Seguretat i privacitat de les dades

PID_00251624

David Cabanillas Barbacil

Temps mínim de dedicació recomanat: 4 hores

Universitat Oberta de Catalunya

Índex

Introducció

Com ja sabem actualment, la dada s'ha convertit en un dels actius més importants. Vivim una època en la qual la informació flueix com mai abans ho havia fet, i es multipliquen les formes per capturar, processar, emmagatzemar, analitzar i visualitzar dades, a més dels seus casos d'ús. Això provoca l'aparició de múltiples repositoris de dades com el *data warehouse* (magatzem de dades) i el *data lake* (llac de dades), i serveis fonamentats en dades, com *big data* (dades massives) i *machine learning* (aprenentatge). Aquest detonant en tecnologia i dades ha disparat també les bretxes en seguretat en tots els sectors.* Pel que tota organització té la imperiosa necessitat de protegir els seus actius de dades, tal com apunta Gartner.

Lectura complementària

B. Lowans; N. MacDonald; M. Meunier; B. Reed (2016). *Predicts 2017: Application and Data Security*. Gartner

*** Més informació a: https://goo.gl/fqlZq1**

Aquesta necessitat té dues vessants:

- Com a **organitzacions**, hem d'invertir en capacitats de ciberdefensa per protegir la nostra marca, el nostre capital intel·lectual, la informació dels clients i la infraestructura crítica; també hem de crear mecanismes per a la detecció d'incidents i una resposta per protegir els interessos de l'organització i els seus elements més importants: persones, processos, tecnologia i dades.

- Com a **usuari**, quan tenim una interacció amb una organització (ja sigui obrint un compte bancari, creant un usuari en una xarxa social o reservant un vol en una companyia aèria), es lliura informació personal com el nom, l'adreça o el número de la targeta de crèdit. Múltiples preguntes que ens solen assaltar en tots aquests casos són: què passa amb aquestes dades? Podrien caure en mans equivocades? Quins drets tinc pel que fa a la meva informació personal?

Aquestes dues vessants conflueixen. D'una banda, tota persona té dret a la protecció de les seves dades personals. De l'altra, segons la legislació del país en què opera l'organització, les dades personals només poden recopilar-se legalment en condicions estrictes, amb un fi legítim. A més, les persones o organitzacions que recullen i gestionen la seva informació personal han protegir-la de l'ús indegut i respectar certs drets dels propietaris de les dades. Per tant, les organitzacions estan obligades per llei a oferir seguretat i privacitat en les dades que emmagatzemen.

En aquest mòdul, es descriuen la legislació, les polítiques i les millors pràctiques que s'han d'incloure perquè les organitzacions disposin de dades segures i privades, mitjançant l'ús de processos documentats, transparència de l'ús, co-

municació eficaç, revisió i aplicació de les pràctiques de seguretat, capacitació suficient del personal i un compromís de protegir la integritat i l'ús autoritzat de les dades dels usuaris.

La seguretat de la dada s'emmarca també dins de l'àmbit del govern de la dada, de forma natural. L'explotació eficient de la dada passa per tenir la capacitat de planificar, desenvolupar i executar polítiques i procediments per assegurar l'autenticació, l'autorització, l'accés i l'auditoria dels actius de dades i d'informació.

En aquest mòdul, estudiarem la necessitat i la importància de la seguretat i la privacitat de la dada, en què consisteix, què aporta, com implementar-la, què hem de tenir en compte com a millors pràctiques i quines tecnologies suporten la seguretat i la privacitat de la dada.

Objectius

Aquest material didàctic està adreçat a:

1) Desenvolupadors i consultors que volen saber què significa la seguretat i la privacitat dins el *data governance* (govern de la dada).

2) Desenvolupadors i consultors que volen ajudar al desenvolupament d'estratègies de seguretat i privacitat dins el *data governance*.

3) Gestors i juristes que estan interessats en la transformació digital de la seva organització i en la inclusió del govern de la dada i la seva seguretat.

En els materials didàctics d'aquest mòdul, trobarem les eines indispensables per assimilar els objectius següents:

1. Entendre el concepte de privacitat i de seguretat en el context del *data governance*.
2. Entendre els problemes de seguretat i de privacitat, a més de les seves normatives.
3. Aplicar sistemes de seguretat en el *data governance*.

Si bé l'obra és autocontinguda en la mesura del possible, els coneixements previs necessaris són:

1) Coneixements bàsics sobre *business intelligence* (intel·ligència empresarial) i *big data* (dades massives).

2) Coneixements sobre estratègia i gestió de les tecnologies de la informació (TI).

S'introduiran els conceptes necessaris per al seguiment d'aquest material.

1. La seguretat de la dada

1.1. El repte de la seguretat de la dada

En els últims anys, la seguretat de la dada ha passat de pertànyer fonamentalment a l'àmbit tècnic a convertir-se en una prioritat de negoci. Aquest canvi de percepció es deu a l'aparició de mesures legislatives, de l'ús de la tecnologia, tant en l'àmbit professional com personal, i als creixents problemes generats per una escassa atenció a aquest punt.

Les organitzacions han de conèixer quins riscos existeixen i com mitigar-los. En essència, l'organització ha de ser capaç de:

- Treballar en un entorn de flexibilitat i mobilitat organitzativa, sense perdre la confidencialitat, la integritat o la disponibilitat de les dades.
- Conèixer i comprendre el compliment normatiu per evitar sancions i conseqüències penals.
- Conèixer i aplicar les cobertures existents davant el robatori d'informació o atac als sistemes empresarials.
- Custodiar i mantenir la confiança dels clients i la reputació de la marca.

No obstant això, el repte de la seguretat de la dada és complex, ja que podem trobar els riscos en persones, processos i tecnologia.

Estudis d'Osterman Research com *SMB Rogue Access Study*, publicat al 2014, posen de manifest que els empleats són freqüentment l'origen de problemes de les bretxes de seguretat, ja que el 68% dels enquestats van manifestar que han guardat documents corporatius en algun servei d'emmagatzematge en el núvol (com Dropbox o Google Drive). Aquestes bretxes de seguretat de dades poden ser per desconeixement o propòsit, com en el cas dels documents desclassificats per Snowden.

El juny del 2013, Snowden va fer públics, per mitjà de *The Guardian* i *The Washington Post*, documents classificats com a alt secret sobre diversos programes de la National Security Agency (NSA), incloent-hi els programes de vigilància massiva PRISM i XKeyscore.*

*** Més informació a: https://goo.gl/5dBkRa**

Tot tipus d'organitzacions estan tenint problemes relacionats amb la seguretat de dades. Per exemple, el sistema de contrasenyes de LinkedIn ha estat compromès diverses vegades.* El 2012, va afectar 6,5 milions d'usuaris. El 2014, 117 milions. El 2015, 37 milions d'usuaris d'Ashley Madison, servei de cites en línia, es van veure compromesos.**

* Més informació a: https://goo.gl/9p4cP8

** Més informació a: https://goo.gl/le0Vj1

Com és possible d'imaginar, el tema de la seguretat i de la privacitat de dades no és nou. Ja a la dècada dels setanta, era una preocupació reconeguda en àmbits com registres mèdics o informació financera. En aquesta dècada, es van adoptar les pràctiques d'informació justes (FIP, acrònim de *fair information practices*), que seguien aquests punts:

- **Franquesa**: no ha d'haver sistemes per recol·lectar dades personals sense el consentiment/coneixement dels individus.
- **Revelació**: les organitzacions han de revelar a les persones de quina informació disposen i com la utilitzen.
- **Ús secundari**: la informació recollida per a un propòsit no s'hauria d'utilitzar per un altre propòsit sense el consentiment de l'individu.
- **Correcció**: les persones han de tenir la capacitat de corregir o esmenar la seva pròpia informació.
- **Seguretat**: tota organització que creï, mantingui, utilitzi o difongui dades personals identificables ha d'assegurar que les dades s'estan utilitzant correctament i ha de prendre precaucions per evitar-ne l'ús indegut.

Avui dia, els reptes s'han magnificat però els cinc punts descrits en les pràctiques d'informació justes segueixen sent vàlids. Es tracta d'un escenari més complex, producte d'un entorn canviant i molt més descentralitzat, en el qual la dada permet proporcionar serveis més personalitzats a canvi de la privacitat, tal com comenta Enrique Dans.*

* Més informació a: https://goo.gl/x6Mrnp

> Encara que sembla un futur llunyà, ja hi ha sistemes autònoms sense interacció humana que es fonamenten en les nostres preferències i comportaments. Ja hi ha semàfors que s'adapten al flux del trànsit, botons que ens permeten demanar de nou la nostra pizza preferida i fins i tot termòstats que gestionen la temperatura adequada a casa nostra.
>
> A mesura que més elements generen dades (com comptadors intel·ligents d'aigua, d'electricitat o de gas, o dispositius com Amazon Echo), és possible inferir comportaments anòmals o descobrir aspectes personals i privats. Això ens pot dur a plantejar-nos preguntes com:
>
> - el desenvolupament dels *smart homes* ens porta a un desequilibri entre conveniència i privacitat?
> - Amazon hauria d'alertar la policia, per exemple, si el seu dispositiu captura determinades gravacions, bé efectuades expressament o bé accidentals, que permetin deduir que s'està cometent un delicte?
> - Es por presentar Amazon Echo com a prova en un delicte?

- Si Amazon hagués eliminat les dades, es podria considerar l'organització encobridora d'un assassinat?

- Què passa si s'accepta com a prova la gravació del dispositiu i al final el culpable no ho era? Què passa si dades de diferents dispositius no aclareixen amb exactitud l'assassinat? Per exemple, que una altra gravació d'un altre dispositiu es contradigui amb la gravació del d'Amazon Echo o demostri que no podia estar en aquest moment en l'escena del crim.

Aquests escenaris posen en evidència que les organitzacions s'enfrontaran a més i més desafiaments de seguretat i de privacitat, motivats per:

- ***Big data***: tal com apunta *The Economist*,* *big data* obre la porta al següent:

*** Més informació a l'article de l'any 2012: *The challenge of big data for data protection***

– La recol·lecció de dades a gran escala permet el seguiment i la creació de perfils d'usuaris.

– La seguretat de les dades distribuïdes.

– L'inexactitud i la duplicitat a gran escala.

– L'augment de les possibilitats de vigilància per part del govern o d'organitzacions.

- ***Cloud computing***: l'emmagatzematge de dades en el núvol genera dubtes sobre la legislació que s'aplica en el centre de dades remot i en la transmissió de dades.

- **Enriquiment de dades**: quan es creuen dades de múltiples fonts, emergeixen patrons que poden vulnerar la privacitat dels usuaris. Per exemple, si els bancs revisen totes les nostres compres, poden saber quins medicaments estem utilitzant i, així, oferir-ne diferents preus en les seves assegurances o en l'obtenció de préstecs.

- **Fusions i adquisicions**: què passa amb la dada, com a actiu de valor, quan dues organitzacions es fusionen o una compra una altra? Tal com il·lustra la figura 1, aquesta situació és molt comú. En el cas de la compra de WhatsApp per part de Facebook, la Comissió Europea va avaluar aquesta situació de consolidació per determinar si afectava el mercat competitiu.

