Implementació d'un procés de gestió d'incidents per a complir amb la nova regulació de protecció de dades.

Enric Arrazola
Grau d'Enginyeria Informàtica – Itinerari en Sistemes d'Informació
Gestió de Projectes

Xavier Martínez Munné
Atanasi Daradoumis Haralabus

8 Juny 2018

FITXA DEL TREBALL FINAL

Títol del treball:	*Implementació d'un procés de gestió d'incidents per a complir amb la nova regulació de protecció de dades.*
Nom de l'autor:	*Enric Arrazola Diaz*
Nom del consultor/a:	*Xavier Martínez Munné*
Nom del PRA:	*Atanasi Daradoumis Haralabus*
Data de lliurament (mm/aaaa):	*07/2018*
Titulació o programa:	*Grau d'Enginyeria Informàtica – Itinerari en Sistemes d'Informació*
Àrea del Treball Final:	*Gestió de Projectes*
Idioma del treball:	*Català*
Paraules clau	*Protecció de dades, problemes, seguretat*

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

El propòsit d'aquest treball final de grau és exposar com implementar els canvis necessaris a una empresa per tal d'aplicar les noves regulacions de protecció de dades (GDPR 2018).

Amb aquest objectiu, en aquest treball descriuré l'expansió global de les empreses, l'externalització de serveis i la utilització de noves tecnologies "cloud" amb les dificultats que impliquen les noves regulacions de protecció de dades. Tot això també ho relacionaré amb els tractaments dels incidents de seguretat, que han de fer i que hauran de fer les empreses en el moment que tinguin una fuga de dades o un atac una vegada s'apliqui la nova regulació europea.

Explicaré les diferencies de la LOPD amb la nova regulació i resoldrem els

problemes que s'estan trobant les empreses per implantar aquestes regulacions i sobretot aquelles empreses multinacionals que tenen diferents serveis en diferents regions del món.

Amb aquest treball, es pretén demostrar que ara mateix és molt important complir amb la nova regulació per evitar possibles sancions i mostrar la importància que tenen aquestes regulacions amb els serveis que ofereixen les empreses.

Abstract (in English, 250 words or less):

The purpose of this work is to explain how to implement the necessary changes within a company to comply with the new data privacy regulations.
To this end, the work describes the global expansion, the outsourcing of services and the usage of cloud technologies done by corporations with the roll-out of new data protection regulations. I would link all those topics with the security incident management processes and the new steps that all companies would need to do when suffering ad data breach or an attack.

I would explain the differences between the existent LOPD and the new data privacy regulation and we would resolve problems that corporations are suffering to implement these regulations, specially related to the companies with presence within different regions across the world.

This work aims to demonstrate that nowadays is very important to comply with new privacy regulation to avoid sanctions and to explain the importance of those regulations with the services that companies offer to their clients.

Índex

Llista de figures

1. Introducció

1.1 Context i justificació del Treball

Avui en dia, la protecció de dades és un aspecte vital per a qualsevol empresa. La protecció de dades forma part de la mesura que tenen els clients de la qualitat del servei. Un client no considerarà un bon servei si no se'n té una bona protecció de les dades. Les expectatives de tots els clients recauen en el manteniment, la gestió i en la protecció de les dades que se'n tenen. En els últims anys, la quantitat de dades que es generen i es guarden ha crescut de manera molt notòria i, a la vegada, també n'han augmentat les exigències en la seva protecció. Aquest augment de les dades gestionades i guardades i l'expansió global a través d'internet han fet que les empreses es vegin obligades a respondre a les exigències d'un entorn cada cop més internacional.

A més a més, la combinació d'aquesta internacionalització amb l'aparició de noves tecnologies com el "cloud" fan que cada cop sigui més difícil conèixer la ubicació real de les dades i poder-ne controlar els accessos o l'ús que se'n fa de les dades controlades per a les empreses.
I, si a tot aquest estat, hi afegim l'augment dels atacs informàtics tenim una situació que requereix ser analitzada amb molt detall i amb molta cura.

Tot i que a Espanya ja existia una regulació per a protegir les dades, no passava el mateix a tots els països europeus. Degut a que, actualment, les empreses tenen una expansió global i, degut a que cada cop més tenen presència en diferents països, la comunitat europea ha optat per crear una nova regulació que s'aplica a tots els països europeus des del mes de Maig. Això fa que totes les empreses s'hagin hagut d'adaptar i hagin hagut de canviar els seus processos, no sols per protegir les

dades sinó també per a notificar-ne qualsevol problema existent en la gestió de les dades a les autoritats reguladores pertinents.

En el present treball final de grau s'explica el projecte de redacció i adaptació als que s'ha hagut de sotmetre una empresa per tal d'adaptar-ne els seus procediments per a complir amb la nova regulació. La idea del treball sorgeix de l'estudi de la nova regulació i l'aplicació d'aquesta a una multinacional amb totes les implicacions que aquesta nova regulació té en l'aspecte tecnològic i en l'actualització de processos i de serveis que s'ofereixen als clients.

El treball neix de la inquietud que sorgeix en la lectura de la nova regulació conjuntament i amb la utilització creixent de serveis "cloud" per a guardar-ne les dades personals.

1.2 Objectius del Treball

Els objectius per aquest treball final de grau són els següents:

- Definir la metodologia o el procés per a implementar els canvis necessaris a una empresa per tal d'aplicar les noves regulacions de protecció de dades (GDPR 2018).
- Dissenyar les propostes estructurals i d'adaptació a la nova regulació de protecció de dades.

1.3 Enfocament i mètode seguit

L'enfocament del treball és de tipus qualitatiu. És una descripció, anàlisi i redacció de propostes per a implementar canvis als processos d'una empresa per a complir amb la nova regulació de protecció de dades.

La metodologia que s'ha seguit per a fer el treball consta de diferents fases per tal d'analitzar la nova regulació de protecció de dades, així com revisar els canvis existents en relació a la regulació vigent (LOPD).

Una vegada analitzada la nova regulació, hem revisat els processos que té una multinacional amb els seus serveis al “cloud” i que, a la vegada, té serveis externalitzats. També s’ha centrat l’estudi en les problemàtiques que s’han trobat les empreses que puguin tenir una fuga de dades i quines accions han de fer per tal de complir amb la nova regulació.

Si ens centrem en el detall de les fases. La primera fase es va orientar en la cerca d’informació generalista sobre la protecció de dades. Per a poder orientar el treball, es va analitzar l’estat de la protecció de dades a Espanya i Europa i fer-ne una comparació a nivell mundial. D’aquesta manera s’identifiquen les necessitats que tenen les empreses en adaptar els processos a nivell global.

La segona fase d’estudi va enfocar-se en la revisió de la normativa espanyola i la comparativa amb la normativa europea. Es va treballar en la detecció de les similituds i les diferències que tenen les dues normatives. D’aquesta manera es van poder identificar les àrees que una empresa necessitava revisar per tal d’adaptar els seus processos a la nova normativa.

La darrera fase de l’estudi es va enfocar en la cerca de millores en els processos i en la cerca de noves solucions tecnològiques que ajudessin a complir amb la nova normativa europea.

Durant tota la fase del treball, vam consultar diferents fonts d’informació i especialment la web de la Unió Europea amb el detall de la nova regulació i tot un seguit de dades i articles publicats a internet.

Una altra manera d’enfocar el treball hagués estat centrant-se únicament en la nova normativa, identificar-ne tots els requeriments i cercar noves solucions des d’aquests requeriments. Però he cregut que era més fàcil partir de la normativa existent a Espanya. La regulació existent ja identificava uns requeriments mínims a complir i serveix de punt de

partida per a identificar solucions tecnològiques que ja existeixen al mercat. D'aquesta manera només cal centrar-se en la diferència de les dues normatives i trobar solucions per a aquestes diferències. A més a més, la regulació espanyola era, juntament, amb l'alemanya una de les més restrictives a Europa, això fa que part dels nous requeriments no siguin tan complicats d'implementar a Espanya com ho poden ser a la resta de països.

1.4 Planificació del Treball

L'organització del treball ha correspost a les entregues de les proves d'avaluació continuada que hi ha al llarg del semestre.

La primera fita de la planificació ha estat el lliurament de la PAC 1. Aquesta fita es centra en l'elaboració del pla de treball.

FITA 1:

- Introducció del treball
    - Context i justificació del treball.
    - Objectius del treball.
    - Enfocament i mètode seguit.
    - Planificació del treball.
    - Breu sumari dels productes obtinguts.
    - Breu descripció dels capítols de la memòria.

La segona i la tercera fita corresponen a l'execució de les tasques del pla de treball.

La segona fita es va centrar en la descripció de la nova regulació i la revisió de la LOPD.

FITA 2:

En aquesta segona fita es van reorganitzar part de les tasques per un imprevist en la planificació (malaltia). També es van redefinir alguns apartats del treball.

- Privacitat i protecció de dades
    - Protecció de dades a Espanya i Europa
    - Visió global de la protecció de dades.
- Descripció de la nova Regulació Europea (GDPR)
    - Dates clau en la implementació de la nova regulació
- Descripció de la LOPD
- Impacte del GDPR
    - Diferències entre GDPR i LOPD.

La tercera fita es va centrar en les oportunitats i problemàtiques de les empreses i també es va acabar amb les tasques pendent de la descripció de la LOPD.

FITA 3:

En aquesta tercera fita es van replantejar part de les tasques i dels dies de treball per motius laborals. Degut a uns imprevistos a la feina, es van haver d'utilitzar alguns dels dies reservats per imprevistos entre setmana. També es van readaptar els apartats dels treball per a centrar-nos en els incidents de seguretat, en les possibles solucions tecnològiques i en les millores de processos dels empleats.

