Conceptes bàsics

Seguretat informàtica, anàlisi forense, sistema legal i estàndards

PID_00273499

Josep Maria Arqués Soldevila
Miquel Colobran Huguet
Erik de Luis Gargallo

Temps mínim de dedicació recomanat: 5 hores

Universitat Oberta de Catalunya

Josep Maria Arqués Soldevila

Enginyer en informàtica per la Universitat Autònoma de Barcelona. Va fer el treball de recerca al Departament d'Enginyeria de la Informació i de les Comunicacions (DEIC) de l'esmentada universitat. Ha treballat, com a professor ajudant i associat, al DEIC, i ha exercit de professor docent col·laborador de diverses assignatures de la Universitat Oberta de Catalunya. Actualment, exerceix d'analista en informàtica forense i especialista en gestió de la qualitat en ciències forenses.

Miquel Colobran Huguet

Doctor en informàtica per la Universitat Autònoma de Barcelona. És professor docent col·laborador a la UOC i coautor de diversos materials centrats en l'administració i seguretat de sistemes i informàtica forense. La seva recerca s'emmarca dins de la seguretat i del *social computing*, és a dir, com els ordenadors influeixen i són influïts per la societat, i com intervé la seguretat informàtica en aquest procés.

Erik de Luis Gargallo

Enginyer en informàtica i Màster en Seguretat de la Informació per la Universitat Oberta de Catalunya. Té més de 10 anys d'experiència en seguretat de la informació, auditories informàtiques, informàtica forense i enginyeria de seguretat. Actualment, treballa establint línies estratègiques en l'àmbit de la seguretat de les TIC i desplegament de les tecnologies que les assegurin. També és professor col·laborador de diversos cursos i assignatures de la Universitat Oberta de Catalunya.

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats pel professor: Jordi Serra (2020)

Primera edició: febrer 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Realització editorial: FUOC

Índex

Introducció

La informàtica s'ha convertit en l'eix vertebrador de totes les organitzacions i de bona part de la societat. La informació que circula per les seves xarxes és vital per al seu funcionament i, en conseqüència, s'ha convertit en el nou objectiu dels criminals del segle XXI. La informació és un valor en si mateixa i, per tant, un objecte cobejat pels nous delinqüents i una via per a provocar quantiosos danys. Així mateix, la seva destrucció pot comportar pèrdues econòmiques importants als seus propietaris, i fins i tot comprometre la continuïtat de les organitzacions.

Qualsevol organització s'ha de plantejar la implantació de mesures de seguretat en els sistemes d'informació (tant de caràcter tecnològic com organitzatiu) i haurà de cercar els objectius següents: evitar els incidents de seguretat i reduir les conseqüències dels que no es puguin evitar.

Malgrat això, convé ser conscient que, per més recursos que es destinin a millorar la seguretat, mai no es podrà aconseguir en la seva màxima expressió, ja que sempre s'estarà exposat a patir algun tipus d'incident que provocarà algun impacte en l'organització (en més o menys mesura). Per tant, l'adequat és que les organitzacions es plantegin com actuar davant un incident de seguretat. La gestió d'incidents permet a les organitzacions estructurar un protocol d'actuació davant una incidència per a minimitzar-ne l'impacte i el temps de resolució.

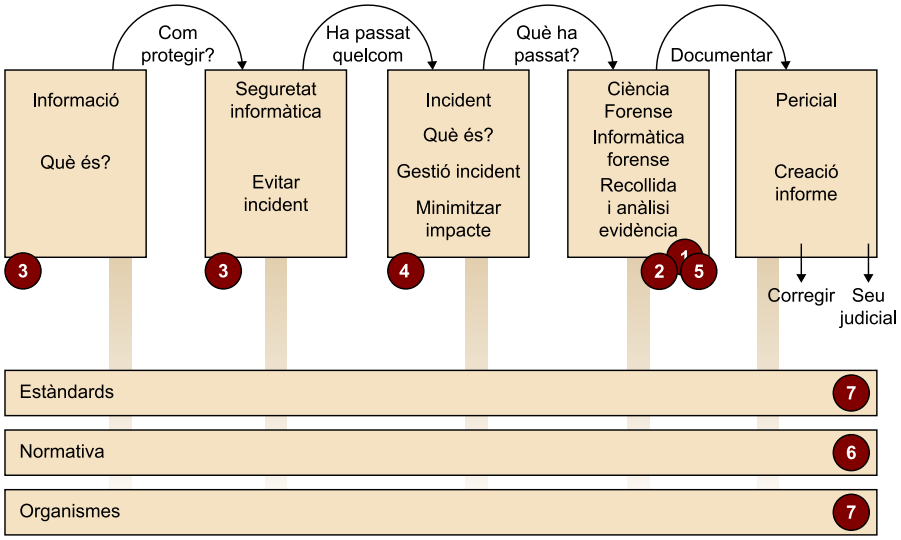
Quan es produeix un incident, s'ha de determinar què ha passat. El conjunt de tècniques, conegut de manera genèrica com a informàtica forense, a més d'esclarir els fets, ens permetrà reunir proves de manera ordenada i metòdica. Aquestes, probablement, hagin de tenir valor probatori per a poder-les utilitzar posteriorment en l'àmbit processal (davant d'un jutge).