- **Transferència automàtica de dades**: aquest procés requereix ser validat per assegurar que les dades no pateixen modificacions durant la transferència. De fet, aquí sorgeixen iniciatives com *blockchain* (cadena de blocs). Com s'enfrontaran les organitzacions en un món interconnectat de manera omnipresent, amb dades distribuïdes i amb milers d'intercanvis de dades diàries?

Figura 1. Fusions entre organitzacions que treballen amb dades

Font: David Cabanillas

1.2. Què és la seguretat de la dada?

En la seguretat i privacitat de la informació, l'objectiu principal és la protecció de les dades i evitar que s'hi pugui accedir, que es perdin dades o que es modifiquin de forma no autoritzada. La seguretat i la privacitat han de garantir, en primer lloc, la **confidencialitat**, la **integritat** i la **disponibilitat** de les dades. Aquests punts coincideixen amb el govern i la gestió de la dada. No obstant això, hi ha més requisits com, per exemple, l'**autenticitat** o la possibilitat per part de l'usuari de poder **verificar/modificar/eliminar** les dades que contenen les organitzacions.

Tal com articula la **Declaració Universal dels Drets Humans** (DUDH), la seguretat i la privacitat de les persones són un dret, raó per la qual els diferents estats han creat lleis referents a aquest tema. Aquestes mesures estan dirigides a regular els diversos aspectes de l'activitat de negoci relacionats amb les tecnologies de la informació i la societat. El compliment de les obligacions legals proporciona unes garanties de protecció dels drets sobre els actius d'informació empresarial (carteres de clients, contractes, patents, etc.) que són transcendentals per al negoci, sense oblidar que així es respecten els drets de clients i usuaris.

DUDH

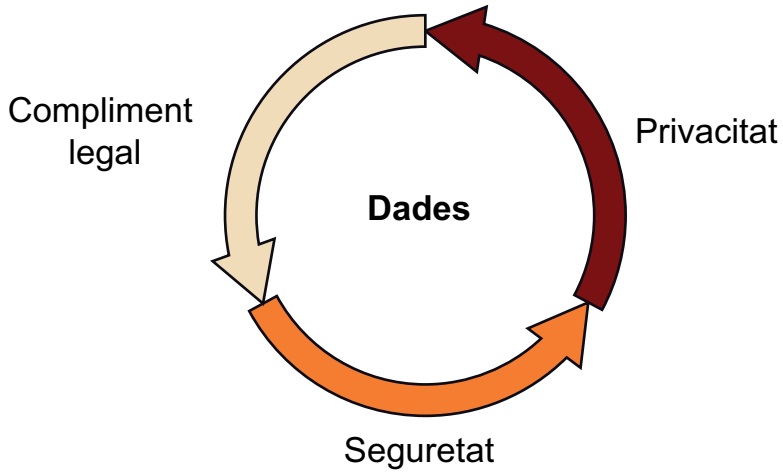
La Declaració Universal dels Drets Humans (DUDH) és un document declaratiu adoptat per l'Assemblea General de les Nacions Unides en la seva Resolució 217 A (III), el 10 de desembre de 1948, a París, en què mitjançant trenta articles s'enumeren els drets humans considerats bàsics.

El compliment legal es refereix al conjunt de processos, regles, eines i sistemes utilitzats pels departaments jurídics corporatius per adoptar, implementar i monitorar un enfocament integrat d'aquestes lleis dins de les organitzacions.

El compliment legal no és només una obligació, sinó que reverteix també en el negoci i en la bona imatge de l'organització.

La figura 2 mostra les relacions entre aquests tres elements.

Figura 2. Elements que engloben la seguretat i la privacitat



Font: John Sotiropoulos

Al llarg d'aquests materials, parlarem de la seguretat i la privacitat de la dada en la seva vinculació amb el programa de govern de la dada, si bé molts dels aspectes de què tractarem formen part de l'àmbit de la seguretat de la informació.

S'entén per **seguretat d'informació** el conjunt de mesures preventives i reactives de les organitzacions i dels sistemes tecnològics que permeten resguardar i protegir la informació, i que busquen mantenir la confidencialitat, la disponibilitat i la integritat de les dades.

El respecte de la privacitat i la seguretat de les dades ha de ser una consideració clau per a qualsevol organització, més enllà del compliment mateix de les regulacions existents. Mentre que les regulacions poden ser la part visible, les organitzacions, abans de res, han de considerar com les seves accions poden afectar les seves relacions amb els seus clients. Aquesta és una qüestió de confiança i de respecte, no simplement de compliment. Sens dubte, hi ha molt que podem aprendre aquí del que s'ha implementat en el sector de la salut. En l'entorn sanitari, més enllà d'obtenir un diagnòstic precís, les persones generalment se senten còmodes, ja que tenen confiança en els seus metges, perquè entenen clarament que la informació es mantindrà en confiança. De fet, els metges tenen un codi de conducta molt conegut, el jurament hipocràtic. Per a les organitzacions, un acord similar ha de ser assolit amb els seus clients. S'ha de ser franc i clar pel que fa a quina informació s'està recopilant, com es farà servir i com beneficiarà el client.

Jurament hipocràtic

Un dels paràgrafs del jurament diu: «Respectaré el secret de qui hagi confiat en mi».

La informació és un dels actius més importants d'una organització. La defensa d'aquest actiu és una part essencial per assegurar la continuïtat i el desenvolupament del negoci, de manera que les organitzacions han d'adoptar una actitud proactiva, en la qual es responsabilitzin del següent:

Proactiva

Implica tenir iniciativa en el desenvolupament d'accions per generar-hi millores.

- **Les dades de l'organització han de ser segures i privades**: avui dia, les dades es consideren els actius més importants de les organitzacions. Se n'ha d'assegurar la seguretat i la privacitat.

- **Les dades personals dels clients han de ser segures i privades**: sense les dades, l'organització no pot posar-se en contacte amb el client, no pot referir-se a transaccions anteriors, no pot entendre el seu comportament. Per tant, les dades són essencials per ajudar-nos a entendre el nostre negoci però, al mateix temps, s'ha de respectar, preservar i fer complir l'elecció i el consentiment del client al llarg del cicle de vida de la informació, particularment quan es tracta de decidir com es fa servir i es distribueix la informació personal dins i fora de l'organització.

1.3. Competint amb dades sota la premissa de seguretat i privacitat

Quan una organització inicia el seu camí cap a convertir-se en una organització orientada a la dada, ha de prendre decisions importants respecte a l'ús de les dades dels clients, la seguretat i la privacitat. Mentre que no hi ha dubte que s'ha de protegir la dada i consegüentment se'n prenen les mesures respectives, la interpretació de l'ús de vegades menyscaba la privacitat.

Considerem un parell de casos. D'una banda, revisem l'enfocament de Google:

> El negoci de Google es fonamenta en els anuncis al seu cercador. Una de les grans preguntes és si aquests anuncis en línia realment empenyen la gent a comprar. Amb l'objectiu de respondre a aquesta pregunta, Google ha començat a fer servir totes les dades possibles a les quals pot accedir com, per exemple, les transaccions de bilions de targetes de crèdit dels seus clients per mitjà dels seus sistemes de compra i pagament, i també la informació de la resta dels serveis: Google, Gmail, Google+, Google Maps, Chrome, YouTube, etc.
>
> La combinació de tots aquests conjunts de dades permetrà determinar quantes vendes han estat generades amb campanyes digitals, que és el somni fet realitat per a la indústria.*

*** Més informació a: https://goo.gl/xm7Xoa**

Com és possible imaginar, aquest comportament ha generat preguntes sobre l'ús de dades del client pel que fa a la seva privacitat per part de la companyia. Això no obstant, aquests dubtes no són nous, ja que Google fa servir les dades personals dels seus usuaris per optimitzar els seus anuncis.

Un comportament similar és el de Facebook, que combina totes les dades possibles del client per optimitzar els seus anuncis.

D'altra banda, recordem l'enfocament d'Apple:

> «La gent ens ha confiat les seves dades més personals. La nostra obligació és la d'aconseguir les millors mesures de seguretat que la tecnologia ens ofereix. La història ens ha ensenyat que sacrificar el nostre dret a la privacitat pot tenir conseqüències».
>
> Tim Cook (CEO d'Apple).

L'enfocament d'Apple està fonamentat en un estricte control sobre tot el seu ecosistema, que comprèn maquinari, programari, aplicacions i accessoris. La seva explotació de les dades del client es fonamenta en la premissa de la privacitat, cosa que comporta, en la pràctica, limitar l'explotació d'aquestes dades i utilitzar tècniques d'analítica que en respecten la privacitat.

En indústries molt regulades, com la financera, les empreses han de seguir de manera estricta la regulació que protegeix les dades del client. Això limita també la seva forma d'explotació.

Per tant, en abordar la privacitat i la seguretat de les dades, les organitzacions han de considerar els punts següents:

- Adoptar un enfocament holístic de les necessitats de privacitat i seguretat de les dades, és a dir, analitzant la seguretat en el seu conjunt i no només mitjançant les parts que els componen. Aquest enfocament de la planificació i la implementació de la privacitat i de la seguretat reuneix els participants següents:

  – Processos empresarials propis que generen, recopilen i fan servir dades.

  – Tenir rols específics pel que fa a dades confidencials, com ara el director de privacitat i el departament de TI.

- Augmentar els enfocaments que se centren en el simple compliment de la llei, fent respectar la privacitat de les dades i les mesures de seguretat basades en principis generalment acceptats. Es refereix a les millors pràctiques del sector i a les mesures d'autoregulació que van més enllà del simple compliment dels reglaments i de les normes.

- Augmentar els paradigmes prevalents de privacitat i seguretat de TI (que aborden les amenaces, en restringir l'accés a les dades i evitar que s'escapi de límits ben definits mitjançant l'avaluació d'amenaces a dades en diferents etapes del cicle de vida de la informació). Aquest enfocament ajuda les organitzacions a identificar tècniques i altres mètodes que poden reduir els riscos de la seguretat i de la privacitat a nivells acceptables.

2. Privacitat i normativa de dades

2.1. Privacitat de dades

Com hem comentat, les lleis de seguretat sobre les dades es perceben com un factor important entre els usuaris i les organitzacions. No obstant això, la privacitat s'ha convertit en el més oblidat de tots els principis de seguretat de dades. Per exemple, una organització pot tenir en forma segura les dades dels seus clients, però per mitjà de l'anàlisi i de l'ús d'aquesta informació en el seu propi benefici o el de tercers pot estar perjudicant els seus clients, en vulnerar la seva privacitat (fins i tot per desconeixement).

Lectura complementària

D. E. Bambaeur (2013). «Privacy Versus Security». *Journal of Criminal Law and Criminology* (núm. 3, vol. 10, pàg. 667-684).

Tot i que la seguretat és un element essencial de la privacitat, no és suficient per assegurar-la. La privacitat i la protecció de dades comprenen un conjunt molt més ampli de proteccions. Per poder entendre la relació entre totes dues, definirem seguretat i privacitat. Ja sabem que la seguretat consisteix a habilitar i protegir les activitats i els actius tant de les persones com de les organitzacions, mentre que:

S'entén per **privacitat** el respecte i la protecció de la informació personal.