- Incidents de seguretat

    - Què fer?
    - Què passa quan hi ha un problema?
    - Persones, processos, tecnologia

- Recomanacions i Proposta per a complir amb la regulació
- Conclusions
- Bibliografia

La última fita ha consistit en el lliurament de la memòria i la seva defensa.

FITA 4:

- Lliurament memòria
- Preparació defensa
- Informe autoavaluació
- Defensa memòria

El treball el vam iniciar el dia 1 de Març de 2018 i finalitza el dia 18 de Juny de 2018 amb la defensa de la memòria.
Les dates clau són les següents:

- Lliurament PAC 1 (16 de Març de 2018)
- Lliurament PAC 2 (13 d'Abril de 2018)
- Lliurament PAC 3 (11 de Maig de 2018)
- Lliurament Final (8 de Juny de 2018)
- Defensa Virtual (18 de Juny de 2018)

Es preveuen 27 jornades de 8 hores i 15 jornades de 3 hores de dedicació al treball. Això fa un total de 261 hores de dedicació

Es reserven tots els dies de dilluns a dijous (55 dies) per a possibles eventualitats no planificades a on la jornada seria de 2 hores.

La suma total d'hores de dedicació serà de 371 en cas de necessitar tots els dies disponibles.

Hi ha un seguit de dies que no hi ha dedicació al treball degut a situacions personals. Del 29 de Març fins el 2 d'Abril de 2018 i del 19 de Maig fins el 21 de Maig.

La distribució de les jornades s'indica al següent gràfic:

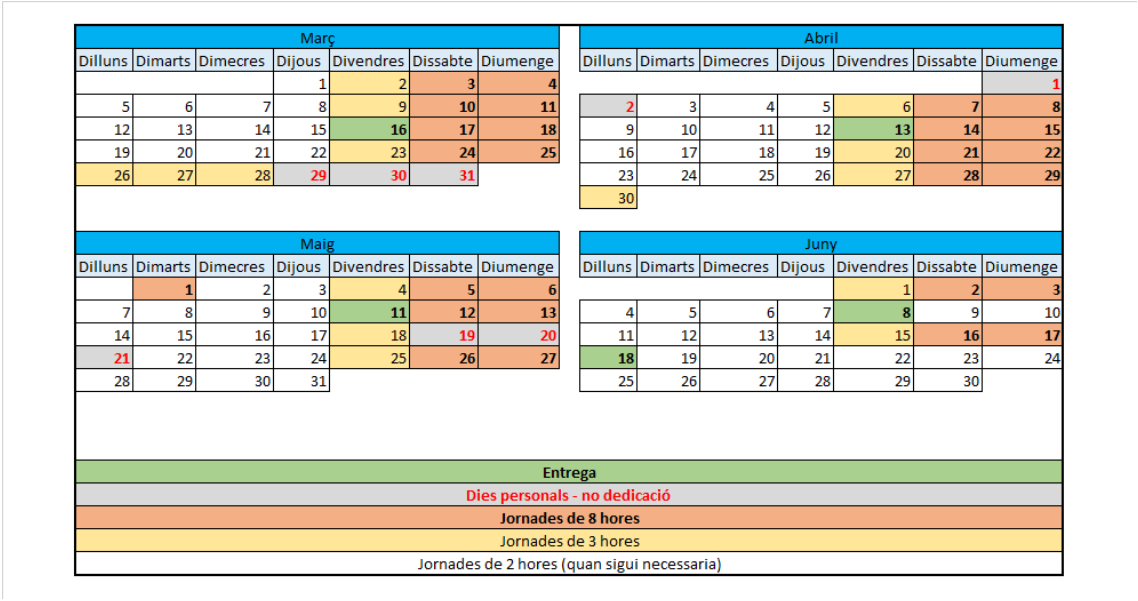

Figura 1: Cronograma del treball

A continuació es pot observar el diagrama de Gantt derivat de la seva temporització:

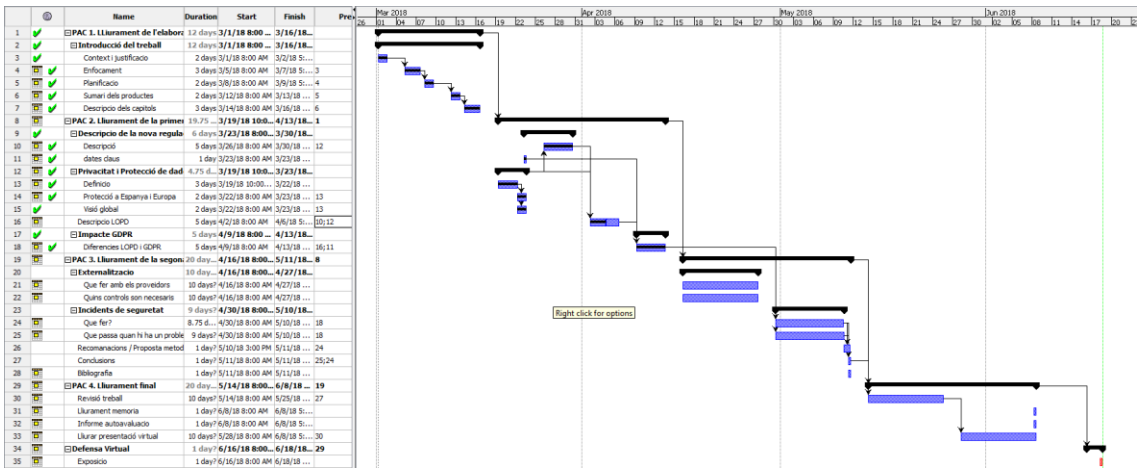

Figura 2: Diagrama de Gantt

1.5 Breu sumari de productes obtinguts

El resultat final del treball ha estat una revisió de la nova regulació i un conjunt de recomanacions per a ajudar a una empresa a implantar aquesta regulació en la gestió de les seves aplicacions, els seus proveïdors i la gestió de les dades.

També s'han analitzat i incorporat possibles solucions tecnològiques per a les empreses per tal d'evitar els possibles impactes que es puguin derivar de l'aplicació de la nova regulació.

El treball està dividit en diferents parts que s'han inclòs a la memòria:

- Proposta i pla de treball.
- Estudi de la regulació de protecció de dades.
- Comparació amb la LOPD.
- Anàlisi de les noves tendències globals (cloud, externalització de serveis).
- Tractament incidents amb la seguretat de les dades.
- Recomanacions per a adaptar els processos de les empreses.
- Conclusions, memòria i defensa.
    - Món evoluciona
    - Xarxes personals
    - Monedes virtuals

1.6 Breu descripció dels altres capítols de la memòria

En el següent capítol de la memòria s'explica què cal saber sobre la nova regulació de protecció de dades. Expliquem els inicis de la nova regulació, les dates en les que s'ha començat a implantar i els principals canvis proposats a la regulació. També s'hi troben conceptes necessaris per entendre el concepte de privacitat i la tipologia de les dades.

Posteriorment, hem explicat els canvis principals en relació a la LOPD existent a Espanya.

En el quart capítol, ens hem centrat a explicar les situacions que es troben els enginyers en la implantació de la nova regulació quan hi ha serveis externalitzats o serveis “cloud” gestionats per altres empreses.

Després d’aquestes temàtiques, hem explicat quines accions hauran de fer les empreses en cas de tenir un incident de seguretat a on hi hagi dades impactades. I, a continuació, hem identificat tot un seguit de recomanacions per a les empreses i els seus departaments de TI.

Per últim, acabem amb un seguit de conclusions d’aquest treball, la bibliografia i les referències utilitzades.

2. Privacitat i protecció de dades

Per a començar a introduir-nos en la temàtica del treball de final de grau, definim una sèrie de conceptes bàsics que ens ajudaran a poder desenvolupar les diferents propostes que es desenvoluparan al llarg del treball.

El Termcat defineix privacitat com "*la condició de les informacions que fan referència o pertanyen a una persona física o jurídica, segons la qual no poden fer-se públiques sense el consentiment de l'afectat*." [3]. En aquesta definició ja apareixen una sèrie de conceptes que són de gran importància per als gestors de SI /TI com són consentiment, afectat o informació personal. Per això, descriurem amb una mica més de detall aquests conceptes bàsics i alguns altres que també aniran sortint al llarg del treball.

La nova regulació Europea o l'antiga Llei Orgànica de protecció de dades, així com la IAPP (International Association of Privacy Professionals) defineixen les dades personals com *"informació sobre una persona física identificada o identificable (el subjecte / l'interessat/ l'afectat / l'individu)".*

La llei orgànica de protecció de dades (LOPD) defineix una sèrie de conceptes que són molt presents al llarg del treball com són afectat, tractament de dades, consentiment, processador de dades o controlador.

Afectat: la persona física titular de les dades que són subjectes al tractament.

Tractament de les dades: Conjunt d'operacions realitzades sobre dades personals.

Consentiment: Acceptació inequívoca, lliure, específica i informada amb la que l'interessat accepta el tractament de les dades.

Processador de dades: Persona física o jurídica, autoritat pública, servei o organisme que tracta les dades personals per compte del controlador.

Controlador / Encarregat de dades: Persona física o jurídica, autoritat pública, servei o organisme que defineix la finalitat del tractament de les dades.

El diccionari de Cambridge defineix la bretxa de seguretat com la situació en la que les dades personals han estat vistes / accedides / esborrades / etc. de manera accidental per un individu no autoritzat.