Les tècniques d'informàtica forense no només són útils a l'hora d'aplegar les proves d'un incident de seguretat, sinó que en general també es poden emprar per a preservar, analitzar i presentar (mitjançant un informe pericial) qualsevol evidència continguda en un dispositiu digital o emmagatzemada a la xarxa. L'informe mitjançant el qual es presenten, de manera ordenada, aquestes evidències, pot anar, doncs, adreçat a múltiples destinataris: jutges, caps d'una empresa, tècnics, etc.

Finalment, no s'ha de perdre de vista que tant la protecció de la informació com les tècniques de seguretat i la informàtica forense estan molt lligades a estàndards i al sistema legal.

El text relaciona estàndards, normativa i organismes amb els 5 conceptes bàsics que veurem en el mòdul. En vermell hi ha els apartats on apareixen cadascun d'aquests conceptes.

Figura 1. Representació dels diferents conceptes, relació i lloc del mòdul en què es desenvolupen



Objectius

Amb el treball que s'ha de fer sobre aquests materials didàctics, pretenem que l'estudiant assoleixi els objectius següents:

1. Saber què són les ciències forenses i en especial la informàtica forense.

2. Comprendre la relació que es produeix entre la informació, la seguretat informàtica, l'incident, l'anàlisi forense i el sistema legal.

3. Conèixer la regulació legal més important a tenir en compte.

4. Adquirir les nocions bàsiques en seguretat informàtica, gestió d'incidents i el seu tractament mitjançant les ciències forenses.

5. Facilitar la comprensió del context de seguretat de la informació i el vocabulari bàsic en aquest àmbit.

6. Conèixer un vocabulari tècnic bàsic en aquest àmbit.

7. Saber quins són els fonaments bàsics de seguretat i la legislació vigent en protecció de dades.

8. Tenir coneixement de l'origen de la informàtica forense i de la seva vinculació amb la criminalística.

9. Tenir coneixement sobre els incidents de seguretat i la seva gestió.

10. Tenir coneixement dels delictes informàtics i la legislació associada.

1. Disciplina forense

La paraula forense és llatina (*forensis*), «pertanyent o relatiu al fòrum». L'origen és de l'antiga Roma on l'acusació, l'argumentació i les proves d'un crim requerien ser presentades en un fòrum de persones considerades notables. Eren aquestes les que en determinaven el veredicte.

Ràpidament la fonamentació dels casos va requerir altres coneixements, com per exemple el coneixement mèdic (medicina forense). Al llarg de la història, s'han desenvolupat altres disciplines com la criminologia, la psiquiatria forense i la criminalística a partir de la medicina forense.

1.1. Ciència forense

Coneixem per ciència forense aquella que té per objecte l'aplicació de pràctiques científiques dins el procés legal. Normalment, la ciència forense és referida només amb el terme **forense**, el qual, acceptat arreu del món, s'usa sovint com a sinònim de legal. La ciència forense inclou tant la branca civil del dret com la penal.

Ciències forenses

El conjunt estructurat i sistematitzat de coneixements, de caràcter tècnic i científic, generats per la investigació i anàlisi dels indicis d'un fet presumptament delictiu, amb la finalitat de presentar aquests resultats davant l'autoritat jurídica corresponent i coadjuvar en la prevenció del delicte, i en la procuració i administració de la justícia.