D'aquesta manera, la privacitat estableix el marc normatiu que permet decidir qui té la capacitat d'accedir a informació de forma legítima i alterar-la. La seguretat implementa aquestes opcions mitjançant mecanismes tecnològics.

Encara que la privacitat requereix que la informació personal i identificable sobre les persones estigui protegida contra l'accés no autoritzat, és important entendre que la privacitat implica molt més que garantir l'accés segur a les dades. En una paraula, la privacitat té a veure amb el control de les seves pròpies dades, i ha de permetre als individus mantenir el control personal sobre la seva informació pel que fa a la seva recol·lecció, ús i divulgació. El significat d'aquest concepte de privacitat potser s'expressa millor com a autodeterminació de la informació.

Autodeterminació de la informació

És la facultat de tota persona per exercir un control sobre la informació personal que li concerneix, continguda en registres públics o privats, especialment, però no exclusivament, els emmagatzemats en mitjans informàtics.

2.2. Privacitat per disseny

Si la privacitat és tan important en el context de la seguretat, què poden fer les organitzacions per tenir-la sempre present? Poden aplicar un marc de disseny de sistemes d'informació que la inclou per defecte.

S'entén per **privacitat per disseny** el marc basat en la integració proactiva de la privacitat en el disseny i l'operació de sistemes de TI, infraestructura en xarxa i pràctiques empresarials.

En essència, la privacitat per disseny està destinada a reflectir un enfocament holístic de la privacitat, en un àmbit organitzatiu, i és un procés que involucra diferents components tecnològics i organitzatius, que implementen principis de privacitat i de protecció de dades. Aquests principis i requisits deriven sovint de la normativa en la qual opera l'organització. Com qualsevol procés, la privacitat per disseny ha de tenir objectius ben definits, metodologies i mitjans d'avaluació.

Lectura complementària

G. Danezis; J. Domingo-Ferrer; M. Hansen; J. H. Hoepman; D. Li Métayer; R. Tirtea; S. Schiffner (2014). *Privacy and Data Protection by Design from policy to engineering*. Enisa.

Per posar en pràctica aquest enfocament, és essencial l'elaboració d'un **anàlisi d'impacte en la privacitat** (PIA, acrònim de *privacy impact assessment*), que no és més que l'exercici d'anàlisi de riscos amb què s'intenta identificar tots els possibles riscos per a la privacitat que pot implicar un nou procés, i als quals caldrà posar remei. Com a conseqüència, el disseny incorpora, des de la seva pròpia concepció, controls per mitigar les possibles vulnerabilitats de protecció de dades i privacitat.*

*** Més informació a: https://goo.gl/hhyL09**

Aquest enfocament ha de ser pres també en el moment d'implementació d'aplicacions d'intel·ligència de negoci, analítica o *big data*.

2.2.1. Principis de la privacitat per disseny

Els sis principis fonamentals de privacitat per disseny són els següents:

1) Proactiu i no reactiu: anticipar, identificar i prevenir esdeveniments invasius abans que succeeixin. Això vol dir prendre mesures abans que es produeixin.

2) Disposar de privacitat com valor per defecte: assegurar-se que les dades personals es protegeixin automàticament en tots els sistemes de TI o pràctiques empresarials, sense que es requereixi cap acció addicional per part de cap individu.

3) Integrar la privacitat en el disseny: les mesures de privacitat no han de ser complements, sinó components totalment integrats del sistema.

4) Mantenir la funcionalitat completa: la privacitat per disseny empra un enfocament de guanyar les dues parts, o *win-win*, a tots els objectius legítims del disseny del sistema; és a dir, tant la privacitat com la seguretat són importants, i no cal fer concessions innecessàries per assolir-les.

5) Assegurar la seguretat de punt a punt: la seguretat del cicle de vida de les dades vol dir que totes les dades han de ser utilitzades i emmagatzemades de forma segura quan sigui necessari, i destruïdes quan ja no es necessitin.

6) Mantenir la visibilitat i la transparència oberta: assegurar a les parts interessades que les pràctiques i tecnologies empresarials operen d'acord amb els objectius i estan subjectes a verificacions.

2.2.2. Avantatges de la privacitat per disseny

La certificació de privacitat per disseny ofereix a les organitzacions que l'apliquen la capacitat de:

- Assegurar el compliment de la privacitat, en avançar-se a la legislació i minimitzar-ne el risc d'incompliment.
- Reduir la probabilitat de multes i sancions, incloses les pèrdues financeres o la responsabilitat associada amb violacions a la privacitat.
- Construir una marca amb més confiança per part dels consumidors, guanyant així un avantatge competitiu sostenible.
- Gestionar millor els incidents posteriors a la infracció, per recuperar la confiança del consumidor.
- Mantenir les millors pràctiques mitjançant la recerca de proves independents dels controls de privacitat i seguretat, en comptes de més autoinformes o proves.

2.2.3. Barreres de la privacitat per disseny

Les organitzacions solen justificar la no implantació de la privacitat per disseny, i argumenten alguna o diverses de les justificacions següents:

- Dificultats per part de la direcció de les organitzacions per percebre els riscos i els beneficis de la protecció de dades. La inversió necessària no es percep com a justificada.
- Per motius similars, les empreses proveïdores de solucions de programari no troben en la inclusió de funcionalitat orientada a preservar la privacitat un avantatge competitiu, de manera que el programari comercialitzat té carències d'aquest tipus de funcionalitat.
- La seguretat de la informació (i, encara més, la protecció de dades) no està inclosa encara de manera generalitzada com a element integrant i impor-

tant en el cicle de desenvolupament de programari utilitzat per les organitzacions.

- Les organitzacions solen tenir dubtes sobre com implementar solucions tangibles per donar resposta als requisits de control de la normativa de protecció de dades. A aquesta situació contribueix l'absència d'estàndards pràctics en un àmbit internacional, i que orientin les organitzacions en la implementació efectiva de controls.

2.3. Normatives de dades

El coneixement i la seguretat legal són necessaris per a un ús responsable de les dades. El coneixement dels usuaris sobre la normativa de protecció de dades és cada vegada més gran i, per aquest motiu, són cada vegada més exigents. Les exigències dels drets dels consumidors i la protecció de dades personals són elements clau. La tendència en el nombre de lleis de privacitat de dades ha anat en augment en els últims anys. De fet, s'ha passat de set en els anys setanta a dos-cents deu el 2016, i aquesta tendència seguirà en els propers anys.*

Normativa

Una normativa és l'agrupació de totes aquelles normes que són o poden ser aplicables en una matèria específica.

*** Més informació a: https://goo.gl/qjfe5u**

L'esperit de tota norma ha de ser un processament just, lícit i transparent. En el cas que ens ocupa, orientat a la dada.

2.3.1. Normatives

Els diferents estats i zones a què pertanyen solen tenir diferents enfocaments en matèria de protecció de dades. En aquest material, ens centrarem principalment en comparar normatives que s'apliquen als Estats Units, Europa i Espanya, si bé cal comentar que caldria contextualitzar els aspectes de què es tractarà, en funció del país del lector. A Europa, la protecció de dades és declarada com un dret humà i regulada per la legislació de protecció de dades. En canvi, als Estats Units, l'actitud cap a la protecció de dades es regeix principalment per les forces del mercat.

Aquestes diferències incideixen profundament en el que s'entén per **privacitat** a cada país des d'un punt vista normatiu. Per posar-ne alguns exemples:

- EUA no disposa de cap tipus de llei semblant a la LOPD (Llei orgànica de protecció de dades) espanyola, ni a la directiva europea que unifica normatives en els estats membres.

- A EUA, les sancions per les diferents infraccions contra la protecció de dades es decideixen cas per cas. A Europa, però, ja estan estipulades per

endavant i quan es cometen, s'aplica la multa pertinent, depenent del grau de la infracció.

- A EUA, les lleis de protecció de dades protegeixen només els ciutadans americans. En canvi, a Europa es protegeix tot aquell que estigui dins de la UE.

A aquestes diferències se suma el fet que l'antic conveni de col·laboració entre EUA i Europa, anomenat *safe harbor*, va ser declarat invàlid l'octubre del 2015, arran de la denúncia d'un ciutadà austríac que va demanar a les autoritats irlandeses que suspenguessin la transferència de les seves dades personals a EUA per part de Facebook. Aquest acord comprometia les empreses i les entitats d'EUA adherides a respectar els principis de la protecció de dades i adoptar les mesures de seguretat oportunes.

Encara que hi hagi lleis per a la protecció de la privacitat, freqüentment els governs les modifiquen per situacions d'excepció. Per exemple, la Stasi, el servei oficial de seguretat de l'Estat de la República Democràtica Alemanya o RDA (informalment coneguda com Alemanya Oriental), va emprar cinc-cents mil informants secrets. La tasca de deu mil d'aquests informants era escoltar i transcriure les trucades telefòniques dels ciutadans. Amb l'adopció de la Llei patriota dels Estats Units, en resposta als successos ocorreguts l'11 de setembre del 2001, els Estats Units va reduir considerablement les restriccions en la recopilació de dades personals per part dels organismes encarregats de fer complir la llei.

Als Estats Units, la legislació sobre privacitat ha adoptat un enfocament més sectorial. Diferents lleis regulen com les organitzacions recullen, fan servir i protegeixen la confidencialitat de la informació personal identificable (PII) en diferents sectors. Alguns exemples inclouen la Llei de portabilitat i responsabilitat d'assegurances de salut (HIPAA), la Llei de transacció de crèdit justa i precisa (FACTA) i la Llei de protecció de la privacitat de nens en línia (COPPA). Les preocupacions sobre les bretxes de dades que podrien conduir a un augment en el robatori d'identitat han portat a la majoria dels estats a promulgar lleis de notificació de violació de dades. La legislació federal sobre aquest assumpte està sent considerada en el Congrés dels Estats Units. Impulsats per les mateixes preocupacions, estats com Massachusetts i Nevada també han promulgat lleis que requereixen l'adopció de tecnologies de xifrat per protegir la informació personal privada dels residents de l'Estat, en diferents escenaris.

Aquesta preocupació és universal. Moltes altres nacions també han promulgat una legislació integral sobre privacitat. Alguns exemples són la Llei de privacitat d'Austràlia, la Llei de protecció de dades personals de l'Argentina i la Llei de protecció de dades personals (PIPEDA) de Canadà.

Tenint en compte aquest panorama fragmentat per països i sectors, algunes institucions han decidit crear recopilacions de millors pràctiques per evitar riscos. La Cloud Security Alliance (CSA) ha elaborat les cent millors pràctiques per optimitzar la seguretat i la privacitat dins el *big data*.

Lectura complementària

Diversos autors (2016). *Big Data Security and Privacy Handbook: 100 Best Practices in Big Data Security and Privacy*. Cloud Security Alliance.

2.3.2. Normativa europea

El 25 de gener del 2012, la Comissió Europea (CE) va anunciar que intentaria unificar la llei de protecció de dades a la Unió Europea amb una proposta de llei denominada Reglament general de protecció de dades (GDPR, acrònim de General Data Protection Regulation). Aquestes noves normes de la UE sobre protecció de dades reforcen els drets de les persones sobre les seves dades personals i imposen multes per a les organitzacions que no protegeixen les seves dades. Els objectius de la CE amb aquesta nova legislació inclouen:

GDPR definició

Pel reglament (UE) 2016/679/CE *General Data Protection Regulation* (GDPR), el Parlament Europeu, el Consell Europeu i la Comissió Europea reforcen i unifiquen la protecció de dades per als individus dins de la Unió Europea (UE).