Les dades de caràcter personal s'estructuren en diferents nivells. I hi ha moltes dades de caràcter personal. En general, qualsevol dada que permeti identificar algun subjecte es considera dada personal, per exemple:

- noms i cognoms
- números de DNI, NIF i passaport
- adreces físiques
- telèfons
- adreces de correu electrònic
- fotografies
- dades genètiques i mèdiques
- dades biomètriques
- dades referides a creences, afiliació política o sindical
- dades referides a la raça

2.1 Protecció de dades a Espanya i Europa.

L'any 1995, la Unió Europea va adoptar la directiva 95/46/EC en relació a la protecció dels individus quan es tractaven les dades personals i la distribució d'aquestes dades.

L'any 1999, Espanya va aprovar la llei orgànica 15/1999 (LOPD) amb el que s'establia un procés sancionador si es cometia una infracció en la protecció de

les dades. Protegia la informació de caràcter personal que era responsabilitat de les empreses espanyoles, independentment de la localització de les dades i els sistemes.

L'any 2007, va actualitzar-se la LOPD per tal d'incloure un reglament amb les mesures a aplicar en els sistemes d'informació i en la gestió de fitxers no automatitzats (en paper).

L'any 2016, va entrar en vigor el nou Reglament General de Protecció de Dades (GDPR) encara que es van donar un parell d'anys de marge per a adoptar-la a les diferents empreses.

L'any 2018, s'aplica el nou reglament a tots els estats de la Unió Europea.

2.2 Visió global de la protecció de dades

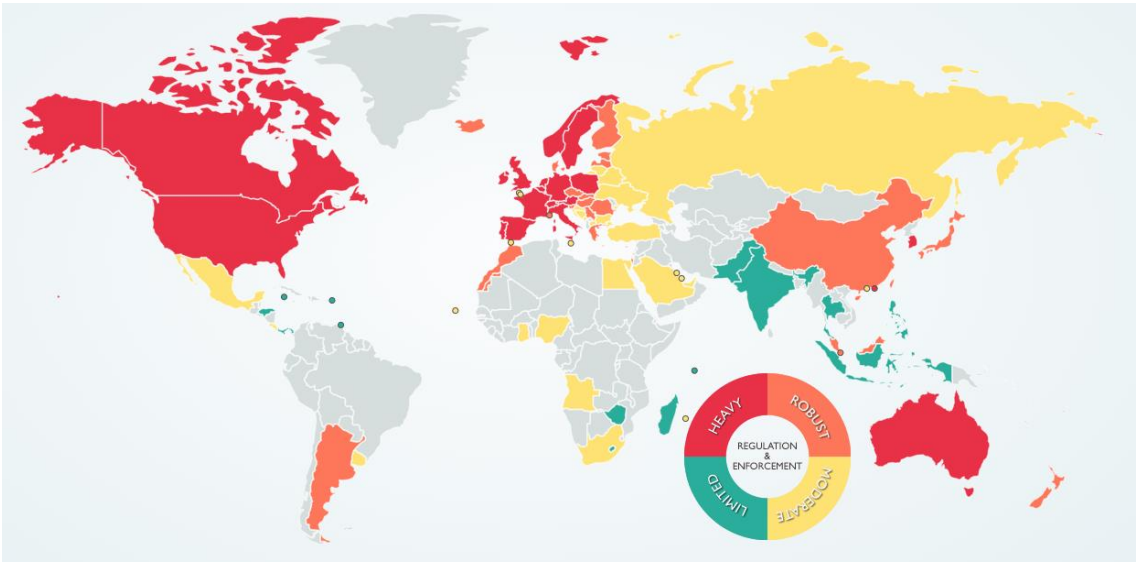

Figura 3: Protecció de dades al món [11]

La protecció de dades no és únicament una tendència europea sinó que s'està convertint en una necessitat global. Molts països tenen les seves lleis de protecció de dades i cada cop són més restrictives.

Aquestes lleis conjuntament amb la globalització fan que les diferents organitzacions que treballin en diversos entorns hagin de realitzar més esforços per tal d'adaptar els seus processos i els seus sistemes per a complir amb les noves regulacions.
Com es veu en el gràfic anterior, encara queden zones al món (representades en gris) a on la majoria de països no tenen cap llei que reguli la protecció de dades com són les regions d'Àfrica, de Sud-Amèrica i una part d'Àsia.
Però també es pot veure com, en els països més desenvolupats, hi ha una tendència a tenir lleis de protecció de dades. Es cert que hi ha països a on no hi ha una regulació especifica per a protegir les dades personals però si que es comencen a tenir regulacions per a protegir part de les dades electròniques que es generin (representats en verd).

En d'altres països, s'han començat a redactar lleis especifiques de protecció de dades però encara no s'apliquen (representats en groc) o, ara bé, tenen diferents lleis que inclouen part de la protecció de dades, encara que no sigui una llei dedicada a la protecció de dades (representats en taronja).

Per últim, trobem la gran majoria de països europeus, Australia i Nord-Amèrica a on hi ha lleis específiques de protecció de dades i aquestes són de compliment obligatori i amb les corresponents sancions si no s'apliquen (representats en vermell).

3. Descripció de la nova Regulació Europea de protecció de dades (GDPR)

La “General Data Privacy Regulation” (GDPR) és la nova regulació Europea de protecció de dades que va entrar en vigor el Maig del 2016 i que s’aplica a Europa des del Maig de 2018.

Durant aquest període de temps les empreses han hagut d’adaptar els seus processos i els seus sistemes informàtics per tal de garantir-ne el compliment.

La nova regulació substitueix a la llei orgànica de protecció de dades (LOPD) i obliga a les empreses a una sèrie de tasques extres en la gestió i el manteniment de les dades.

Aquesta regulació europea serveix per a garantir la protecció de la informació personal dels diferents individus de la unió europea i que aquests puguin tenir major control de les seves dades. També serveix per a unificar els criteris de protecció de dades a tots els països. Aquest últim punt facilita a les empreses que operen en diferents països a tenir un únic criteri per a tractar i protegir les dades dels individus.

“*La nova regulació assenyala que les mesures dirigides a garantir el seu compliment han de tenir en compte la naturalesa, l’àmbit, el context i els fins del tractament així com el risc per als drets i les llibertats de les persones. D’acord amb aquest enfoc, algunes de les mesures que el GDPR estableix s’aplicaran només quan existeixi un alt risc per als drets i les llibertats, mentre que altres hauran de modular-se en funció del nivell i tipus de risc que els tractaments presentin.*

L’aplicació de les mesures previstes per al GDPR han d’adaptar-se, per tant, a les característiques de les organitzacions. El que pot ser adequat per a una organització que gestiona dades de milions d’interessats en tractaments complexes que involucrin informació personal sensible o volums importants de

dades sobre cada afectat no es necessari per a una petita empresa que gestioni un volum limitat de tractament de dades no sensibles. " [7].

Segons el reglament, és molt important que les empreses tinguin clarament identificat la base legal sobre la que desenvolupen els tractaments de les dades ja que els interessats podran exigir-ne informació. El nou reglament garanteix el dret dels interessats a ser esborrats dels sistemes, a rebre evidències dels accessos o a rebre una còpia de les dades que s'estan tractant. A més a més, quan hi ha un consentiment d'ús, aquest ha de ser inequívoc. Per tant, les organitzacions han d'adaptar els seus sistemes per tal d'incloure l'acceptació del consentiment i tenir uns sistemes a on es puguin fer esborrats parcials de les bases de dades en cas de necessitat.

Tots aquests temes són essencials per als gestors de sistemes informàtics ja que les seves tasques són vitals per a complir amb la nova regulació. Si ens fixem en possibles situacions:

- Hi ha organitzacions que fa dècades que operen a Espanya. Què ha de fer una organització amb les còpies de seguretat que es guarden durant anys si un individu vol ser esborrat? I si es una empresa sencera? I si l'individu deixa l'empresa?
- Si un individu reclama rebre la còpia de les seves dades, com s'han d'entregar? En quin format?

L'esborrat de les dades, s'ha convertit en un dels temes de discussió de moltes organitzacions ja que el dret a l'oblit que tenen els individus fa que la gestió de base de dades que es feia fins ara quedi obsoleta i que els sistemes de seguretat hagin de ser fàcilment accessibles per a poder complir amb la nova regulació.

Per altra banda, un dels altres punts claus en la nova regulació i que afecta a les organitzacions són les mesures de seguretat i especialment les notificacions de les violacions en la seguretat de les dades han de fer-se a les autoritats de protecció de dades competents en els diferents països de la unió europea. Des de maig, la notificació per una bretxa de dades ha de fer-se sense retard, i a

ser possible en les primeres 72 hores següents a que el controlador de les dades n'ha tingut constància.

La nova regulació també és especialment important en identificar les obligacions que tenen les organitzacions en quant a la transferència de dades internacionals a països de fora del Espai Econòmic Europeu. La regulació no nega la possibilitat de transferir dades però si que especifica que el receptor de la informació ha de garantir un nivell de protecció de dades adequat. Això implica un major control en la transferència de dades i en tota la gestió de proveïdors de l'empresa. Els gestors de sistemes han de tenir identificat tots els fluxos de dades, així com conèixer a tots els proveïdors i els seus serveis.

Si ens centrem en la gestió de sistemes, la nova regulació també implica un control més alt i més restrictiu en tot el que significa el desenvolupament dels sistemes informàtics. La privacitat passa a ser la base sobre la qual desenvolupar els nous sistemes. Els processadors de dades i els creadors de sistemes de TI han de dissenyar els serveis per tal que aquests guardin el mínim de dades necessàries per a fer la tasca.