És a dir, qualsevol disciplina els principis científics de la qual s'utilitzin per a ajudar la justícia.

La ciència forense s'ha expandit tant, que actualment hi ha moltíssimes branques de les ciències que li donen suport en la resolució dels problemes que planteja el dret. A títol orientatiu, algunes són les següents[1]:

(1)La darrera en incorporar-se a aquesta llarga llista ha estat la informàtica forense.

- **Comptabilitat forense**: adquisició, interpretació i estudi de la comptabilitat.

- **Informàtica forense**[2]: recuperació, reconstrucció i interpretació dels mitjans digitals que estan emmagatzemats en un ordinador, per a la seva utilització com a prova.

(2)El seu ús i la seva utilitat s'han estès molt més enllà dels tribunals, com veurem més endavant.

- **Economia forense**: adquisició, estudi i interpretació de les proves relacionades amb el dany econòmic. Inclou la determinació de la pèrdua de beneficis i guanys, el valor del negoci i la pèrdua de beneficis, etc.

- **Enginyeria forense**: reconstrucció, estudi i interpretació d'una fallada mecànica o estructural (d'edificis, ponts, etc.).

- **Lingüística forense**: estudi i interpretació de la llengua per a utilitzar-la com a prova jurídica.

- **Psicologia i psiquiatria forense**: estudi, avaluació i identificació de malalties relacionades amb el comportament humà i la seva ment, per a l'obtenció de proves jurídiques.

- **Odontologia forense**: estudi de les dents, específicament la unicitat de la dentició.

- **Patologia forense**: combina les disciplines de la medicina i la patologia per a determinar les causes de les lesions o de la mort.

- **Toxicologia forense**: estudi, avaluació i identificació dels efectes dels verins, productes químics o de les drogues en el cos humà.

1.2. Informàtica forense

L'anàlisi forense en informàtica va sorgir de la necessitat de poder aportar elements rellevants en els processos judicials en els quals les noves tecnologies es trobaven presents, bé com a objectiu (per exemple, una intrusió que comporti danys en un sistema informàtic) o bé com a mitjà (per exemple, l'enviament de correus electrònics amenaçadors a un personatge públic). Així doncs, és una ciència forense que s'ocupa de l'ús dels mètodes científics aplicables als sistemes informàtics[3].

(3)Tot dispositiu físic o lògic utilitzat per a crear, generar, enviar, rebre, processar, comunicar o emmagatzemar, de qualsevol forma, missatges de dades.

La informàtica forense és la **ciència forense** que s'encarrega d'**assegurar, identificar, recollir, preservar, analitzar i presentar** l'evidència[4] digital, de manera que aquesta sigui acceptada en un procés judicial.

(4)Qualsevol element que proporcioni informació de la qual es pugui inferir alguna conclusió o bé que constitueixi una troballa relacionada amb el fet que s'investiga.

No obstant això, la informàtica forense també s'ha revelat com una àrea de la informàtica amb moltes més utilitats, de manera que la definició anterior només s'aplica a part del seu ús. Així doncs, també podríem considerar la informàtica forense sota la definició següent:

La informàtica forense investiga els sistemes d'informació a fi de detectar-hi evidències de vulnerabilitat.

Aquesta definició subratlla que s'apliquen les tècniques, els procediments i les eines de maquinari i programari necessàries per a determinar dades i fets rellevants. Aquestes tècniques es poden dur a terme abans o després que es produeixi un succés i amb finalitats judicials o no.

Sota aquesta òptica, la informàtica forense apareix amb diferents finalitats i objectius:

		Objectius	
		Preventiu	**Correctiu**
Finalitat	Probatòria	---	Hi ha hagut un incident i s'han de reunir proves per a un procés judicial.
	Auditora / monitorització	Verificació que el sistema informàtic està funcionant correctament usant tècniques forenses.	Hi ha hagut un incident i s'han de conèixer els fets per a modificar les polítiques de seguretat.

- **Objectius preventius**: es pretén anticipar al problema. En aquest escenari la informàtica forense forma part del sistema de seguretat. S'utilitza per a verificar i per a auditar. Mitjançant la pràctica de diverses tècniques es verifica que els sistemes de seguretat instal·lats compleixen amb certes condicions bàsiques de seguretat. Els resultats de les auditories serviran per a poder corregir els errors trobats i poder millorar el sistema.

