en arxivadors amb clau.
- Exigència als empleats d'assegurar l'oficina i els arxivers amb clau.
- Establir controls d'accessos a les oficines.

Les mesures de seguretat electròniques estan incloses en les referides en la RGPD com la seguretat de les contrasenyes, implantació de tallafocs, etc. A més, es fa referència a capacitar al personal en aquestes mesures de seguretat, requisit també inclòs en les normatives europees i mexicanes.

Eliminar l'innecessari

Si abans es feia referència a la necessitat de justificar la legitimitat de les dades de caràcter personal, aquest principi fa referència a la destrucció de les dades mitjançant medis electrònics i físics, com trituradores de paper o software del tipus '*wipe utility*'. Per tant, en aquest cas, caldria afegir a la taula de requisits la necessitat d'implementar un Pla de Destrucció de Dades a l'organització.

Planificar amb antelació

La idea principal d'aquest element és l'elaboració d'un pla de seguretat integral en el tractament de les dades personals, tal com hem vist en la legislació

mexicana, i al mateix temps, estableix la necessitat de notificar les violacions de seguretat, requisit també inclòs en la LFPDPPP.

Taula de requisits

Per tant, la taula simplificada de requisits a complir per adaptar les bases de dades a les regulacions nord-americanes són les següents:

Document de política de seguretat	Creació d'un document descrivint la política de seguretat de l'organització, l'àmbit, els objectius i els responsables del tractament de les dades.
Registre d'activitats	Creació d'un registre d'activitat de tractament per part del responsable o encarregat.
Inventari de les Bases de Dades	Elaboració d'un inventari de dades personals i dels seus sistemes de tractament.
Circular de vulneració seguretat	Creació d'una circular model amb les informacions requerides en cas de vulneració de la seguretat.
Document d'informació al personal	Elaboració i distribució d'un document dirigit al personal amb accés a les dades.
Mesures tècniques de seguretat	Perfils usuaris
	Contrasenyes 8 alfanumèrica

	Identificació inequívoca
	Confidencialitat de les contrasenyes
	Actualitzacions periòdiques
	Antivirus
	Tallafocs
	Xifrat dispositius externs
	Còpies de seguretat periòdiques
Mesures físiques de seguretat	Establir controls d'accés a les instal·lacions.
	Emmagatzemar amb clau els suports físics i electrònics amb informació.
Pla d'Eliminació de Dades	Creació d'un document descrivint el pla d'eliminació de les dades de caràcter personal.

Taula 3. Normativa EUA

3.5. Document de proposta d'implantació

Un cop analitzada la situació actual de les bases de dades de l'organització i recopilades totes les taules de requisits, és el moment d'elaborar el document de proposta d'implantació per complir la legislació internacional en matèria de protecció de dades de caràcter personal.

Taula global de requisits

La primera tasca a realitzar és unificar les taules de requisits per obtenir la taula global de requisits a aplicar en l'organització. Aquesta taula global és el resultat de sobreposar les taules de requisits a la UE, Mèxic i els EUA:

Requisit	Característiques	UE i UK	Mèxic	EUA
Document de política de seguretat	Creació d'un document descrivint la política de seguretat de l'organització, l'àmbit, els objectius i els responsables del tractament de les dades		✓	✓
Inventari de les Bases de Dades	Elaboració d'un inventari de dades personals i dels seus sistemes de tractament.		✓	✓
Valoració de riscos	Elaborar un informe de valoració de riscos utilitzant alguna de les metodologies d'anàlisis de riscos existents.	✓	✓	
Auditoria de seguretat	Realització d'auditories de seguretat i revisions, i establir mecanismes de correcció de seguretat.		✓	
Registre d'activitats	Creació d'un registre d'activitat de tractament per part del responsable o encarregat.	✓		✓
Circular de vulneració seguretat	Creació d'una circular model amb les informacions requerides en cas de vulneració de la seguretat.	✓	✓	✓
Clàusules de seguretat	Adició de les clàusules de seguretat obligatòries en formularis i sol·licituds.	✓		
Document d'informació al personal	Elaboració i distribució d'un document dirigit al personal amb accés a les dades.	✓	✓	✓
Mesures tècniques de seguretat	Perfils usuaris	✓	✓	✓
	Contrasenyes 8 alfanumèrica	✓	✓	✓
	Identificació inequívoca	✓	✓	✓
	Confidencialitat de les contrasenyes	✓	✓	✓
	Actualitzacions periòdiques	✓	✓	✓
	Antivirus	✓	✓	✓
	Tallafocs	✓	✓	✓
	Xifrat dispositius externs	✓	✓	✓
	Còpies de seguretat periòdiques	✓	✓	✓
Mesures físiques de seguretat	Establir controls d'accés a les instal·lacions.			✓
	Emmagatzemar amb clau els suports físics i electrònics amb informació.			✓
Pla d'Eliminació de Dades	Creació d'un document descrivint el pla d'eliminació de les dades de caràcter personal.			✓