3.1 Dates clau en la implementació de la nova regulació

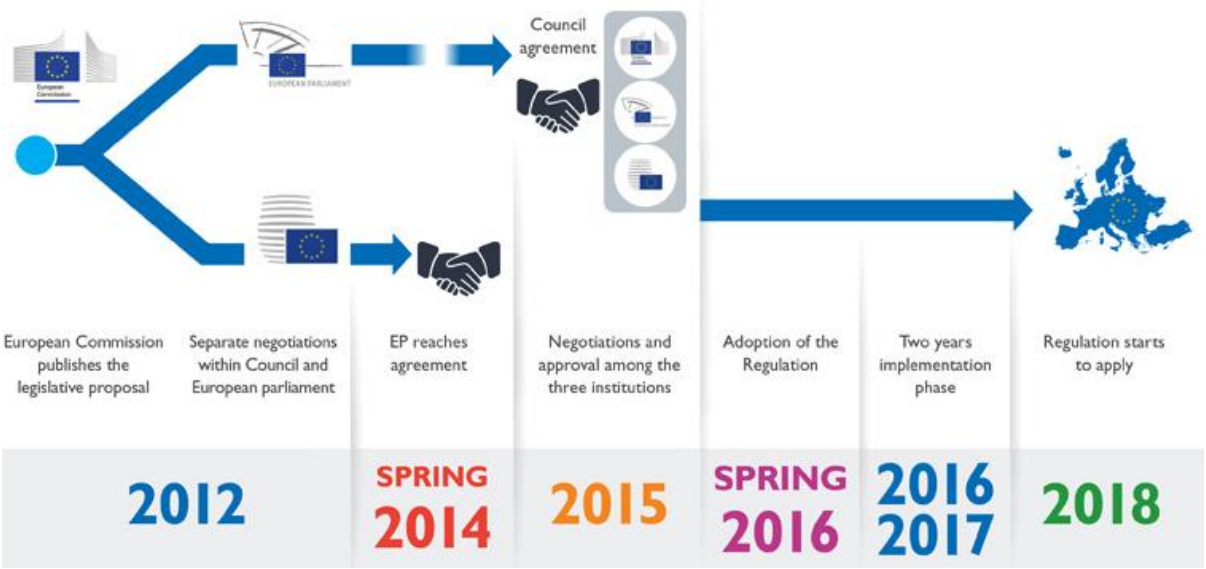

Figura 4: Calendari d'implementació del GDPR

En aquesta figura, s'expliquen les dates claus a Europa en relació a la creació, aprovació i desplegament de la nova llei de protecció de dades.

La proposició de llei va ser feta el 2012 per part de la Comissió Europea i es va estar discutint amb el Consell d'Europa i el Parlament Europeu per a fer-la efectiva.

La primavera del 2014, el Parlament Europeu aprova la proposta de llei. Durant el 2015, les diferents institucions europees tenen reunions per a arribar a la proposta definitiva de la llei. La primavera del 2016, s'accepta la regulació i es dona un marge de dos anys per tal d'implementar la llei als diferents països de la Unió Europea.

El 25 de Maig de 2018, s'acaba el període d'implementació i la llei passa a ser efectiva. Totes les empreses han de complir amb la nova regulació. Si aquesta no es compleix, arribaran les primeres sancions econòmiques per part de les autoritats de protecció de dades.

3.2 Estan les empreses preparades?

Si ens centrem en diferents estudis i articles d'opinió, la gran majoria d'empreses no estan preparades per a complir amb la nova regulació. Una de les característiques importants es que la nova normativa no és només important a Europa sinó que afecta a tot el món.

Familiarity with GDPR	Small firms	Medium firms	Large firms
Very familiar	13%	25%	33%
Somewhat familiar	38%	39%	35%
Aware of the name only	17%	17%	9%
Not familiar with GDPR	31%	18%	23%

Figura 5: Familiaritat de les empreses americanes amb GDPR [19]

Com es pot veure a l'anterior gràfic, les empreses americanes, també estan revisant si la nova regulació té implicacions en elles. El que queda clar es que la nova regulació té un impacte global.

4. Descripció de la LOPD

La Llei Orgànica de Protecció de Dades (LOPD) és la legislació existent a Espanya per a protegir les dades de caràcter personal dels individus. És un dret fonamental de totes les persones que es basa en garantir que tota persona pugui controlar l'ús de les seves dades personals. És una llei que serveix per evitar que terceres persones puguin tenir informació sobre nosaltres que afecti a la nostra intimitat, als nostres drets i a les nostres llibertats.

Es una llei aprovada l'any 1999 i revisada el 2007 que defineix les mesures de seguretat mínimes a aplicar als nostres sistemes i a les dades que es tinguin en paper.

Es una llei que tothom ha de complir ja que sinó pot implicar sancions econòmiques per part de l'agencia espanyola de protecció de dades. Però, el problema no és només econòmic sinó que també és un problema de reputació i d'imatge. Quan hi ha un incompliment de la protecció de dades per part d'una organització, una de les grans pèrdues no és l'econòmica sinó que és la credibilitat per part dels individus.

Una de les característiques de la LOPD és que no totes les dades són igual d'importants. Hi ha dades que s'han de tractar de diferent manera depenent del nivell de seguretat assignat. Hi ha tres nivells de dades:

- Bàsic: Dades identificatives (nom, cognoms, DNI, imatge,...)
- Mig: Dades financeres, infraccions administratives, avaluacions personals.
- Alt: Dades de ideologia, religió, origen ètnic o racial, salut, orientació sexual i fitxers policials.

Dins de la LOPD també fan moltes referències a la definició d'un fitxer i, aquest, és tot conjunt organitzat de dades de caràcter personal que permeti l'accés a les dades.

A la LOPD hi ha moltes referències a com s'han de tractar però també s'explica com s'han de recollir les dades. Aquesta llei reconeix a tota persona el dret a saber perquè, per a què i com es tractaran les dades personals i a que l'individu pugui decidir sobre el seu ús. Això implica que a totes les organitzacions, hi ha d'haver clàusules legals i informatives per a que els individus entenguin la situació.

Un altre aspecte molt rellevant en les organitzacions i, especialment, en els departaments de sistemes i que està recollit a la LOPD són totes les tasques relacionades amb els mecanismes d'identificació i autenticació i de control d'accés a les dades. Els responsables de sistemes han de garantir que les contrasenyes caduquin, que es distribueixen de manera segura, que els usuaris es bloquegin i que es té control de qui accedeixes a les dades.

Altres temàtiques que estan recollides a la LOPD són el tractament dels fitxers en paper i la seva destrucció i els drets dels interessats. Aquests drets s'anomenen ARCO:

- Accés
- Rectificació
- Cancel·lació
- Oposició

Aquests són els drets fonamentals que, en qualsevol moment, el titular de la informació pot exercir.

5. Impacte del GDPR

Un punt important per entendre l'impacte és que aquestes organitzacions han tingut dos anys per a estudiar totes les implicacions del nou reglament, desenvolupar un pla d'acció i implementar un programa de millora en la protecció de dades. Com que la nova regulació europea té una sèrie de diferències amb la LOPD existent, això suposa que les organitzacions han d'adequar els processos i els seus sistemes per a poder complir amb la regulació.

La nova regulació també té una major presència a les organitzacions ja que cobreix més aspectes dels controladors. Un dels impactes més importants està en les noves multes per infringir la nova regulació. Amb l'entrada en vigor de la nova regulació, els reguladors poden imposar una multa de fins el 4% de la facturació anual de les organitzacions.

Per altra banda, també hi ha canvis clau en el consentiment i amb els nous drets que tenen els individus. Dins d'aquests drets, un dels que té certa rellevància és el dret a l'oblit, el dret de demanar als processadors de les dades que hagin d'esborrar les dades immediatament en certes situacions. Un altre dret que ha fet replantejar les estratègies de les organitzacions és el dret a la portabilitat de les dades ja que els individus poden exigir el canvi de dades personals a un altre proveïdor. Aquestes dues temàtiques han obligat a les empreses a redefinir processos d'emmagatzematge de les dades per a poder complir amb aquesta normativa.

Un altre canvi clau amb la nova regulació és la necessitat de realitzar Anàlisis d'Impactes de Privacitat (PIA) en tots aquells processos que involucrin una gran quantitat de dades de caràcter personal. Aquí és on entra la subjectivitat de cada empresa ja que no hi ha cap definició concreta del que significa "gran quantitat de dades".

Altres canvis també importants per a les organitzacions i els departaments de sistemes són la necessitat d'incloure la privacitat en el disseny de les aplicacions, la necessitat de designar a una figura com a responsable de privacitat de les empreses (DPO) en el cas que la companyia tingui una gran quantitat de dades personals o que es dediqui a la gestió de dades personals.

Per últim, la nova regulació té un impacte en la notificació de les bretxes de seguretat. La nova regulació obliga a una reacció immediata a l'hora de tractar aquestes situacions però també de notificar a les autoritats pertinents i als clients impactats.

5.1 Diferències principals entre GDPR i LOPD

LOPD	GDPR
Fitxers	Registre de les activitats de tractament
Registre d'incidents	Notificació de les bretxes a la autoritat reguladora
Drets ARCO	Ampliació de drets (oblit, portabilitat)
Responsable de seguretat	Responsable de protecció de dades
Multes de 900 a 600000€	Multes fins a un 4% de la facturació anual
Consentiment tàcit	Consentiment inequívoc
Informe d'auditoria	Drets d'auditoria dels clients

Figura 6: Taula comparativa GDPR – LOPD

6. Seguretat de la informació

Una de les grans àrees de treball amb la nova regulació és la part relacionada amb els incidents de seguretat. La nova regulació posa molt èmfasis en la necessitat d'identificar, notificar, corregir i evitar repeticions del problema. A més a més, la nova regulació té identificades unes grans sancions per a les empreses que no protegeixin correctament les dades de que disposin. En cas de tenir una bretxa de seguretat, les autoritats podran posar multes que podrien arribar a ser del 4% de la facturació anual de l'empresa.