- **Objectius correctius**: aquest escenari suposa la detecció d'un incident. S'ha de conèixer la causa per a poder aplicar les mesures correctives que permetin evitar nous incidents per aquesta mateixa via.

Vegeu també

Consulteu l'apartat «Gestió d'incidents de seguretat» per a conèixer les etapes amb més detall.

- **Finalitat probatòria**: especialment si l'incident ha ocasionat danys, estem davant un escenari que s'ha de gestionar amb molta cura. L'obtenció de proves és molt important. La informàtica forense permet realitzar un rastreig de la intrusió, descobrir el dany realitzat i recopilar les evidències digitals. En aquest context parlem de recuperació d'informació i fins i tot de descobriment d'informació. Podem arribar a conèixer l'origen de l'atac i els canvis realitzats en el sistema (fugues d'informació, pèrdua o manipulació de dades). Posteriorment, les evidències trobades podran ser utilitzades en el marc legal.

- **Finalitat auditora**: periòdicament s'ha de comprovar, a tots els nivells, la robustesa del sistema informàtic. Les tècniques forenses s'han revelat com extremadament útils en aquests escenaris.

1.3. La informàtica en el delicte

En l'àmbit de la informàtica forense el delicte s'anomena col·loquialment *ciberdelicte*, en tant que d'alguna manera està quasi sempre vinculat a les tecnologies de la informació. És especialment destacable que hi ha poques àrees de delinqüència on no és possible aplicar la investigació forense lligada a les TIC.

Dins d'aquest àmbit, els ordinadors poden constituir:

- **Objecte** del delicte. Per exemple, amb atacs de pirateria, denegació de servei, intrusió informàtica[5] o *hacking*[6].

- **Mitjà** per cometre el delicte. És el cas més corrent, ja que inclou la majoria de delictes «tradicionals» en què s'hi ha incorporat la tecnologia (ja sigui usant ordinadors o dispositius mòbils com telèfons o tauletes). El ventall és molt variat i es pot trobar, per exemple, l'extorsió, l'estafa (*phishing*), el tràfic de drogues, la pornografia infantil, el *ciberbulling*, el ciberassetjament o el *sexting*.

- **Element material probatori**[7] en un delicte. En molts delictes els ordinadors apareixen a «l'escena d'un delicte» de manera circumstancial. Així, per exemple, poden contenir proves en forma de missatges de correu electrònic o fitxers rellevants per a delictes com assassinats, segrestos, consultes a Internet, etc.

(5) Accés a un sistema informàtic «saltant-se» la seguretat establerta. Article 197bis del Codi Penal.

(6) Accedir de manera il·legal a dades emmagatzemades en un ordinador o servidor.

(7) Objecte que serveix per a provar uns fets (per exemple una pistola que es troba en l'escena del crim).

2. Marc conceptual de la informàtica forense

2.1. Breu ressenya històrica

Abans del 1985. De fet, el terme simplement no existia. Des dels anys seixanta fins a principis dels anys vuitanta, els ordinadors eren principalment un aparell industrial, propietat i operat per empreses, universitats, centres de recerca i agències governamentals. Necessitaven una gran infraestructura física, incloent quantitats massives d'energia i aire condicionat, i un personal dedicat i altament qualificat. El llibre de Donn Parker (1976), *Crime by Computer*, és el primer en descriure l'ús de la informació digital per a investigar i processar delictes comesos amb l'ajut d'un ordinador. El govern i l'FBI van notar que els criminals començaven a fer servir la tecnologia com a mitjà per cometre delictes. El 1984, l'FBI va iniciar un programa denominat Programa de Mitjans Magnètics que va ser l'origen del CART (*Computer Analysis and Response Team*), un equip d'anàlisi per ordinador.

Dècada del 85 al 95. L'arribada de l'ordinador personal a la dècada dels 80 va provocar l'aparició de molts ordinadors en llars i petites organitzacions, i va posar de relleu l'existència de problemes de seguretat.

> Entre els afeccionats a la informàtica hi havia gent de moltes organitzacions. Algunes de les persones clau van ser Mike Anderson, Danny Mares i Andy Fried de l'IRS; Ron Peters i Jack Lewis del servei secret dels Estats Units; Jim Christy i Karen Matthews del Departament de Defensa; Tom Seipert, Roland Lascola i Sandy Mapstone de les agències locals d'aplicació de la llei dels EUA; i els canadencs, Gord Hama i Steve Choy.