Figura 4. Taula global de requisits

A partir d'aquesta taula de requisits i partint de la situació actual analitzada amb anterioritat, es realitza el següent document de proposta d'implantació:

Document de proposta d'implantació

I. Introducció

Després d'un exhaustiu examen de la situació en matèria de protecció de dades de caràcter personal en les societats pertanyents al GRUP JPV així com a la FUNDACIÓ JPV, el present resum executiu detalla les tasques i mesures que cal dur a terme per les set societats del GRUP JPV així com per la FUNDACIÓ JPV per dur a terme l'adaptació de les mateixes a la normativa vigent en matèria de Protecció de Dades de Caràcter Personal en l'àmbit internacional.

II. Mesures d'adaptació a la normativa vigent en matèria de protecció de dades per les societats del GRUP JPV

1r. Elaborar un document conjunt de política de seguretat

La legislació mexicana estableix la necessitat d'elaborar un document de política de seguretat definint l'àmbit, els objectius i els responsables del tractament de les dades de caràcter principal, i les recomanacions de la FTC als EUA al mateix temps aconsellen planificar amb antelació realitzant un pla de seguretat integral en el tractament de les dades personals. Per tant, la primera mesura a adoptar és l'elaboració del document conjunt de política de seguretat.

Aquest document haurà d'incloure necessàriament els següents elements:

- L'àmbit del tractament de les dades
- Els objectius del tractament de les dades
- Els responsables del tractament de les dades
- Les accions efectuades per protegir les dades

Aquests elements ja són inclosos en els Documents de Seguretat realitzats l'any 2015 amb motiu de l'adaptació a la LOPD de l'organització, per tant, l'única feina que cal fer al respecte és **revisar i actualitzar els Documents de Seguretat.**

2n. Realitzar un inventari exhaustiu de les bases de dades

La FTC estableix que el punt essencial a considerar en l'avaluació de les vulnerabilitats de seguretat és la identificació del procés d'obtenció, processament i eliminació de la informació i recomana l'elaboració d'un inventari exhaustiu de les dades. A més, l'art. 61, Fracció I de la LFPDPPP considera també l'elaboració d'aquest inventari. Per tant, la segona mesura a adoptar és l'elaboració d'un inventari exhaustiu de les bases de dades registrades en l'organització.

Aquest inventari ja es va realitzar parcialment l'any 2015 en identificar aquests registres i bases de dades i efectuant el registre en el Registre General de Protecció de Dades. Per tant, només caldria **actualitzar l'inventari de les bases de dades.**

3r. Crear un informe de valoració de riscos de l'organització

La RGPD estableix que els responsables en el tractament de dades hauran de realitzar una valoració del risc de les dades gestionades per establir les mesures a aplicar i com aplicar-les. Per la seva banda, l'art. 60 de la LFPDPPP també obliga al fet que el responsable en el tractament de dades realitzi una valoració del risc de les dades gestionades considerant diferents factors com el risc inherent pel tipus de dada personal, la sensibilitat de les dades, el desenvolupament tecnològic i les possibles conseqüències de la vulneració de les dades. Mentre que la legislació mexicana no especifica cap metodologia, la RGPD a través de les agències nacionals recomana l'adopció d'una

metodologia existent en l'anàlisi de riscos com MAGERIT v3, OCTAVE o CRAMM.

Aquest informe no està present actualment a l'organització i per tant, per fer efectiva aquesta mesura s'ha de **realitzar un informe de valoració de riscos de l'organització.**

4t. Elaborar una auditoria de seguretat

Encara que les auditories de seguretat no estan definides en el reglament, ni les seves metodologies, la LFPDPPP mexicana recomana en els seus art. 61 i 62 la realització d'auditories de seguretat i revisions. Així mateix, també assenyala l'obligatorietat d'establir mecanismes de correcció de seguretat en funció dels resultats d'aquestes auditories.