Aquest increment de les sancions en cas de patir una fuga de dades és el que ha provocat que les empreses tinguin un gran maldecap a l'hora de protegir-ne les dades.

Totes les empreses han hagut de revisar els seus processos i han hagut de revisar com gestionen tota la informació de que disposen o de que en fan ús per tal de garantir-ne una protecció adequada. Però, aquesta tasca, no es tan simple com es podien pensar les empreses ni es tan evident com fa uns anys.

Cada cop més, les empreses tenen entorns més globalitzats i, a la vegada, tenen més serveis externalitzats a proveïdors. Això que té uns beneficis molt importants en alguns aspectes de la gestió de sistemes informàtics i en els costos associats a aquests manteniments ha fet que la revisió dels processos s'hagi complicat. La nova regulació no només implica tenir un major control d'aquests serveis sinó que obliga a millorar els accessos a les dades que aquests proveïdors poden fer o poden manipular.

Per altra banda, les noves solucions "cloud" també han fet que moltes empreses no tinguin les dades tan controlades com es pensaven. Fa uns anys, moltes empreses sabien que les seves dades estaven al seu servidor i, aquest, estava a la seva sala de servidors. Però això tenia uns costos de manteniment que moltes empreses es van voler estalviar. I van veure que les solucions "cloud" eren perfectes per a estalviar en aquest aspecte. Ja no s'havien de tenir

ni mantenir els servidors, aquests podien estar al “cloud” i allà, ja hi havia experts que ho controlaven. I, també, els actualitzaven.

Aquesta millora evident en certs aspectes, ha quedat desvirtuada amb la nova regulació. La nova regulació obliga a controlar les dades però, es pot controlar el “cloud”?

Les empreses han hagut i hauran de continuar treballant en aquest àmbit per tal de continuar complint amb la nova regulació. Una de les característiques importants a millorar és redefinir el procés per tal que aquests proveïdors de “cloud” i aquests equips externs notifiquin els incidents de seguretat.

6.1 Què és la seguretat de la informació?

La seguretat de la informació es garanteix quan s’asseguren que les dades estaran disponibles per als usuaris, que les dades no seran modificades sense control i que només s’accedirà a les dades per les persones autoritzades.

Com s’indica al termcat, la disponibilitat és la capacitat d'un sistema o d'un component informàtic per a garantir plenament les seves funcions en el moment de fer una sol·licitud.

Com s’indica al termcat, la integritat és la característica per la qual una informació emmagatzemada o transmesa no pot ser alterada sense que el lector o destinatari ho detecti.

Al termcat, la confidencialitat és la condició de les informacions que fan referència o pertanyen a una persona física o jurídica, segons la qual no poden fer-se públiques sense el consentiment de l'afectat.

En definitiva, que hi hagi disponibilitat, integritat i confidencialitat de les dades és el que determina que les empreses tinguin les mesures necessàries per a assegurar la seguretat de la informació.

6.2 Què és un incident de seguretat?

Un incident de seguretat es produeix quan qualsevol de les mesures de control per garantir la disponibilitat, la integritat o la confidencialitat de les dades falla.

Dins d'aquests errors, els que són més crítics per a la nova regulació són els que afecten a la integritat i/o a la confidencialitat.

Si les dades dels sistemes no estan disponibles serà un problema en la continuïtat del nostre negoci. Això, tindrà un dany en la reputació de la marca de l'empresa però no estarà subjecte a una multa per part de l'agència reguladora de la protecció de les dades. Ara bé, qualsevol dels altres errors si que pot ser susceptible d'una sanció amb la nova regulació.

Si una empresa no és capaç de garantir que les dades no s'han modificat o, no sap qui les ha modificat, això pot provocar una investigació per part de l'agència reguladora i una possible sanció. I, el pitjor dels casos, si una empresa no pot garantir que les dades només s'han accedit per personal autoritzat, això és el mes greu en aspectes de protecció de dades. Dins d'aquest últim aspecte, es troben tan els atacs informàtics com aquelles situacions internes en que els empleats envien dades a qui no toca, en que es crea un usuari a un sistema incorrecte o en que es programa malament el codi d'una aplicació.

Quan es pensa en un incident de seguretat, molta gent ho relaciona amb els "hackers" però, també s'haurien de plantejar algunes preguntes més simples:

- S'han enviat correus electrònics a persones incorrectes?
- S'han donat accessos a persones incorrectes?
- S'han programat malament les aplicacions?
- S'han perdut ordinadors o mòbils de feina?

Si a qualsevol d'aquestes preguntes es respon amb un si, es quan la nova regulació entra en joc. Qualsevol d'aquestes situacions té un impacte amb la nova regulació europea.

És per això que per tal de complir amb la nova regulació es planteja la creació d'una gestió d'incidents adequada per tal d'evitar les possibles sancions o com a mínim que aquestes sancions siguin el menys elevades possibles.

6.3 Què fer per no tenir problemes?

Per a no tenir problemes es pot treballar de dues maneres, de manera reactiva i de manera proactiva.

De manera proactiva i per tal d'evitar els incidents de seguretat, hi ha tota una sèrie d'implicacions en l'àmbit tecnològic que es poden aplicar. Aquestes implicacions tenen un impacte a les empreses i, especialment, en els departaments de gestió de la informació.

Una de les primeres mesures tracta d'aplicar controls de privacitat des del moment del disseny de l'aplicació. Les noves aplicacions i els nous sistemes es pensaran amb la privacitat com a concepte clau en el seu disseny i, per tal de fer això, els departaments de sistemes han d'estar involucrats en totes les fases de disseny dels sistemes i en totes les iniciatives del negoci a on hi hagi tractament de dades personals.

Una altra mesura clau per a complir amb la regulació és l'anonimització de les dades i l'esborrat de dades personals quan ja no siguin necessàries.

Un aspecte clau en la nova regulació és la prevenció amb controls tecnològics que minimitzin el risc i els impactes dels problemes. Aquí s'hi inclourien totes les solucions per evitar la fuga de dades (DLP), la gestió d'esdeveniments (SIEM), la protecció contra "spam" o "malware" o les mesures d'encriptació de les dades.

6.4 Què passa quan hi ha un problema?

En els apartats anteriors, s'expliquen diferents situacions quotidianes que tindran un impacte en la gestió de les dades que tenen les empreses. Però, encara que tot sembli molt complicat, les empreses a Espanya ja parteixen d'una bona situació gràcies a les accions que ja havien fet per a complir amb la LOPD.

El que canvia en relació a les accions que han de fer els processadors o els controladors de les dades amb la seguretat de les dades i els incidents en la nova regulació són els temps de resposta.

En el cas dels processadors, la nova regulació obliga a notificar al controlador de les dades sense cap tipus de retard ni demora. I aquest controlador haurà de notificar a les autoritats en menys de 72 hores.

Això implica que els processos de gestió d'incidents hagin de ser àgils i ràpids. I un altre aspecte important, encara que no estigui explícitament inclòs en la regulació és el fet d'aplicar millores en els sistemes informàtics una vegada s'hagi tingut un incident de seguretat o que es treballi en la prevenció d'aquests. I aquí es quan de manera reactiva, s'han de millorar els processos existents.

6.5 Persones, processos, tecnologia

És per això que el treball s'ha centrat en analitzar els processos de gestió d'incidents i la seva detecció focalitzant les millores en tres possibles àmbits d'actuació.

Per una banda necessitem que la tecnologia ens ajudi a limitar les ocurrències, per altra banda, hem de millorar els processos existents a la companyia i, per últim, hem de centrar els esforços en millorar les accions que fan els empleats de les empreses.

Figura 7: Elements d'actuació per una gestió satisfactòria. [26]

Com es pot veure al gràfic anterior, per a poder tenir èxit en la implantació de canvis a la empresa s'ha treballat en tres àmbits d'actuació diferents. Per una banda es tracta de millorar els processos, per altra banda de millorar les actuacions dels humans i per últim de millorar les solucions tecnològiques.

6.6 Què fer si hi ha una bretxa de seguretat?

Per tal de tractar una bretxa de seguretat, s'han analitzat els requeriments de la nova regulació i utilitzant la base d'ITIL de gestió d'incidències, s'ha adaptat el procés per tal d'incloure els nous requeriments per a complir amb la nova regulació i definir les tasques necessàries a fer en les primeres 72 hores.