- L'harmonització de vint-i-set reglaments nacionals de protecció de dades en una única reglamentació.
- La millora de les normes de transferència de dades empresarials fora de la Unió Europea.
- La millora del control de l'usuari sobre les dades d'identificació personal.

El fet que es tracti d'un reglament en lloc d'una directiva vol dir que serà directament aplicable a tots els estats membres de la UE, sense necessitat de legislació nacional aplicable.

De manera prèvia a la GDPR, els països membres de la Unió Europea estan obligats a promulgar lleis que compleixin amb la Directiva 95/46/CE, relativa a la protecció de dades (DPD). Les directrius de la directiva es consideren una base per a les lleis nacionals, i els òrgans legislatius locals dels països membres poden incloure disposicions que van més enllà.*

*** Per saber-ne més: https://goo.gl/h9HMpO**

En comparació de la Directiva 95/46/CE, el GDPR pretén ampliar l'abast de la legislació comunitària en matèria de protecció de dades. Els principis de protecció de dades són àmpliament similars als principis establerts en la Directiva 95/46/CE: equitat, legalitat, transparència, limitació del propòsit, minimització de dades, qualitat de les dades, seguretat, integritat i confidencialitat.*

*** https://goo.gl/LhXeGS**

Pel que fa al concepte de dades personals, a la Directiva es defineix com qualsevol informació relativa a una persona física identificada o identificable. En virtut de l'GDPR, una violació de dades personals és qualsevol destrucció accidental o il·legal, pèrdua, alteració, divulgació no autoritzada o accés a les dades personals transmeses, emmagatzemades o processats per un altre ús. Aquesta àmplia definició difereix de la majoria de les lleis estatals de violació de dades estatals; per exemple, només després de l'exposició d'informació que pot

conduir a frau o robatori d'identitat, com la informació financera del compte. Quan les dades perden la seva condició de personals i deixen d'estar vinculades a un titular concret, queden fora de l'àmbit d'aplicació de la normativa de protecció de dades.*

*** Més informació a: https://goo.gl/8SBICW**

En definitiva, la GDPR busca protegir les dades personals i la forma en què les organitzacions les processen, les emmagatzemen i, finalment, les destrueixen quan aquestes dades ja no són requerides. La llei proveeix control individual sobre com les companyies poden fer servir la informació que està directament i personalment relacionada amb els individus, i atorga vuit drets específics. A més, estableix normes molt estrictes que regeixen el que succeeix si es viola l'accés a dades personals i les seves conseqüències.

Aquesta llei té un impacte considerable als sistemes d'informació i d'anàlisi de les empreses. L'existència d'un programa de govern de la dada i la funció vinculada a la seguretat de la dada han ajudat a estar preparats per endavant.

2.3.3. Normativa espanyola

A l'Estat espanyol, hi ha múltiples normes vinculades a la seguretat de la dada i la privacitat de la dada que es publiquen al *Butlletí Oficial de l'Estat* (BOE). Aquesta llista té el seu equivalent en altres països, i va creixent o rebent extensions any rere any. Presentem tan sols les normes generals, i caldria determinar les que s'apliquen al sector.

Les podem agrupar en diferents àmbits d'aplicació:

- **Normativa relacionada amb els serveis de la societat de la informació**:

– Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i comerç electrònic (LSSI-CE) (BOE 166, de 12 de juliol del 2002).

– Llei 56/2007, de 28 de desembre, de mesures d'impuls a la societat de la informació (BOE 312, de 29 de desembre 2007).

– Reial decret 889/2009, de 22 de maig, pel qual s'aprova la Carta de drets de l'usuari dels serveis de comunicacions electròniques (BOE 131, de 30 de maig del 2009).

- **Normativa relacionada amb el tractament de les dades de caràcter personal**:

– Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD) (BOE 298, de 14 de desembre de 1999).

– Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (BOE 17, de 19 de gener de l'2008).

– Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions (BOE 251, de 19 d'octubre 2007).

- **Normativa relacionada amb la propietat intel·lectual**:

– Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de propietat intel·lectual (LPI), i que regularitza, aclareix i harmonitza les disposicions vigents en la matèria (BOE 97, de 22 de abril de 1996).

– RD 28/2003 de 7 de març, pel qual s'aprova el Reglament del registre central de la propietat intel·lectual (BOE 75, de 28 de març del 2003).

– Llei 23/2006, de 7 de juliol, per la qual es modifica el text refós de la Llei de propietat intel·lectual, aprovat pel Reial decret legislatiu 1/1996, de 12 d'abril (LPI) (BOE 162, de 8 de juliol del 2006).

- **Normativa relacionada amb l'Administració electrònica**:

– Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics (LAECSP) (BOE 150, de 23 de juny del 2007).

– Reial decret 3/2010, de 8 de gener, pel qual es regula l'esquema nacional de seguretat en l'àmbit de l'Administració electrònica (ENS) (BOE 25, de 29 de gener de 2010).

– Reial decret 4/2010, de 8 de gener, pel qual es regula l'esquema nacional d'interoperabilitat en l'àmbit de l'Administració electrònica (ENI) (BOE 25, de 29 de gener de 2010).

– Reial decret 1671/2009, de 6 de novembre, pel qual es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics (BOE 278, de 18 de novembre del 2009).

– Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú (BOE 285, de 27 de novembre de 1992).

– Reial decret 209/2003, de 21 febrer, que regula els registres i les notificacions telemàtiques, a més de l'ús de mitjans telemàtics per a la substitució de l'aportació de certificats pels ciutadans (BOE 51, de 28 de febrer del 2003).

– Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic (BOE 276, de 17 de novembre del 2007).

– Ordre PRE / 2971/2007, de 5 d'octubre, sobre l'expedició de factures per mitjans electrònics quan el destinatari sigui l'Administració general de l'Estat o organismes públics vinculats o dependents d'ella, i sobre la presentació davant l'Administració general de l'estat o els seus organismes públics vinculats o dependents de factures expedides entre particulars (BOE 247, de 15 d'octubre del 2007).

• **Normativa relacionada amb la signatura electrònica**:

– Llei 59/2003, de 19 de desembre, de signatura electrònica (BOE 304, de 20 de desembre del 2003).

– Ordre de 21 de febrer del 2000, per la qual s'aprova el Reglament d'acreditació de prestadors de serveis de certificació de determinats productes de signatura electrònica (BOE 45, de 22 de febrer del 2000).

– Reial decret 1496/2003, de 28 de novembre, pel qual s'aprova el Reglament que regula les obligacions de facturació (BOE 286, de 29 de novembre del 2003).

– Ordre EHA/962/2007, de 10 d'abril, per la qual es desenvolupen determinades disposicions sobre facturació telemàtica i conservació electrònica de factures, contingudes en el RD 1496/2003 (BOE de 14 de abril del 2007).

– Resolució de 24 d'octubre del 2007, de l'Agència Estatal d'Administració Tributària, sobre procediment per a l'homologació de programari de digitalització contemplat en l'Ordre EHA/962/2007, de 10 d'abril (BOE 262, d'1 de novembre del 2007) .

– Reial decret 1553/2005, de 23 de desembre, pel qual es regula l'expedició del document nacional d'identitat i els seus certificats de signatura electrònica (BOE 307, de 24 de desembre del 2005).

– Reial decret 1586/2009, de 16 d'octubre, pel qual es modifica el Reial decret 1553/2005, de 23 de desembre, que regula l'expedició del document nacional d'identitat i els seus certificats de signatura electrònica (BOE 265, de 3 de novembre del 2009).

• **Altres normes d'interès**

– Llei 2/2011, de 4 de març, d'economia sostenible (BOE 55, de 5 de març del 2011) que modifica en part la LAESCP, la LSSI-CE i la LPI.

– Llei 32/2003, de 3 de novembre, general de telecomunicacions (BOE 264, de 4 de novembre del 2003).

– Ordre ITC/1542/2005, de 19 de maig, que aprova el Pla nacional de noms de domini d'Internet sota el codi de país corresponent a Espanya («es») (BOE 129, de 31 de maig del 2005).

– Reial decret 424/2005, de 15 d'abril, pel qual s'aprova el Reglament sobre les condicions per a la prestació de serveis de comunicacions electròniques, el servei universal i la protecció dels usuaris (BOE 102, de 29 d'abril del 2005).

– Reial decret legislatiu 1/2007, de 16 de novembre, pel qual s'aprova el text refós de la Llei general per a la defensa dels consumidors i usuaris i altres lleis complementàries (BOE 287, de 30 de novembre del 2007).

– Reial decret 1906/1999, de 17 de desembre, pel qual es regula la contractació telefònica o electrònica amb condicions generals en desenvolupament de l'article 5.3 de la Llei 7/1998, de 13 d'abril, de condicions generals de la contractació (BOE 313 , de 31 de desembre del 1999).

– Reial decret 225/2006, de 24 de febrer, pel qual es regulen determinats aspectes de les vendes a distància i la inscripció en el registre d'empreses de vendes a distància (BOE 72, de 25 de març del 2006).

2.3.4. Més enllà de les normatives de dades

En aquest apartat, ens hem centrat en la seguretat i la privacitat de la dada. No obstant això, la dada és només un dels components de la transformació en una organització orientada a la dada. Hem de recordar que l'altre element rellevant és l'algoritme.

Els algoritmes s'estan fent servir al sector privat i públic, i proporcionen millores des de l'educació, el rendiment empresarial o fins i tot serveixen per combatre el crim. No obstant això, els mateixos algoritmes poden dur a escenaris en els quals es deteriori o ometi la privacitat. Estem parlant de possibilitats d'amplificar la discriminació estructural, produir errors per denegar serveis a individus o fins i tot modificar el comportament d'individus.

Tot i que no existeixen encara normatives en aquest aspecte, entre la comunitat estan començant a aparèixer les primeres veus perquè en l'aplicació d'aquests algoritmes (com *machine learning*) es tinguin en compte principis ètics o el que podríem anomenar un «govern d'algoritmes»:

- **Responsabilitat**: per a cada sistema d'algoritmes, hi ha d'haver una persona amb l'autoritat de gestionar amb efectes adversos la societat o individus particulars, de forma ràpida i eficient.

- **Explicació**: els efectes d'un sistema d'algoritmes han de poder ser explicats a les persones afectades per aquestes decisions. Aquestes explicacions han de ser accessibles i, sobretot, comprensibles per a tot tipus de públic.

- **Exactitud**: els algoritmes poden cometre errors, ja sigui per la manca de qualitat de la dada o pel model triat. Aquestes fonts d'errors han de ser identificades, registrades i comparades, cosa que permetrà mitigar els seus efectes.

- **Auditoria**: els sistemes d'algorismes han de ser dissenyats de manera que puguin ser auditats per tercers per validar el comportament de l'algoritme. En aquest sentit, estem parlant d'una auditoria privada, similar a les proporcionades a les auditories financeres.

- **Equitat**: els algoritmes són susceptibles de contenir biaixos dels seus programadors, fins i tot pel seu mateix objectiu. Cal determinar si l'algoritme produeix efectes discriminatoris.