Per tant, amb l'objectiu de satisfer aquest requisit, és necessari **l'elaboració periòdica d'auditories de seguretat i un document de correcció en funció dels resultats de les auditories.**

5è. Establir un registre d'activitats de tractament de les dades

La RGPD estableix l'obligatorietat d'establir una sèrie de procediments i mecanismes enfocats en els tipus d'operacions de tractament de les dades personals i documentar aquestes activitats mitjançant el Registre d'Activats de Tractament. Aquest registre ha d'estar mantingut pel responsable o l'encarregat del tractament de les dades i ha de contenir els següents elements:

- Identificació i dades de contacte del responsable, representant i delegat de protecció de dades.
- Fins del tractament.
- Descripció de categories d'interessats i dades.

- Categories de destinataris existents o previstos (inclusives en tercers països u organitzacions internacionals).
- Transferències internacionals de dades i documentació de garanties per transferències de dades internacionals.

Aquest Registre d'Activitats és obligatori per organitzacions amb més de 250 treballadors. Per tant, en el cas del Grup JPV no és obligatori. No obstant això, si està recomanat en la resta d'organitzacions, i a més, les recomanacions de la FTC als EUA citen el principi 'Reduir els arxius', que es basa en la legitimació de la informació, i que estableix la necessitat de justificar la conservació de les dades de caràcter personal, és a dir, la base jurídica de la informació, aspecte que ja contempla el Registre d'Activitats de Tractaments previst per la RGPD.

En conclusió, és imprescindible **l'elaboració d'un Registre d'Activitats de tractament de les dades a l'organització.**

Aquest registre d'activitats té implícit un requisit addicional a considerar en el disseny de l'organització de les dades de caràcter personal, i és la **necessitat d'emmagatzemar i aïllar les dades de ciutadans de la UE en servidors i instal·lacions ubicades en territori de la UE.**

6è. Documentar una circular de vulneracions de seguretat

La RGPD dicta l'obligatorietat que el responsable notifiqui a l'autoritat de protecció de dades competent quan es produeixi una violació de la seguretat de les dades, tret que sigui improbable que la violació suposi un risc per als drets i llibertats dels afectats. La notificació ha d'incloure com a mínim:

- La naturalesa de la violació.
- Categories de dades i d'interessats afectats.
- Mesures adoptades pel responsable per solucionar la fallida.
- Si escau, les mesures aplicades per pal·liar els possibles efectes negatius sobre els interessats.

Al seu torn, la legislació mexicana estableix en l'art. 64 de la LFPDPPP l'obligatorietat que el responsable de les dades informi el titular de les vulneracions que afectin de forma significativa els seus drets patrimonials o morals, i prengui les accions encaminades a revisar exhaustivament la magnitud de l'afectació, a fi que els titulars afectats puguin prendre les mesures corresponents. Aquesta informació es desenvolupa en l'art. 65 de la mateixa llei, i estableix els següents elements que ha de tenir aquesta informació:

- La naturalesa de l'incident.
- Les dades personals compromeses.
- Les recomanacions al titular sobre les mesures que aquest pugui adoptar per protegir els seus interessos.
- Les accions correctives realitzades de forma immediata.
- Els mitjans on pot obtenir més informació sobre aquest tema.

D'altra banda, la FTC estableix la necessitat de notificar les violacions de seguretat als titulars de les dades, sota el principi de planificar amb antelació el tractament de les dades de caràcter personal.

Amb el fi de preveure aquestes notificacions, serà necessari **elaborar un model de circular de notificacions de vulneracions de la seguretat de les dades** per informar el titular d'aquestes.

7è. Addicionar clàusules de confidencialitat en formularis i peticions

La RGPD estableix el deure d'informar a les persones interessades sobre les dades personals registrades en poder d'una organització. Aquesta obligació enumera els següents elements obligatoris a afegir en les clàusules de confidencialitat dels formularis i peticions d'informació:

- Existència del fitxer, finalitat i destinataris.

- Caràcter obligatori o no de la resposta.
- La possibilitat d'exercir el dret d'accés, rectificació, cancel·lació i oposició.
- La identitat i les dades de contacte del Responsable del Tractament.
- La identitat i les dades de contacte del Delegat de Protecció de Dades.
- La base jurídica o legitimació del tractament.
- Criteri i termini per la conservació de les dades.
- Existència d'automatització de les dades.
- Previsió de transferència a tercers països.
- Dret a presentar una reclamació davant les autoritats de control.
- L'origen de les dades, en el cas que no s'obtinguin directament del mateix interessat.
- La categoria de les dades.