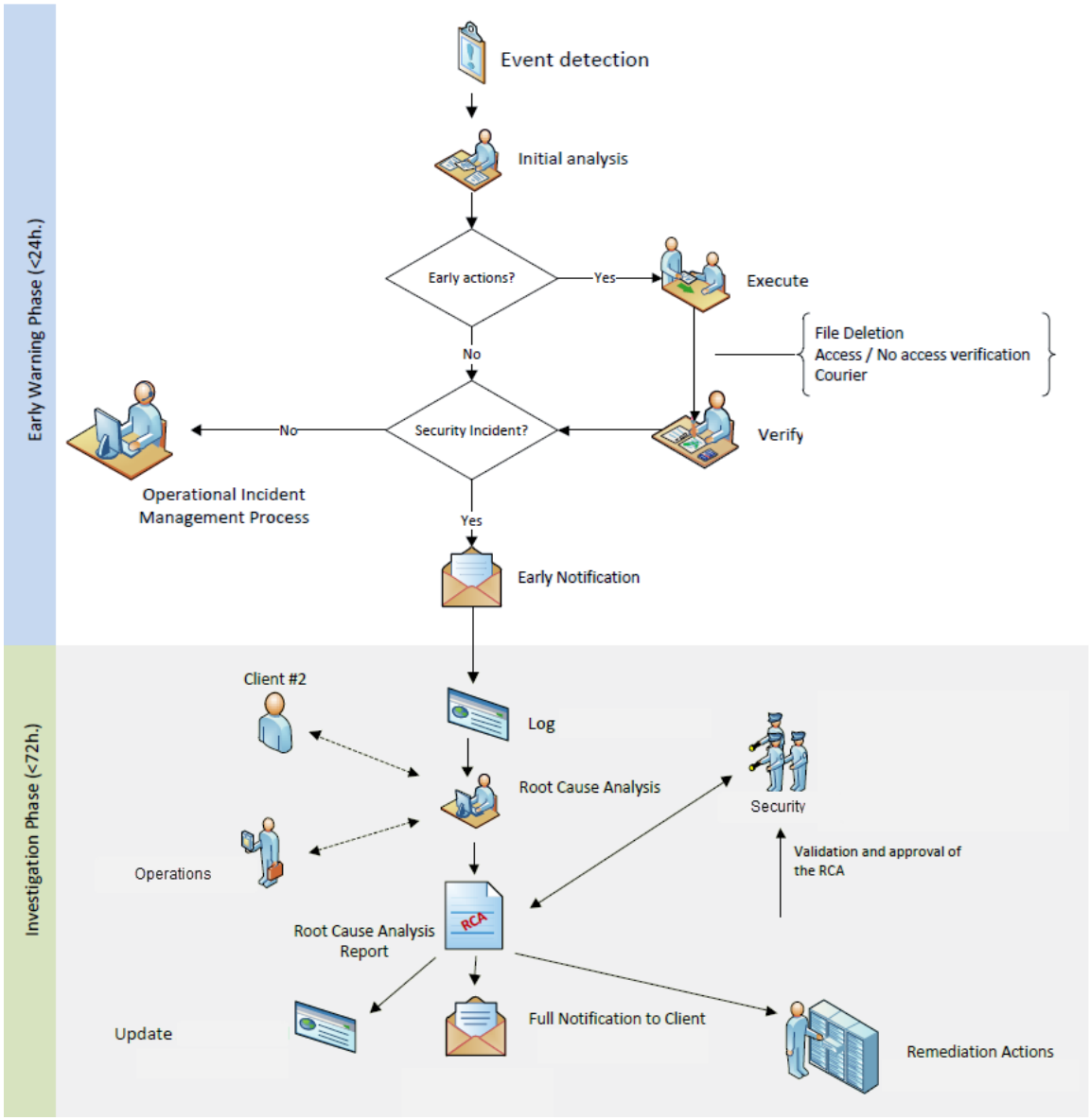

Figura 8: Procés incidents vinculat a ITIL.

Com es pot veure en la figura anterior, hi ha dos fases molt importants en la gestió d'una possible bretxa de seguretat.

La primera fase, que s'ha d'efectuar en les primeres 24 hores serà molt important per tal d'efectuar una primera revisió del fet detectat per tal de fer les primeres accions per corregir el problema o per a discriminar falsos positius.

La segona fase que s'ha hagut d'adaptar a la nova regulació és en l'anàlisi i la notificació a client. És aquí quan s'han hagut de revisar les notificacions que s'han de fer als clients per tal d'incloure la informació mínima que ells necessiten per tal de notificar a les autoritats reguladores. Com es pot veure al

gràfic, la nova metodologia creada implica la creació d'un document i una notificació del cas en menys de 72 hores.

El problema és si no s'arriba a tenir tota la informació del cas i les possibles correccions del problema en aquestes 72 hores. Si aquest és el cas, llavors s'opta per fer una notificació amb els mínims obtinguts de l'anàlisi ja que és una obligació de la nova regulació de complir els terminis de notificació.

En aquest nou procés també s'especifica la necessitat de posar-se en contacte amb qualsevol altre client o departament impactat per tal d'avaluar-ne els riscos i identificar si hi ha un risc gran de pèrdua de dades o si l'impacte cap al client serà menor ja que es coneix l'abast del problema.

Una de les grans característiques d'aquest nou procés és que inclou la figura del gestor d'incidents i a la vegada que depèn d'un treball multidisciplinari. Les tasques de gestió del incident recauen en diferents departaments ja que es demanarà ajuda a Operacions, a departament de TI i també als equips de gestió amb clients.

7. Recomanacions i Proposta per a complir amb la regulació

En aquest capítol s'exposen les possibles recomanacions que s'han de fer a les empreses per tal de complir amb la nova regulació i que aquestes tinguin un impacte satisfactori en la transformació de la organització.

És per això que s'enfoquen els canvis en els tres elements claus:

TECNOLOGIA:

En aquest aspecte, la recomanació es centra en la implementació de nous sistemes i en el canvi en la manera de programar.

En l'apartat de sistemes, l'estudi s'ha centrat en l'anàlisi de la implementació de sistemes de prevenció de pèrdua de dades ("Data Loss Prevention" o DLP), i en els sistemes de gestió d'esdeveniments i d'informació de seguretat (SIEM). Amb la implantació d'aquests sistemes es poden identificar amb més rapidesa i de manera més acurada les alertes dels sistemes de les empreses.

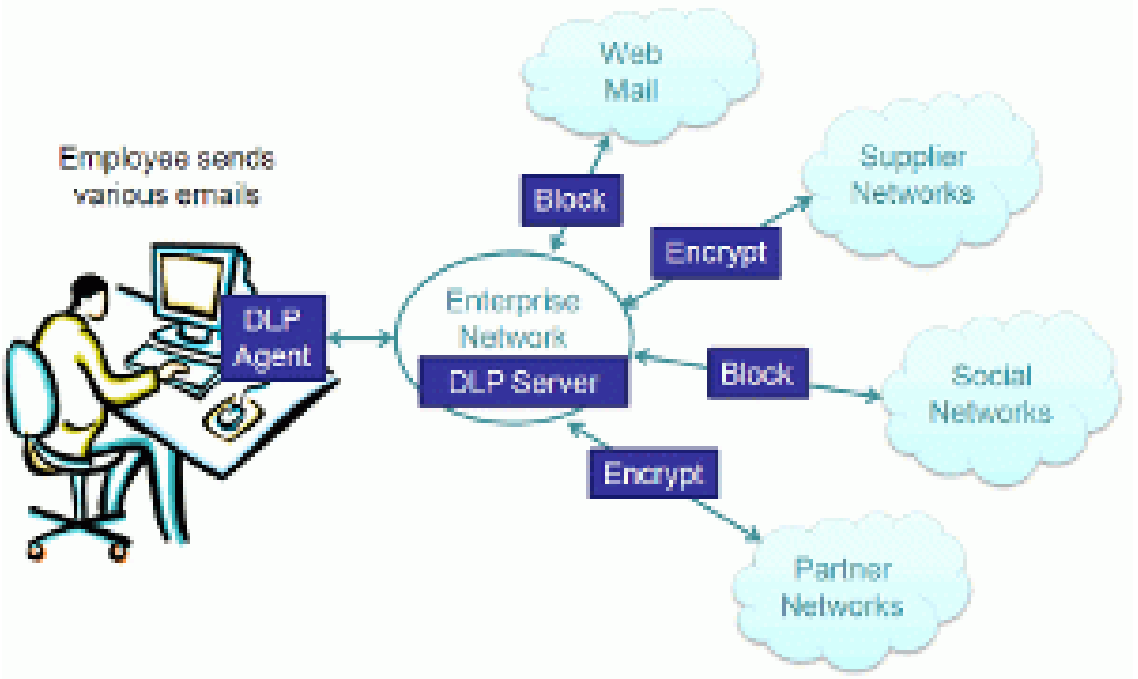

Figura 9 : Funcionalitat DLP [21]

Com es pot veure en aquesta imatge, la implantació d'un sistema DLP, permet a les empreses tenir control sobre les transferències que es puguin fer de les dades cap a entorns i sistemes externs. En el cas que s'identifica a la imatge anterior, si un empleat intenta enviar diferents correus electrònics, el sistema de DLP bloquejarà aquells correus que tinguin dades personals o, en el seu defecte, els encriptarà si van a persones autoritzades. D'aquesta manera s'evita la possible pèrdua de dades a través de canals de comunicació no autoritzats.