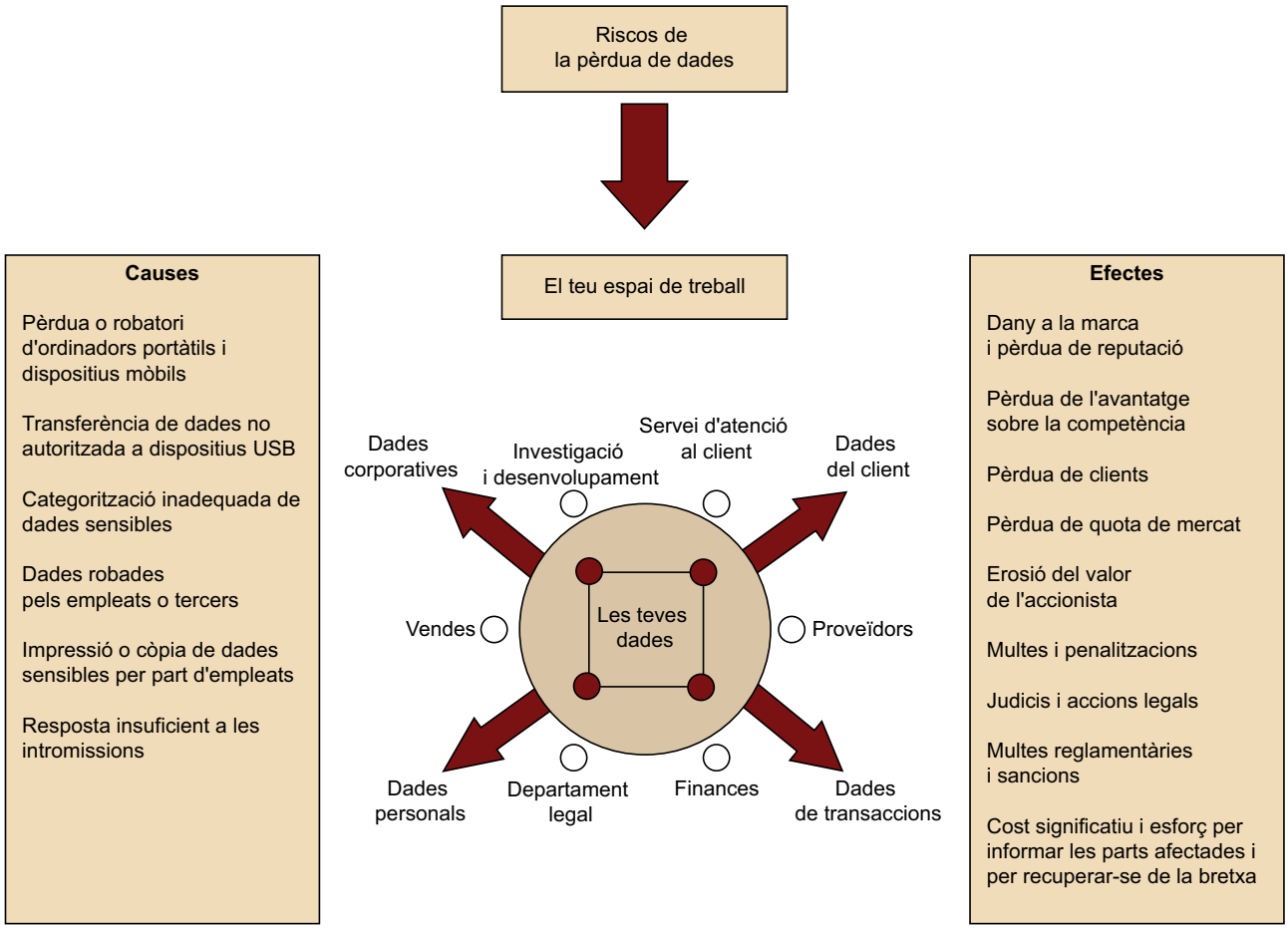
3. Programa de seguretat de dades

En un món hiperconnectat, les organitzacions necessiten estar preparades per les implicacions que tenen sobre les seves dades. McKinsey, en conjunt amb el Fòrum Econòmic Mundial, va estimar que les fallades de seguretat en les organitzacions podrien tenir un impacte en la tecnologia i en la innovació empresarial de tres bilions de dòlars el 2020.*

*** Més informació a: https://goo.gl/w5wUQB**

Hi ha múltiples riscos de seguretat, tal com il·lustra la figura 3.

Figura 3. Riscos de seguretat dins d'una organització



Font: Ernst and Young

Les organitzacions han de pensar que les bretxes de seguretat afecten tot tipus de dades, com els que s'inclouen a la taula 1.

Taula 1. Tipologies de dades

Corporatius	Transaccionals	Clients	Personals
Preus/Costos	Pagaments bancaris	Llistat de clients	Nom i cognoms
Clients	Operacions B2B	Hàbits de compres	Data de naixement
Nous dissenys	Dades dels venedors	Detalls de contacte	DNI, passaport
Patents	Volums de vendes	Preferències	Dades genètiques
Anàlisis financeres	Ràtios de descomptes	Perfil del client	Carnet de conduir, matrícula del cotxe
Documents legals	Poder de compres	Històric	Dades demogràfiques
Avaluacions d'empleats	Potencial d'ingressos	Saldo de comptes	Preferències

És tan important explotar les dades com assegurar-les. Segons Scott Koegler, de Big Data Forum, obtenir **dades protegides però processables** és clau per desenvolupar pràctiques empresarials avançades mentre es protegeix la identitat del client. Això ens porta a considerar la implementació d'un programa de seguretat de dades fonamentat en bones praxis.

Bones praxis

Per bones o millors pràctiques s'entén un conjunt coherent d'accions que han rendit un bon o fins i tot un excel·lent servei en un determinat context, i que s'espera que, en contextos similars, rendeixin resultats similars.

S'entén per **programa de seguretat de dades** la metodologia estratègica i sistemàtica per assegurar les dades dins d'una organització.

En definitiva, el programa persegueix analitzar i proporcionar una guia per millorar la seguretat i privacitat de les dades. Instituir un programa de seguretat i privacitat de les dades dins d'una organització significa alguna cosa més que l'adquisició d'eines de seguretat i privacitat de les dades o la creació d'uns rols o una col·lecció de processos relacionats amb la seguretat i la privacitat de les dades.

És necessària l'elaboració d'un programa on es determini la manera d'actuar, es defineixin objectius i es designi els responsables de cada iniciativa i les accions que cal prendre. I tot això d'una manera orquestrada, en què es conegui des de quin punt es parteix en un àmbit de seguretat i privacitat, i fins a quin punt es vol arribar, a més dels costos i els beneficis d'aquesta transició.

3.1. Principis del programa de seguretat de dades

Els quatre principis següents estan dissenyats per ajudar les organitzacions a seleccionar les activitats que protegiran les seves dades confidencials.

- **Principi 1**: les polítiques han d'assegurar al llarg de la vida de les dades la seva confidencialitat. Això inclou el compromís de processar totes les dades d'acord amb les lleis i regulacions aplicables, preservar-ne la privacitat, respectar l'elecció i el consentiment del client i permetre als individus de revisar i corregir la seva informació, si cal.

- **Principi 2**: minimitzar el risc d'accés no autoritzat o l'ús indegut de dades confidencials. El sistema de gestió de la informació ha de proporcionar accions administratives, tècniques i físiques raonables per garantir la confidencialitat, la integritat i la disponibilitat de les dades.

- **Principi 3**: minimitzar l'impacte de la pèrdua de dades confidencials. Els sistemes de protecció de la informació han de proporcionar salvaguardes. Cal establir també plans adequats de resposta a la violació de dades, i tots els empleats que puguin estar involucrats en la resposta a la bretxa han d'estar capacitats per aplicar-hi les mesures oportunes.

- **Principi 4**: documentar els controls creats i demostrar la seva efectivitat. Perquè l'organització ajudi a garantir els principis de privacitat i confidencialitat de dades, han de poder ser verificats gràcies al monitoratge, l'auditoria i l'ús de controls apropiats. A més, l'organització ha de tenir un procés per informar de l'incompliment i un full de ruta de les accions clarament definit.

3.2. Persones, processos i tecnologia

Els tres elements de qualsevol programa de seguretat de dades són les persones, els processos i la tecnologia. Vegem-los:

- **Persones**: els processos i les eines de gestió de dades són tan efectius com les persones que els utilitzen i els gestionen. Un primer pas important és establir un equip d'individus de l'organització, i dotar-los de rols clarament definits i responsabilitats, i també de recursos adequats per exercir les seves funcions requerides i orientació sobre els objectius generals de la seguretat de les dades. Essencialment, es tracta d'una organització els membres de la qual són col·lectivament responsables de definir principis, polítiques i procediments que regeixen els aspectes clau de la classificació, la protecció, l'ús i la gestió de dades. Aquests individus desenvolupen els perfils de control d'accés de l'organització, determinen què constitueix un ús de dades compatible amb les polítiques, la notificació d'infraccions de dades i les rutes d'escalament i supervisen altres àrees de gestió de dades relacionades amb la seguretat.

- **Processos**: amb les persones adequades involucrades, l'organització pot centrar-se en definir els processos involucrats en la seguretat i la privacitat de les dades. Això comença amb l'examen de diversos documents d'autoritat (estatuts, reglaments, normes en un àmbit d'organització o estatals, polítiques de l'empresa i documents estratègics) que especifiquen els requisits que s'han de complir. Finalment, l'organització ha d'identificar amenaces contra la seguretat de les dades, la privacitat i el compliment en el context de fluxos de dades específiques. A continuació, haurà de determinar les accions de control apropiades.

- **Tecnologia**: el pas següent és aplicar les eines per analitzar els fluxos de dades, identificar-ne els riscos i aplicar-hi les mesures necessàries de seguretat i privacitat.

Un programa consisteix en un cicle iteratiu d'avaluació, planificació, execució, gestió i revisió per a la seguretat i privacitat de les dades. Això requereix processos repetibles que s'uneixin a les persones amb una formació i que disposin de les habilitats adequades amb els instruments adequats per passar de la teoria a la pràctica.

En el context de la seguretat, els usuaris són la baula «més feble» de la seguretat en una organització, ja que es tracta de la primera línia de defensa davant els atacs a la seguretat cibernètica. Javier Perea, director regional d'Intel Security a Espanya, fa un comentari sobre això en aquest informe:

Lectura complementària

R. Raj; C. McFarland (2016). *Hacking the Human OS*. Intel Security.

> Les últimes tècniques d'enginyeria social posades en marxa pels cibercriminals són cada vegada més sofisticades i difícils de detectar i de solucionar. Aquestes noves tècniques tenen en el punt de mira els treballadors de les organitzacions com a objecte de l'atac. Aquest informe destaca la importància de conscienciar i educar l'usuari/treballadors, perquè assumeixin la seguretat de les dades com un fet cultural. Per exemple, avui dia qualsevol treballador pot disposar d'un *pendrive* de diversos gigues en què emmagatzemi informació tant de l'organització com dels seus clients. Per molta seguretat i privacitat que impulsi l'organització, si un treballador utilitza la informació de l'organització fora de l'entorn, segur que provoca que tota aquesta seguretat sigui en va.