Aquesta és una obligatorietat exclusiva de la RGPD, però això no eximeix del seu compliment. No obstant això, en l'anterior adaptació de la LOPD ja es va realitzar una tasca en aquest sentit, per tant, només caldrà **adaptar les clàusules de confidencialitat dels formularis i peticions d'informació a la RGPD.**

8è. Elaborar i distribuir entre el personal un document d'informació

A més d'establir garanties de seguretat adequades contra el tractament no autoritzat o il·lícit amb mesures tècniques, la RGPD determina l'adopció de mesures organitzatives encaminades a assegurar la integritat i confidencialitat de les dades personals i la possibilitat de demostrar que aquestes mesures s'han portat a la pràctica (responsabilitat proactiva). La principal mesura organitzativa és l'elaboració i distribució de la informació d'obligat coneixement pel personal de l'organització amb accés a les dades de caràcter personal.

La legislació mexicana, a la fracció VIII de l'art. 61 de la LFPDPPP també estableix l'obligatorietat de capacitar al personal que efectuí el tractament de les dades personals a fi d'establir i mantenir la seguretat d'aquestes dades.

Per últim, la FTC recomana sota el principi de 'tancar amb clau' la necessitat de capacitar al personal en les mesures de seguretat adoptades.

En conseqüència, és imprescindible **realitzar el document d'informació al personal** que enregistrarà el deure de confidencialitat i secret, els drets dels titulars de les dades, les violacions de seguretat de dades de caràcter personal i la captació d'imatges amb càmeres de seguretat.

9è. Adoptar mesures tècniques de seguretat

La RGPD estableix l'obligatorietat d'establir garanties de seguretat tècniques, i per tant, l'adopció de mesures tècniques encaminades a assegurar la integritat i confidencialitat de les dades personals. Les mesures tècniques que menciona són les següents:

- Creació de diferents perfils en els ordinadors que accedeixen a les dades amb usuaris sense privilegis d'administració.
- Garantia d'accés a les dades mitjançant contrasenyes d'almenys 8 caràcters alfanumèrics.
- Identificació d'usuaris inequívoca.
- Confidencialitat de les contrasenyes.
- Actualitzacions periòdiques d'ordinadors i dispositius.
- Adopció d'un sistema antivirus i malware en els ordinadors amb accés a les dades.
- Implantació d'un sistema de tallafocs per evitar accessos remots.
- Xifrat de les dades per a la seva extracció fora del recinte de l'organització.

- Elaboració periòdica de còpies de seguretat en un suport distint i emmagatzemat en un lloc segur.

Al mateix temps, la LFPDPPP determina la necessitat d'establir garanties de seguretat tècniques i l'adopció de mesures tècniques encaminades a assegurar la integritat i confidencialitat de les dades personals. En aquest cas dona total llibertat a les empreses a establir les seves mesures de seguretat sense cap tipus de directiva ni recomanació.

Finalment, la FTC enumera un seguit de recomanacions sota el principi de 'Tancar amb clau' ja incloses en les mesures de seguretat electròniques referides en la RGPD com la seguretat de les contrasenyes, implantació de tallafocs, etc.

Aquests requisits ja estan implementats en la infraestructura informàtica de l'organització, amb l'excepció del xifrat de les dades. Per tant, s'ha d'**establir un mecanisme de xifrat per l'extracció de les dades de caràcter personal fora del recinte.**

10è. Adoptar mesures físiques de seguretat

Sota el principi de 'Tancar amb clau', la FTC fa referència a l'establiment de mesures de seguretat tant físiques com electròniques per assegurar la informació registrada a l'organització. En referència a les mesures físiques de seguretat, enumera les següents:

- Assegurar amb clau els suports electrònics que emmagatzemen la informació.
- Emmagatzemar la informació en suport paper en arxivadors amb clau.
- Exigència als empleats d'assegurar l'oficina i els arxivers amb clau.
- Establir controls d'accessos a les oficines.

Encara que aquestes mesures puguin resultar trivials, és necessari **verificar que l'accés tant als servidors, ordinadors, suport electrònics, arxivadors i documentació en paper està restringida i controlada.**

11è. Elaborar un pla d'eliminació de dades

Sota el principi de 'Eliminar l'innecessari', la FTC aconsella, un cop analitzada la legitimitat de les dades de caràcter personal, la destrucció de les dades no legitimades i innecessàries mitjançant medis electrònics i físics, com trituradores de paper o software del tipus '*wipe utility*'. En conseqüència, és necessari **implementar un Pla de Destrucció de Dades a l'organització**.