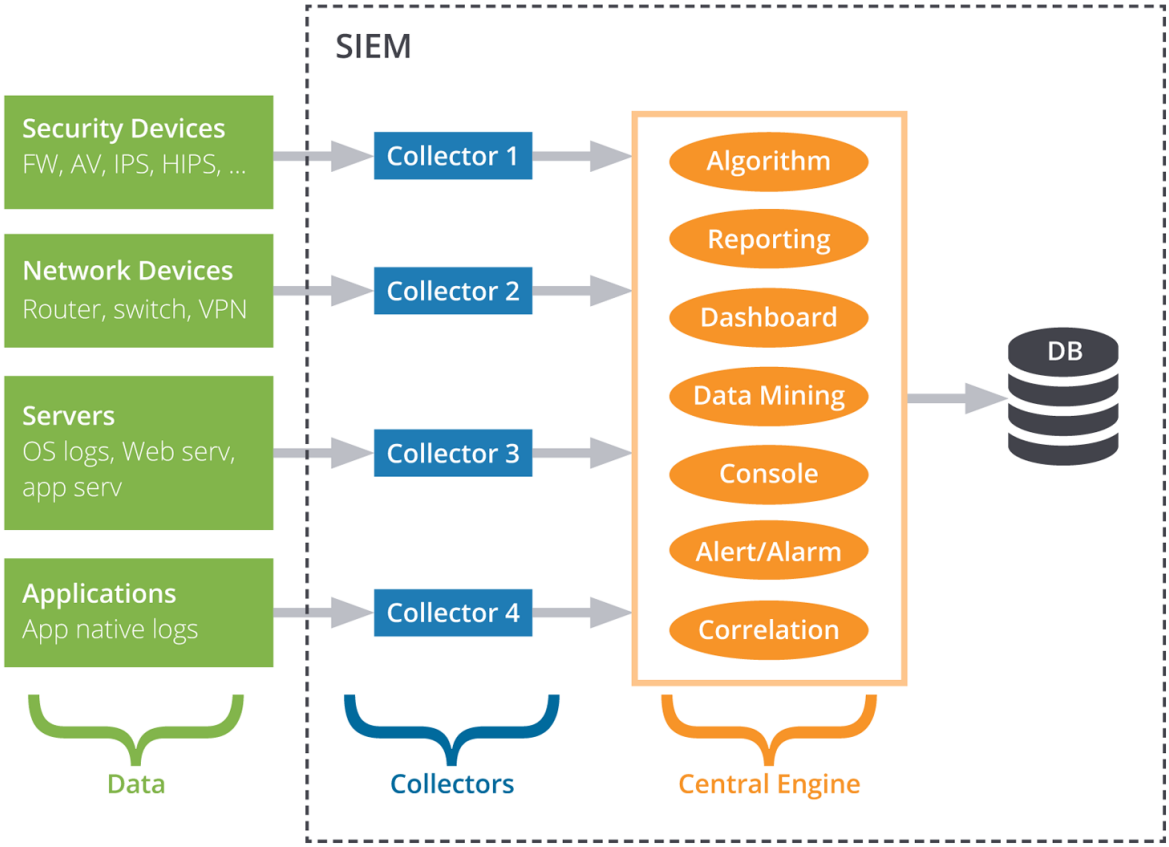

Figura 10: Funcionalitat SIEM [22]

Un altre àmbit d'actuació tecnològica que s'ha revisat en aquest estudi és el que s'aplica a les diferents màquines que es tenen als sistemes. Les empreses s'han de plantejar canvis en els sistemes de protecció per tal d'utilitzar sistemes de protecció "endpoint". Aquests sistemes han de permetre millorar aquells dispositius que tenen accés a la xarxa informàtica i poder restringir l'ús de determinades pàgines webs que poden servir de punts de fuga en cas d'un mal ús per part dels empleats.

A més a més, també s'ha analitzat la necessitat de tenir nous sistemes de contacte amb el client com poden ser sistemes CRM o nous sistemes de registre de riscos i de gestió d'incidents com són els sistemes GRC.

Una altra àrea d'actuació tecnològica ha d'estar orientada a la detecció de sistemes antics i la substitució d'aquests per entorns més actuals. S'han d'eliminar tots els sistemes heretats (legacy) per altres més nous i amb millors mesures de seguretat. Per aconseguir que aquests canvis siguin efectius i ràpids s'ha de replantejar la metodologia de creació de software.

En l'aspecte de programació s'ha de treballar i redefinir la metodologia per entregar noves aplicacions. Per a aconseguir que les entregues siguin més ràpides i es pugui adaptar la nova regulació de manera efectiva, s'ha hagut de treballar en adaptar les fases de disseny i creació a una metodologia "Agile". D'aquesta manera els canvis que es necessitin aplicar es fan de manera molt més ràpida ja que el fet de tenir entregues molt més curtes facilita la integració de canvis i evita retards en el projecte.

La metodologia clàssica que s'utilitzava fins ara a la gran majoria d'empreses "més clàssiques" feia que les entregues de les aplicacions necessitessin de molt més temps per tal d'adaptar-se als canvis i això complicava la introducció dels canvis de la nova regulació. Amb el canvi cap a la metodologia "Agile" es simplifiquen els temps d'entrega i, a la vegada, es garanteix que les demandes dels clients s'apliquin de manera més efectiva.

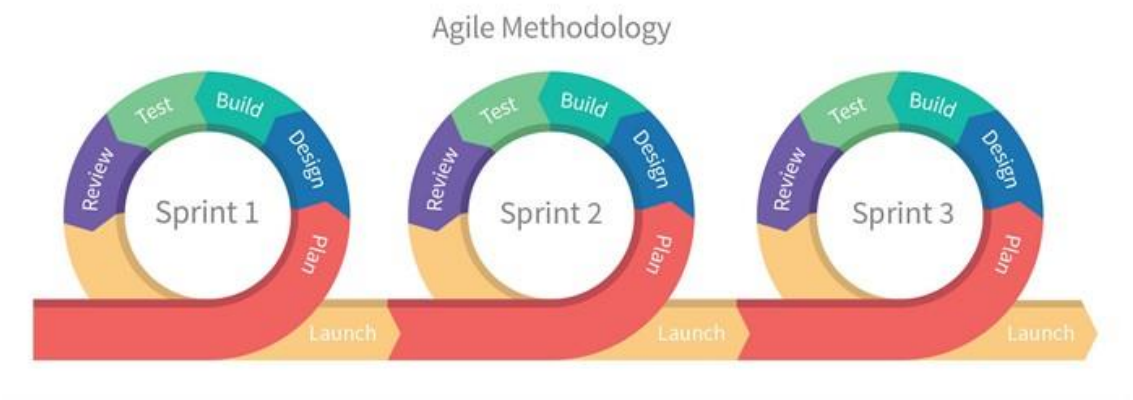

Figura 11: Metodologia Agile [24]

Amb la introducció d'aquests diferents sistemes es millora la seguretat de les dades però, a la vegada, també s'incorporen unes complicacions per als empleats. La feina diària es pot veure afectada per un canvi en els processos a seguir.

És per això que també s'ha de treballar en altres aspectes per a que les mesures tecnològiques puguin ser efectives i és per això que la proposta treballada en aquest treball de final de grau també es centra en la millora dels processos corporatius.

PROCESSOS:

En l'àmbit dels processos, l'estudi ha identificat les necessitats de treballar en diferents grups multidisciplinaris per analitzar els processos de les diferents àrees de les empreses. Per a millorar en aquest àmbit, la metodologia Kaizen és una de les opcions que permetran millorar els processos de les empreses en relació a la comunicació i la gestió dels incidents. Però a la vegada, també s'ha identificat que la mateixa metodologia ha de servir per a millorar els processos generals de l'empresa per tal d'evitar les activitats innecessàries i que no aporten valor al procés principal i que realment no donen valor al producte final.

A més a més, per tal d'arribar a aquesta situació s'ha de fer un anàlisis previ i detallat del flux de dades dins de l'empresa per tal d'identificar tots els actors i els diferents sistemes a on es guarden les dades. En aquest aspecte dels

processos, s'ha de fer una tasca de revisió dels processos interns però a la vegada s'han de revisar tots els processos de contacte amb els clients i els proveïdors per tal de trobar-ne qualsevol duplicitat o mancança.

Juntament amb aquesta detecció dels processos amb els proveïdors també s'ha identificat una necessitat global ja que la nova regulació obliga a revisar els actuals contractes amb aquests per tal d'adaptar-los a les noves necessitats.

Per altra banda, s'ha identificat la necessitat de redefinir els processos existents de notificació d'incidents de les empreses per tal de reduir-ne els temps de demora i poder notificar a les autoritats en el temps establert. El nou procés ha de garantir que sigui escalable en cas de necessitat i a la vegada ha de garantir que tot estigui documentat ja que en el cas d'una auditoria per part de l'autoritat reguladora serà molt important demostrar totes les accions que s'han fet i totes les comunicacions que s'han enviat en relació a un incident. És per això que les noves eines de comunicació amb els clients adquireixen una gran rellevància.

PERSONES:

L'última àrea de treball i de recomanació es centra en les persones i en els tipus de cursos de formació que tenen els empleats. Per tal de poder complir i implementar la nova regulació s'han d'incloure unes noves polítiques de privacitat a les empreses que els empleats hauran de revisar i acceptar. Per altra banda, s'han identificat necessitats de crear nous cursos de formació a on s'expliquin les novetats de la llei. D'aquesta manera les empreses s'asseguren que els seus treballadors coneixen el contingut de la nova llei i les accions que se'ls demana.

A més a més també s'ha treballat en l'assignació de tasques en el cas que hi hagi un incident de seguretat. Una de les grans necessitats de la nova regulació és la comunicació del incident cap a les autoritats. És per això que per tal de poder complir amb la nova llei s'ha de treballar en la redacció d'un

nou procés però també en l'assignació de tasques específiques dels diferents empleats de l'empresa. Cada persona té unes obligacions i unes responsabilitats. Per a cobrir aquest aspecte s'han de repensar les matrius de responsabilitats de les persones i s'han de redissenyar aquestes matrius RACI.

El que també s'ha identificat és que tothom té una part de responsabilitat en el procés. La necessitat d'immediatesa fa que s'hagin de redefinir els models de gestió d'incidents per tal de tenir equips dedicats a detectar els problemes però a la vegada a gestionar-los.

La gestió d'incidents de seguretat ja no és una tasca que es fa quan es pot o que es fa amb la millor de les voluntats sinó que ha passat a ser una tasca dedicada.

8. Conclusions

Una vegada finalitzat el treball final de grau, és important destacar les conclusions a les que hem arribat i les línies de treball futures que les empreses han de seguir aplicant per tal de mantenir un nivell de qualitat i un correcte compliment de la nova regulació.