Casos com l'atac de *ransomware* (programari maliciós de rescat) fonamentat en WannaCry, l'any 2017, posen de manifest la necessitat de millorar l'educació i la formació en seguretat en les organitzacions, per reduir els casos fonamentats en l'enginyeria social. Per a això, necessitem rols que liderin aquestes iniciatives.

Tradicionalment, el C(I)SO, acrònim de *chief (information) security office*, ha estat responsable de la seguretat en les organitzacions. A mesura que van incrementant-se les normatives vinculades a la dada, s'han ampliat les competències d'aquest paper o ha emergit un de nou anomenat DPO, acrònim de *data protection officer*. Les tasques principals del DPO són:

- Educar l'empresa i els seus empleats sobre els requisits de compliment importants de seguretat de dades.
- Capacitació del personal involucrat en el processament de dades.
- Dur a terme auditories per assegurar-se del compliment de les mesures i abordar les possibles qüestions de manera proactiva.
- Servir de punt de contacte entre l'organització i les lleis i institucions que regulen la seguretat.

- Supervisar l'acompliment i l'assessorament sobre l'impacte dels esforços de la protecció de dades.

- Mantenir els registres de totes les activitats de processament de dades efectuades per l'organització, incloent el propòsit de totes les activitats de processament.

- Interactuar amb els clients per informar-los de com s'estan utilitzant les seves dades, els seus drets d'esborrar les seves dades personals i les mesures que l'organització ha posat en marxa per protegir la seva informació personal.

Evidentment, a part del DPO, la resta dels membres de l'organització també són responsables de la seguretat i de la privacitat de les dades.

3.3. Seguretat de dades en el context de govern de la dada

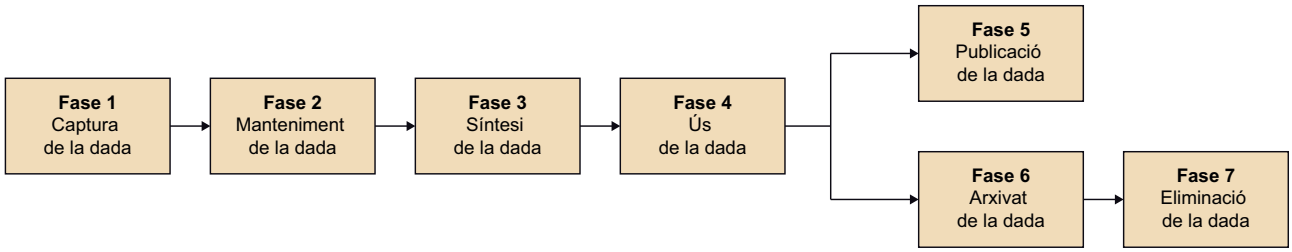
En el context de govern de la dada, la seguretat i la privacitat de dades és una funció més que cal fer. Com ja sabem, cada funció té diferents activitats (planificació, control, de desenvolupament i operatives), cadascuna de les quals efectuada pel rol corresponent.

Per a la gestió de la seguretat de dades, aquestes activitats són:

- Comprensió de les necessitats de privacitat, confidencialitat i seguretat de dades (activitat de planificació).
- Definició de les polítiques i estàndards de privacitat i confidencialitat (activitat de planificació).
- Definició dels estàndards i procediments de contrasenyes (activitat de planificació).
- Disseny i implementació dels controls de seguretat de dades (activitat de desenvolupament).
- Gestió d'usuari, contrasenyes i grups d'usuaris (activitat de control).
- Gestió de vistes d'accés de dades (activitat de control).
- Gestió de permisos d'accés de dades (activitat de control).
- Monitoratge de l'autenticació i del comportament d'usuaris (activitat de control).
- Classificació de la confidencialitat de la informació (activitat de control).
- Auditoria de la seguretat de dades (activitat de control).

El programa de la seguretat de dades cobreix aquestes funcions, que formen part del marc més general al llarg del cicle de vida de la dada, que es mostra a la figura 4.

Figura 4. Cicle de vida de la dada



Font: Marcos Pérez González

De manera que:

- A la **fase 1**, l'organització ha d'assegurar que la captura de la dada respecta la privacitat i la regulació pròpies del país on opera l'organització, i que està alineada amb les necessitats de l'organització.

- A la **fase 2** i **3**, l'organització s'ha d'assegurar que el manteniment i la síntesi de la dada segueixen les polítiques i els estàndards d'accés, confidencialitat i privacitat. En aquest punt, és rellevant tenir en compte com l'anàlisi de la dada pot convertir dades anònimes en dades personalitzades.

- A la **fase 4**, l'ús de la dada ha de controlar-se mitjançant les activitats de control del pla per assegurar que es treballa en el context de vistes i permisos definit.

- A la **fase 5**, hem de assegurar-nos que la dada que es publica és correcta i, si són dades de clients, assegurar-nos que siguin anònimes.

- A la **fase 6**, s'ha d'assegurar que les dades estiguin segures i que, en tot moment, les seves metadades (és a dir, dades sobre les dades) en mostrin la rellevància. Si algunes dades tenen caducitat, s'han d'arxivar i, si els usuaris ho sol·liciten, s'han de modificar.

- Finalment, a la **fase 7**, hem d'assegurar-nos que les dades són correctament eliminades i, si en qualsevol moment un usuari ens sol·licita la baixa del nostre sistema, que realment es porta a terme l'eliminació de les dades.

3.4. Millors pràctiques

A continuació, llistem algunes de les millors pràctiques en l'àmbit de la seguretat i la privacitat de la dada:

- **Prioritzar els actius d'informació basats en els riscos del negoci**: la majoria de les institucions no tenen prou informació sobre la prioritat amb la qual necessiten protegir les seves dades. En lloc d'intentar assegurar-ho tot, les organitzacions necessiten aplicar l'enfocament 80-20 i centrar-se

en aquest 20% de les dades que és més crític. Una bona praxi consisteix a crear un full de ruta d'implementació sobre la seguretat que cal aplicar a les dades: per on s'ha de començar, quina importància té i, per tant, quins esforços hem d'aplicar-hi, i construir una temporització sobre les accions que s'han d'aplicar.

- **Proporcionar una protecció diferenciada, basada en la importància dels actius**: l'ús de controls diferenciats (per exemple, xifrat, contrasenyes més rigoroses...) permet a les institucions concentrar temps i recursos en la protecció dels actius d'informació que més importen.

- **Integrar la seguretat en l'entorn tecnològic per impulsar la seva escalabilitat**: les eines de seguretat de dades necessiten ser automatitzades. Els actuals conjunts d'eines requereixen una considerable inversió en la gestió quotidiana per arribar a ser eficaços. Les institucions han de passar de simplement aplicar seguretat *ad hoc* a capacitar tot el seu personal per incorporar-la des del primer dia en projectes tecnològics amb dades segures i privades.

- **Implementar defenses actives per descobrir atacs de forma proactiva**: hi ha una gran quantitat d'informació disponible sobre possibles atacs. Cada vegada més, les empreses hauran de desenvolupar capacitats per afegir informació rellevant i analitzar i ajustar els seus sistemes de defensa en conseqüència (per exemple, tallafocs).

- **Provar contínuament, amb l'objectiu de millorar la resposta a incidents**: una resposta inadequada a una infracció (no només per l'equip TI, sinó també pel màrqueting, és a dir, la part de negoci, els assumptes públics o les funcions de servei al client) pot ser tan perjudicial com l'incompliment pròpiament dit. Un programa no és un esdeveniment únic, sinó un procés continu que evolucionarà amb el temps. Sovint, és un canvi cultural en una organització i, per tant, la seva implantació porta temps. El programa ha de ser revisat periòdicament i modificat quan sigui necessari.

- **Formar el personal de primera línia per ajudar a entendre el valor dels actius d'informació**: els usuaris solen ser la major vulnerabilitat que té una institució; cliquen enllaços que no s'haurien d'obrir, seleccionen contrasenyes insegures i envien arxius confidencials per correu electrònic a llistes de distribució àmplies. Les institucions necessiten segmentar els usuaris i ajudar cada grup a comprendre els riscos empresarials dels actius d'informació que toquen cada dia.

- **Integrar la seguretat en els processos de gestió de riscos i governança a tota l'organització**: això significa parlar de seguretat de TI en termes de negoci, en comptes de centrar-se en els termes de TI que no poden capturar el valor real de les dades que cal assegurar. A més, les implicacions de la seguretat s'han d'integrar en l'ampli conjunt de funcions de govern

corporatiu, com la gestió de recursos humans, la gestió de proveïdors i el compliment normatiu.

- **Transparència amb els usuaris**: la informació sobre les polítiques de dades ha de ser fàcil de trobar per al públic (i no enterrada al lloc web). El text ha de ser concís i fàcil de llegir, sense argot. Ha d'indicar com es recullen, es comparteixen i s'utilitzen les dades, qui hi té accés i quins salvaguardes protegeixen la privacitat dels usuaris.

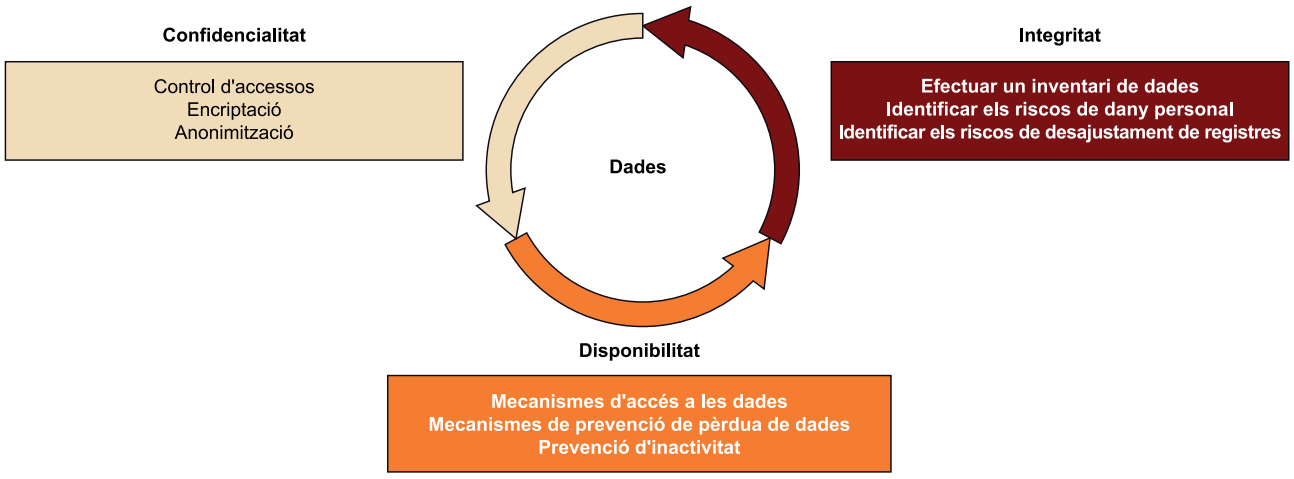
- **Transparència amb els usuaris en cas de bretxes de seguretat**: la notificació oportuna de les infraccions de seguretat és important per a la confiança pública. És improbable esperar que les bretxes en els sistemes de dades acabin algun dia, encara que aquesta és la meta. No obstant això, els retards en la notificació dels usuaris sobre les infraccions els posen en major risc, especialment si els usuaris repeteixen les mateixes contrasenyes en diversos sistemes. La notificació ràpida permet als usuaris canviar de forma proactiva les contrasenyes per mitjà de diverses aplicacions. També els demana que considerin el monitoratge de crèdit o la protecció contra robatori d'identitat si els números de seguretat social o la informació tributària estan compromesos.*

*** Més informació a: *Privacy Rights Clearinghouse, 2016, June. Chronological Database of Data Security Breaches.* Recuperat del web Privacy Rights Clearinghouse <https://goo.gl/28S4BA>**

3.5. Elements clau de la seguretat i la privacitat

La seguretat de dades digitals es basa en tres propietats, sovint identificades amb l'acrònim CIA: *confidentiality*, *integrity*, *availability*. La figura 5 mostra aquests tres elements clau.