4. Valoració econòmica

4.1. Valoració econòmica de les tasques

Utilitzant el Document de Proposta d'Implantació com a referència, a continuació es realitzarà una valoració econòmica d'acord amb les tasques identificades.

Tasca 1. Revisar i actualitzar els Documents de Seguretat.

Els documents de seguretat (vegeu Annex III. Document de seguretat de JPV Inversiones S.L.) realitzats per les societats espanyoles a l'adaptació a la LOPD del 2015 es poden utilitzar com a referència per revisar, actualitzar i crear els nous documents de seguretat en les societats estrangeres. Aquesta tasca hauria de suposar un dia o unes 8 hores de treball per cada societat espanyola i dos dies o 16 hores de treball per cada societat estrangera. Per tant, s'estima una valoració de 104 hores a realitzar per el responsable del tractament de les dades de l'organització.

Tasca 2. Actualitzar l'inventari de les bases de dades.

Actualitzar l'inventari de les bases de dades de l'organització és una tasca relativament simple que no hauria de portar més de tres jornades de treball o 24 hores efectives a un responsable TIC.

Tasca 3. Realitzar un informe de valoració de riscos de l'organització.

Una valoració de riscos en la protecció de dades personals o PIA (*Privacy Impact Assessment*) en l'àmbit d'una organització és una tasca complexa que és necessari encarregar a una consultora especialitzada. El preu aproximat d'aquesta tasca per una organització com el **Grup JPV** és d'uns 3.800 €. (aquesta valoració s'ha obtingut de factures de prestació de serveis)

Tasca 4. Elaborar una auditoria de seguretat.

Igual que una valoració de riscos, és convenient que les auditories de seguretat les realitzin consultores externes especialitzades. Per una organització amb les característiques del **Grup JPV**, el preu d'aquesta auditoria rondarà els 4.500 €. (aquesta valoració s'ha obtingut de factures de prestació de serveis)

Tasca 5. Crear un Registre d'Activitats de tractament de les dades a l'organització.

La creació d'un Registre d'Activitats de Tractament de les dades de l'organització és una tasca molt simple gràcies a l'eina 'Facilita' que posa a disposició en la seva web l'Agència Espanyola de Protecció de Dades (http://www.servicios.agpd.es/Facilita). Es pot veure en Annex VI. Exemple de document realitzat amb l'eina 'Facilita' un exemple del document obtingut amb el Registre d'Activitats llest. Per tant, aquesta tasca s'estima en una hora de treball per societat ha realitzar per un responsable TIC, és a dir, un dia de feina o 8 hores.

Tasca 6. Elaborar un model de circular de notificacions de vulneracions de la seguretat de les dades.

El model de circular de notificacions és global per a totes les societats, i amb els elements seleccionats aquesta tasca implica bàsicament la creació d'una plantilla de Word. Per tant, la valoració és de 4 hores de treball d'un responsable TIC.

Tasca 7. Adaptar les clàusules de confidencialitat dels formularis i peticions d'informació.

Amb l'eina '*Facilita*' abans esmentada, es poden obtenir automàticament totes les clàusules de confidencialitat dels formularis i peticions d'informació, (vegeu Annex VI. Exemple de document realitzat amb l'eina 'Facilita') aprofitant la feina realitzada. Per tant, aquesta tasca no té valoració econòmica.

Tasca 8. Realitzar el document d'informació al personal.

Aquesta tasca també és inclosa en l'eina 'Facilita' (vegeu Annex VI. Exemple de document realitzat amb l'eina 'Facilita') i per tant, no té valoració econòmica.

Tasca 9. Establir un mecanisme de xifrat per l'extracció de les dades de caràcter personal.

Aquesta tasca implica dos conceptes a tenir en consideració: establir les polítiques de seguretat necessàries per part del departament informàtic i disposar dels elements de xifrat com dispositius d'emmagatzematge del tipus *pendrive*. S'estimen dos dies de treball o 16 hores d'un administrador de xarxa per implantar els canvis necessaris a la xarxa i la compra de 4 *pendrives* per societat amb opció de xifrat, valorats en 70 € cadascun.

Tasca 10. Verificar la seguretat física de les instal·lacions.

Verificar i documentar la seguretat física de les instal·lacions de l'organització és una tasca molt simple amb un cost estimat de dues hores per societat. Per tant, es valora en dos dies de treball o 16 hores realitzades per un responsable de seguretat.

Tasca 11. Implementar un Pla de Destrucció de Dades a l'organització.