8.1 Conclusions

Les conclusions que he extret un cop finalitzat el treball són les següents:

- La gestió d'incidents requereix un nou disseny de les aplicacions existents i l'ús de nous sistemes de detecció per tal de tenir un coneixement immediat de les alertes dels sistemes.
- Aquests nous sistemes han d'estar integrats amb sistemes de gestió centrals de les empreses per tal de millorar les comunicacions tant internes com amb els clients.
- La utilització de noves eines requereix d'una adaptació dels processos i d'una nova voluntat d'ús per part dels treballadors.
- Els mètodes de desenvolupament de programari s'han de revisar per tal d'incloure canvis de manera més àgil. Ja no hi ha temps per dubtar. La nova regulació ja s'aplica a les empreses i les empreses han d'estar llestes per a ser avaluades per les entitats reguladores de protecció de dades.
- Les empreses han trigat a adaptar la nova regulació degut a les complexitats i dubtes que genera.
- La nova regulació és molt àmplia i cobreix molts aspectes de la protecció de dades però deixa marge de maniobra en alguns aspectes que no queden clarament explicats. L'antiga regulació espanyola (LOPD) és un bon punt de partida per a les empreses espanyoles. Els canvis no són tant exagerats com a altres països europeus.

- La nova llei té un efecte global. Esta creant un nou paradigma que s'està estenent a molts països del que es considera el primer món.
- És molt important tenir tots els processos identificats i ben definits amb les responsabilitats de tots els actors.
- Les empreses necessiten crear una nova funció per tal de tenir gent i equips dedicats a la gestió d'incidents. La immediatesa fa que no sigui una tasca voluntària sinó que requereixi un perfil dedicat.

8.2 Reflexió

Els objectius planificats en el primer moment han estat majoritàriament assolits encara que hi ha hagut diferents canvis en el plantejament ja que en un primer moment es volia fer una anàlisi molt més gran de la nova regulació. Al final s'ha optat per centrar l'estudi en la gestió d'incidents de seguretat.
Els objectius inicials eren massa genèrics i massa amplis i amb el temps que es disposava per a fer el treball final de grau eren massa grans.

8.3 Anàlisi crítica

La planificació i la metodologia si que s'han seguit però la planificació no ha estat adequada. Degut a les compaginació de les jornades laborals amb la redacció del treball durant molts caps de setmana seguits ha fet que no hi haguessin jornades de descans personal. Això ha fet que les jornades de treball fossin esgotadores i l'agilitat mental no fos l'adequada.

He hagut de refer alguna de les jornades de treball reduint algunes hores de feina durant els caps de setmana i utilitzant les jornades de dilluns a dijous que estaven destinades a utilitzar-les només en cas de necessitat. Això ha fet que les jornades laborals fossin més llargues però que hi haguessin algunes jornades de descans els caps de setmana.

8.4 Línies de treball futur

Hem diferenciat les línies de treball futur que no s'han pogut explorar en aquest treball i han quedat pendents en dues opcions:

Les línies de treball futur a curt termini estarien enfocades en la tria definitiva dels diferents sistemes que s'exposen. També s'hauria de garantir que els cursos de formació que es fan als empleats inclouen les explicacions de les noves tecnologies i el seu ús correcte.

Les línies de treball a llarg termini caldria realitzar la integració de les diferents eines i també es podria analitzar la necessitat d'utilitzar altres solucions tecnològiques que ajudin a tenir millor documentació de tots els processos i de les noves eines. És altament recomanable l'ús d'un gestor documental i dissenyar un pla de formació per a les noves incorporacions de personal.

9. Glossari

Afectat: la persona física titular de les dades que són subjectes al tractament.

Ciberatac: Acció amb l'objectiu de prendre el control d'un sistema informàtic, desestabilitzar-lo o danyar-lo.

Cloud: és un sistema d'emmagatzematge i ús de recursos informàtics basat en el servei en xarxa, que consisteix a oferir a l'usuari un espai virtual, generalment a Internet, en què pot disposar de les versions més actualitzades de maquinari i programari.

Confidencialitat: Condició de les informacions que fan referència o pertanyen a una persona física o jurídica, segons la qual no poden fer-se públiques sense el consentiment de l'afectat.

Consentiment: Acceptació inequívoca, lliure, específica i informada amb la que l'interessat accepta el tractament de les dades.

Controlador / Encarregat de dades: Persona física o jurídica, autoritat pública, servei o organisme que defineix la finalitat del tractament de les dades.

CRM (Customer Relationship Manager): és un software destinat a gestionar la informació dels clients.

Disponibilitat: Capacitat d'un sistema o d'un component informàtic per a garantir plenament les seves funcions en el moment de fer una sol·licitud.

DLP (Data Loss Prevention): és una estratègia per a garantir que els usuaris finals no enviïn informació sensible o crítica fora de la xarxa.

DPO (Data Protection Officer): és el delegat de protecció de dades que la nova regulació requereix a les empreses. Persona que s'encarregarà de garantir el compliment de la normativa.

Endpoint: Punt d'entrada a un servei o un procés.

GRC (Governance, Risk and Compliance): és un software destinat a integrar i gestionar les operacions de TI i gestionar-ne els riscos.

Hacker: Persona que s'introdueix il·legalment en un sistema de seguretat informàtic amb la voluntat de produir-hi un perjudici o de treure'n un profit.

Integritat: Propietat d'una informació que assegura que, durant el tractament, l'emmagatzematge i la transmissió per mitjans electrònics, no patirà cap alteració ni destrucció voluntària o accidental.

Malware: Programari concebut específicament per a prendre el control d'un sistema informàtic, interferir en el seu funcionament normal, desestabilitzar-lo o danyar-lo.

PIA (Privacy Impact Assessment): és un procés que ajuda a les organitzacions a identificar i minimitzar els riscos de privacitat dels nous projectes.

Privacitat: Condició de les informacions que fan referència o pertanyen a una persona física o jurídica, segons la qual no poden fer-se públiques sense el consentiment de l'afectat.

Processador de dades: Persona física o jurídica, autoritat pública, servei o organisme que tracta les dades personals per compte del controlador.

SIEM (Informació de seguretat i gestió d'esdeveniments): són productes i serveis de programari que combinen la gestió de la informació de seguretat (SIM) amb la gestió d'esdeveniments de seguretat (SEM).

SPAM: Conjunt de missatges electrònics importuns, generalment de caràcter publicitari i sense interès per al receptor, que s'envien indiscriminadament a un gran nombre d'internautes.

Tractament de les dades: Conjunt d'operacions realitzades sobre dades personals.

10. Bibliografia

1) http://www.rac1.cat/info-rac1/20180128/44347754804/els-atacs-informatics-a-empreses-i-usuaris-shan-incrementat-un-130-en-un-any.html → 11 Març 2018

2) https://www.elperiodico.cat/ca/mes-valor/20160222/el-valor-de-les-dades-de-la-hiperconnectivitat-4917130 → 11 Març 2018

3) http://aplicacions.llengua.gencat.cat/llc/AppJava/index.html?action=Principal&method=detall&input_cercar=privacitat&numPagina=1&database=TERMCAT&idFont=772429&idHit=772429&tipusFont=Diccionaris+terminol%F2gics+del+TERMCAT&numeroResultat=5&databases_avansada=&categories_avansada=&clickLink=detall&titol=privacitat&tematica=Tecnologies+de+la+informaci%F3+i+la+comunicaci%F3&tipusCerca=cerca.tot → 7 Abril 2018

4) https://www.agpd.es/portalwebAGPD/index-idca-idphp.php → 7 Abril 2018

5) http://apdcat.gencat.cat/ca/inici → 8 Abril 2018

6) BRU, Elisenda (2007). «La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. IDP. Revista de Internet, Derecho y Política. N.º 5. UOC. [Data de consulta: 08/abril/2018]. <http://www.uoc.edu/idp/5/dt/esp/bru.pdf>

7) https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf → 8 Abril 2018

8) http://www.dw.com/en/lifelinks-dataprotection-surveillance/a-18565145 → 8 Abril 2018

9) https://www.smartinsights.com/marketplace-analysis/digital-marketing-laws/timeline-implementing-gdpr-uk/ → 8 Abril 2018

10) https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en → 8 Abril 2018

11) https://www.dlapiperdataprotection.com/ → 8 Abril 2018

12) https://www.eugdpr.org/eugdpr.org.html → 8 Abril 2018

13) https://www.protecciondatos-lopd.com/empresas/nueva-ley-proteccion-datos-2018/ → 8 Abril 2018

14) https://www.linkedin.com/company/the-cyber-security-hub/ → 8 Abril 2018

15) https://www.anonos.com/blog/big-data-needs-bigprivacy?utm_campaign=LinkedinAD&utm_source=ppc → 8 Abril 2018

16) https://www.linkedin.com/pulse/gdpr-1-page-summary-brent-dreyer/ → 18 Abril 2018

17) https://www.puromarketing.com/12/30096/ejecutivos-espanoles-alto-nivel-considera-esta-todo-preparado-para-cumplir-regulacion-materia.html → 5 Maig 2018

18) https://avondhupress.ie/only-5-of-companies-claim-to-be-ready-for-gdpr/ → 5 Maig 2018

19) https://www.helpnetsecurity.com/2018/05/02/not-gdpr-ready/ → 5 Maig 2018

20) https://www.zdnet.com/article/google-for-work-bolsters-gmail-with-data-loss-prevention/ → 5 Maig 2018

21) https://www.veracode.com/security/guide-data-loss-prevention → 5 maig 2018

22) https://www.recordedfuture.com/siem-threat-intelligence-part-1/ → 5 Maig 2018

23) http://cstor.com/cybersecurity-solutions/end-point-security-solutions/ → 5 Maig 2018

24) https://www.pinterest.com/pin/811351689091066251/?showsignup=1 → 5 maig 2018

25) https://www.startupguys.net/take-your-startup-to-the-next-level-using-kaizen-philosophy/ → 5 Maig 2018

26) https://crisbymike.wordpress.com/2017/11/16/what-is-people-processes-technology/ → 5 Maig 2018