El 1988, Michael Anderson, un agent de l'IRS (*Internal Revenue Service*), va crear juntament amb un grup d'especialistes i tres companyies, un grup especialitzat en la recuperació de dades. També aquest any es va crear l'Associació Internacional d'Especialistes en la Investigació Computacional (IACIS).

El 1993, l'FBI va acollir la Primera Conferència Internacional sobre evidència informàtica, on hi van assistir representants de 26 països. El 1995 la segona conferència es va celebrar a Baltimore i es va fundar l'Organització Internacional per a l'Evidència Computacional (IOCE).

> Es volia proveir un fòrum internacional per a l'intercanvi de la informació relacionada amb la investigació computacional i la informàtica forense.

Els casos investigats eren molt bàsics. Gran part de l'enfocament era la recuperació de dades de manera independent d'ordinadors. Internet encara no era popular, però els delinqüents feien servir l'accés telefònic per a comprometre ordinadors. Els temes de les investigacions sobre delictes per ordinador eren

generalment delictes tradicionals que utilitzen ordinadors per donar suport a les seves activitats o jovent que van utilitzar les seves habilitats tècniques per a obtenir accés a ordinadors de manera il·legal.

No obstant això, es va veure la necessitat i el potencial de la ciència forense digital. Es va crear, per exemple, el programa Especialista en Recuperació d'Evidències Informàtiques (SCERS) a l'agència tributària, el Programa d'Agents Especials de Delictes Electrònics (ECSAP) al Servei Secret dels Estats Units, l'equip de resposta i d'anàlisi computacional (CART[8]) a l'FBI. Cada organisme ho feia a la seva manera i la majoria de les investigacions forenses digitals van ser realitzades per persones amb formació mínima, sovint amb equipament personal i sense cap tipus de supervisió o control de qualitat formal.

[8]El CART va començar a operar el 1991. Va ser la resposta a l'increment del nombre de casos en què estava involucrada l'evidència digital. Proporcionava exàmens dels ordinadors i discos (realitzats en els laboratoris de l'FBI) com a suport a investigacions i judicis.

Alguns països varen començar a crear associacions i entitats, i aquestes organitzacions oferien formació. La formació forense es va desenvolupar i sistematitzar tot oferint una formació assequible i de qualitat. Com a conseqüència, la demanda d'aquesta formació es va disparar. Mentrestant la comunitat acadèmica no estava interessada en el camp, amb dues excepcions notables: Gene Spafford i Dorothy Denning.

Dècada del 95 al 2005. És l'etapa de la formalització de la ciència forense digital. L'explosió de la tecnologia, l'arribada de la telefonia cel·lular (molt incipient), Internet com a eix vertebrador i la seva massiva difusió, van canviar l'escenari. A finals del 2005 pràcticament tothom ja tenia correu electrònic i alguna manera de poder accedir a la xarxa. Això va ser un entorn que els delinqüents varen saber aprofitar molt bé.

Arran d'això, en pocs anys hi va haver una explosió de casos de pornografia infantil. El primer, el cas George Stanley Burdynski, Jr., el 1993, va revelar que els ordinadors s'utilitzaven per fer trànsit il·legal d'imatges de menors. Pocs anys més tard, tots els organismes hi tenien grups dedicats. El resultat de tot aquest treball va suposar la confiscació de volums digitals cada vegada més grans i va ser un dels principals motors en el creixement de la investigació forense digital.

> Al 1999, el CART treballava ja en més de 2.000 casos anuals, i examinava de l'ordre de 17 terabytes de dades. Tres anys més tard, el 2003, el CART treballava en 6.500 casos i estava examinant 782 terabytes de dades.

Mentrestant, les eines forenses van canviar radicalment. De les eines en línia de comanda i muntatges casolans es va passar a eines complexes, amb entorns gràfics i paquets d'interfície d'usuari. La primera de les noves eines va ser Expert Witness, un producte dissenyat per Andy Rosen per a la tècnica forense de Macintosh que va evolucionar a EnCase. EnCase, juntament amb Forensic ToolKit (FTK), són ara eines forenses estàndards.