Per últim, la implementació d'un Pla de Destrucció de Dades a l'organització és una tasca que està fora de l'àmbit del personal de la companyia i és necessari encarregar a una consultora especialitzada. El preu aproximat d'aquesta tasca per cada societat és d'uns 400 €, és a dir, 3.200 € en total. (aquesta valoració s'ha obtingut de factures de prestació de serveis)

4.2. Full de costos totals

L'estimació de 40 € per hora s'ha obtingut de la cotització obtinguda en varies pàgines web especialitzades en el sector laboral per un enginyer informàtic.

Concepte	Hores	Persones	Preu hores (50€)	Material	Externs	Total
Tasca 1	104	1 Enginyer	5.200,00 €	- €	- €	5.200,00 €
Tasca 2	24	1 Enginyer	1.200,00 €	- €	- €	1.200,00 €
Tasca 3	-		- €	- €	3.800,00 €	3.800,00 €
Tasca 4	-		- €	- €	4.500,00 €	4.500,00 €
Tasca 5	8	1 Enginyer	400,00 €	- €	- €	400,00 €
Tasca 6	4	1 Enginyer	200,00 €	- €	- €	200,00 €
Tasca 7	-		- €	- €	- €	- €
Tasca 8	-		- €	- €	- €	- €
Tasca 9	16	1 Enginyer	800,00 €	2.240,00 €	- €	3.040,00 €
Tasca 10	16	1 Enginyer	800,00 €	- €	- €	800,00 €
Tasca 11	-		- €	- €	3.200,00 €	3.200,00 €
TOTAL	172		8.600,00 €	2.240,00 €	11.500,00 €	**22.340,00 €**

Figura 5. Taula de valoració econòmica total

5. Conclusions

La realització d'aquest projecte ha suposat una primera tasca de recerca i revisió de les normatives i legislacions internacionals en matèria de protecció de dades personals en la que s'ha constatat les preocupacions de les societats occidentals en preservar els drets dels ciutadans a la privacitat i les grans similituds entre les normatives de protecció de dades personals de cada país.

També s'ha comprovat la manca d'eines d'ajuda estandarditzades - més enllà d'algunes guies molt genèriques i petits formularis web -, que les administracions posen a disposició de les empreses, fet que provoca una considerable inversió en recursos per a les empreses, dificultant la seva aplicació.

Respecte als objectius plantejats inicialment, l'anàlisi del document de proposta d'elaboració indica que la consecució del principal objectiu del projecte, l'obtenció per part del grup JPV d'una certificació oficial en matèria de protecció de dades efectiva abans del 31 de desembre del 2018, és fàcilment assequible i mesurable, més enllà de la inversió econòmica destinada a tal efecte, que no hauria de suposar un gran problema per a una companyia com l'analitzada.

L'objectiu d'incrementar la seguretat de la informació de la companyia en un 30% durant els pròxims dos anys és un altre objectiu fàcilment assolible amb l'aplicació dels requisits obtinguts en aquest treball i mesurable mitjançant les auditories de seguretat necessàries, i com a conseqüència d'aquests dos primers objectius, s'assoleix l'últim objectiu d'augmentar la credibilitat de l'organització davant els seus clients en més d'un 50% durant els pròxims tres anys, xifra que s'haurà d'obtenir mitjançant l'increment dels clients.

En la realització del treball també s'ha verificat que tant la planificació inicial com la metodologia escollida han estat plenament encertades, ja que s'ha

seguit acuradament el cronograma plantejat a l'inici del treball i com s'ha comprovat, s'han obtingut els productes previstos en el termini indicat.

Per últim, aquest projecte ha obert diverses línies de treball a futur molt interessants, com les metodologies de valoració de riscos (MAGERIT v3, OCTAVE o CRAMM), les eines de xifrat per a dispositius d'emmagatzematge, o l'elaboració d'un pla integral de destrucció de dades.

6. Glossari

SAP: SAP és una companyia multinacional alemanya especialitzada en el disseny de productes informàtics de gestió empresarial, tant per a empreses com per a organitzacions i organismes públics. Fundada en 1972, i amb seu en Walldorf, Baden-Württemberg, els seus productes inclouen SAP ERP, SAP Business Warehouse (SAP BW), SAP BusinessObjects i SAP HANA.

Spam: El terme Spam o correu escombraria fa referència als missatges no sol·licitats, no desitjats o amb remitent no conegut (correu anònim), habitualment de tipus publicitari, que generalment són enviats en grans quantitats (fins i tot massives) que perjudiquen d'alguna o diverses maneres al receptor.