Figura 5. Elements clau de la seguretat i la privacitat



Font: David Cabanillas

Només es pot satisfer si es respecten les propietats abans esmentades i es garanteix el següent:

- **Confidencialitat**: es tracta d'una propietat de la informació que pretén garantir l'accés només a les persones autoritzades.

- **Integritat**: el terme integritat de dades es refereix a la correcció i completesa de la informació de les dades. Per exemple, si una empresa té una adreça incorrecta per a un client i envia factures a aquesta adreça incorrecta, els pagaments per part del client podrien retardar-se, fet que podria conduir a deutes incobrables. La informació personal serà tan precisa, completa i actualitzada com sigui necessari per als propòsits per als quals es farà servir. La mesura en què la informació personal serà exacta, completa i actualitzada dependrà de l'ús de la informació, tenint en compte els interessos de l'individu. Les organitzacions poden seguir aquestes tres idees:

– **Dur a terme un inventari de dades**: realment, no hi ha manera de demostrar que la informació personal que s'ha recopilat és exacta i rellevant per als seus usos previstos, llevat que se sàpiga on és i quin procés o qui l'està utilitzant.

– **Identificar els riscos de dany personal**: l'organització té algun procés de negoci que podria fer mal a una persona si s'utilitzés informació inexacta? Els exemples podrien incloure informació de salut inexacta que tingués com a resultat diagnòstics erronis o negacions de cobertura d'assegurança; informació de crèdit imprecisa que dona com a resultat préstecs o treballs negats; o informació inexacta sobre l'acompliment de la feina, que acaba en oportunitats d'ocupació perdudes.

– **Identificar els riscos de desajustament de registres**: l'organització té algun sistema en el qual una persona pugui accedir a la informació confidencial d'una altra persona per mitjà d'una autenticació o d'un registre? Cal concentrar l'atenció en els processos de *customer relationship management* (CRM).

- **Disponibilitat**: les dades han de ser segures i privades, però també han de poder ser explotades per l'organització. La disponibilitat de la dada també s'ha de garantir.

4. Tècniques i tecnologia per a la gestió de la seguretat i la privacitat de la dada

Hem revisat fins ara els aspectes vinculats als processos, el govern, les polítiques i els estàndards en el context de la gestió de dades mestres. En aquest apartat, ens centrarem en les eines, tècniques i tecnologies que suporten la gestió de dades mestres.

4.1. Tècniques

Per poder respectar les preferències dels clients (respecte a com i quan la seva informació personal pot ser recol·lectada i potencialment compartida amb tercers) i les obligacions de conformitat de seguretat i privacitat, aquestes tecnologies han d'incloure les tècniques següents:

- **Classificació**: capacitat d'identificar on es troben les dades sensibles, tant en els sistemes al centre de dades de la organització com en el núvol. Estem parlant, per tant, de tècniques d'autodescobriment, de catalogació i de traçabilitat de dades.

- **Auditoria**: capacitat d'entendre a quines dades sensibles s'accedeix i com es combinen, i qui hi està accedint. Per tant, es fan servir capacitats de traçabilitat de dades.

- **Protecció**: capacitat de protegir les dades sensibles en tots els àmbits. Aquesta protecció es porta a terme amb tècniques d'emmascarament (en anglès, *data masking*), anonimització i encriptació. Les tècniques de protecció són un dels punts calents de mercat, empeses per les regulacions; per exemple, a l'àrea del que es coneix com *differencial privacy*.

- **Monitoratge**: consisteix a saber en temps real quan els usuaris, els dispositius o els sistemes accedeixen a dades confidencials.

Emmascarament

L'emmascarament de dades garanteix el fet que la informació original mai no estarà disponible per a l'usuari final.

Anonimització

Amb la paraula *anonimització* es reconeix la dada dissociada, com aquella que no permet la identificació d'un afectat o interessat.

Xifratge

L'encriptació, o xifrat, fa que es dificulti el robatori d'informació mentre és transmesa per algun mitjà, però no n'impedeix l'abús o que sigui susceptible de filtracions, ni abans que el xifrat es produeixi ni un vegada que la descodificació ha tingut lloc.

4.2. Tecnologies

Respecte a la seguretat TIC (acrònim de tecnologies de la informació i la comunicació), hi ha un ampli ventall de serveis i eines que tenen diferents àmbits d'aplicació. Aquests àmbits són la gestió d'accés i d'identitat, la seguretat en el lloc de treball, la seguretat en aplicacions i dades, la seguretat en els sistemes i la seguretat en xarxa.

Tot i que és cert que tots aquests àmbits són rellevants per a les organitzacions, ens centrarem en aquells que estan vinculats a la seguretat i la privacitat en aplicacions i dades.

Les eines que cobreixen aquest àmbit són:

- **Antifrau**: eines d'*antiphishing*, anti-correu brossa, historial de navegació segura, etc.
- **Anti-programari maliciós**: eines d'antivirus, anti-programa espia, etc.
- **Control de continguts confidencials**: són eines per a la prevenció de fuga d'informació (DLP, acrònim de *data loss prevention*); gestió del cicle de la informació (ILM, acrònim de *information lifetime management*); control d'accés de dispositius extrapolables, etc.
- **Compliment legal i normatiu**: eines per al compliment legal (per exemple, LOPD, LSSID, etc.) i per al compliment normatiu (per exemple, SGIS, gestió de riscos, etc.).
- **Sistemes i eines criptogràfiques**: són eines per a l'encriptació de les comunicacions, dels dispositius mòbils, de discos durs i suports d'emmagatzematge.
- **Contingència i continuïtat**: eines de gestió de plans de contingència i continuïtat, de recuperació de sistemes, de còpies de seguretat i de desplegament ràpid d'infraestructures i virtualització.
- **Tallafocs/VPN/IDS, IPS**: eines de tallafocs en un àmbit de xarxa, d'aplicació, personals i corporatius, i també filtres de continguts, VPN (acrònim de *virtual private network*), IDS (acrònim de *intrusion detection system*) i IDPS (acrònim de *intrusion detection and prevention service*).
- **Auditoria tècnica i forense**: són eines d'auditoria de xarxa i ports, de sistemes i fitxers d'auditoria forense. Inclouen també tests d'intrusió, esborrat segur, gestió de pegats i vulnerabilitats.

Pel que fa als serveis que poden ser contractats, s'inclouen: l'acompliment amb la legislació, la gestió d'incidents (que consisteix en prevenció, detecció i resolució), l'externalització de serveis de seguretat (que inclou seguretat gestionada, *outsourcing* i centres de suport), l'auditoria tècnica (que inclou serveis de detenció d'intrusions i auditoria forense, entre d'altres) i l'implementació i la certificació de normativa (que inclou la certificació i l'acreditació, els plans i les polítiques de seguretat i l'anàlisi de riscos).

D'aquesta manera, els enfocaments tradicionals de seguretat de TI que se centren en la protecció de la infraestructura mitjançant la protecció de la xarxa han de ser augmentats amb mesures de protecció, com les anteriors, que se

centrin de manera específica en la protecció de les dades que s'emmagatzemen i es traslladen mitjançant aquesta infraestructura.

A això també hem d'afegir el fet que els mateixos sistemes d'anàlisi (és a dir, els sistemes que suporten el *data warehouse*, la intel·ligència de negoci, el *big data*, el *business analytics*, etc.) han d'incloure un component de seguretat relacionat amb les eines anteriors; de manera que, en lloc de definir una política per a cadascuna de les eines, pugui ser possible establir mesures en un àmbit de programa des d'un component central.

4.3. Marc tecnològic

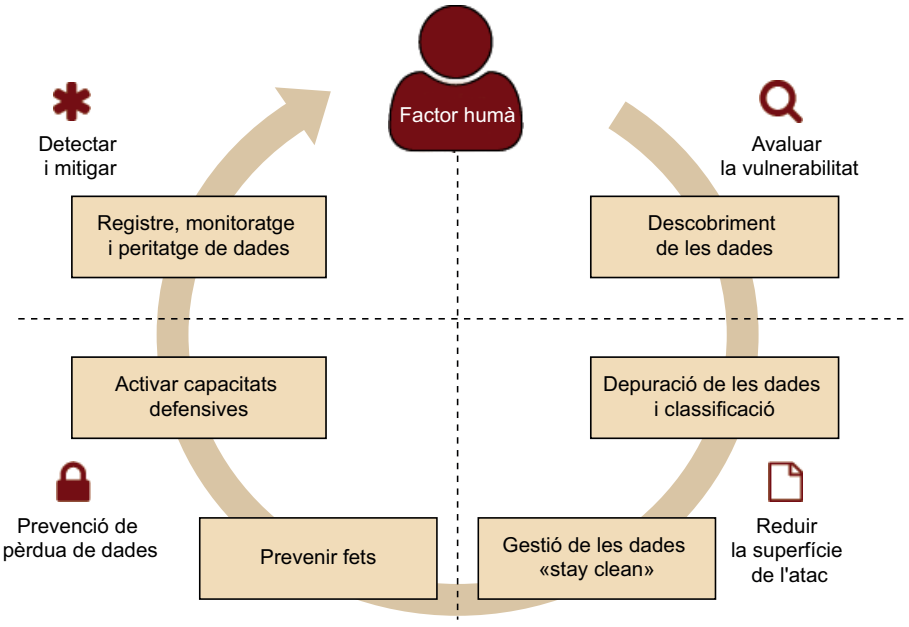
Les eines anteriors han de treballar de forma conjunta. La figura 6 mostra un marc o *framework* de seguretat. Aquest marc es compon de tres àrees:

1) Gestió proactiva i govern de la dada (meitat dreta).

2) Prevenció i monitoratge actius (meitat esquerra).

3) Factor humà.

Figura 6. Marc que engloba la seguretat i la privacitat dins del *data governance*



Font: Infinitive Insights

En els punts següents, es detallen les parts més rellevants dins el marc que engloba la seguretat i la privacitat en el *data governance*.

4.3.1. Classificació / sensibilitat de les dades

Avaluar el nivell de sensibilitat de les dades de cada actiu és una cosa que s'ha de definir en el context de les polítiques governants. Per exemple, en l'àmbit de la cura de la salut, les regles de HIPAA determinen quins elements de dades requereixen protecció, però pot haver-hi molts contextos en què es facin servir aquests elements de dades. Alguns requereixen més protecció que d'altres.