Reglament: El Reglament és una norma jurídica de Dret comunitari de la UE amb abast general i eficàcia directa. Per tant, implica que és directament aplicable en tots els Estats de la Unió Europea per qualsevol autoritat o particular, sense que sigui precisa cap norma jurídica d'origen intern o nacional que la traslladi per completar la seva eficàcia plena.

Directiva: La Directiva és una norma jurídica de Dret comunitari de la UE amb abast general, però deixant llibertat als Estats per escollir els mitjans adequats (mecanisme de transposició).

Llei Orgànica: Una llei orgànica és aquella que es requereix constitucionalment, a causa de la importància de les matèries que regula, per certes matèries (drets fonamentals dels ciutadans o articulació dels diversos poders de l'Estat, per exemple). La Constitució sol prescriure que aquestes normes siguin aprovades, per exemple, per majoria absoluta o per algun altre tipus de majoria qualificada. Amb això es pretén que no sigui una majoria parlamentària conjuntural la que configuri aspectes bàsics i fonamentals de la

convivència ciutadana o l'estructura i organització dels poders polítics d'un Estat.

Reial Decret: Un Reial decret és una norma jurídica amb rang de reglament que emana del poder executiu (el Govern) i en virtut de les competències prescrites en la Constitució.

ERP: Un sistema de planificació de recursos empresarials (*Enterprise Resource Planning* o ERP) són els sistemes d'informació gerencials que integren i manegen molts dels negocis associats amb les operacions de producció i dels aspectes de distribució d'una companyia en la producció de béns o serveis.

GUI: La interfície gràfica d'usuari (*Graphical User Interface* o GUI), és un programa informàtic que actua d'interfície d'usuari, utilitzant un conjunt d'imatges i objectes gràfics per representar la informació i accions disponibles en la interfície. El seu principal ús consisteix a proporcionar un entorn visual senzill per permetre la comunicació amb el sistema operatiu d'una màquina o computador.

CIFS: El Sistema de Fitxers Comú d'Internet (*Common Internet File System* o CIFS) és un protocol de xarxa desenvolupat per Microsoft per a l'ús compartit d'arxius basat en sistemes operatius Windows i altres utilitats de xarxa.

CPD: Un centre de processament de dades o CPD és un edifici o sala gran utilitzada per mantenir una gran quantitat d'equipament informàtic i electrònic. Solen ser creats i mantinguts per grans organitzacions a fi de tenir accés a la informació necessària per a les seves operacions o bé com a espai de venda o lloguer. Pràcticament totes les companyies que són mitjanes o grans tenen algun tipus de CPD, mentre que les més grans arriben a tenir varis.

VPN: Una xarxa privada virtual (*Virtual Private Network* o VPN) és una tecnologia de xarxa de computadors que permet una extensió segura de la xarxa d'àrea local (LAN) sobre una xarxa pública com a Internet. Permet que la

computadora a la xarxa enviï i rebi dades sobre xarxes compartides o públiques com si fos una xarxa privada amb tota la funcionalitat, seguretat i polítiques de gestió d'una xarxa privada. Això es realitza establint una connexió virtual punt a punt mitjançant l'ús de connexions dedicades, xifrat o la combinació de tots dos mètodes.

Tallafocs: Un tallafocs o *firewall* és la part d'un sistema informàtic dissenyada per bloquejar l'accés no autoritzat a la xarxa, permetent al mateix temps les comunicacions autoritzades. Es tracta d'un dispositiu o conjunt de dispositius configurats per limitar, xifrar o desxifrar el tràfic entre els diferents àmbits sobre la base d'un conjunt de normes i altres criteris.

MAGERIT: MAGERIT és la metodologia d'anàlisi i gestió de riscos elaborada pel Consell Superior d'Administració Electrònica. Aquesta metodologia estima que la gestió dels riscos és una pedra angular en les guies de bon govern. Actualment està en la seva versió 3.

OCTAVE: *Operationally Critical Threat, Asset and Vulnerability Evaluation* (OCTAVE, per les seves sigles en anglès), és una metodologia desenvolupada per el *Computer Emergency Response Team* (CERT), que té com a objectiu facilitar l'avaluació de riscos en una organització.

CRAMM: *CCTA Risk Analysis and Management Method* és una metodologia d'administració del risc, actualment en la seva cinquena versió, creada al 1987 en el *Central Computer and Telecommunications Agency* (CCTA).

Malware: El *malware* (de l'anglès *malicious software*), o programari maliciós, és un tipus de programari que té com a objectiu infiltrar-se o danyar una computadora o sistema d'informació. El terme *malware* és molt utilitzat per professionals de la informàtica per referir-se a una varietat de programari hostil, intrusiu o molest.

Wipe utility: *Wipe Utility* és una utilitat de programari basat en la sobreescriptura de les dades per destruir completament totes les dades

electròniques que resideixen en un disc dur o altres mitjans digitals. Utilitza zeros i uns per sobreescriure dades a tots els sectors del dispositiu.

7. Bibliografia

- **Rebollo Serrano, L. ; Serrano Pérez, M. M.** (2008). «*Introducción a la Protección de Datos*». Madrid: Editorial Dykinson.
- **Navarro García, F.** (2012). «*Responsabilidad Social Corporativa: Teoría y Práctica*». Madrid: Editorial ESIC.
- **Giménez Albacete, J. F.** (2015). «*Seguridad en Equipos Informáticos*». Málaga: IC Editorial.
- **Garriga Domínguez, A.** (2004). «Tratamiento de datos personales y derechos fundamentales». Madrid: Editorial Dykinson.
- **Agencia de los Derechos Fundamentales de la Unión Europea, Consejo de Europa** (2014). «*Manual de legislación europea en materia de la protección de datos*». Luxemburgo: Oficina de Publicaciones de la Unión Europea.
- **Sánchez Bravo, A. A.** (1998). «*La protección del derecho a la libertad informática en la Unión Europea*». Sevilla: Universidad de Sevilla.
- **Fuster Sabater, A.** (2012). «Criptografía, protección de datos y aplicaciones : una guía para estudiantes y profesionales». Madrid: RA.MA.SA Editorial.
- **Gutwirth, S; Leenes, R; De Hert, P.** (2016). «*Data Protection on the Move: Current Developments in ICT and Privacy/Data* ». Luxemburgo: Springer Editorial.
- **Pagliari, G. A.; Eterovic, J.** (2012). «Metodología de Análisis de Riesgos Informáticos». Madrid: EAE Editorial.
- **Geraldes Da Cunha Lopes, T. M.; López Ramírez, L.** (2010). «La Protección de Datos Personales en México». Michoacan: Facultad de Derecho y Ciencias Sociales.

Websites

- **CONFIALIS Protecció de Dades**: <http://www.confialis.com> (3 d'octubre de 2017)
- **GADAE 5 raons per complir LOPD**: <http://www.gadae.com/blog/5-razones-para-empezar-cumplir-ya-la-ley-organica-de-proteccion-de-datos/> (4 de octubre de 2017)
- **Agència Espanyola de Protecció de Dades**: <http://www.agpd.es> (17 d'octubre de 2017)
- **European Data Protection Supervisor**: <https://edps.europa.eu> (21 d'octubre de 2017)
- **CNIL**: <https://www.cnil.fr> (23 d'octubre de 2017)
- **CNPD**: <https://www.cnpd.pt> (22 d'octubre de 2017)
- **ICO**: <https://ico.org.uk> (25 d'octubre de 2017)
- **IFAI**: <http://www.ifai.org.mx/> (27 d'octubre de 2017)
- **FTC**: <https://www.ftc.gov> (28 d'octubre de 2017)
- **Ayuda Ley Protección de Datos**: <https://ayudaleyprotecciondatos.es/2017/11/27/registro-actividades-rgpd/>(15 de novembre de 2017)
- **LOPDAT**: <http://www.lopdat.es/noticias/aplicacion-practica-y-progresiva-del-nuevo-reglamento-europeo-de-proteccion-de-datos> (18 de novembre de 2017)
- **Judit Garrido Fontova**: <http://www.juditgarridofontova.com/encargado-del-tratamiento-lopd-vs-rgpd/> (21 de novembre de 2017)
- **INCIBE**: <https://www.incibe.es/extfrontinteco/img/File/empresas/dosieres/plan_director_de_seguridad/plan_director_de_seguridad_metodologias_analisis_de_riesgos.pdf> (22 de novembre de 2017)
- **Diario Oficial de la Federación Mexicana:** <http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013#!> (28 de novembre de 2017)

- FTC:<https://www.ftc.gov/es/consejos/para-empresarios/como-proteger-la-informacion-personal-una-guia-para-negocios> (1 de desembre de 2017)
- Protecció de dades personals: <http://www.protecciondedatospersonales.org/2015/01/23/las-5-claves-para-cumplir-con-la-ley-federal-de-proteccion-de-datos-personales-por-parte-de-las-empresas/> (2 de desembre de 2017)