4.3.2. Auditoria de les dades

L'auditoria i la presentació d'informes són les claus per entendre el que passa amb les dades que no estan sota el control directe de l'organització. Sense aquestes activitats, és difícil de revertir transaccions no desitjades o fraudulentes. L'auditoria també constitueix la base dels règims de compliment. Aquestes són les preocupacions principals en aquesta àrea:

- **Abast de l'auditoria**: què és exactament l'auditoria en el servei? Com de completes són les auditories i quant de temps dura la informació d'auditoria? Es persisteix en la informació de l'usuari per a l'anàlisi forense? Es pot utilitzar la informació d'auditoria per revertir les transaccions impròpies? Les auditories s'ajusten a les lleis, els reglaments, les normes i les pràctiques de la indústria?

- **Integritat d'auditoria**: com es protegeix la informació d'auditoria? Qui hi té accés administratiu? S'emmagatzema la informació d'auditoria d'una manera segura i protegida?

- **Informes**: la informació d'auditoria és fàcilment accessible? Té prou marge per al compliment i els controls de govern? És la informació utilitzable com un artefacte forense per a fins legals?

4.3.3. Anonimització de les dades

Un dels punts més importants per assegurar que les dades no puguin ser explotades per altres organitzacions és l'anonimització de les dades. Si les dades personals són totalment anònimes, ja no són dades personals. En aquest context, l'anonimat significa que no és possible identificar un individu a partir de les pròpies dades o d'aquestes dades en combinació amb d'altres, tenint en compte tots els mitjans raonablement probables de ser utilitzats per identificar-los. No obstant això, no vol dir que no siguin útils, simplement que no es pot identificar l'individu. Un exemple seria que una empresa de màrqueting segmenti els seus clients per edats, no disposi dels identificadors dels seus clients però sí que en sabés els percentatges i trams per edat. Aquesta informació és útil per dirigir les seves campanyes de màrqueting.

Resulta molt il·lustratiu, en aquest punt, l'Informe 0283/2008 de l'Agència Espanyola de Protecció de Dades. En aquest informe, es va establir que serà suficient amb la mera possibilitat, fins i tot remota, que mitjançant la utilització amb caràcter previ, coetani o posterior de qualsevol mitjà (procés informàtic, programa, eina del sistema, etc.) la informació concernent als titulars de les dades en pugui revelar la identitat perquè quedi plenament sotmesa a la Llei orgànica de protecció de dades.

Els tres riscos claus de l'anonimització:

- **Singularització**: consisteix en la possibilitat d'extreure d'un conjunt de dades alguns registres que identifiquen una persona.

- **Vinculabilitat**: consisteix en la capacitat de vincular com a mínim dos registres d'un únic interessat o d'un grup d'interessats, ja sigui en la mateixa base de dades o en dues bases de dades diferents.

- **Inferència**: consisteix en la possibilitat de deduir amb una probabilitat significativa el valor d'un atribut a partir dels valors d'un conjunt d'altres atributs.

En alguns casos, les dades utilitzades per a l'anàlisi de dades s'anonimitzen per als propòsits de l'anàlisi. Per exemple, l'eina *smart steps* de Telefónica utilitza dades sobre la ubicació de telèfons mòbils en la seva xarxa, per tal de rastrejar el moviment de multituds de persones. Això pot ser utilitzat pels minoristes per analitzar quantes persones passen prop d'un lloc concret. Les dades que identifiquen els individus són eliminades abans de l'anàlisi, i les dades anònimes s'afegeixen per obtenir informació sobre la població en el seu conjunt i es combinen amb dades d'investigació de mercat d'altres fonts.*

*** Més informació a: https://luca-d3.com/**

Més enllà de la anonimització: polítiques ètiques

Si bé l'anonimització és un gran aliat per assegurar i atorgar privacitat a les dades, no és suficient. El requisit de processar dades personals de manera justa i legal ha de ser un deure de les organitzacions que exploten les dades, allò que es considera **polítiques ètiques**. S'inclou dins d'aquestes polítiques ètiques, per exemple, l'obligació d'informar les persones de a què es destinaran les seves dades personals. I s'han de complir, com a concepte de polítiques ètiques:

- **Minimització de dades**: el principi de la minimització de les dades és essencialment la idea que, amb poques excepcions, una organització només ha de processar les dades personals que realment necessita processar per aconseguir els seus propòsits.

- **Exactitud**: trobem riscos evidents per a les dades si es processen dades inexactes. Per tant, els controladors són responsables de prendre totes les mesures raonables per garantir que les dades personals siguin exactes.

- **Períodes de retenció de dades**: la idea que les dades personals no s'han de conservar durant més temps del necessari en relació amb els fins per

als quals es van recopilar o per als quals es processen posteriorment és fonamental per garantir-ne un tracte just.

- **Seguretat de dades**: els controladors són responsables d'assegurar que les dades personals es mantenen segures, tant contra amenaces externes (per exemple, *hackers* maliciosos) com contra amenaces internes (per exemple, empleats amb males intencions).

- **Responsabilitat**: el principi de rendició de comptes busca garantir el compliment dels principis de protecció de dades.

Qualsevol normativa ha d'anar orientada a l'adquisició de les polítiques ètiques dins les organitzacions; es tracta d'una mena de jurament hipocràtic, però dins de les organitzacions i referents a com aquestes fan servir les dades dels seus clients.

4.3.4. Monitoratge de les dades

Monitorar les dades es fonamenta en la definició de regles (de manera similar a la qualitat de dades) i en la revisió de patrons de comportament. La idea de fons és que cada registre o grup de registres a la taula o taules en qüestió es comproven mitjançant una sèrie de fases, i es rastreja el nombre d'infraccions de la regla. Aquest monitoratge ve acompanyat de la generació d'informes i d'una revisió contínua de les regles per identificar nous casos més enllà dels establerts, per mitjà del que es coneix com una auditoria forense.

Resum

En aquest mòdul didàctic, hem presentat el concepte de seguretat i privacitat de la dada, que té l'objectiu últim de disposar de dades segures i privades dins d'una organització.

En primer lloc, hem mostrat els nous reptes de seguretat a què ens enfrontem.

A continuació, hem revisat en què consisteix un programa de seguretat i privacitat de dades i les millors praxis, i ho hem contextualitzat dins del govern de la dada. Tot això amb focus en les persones, els processos i les dades.

En l'apartat següent hem descrit el tema de la privacitat, i ens hem centrat en la privacitat per disseny. Després, hem descrit les diferents lleis i normes pel que fa a la seguretat i privacitat de les dades.

Finalment, s'han revisat les tècniques i la tecnologia que formen part del que es coneix actualment com privacitat i seguretat de dades.

Glossari

afectat o interessat *m* Persona física titular de les dades que siguin objecte del tractament.

amenaça *f* Una amenaça informàtica és tota circumstància, esdeveniment o persona amb el potencial de causar algun dany a un sistema en forma de robatori, destrucció, divulgació, modificació de dades o negació de servei (DoS).

autenticació *f* Procediment de comprovació de la identitat d'un usuari.

big data *m* Conjunt d'estratègies, tecnologies i sistemes per a l'emmagatzematge, processament, anàlisi i visualització de conjunts de dades complexes.

xifrat *m* Codificació de dades mitjançant diferents tècniques matemàtiques que en garanteixen la confidencialitat en la transmissió.

confiança *f* Esperança ferma en què un sistema es comporti com correspon.

confidencialitat *f* Requisit de seguretat que indica que l'accés als recursos de sistema ha d'estar limitat exclusivament als usuaris amb accés autoritzat.

control d'accés *m* Mecanisme que, en funció de la identificació ja autenticada, permet accedir a dades o recursos.

criptografia *f* Disciplina que s'ocupa de la seguretat de la transmissió i l'emmagatzematge de la informació.

dada de caràcter personal *m* Qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus, susceptible de recollida, registre, tractament o transmissió, concernent a una persona física identificada o identificable.

dada dissociada *m* Dada que no permet la identificació d'un afectat o interessat.

drets d'accés *m pl* Autoritzacions concedides a un usuari per a la utilització dels diferents recursos d'un sistema, normalment informàtic.

disponibilitat *f* Requisit de seguretat que implica que la informació i els serveis del sistema continuïn en funcionament i que els usuaris autoritzats puguin accedir als recursos quan ho necessitin, on ho necessitin i en la forma en què ho necessitin.

encriptació *f* Mètode de xifrat o codificació de dades per evitar que els usuaris no autoritzats llegeixin o manipulin les dades. Només els individus amb accés a una contrasenya o clau poden desxifrar i utilitzar les dades. De vegades, el programari maliciós utilitza l'encriptació per ocultar-se del programari de seguretat. És a dir, el programari maliciós xifrat regira el codi del programa perquè sigui difícil detectar-ho.

filtració de dades *f* Una filtració de dades succeeix quan es compromet un sistema, i s'exposa la informació a un entorn no fiable. Les filtracions de dades sovint són el resultat d'atacs maliciosos, els quals miren d'adquirir informació confidencial que pot utilitzar-se amb fins delictius o amb altres fins malintencionats.

intrusió *f* Intromissió informàtica en la qual l'atacant aconsegueix obtenir un control complet sobre la màquina. Durant una intrusió, l'atacant pot obtenir i alterar totes les dades de la màquina, modificar el seu funcionament i fins i tot atacar noves màquines.

monitoratge *f* Desplegament de controls que asseguren que les dades segueixen complint amb les regles de negoci que defineixen la qualitat de les dades per a l'organització.

persona identificable *f* Tota persona la identitat de la qual es pugui determinar, directament o indirectament, mitjançant qualsevol informació referida a la seva identitat física, fisiològica, psíquica, econòmica, cultural o social. Una persona física no es considera identificable si aquesta identificació requereix terminis o activitats desproporcionats.

tractament de dades *m* Qualsevol operació o procediment tècnic, sigui o no automatitzat, que permeti la recollida, gravació, conservació, elaboració, modificació, consulta, utilització, modificació, cancel·lació, bloqueig o supressió i també les cessions de dades que resultin de comunicacions, consultes, interconnexions i transferències.

vulnerabilitat *f* Estat viciat en un sistema informàtic (o conjunt de sistemes) que afecta les propietats de confidencialitat, integritat i disponibilitat (CIA) dels sistemes. Les vulnerabilitats poden fer el següent:

- Permetre que un atacant executi ordres com un altre usuari.
- Permetre a un atacant accés a les dades, fet que s'oposa a les restriccions específiques d'accés a les dades.
- Permetre a un atacant fer-se passar per una altra entitat.
- Permetre a un atacant dur a terme una negació de servei.

Bibliografia

Chio, C.; Freeman, D. (2017). *Machine Learning and Security: Protecting Systems with Data and Algorithms*. Londres: O'Reilly.

Harari, Y. N. (2017). *Homo Deus*. Londres: Harvill Secker.

Hayden, L. (2015). *People-Centric Security: Transforming Your Enterprise Security Culture*. Nova York: McGraw Hill Professional.

Jacobs, J.; Rudis, B. (2014). *Data-Driven Security: Analysis, Visualization and Dashboards*. Nova York: Wiley.

O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Londres: Penguin Books Limited.

Payton, T.; Claypoole, T.; Schmidt, H. H. A. (2014). *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*. Nova York: Rowman & Littlefield Publishers.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. Nova York: W. W. Norton & Company.