Del 2005 fins ara. És des del 2005 que la investigació forense digital ha crescut en profunditat i amplitud. Té molts més practicants i hi una gran varietat de formació reglada molt estricte que permet obtenir certificacions que avalen la professionalitat de l'informàtic forense.

El 2006, els tribunals dels Estats Units van adoptar noves normes per al procediment civil que definien la informació digital com a nova forma d'evidència i varen implementar un sistema obligatori anomenat descobriment electrònic o eDiscovery, per a tractar proves digitals.

Nota

El 2007 l'FBI va anunciar que la seva anàlisi informàtica i l'equip de resposta (CART) van examinar més de 2,5 petabytes de proves.

Pràcticament tots els dispositius que utilitzen electricitat ara tenen algun tipus d'emmagatzematge digital, les xarxes connecten molts dels dispositius que utilitzem en la nostra vida quotidiana. Això, al seu torn, ha impulsat el desenvolupament de molts serveis basats en xarxa i web, inclosa la informàtica en núvol.

Els professionals de la seguretat de la informació ara reconeixen la ciència forense digital com una de les habilitats bàsiques. Tot i que els seus objectius i les seves necessitats sovint difereixen d'aquests, pel que fa a l'aplicació de la llei, els conceptes i les eines sovint són idèntics.

Les eines forenses han seguit evolucionant, i s'han mogut a l'entorn de la xarxa i fins i tot al núvol. Aquestes mateixes eines s'adapten als nous entorns i apareixen els laboratoris virtualitzats (utilitzant productes com ara VMWare) i xarxes d'àrea d'emmagatzematge (SAN).

En menys de quaranta anys, la ciència forense digital ha passat de ser un coneixement desenvolupat i difós per uns quants professionals, al seu estat actual, una disciplina sòlida i ben fonamentada.

La investigació forense al núvol (2019)

La demanda de computació i serveis al núvol està augmentant a causa de la popularitat dels dispositius digitals, dels dispositius mòbils i de l'ús intensiu d'Internet.

Així doncs, apareixeran usos maliciosos d'aquests serveis. Aquest tipus d'investigació forense està encara en una etapa molt inicial.

2.2. Àmbit d'actuació

Actualment la informàtica forense ja no tracta només del contingut de correus electrònics, documents i altres fitxers que puguin ser d'interès per als investigadors, sinó també les metadades associades a aquests fitxers i la seqüència temporal d'esdeveniments. Un examen forense informàtic pot desvelar quan un document va aparèixer per primera vegada en un ordinador, quan es va editar per última vegada, quan es va desar o imprimir per última vegada i quins usuaris van dur a terme aquestes accions.

L'àmbit més conegut és el judicial, però la informàtica forense s'ha difós més enllà de l'àmbit criminalístic i s'utilitza també en altres vessants, com per exemple:

1) Persecució criminal: Evidència incriminatòria que pot ser usada per a processar delictes i crims, incloent-hi homicidis, frau financer, tràfic i venda de drogues, evasió d'impostos o pornografia infantil.

2) Litigació civil: Casos relatius a frau, discriminació, assetjament, divorci, etc. Estudis jurídics que necessiten demanar informació, ja sigui per presentar-la davant d'un tribunal, o bé per negociar amb les parts un acord extrajudicial, rescabalament, una renúncia, etc.

3) Investigació d'assegurances: L'evidència trobada en ordinadors pot ajudar a les companyies d'assegurances a disminuir costos de reclamacions per accidents o compensacions.

4) Temes corporatius: Es pot recollir informació en casos que tracten sobre assetjament sexual, robatori, mal ús o apropiació d'informació confidencial o propietària, o espionatge industrial. Empreses que realitzen judicis laborals amb els seus empleats o amb els seus associats per conflictes d'interessos.

5) Finalitat preventiva: Com a mesura preventiva serveix a les empreses per a auditar, mitjançant la pràctica de diverses proves tècniques, que els mecanismes de protecció instal·lats i les condicions de seguretat aplicades als sistemes d'informació són suficients. Permet detectar les vulnerabilitats de seguretat per tal de corregir-les.

6) Recuperació de dades: Situació en la qual cal recuperar informació que ha estat eliminada per error, durant una pujada de tensió, o una caiguda de servidors. En aquest escenari habitualment es coneix la informació que s'està buscant.

7) *Network forensics*: Saber com un atacant ha accedit al sistema informàtic i les accions que hi ha pogut dur a terme.

8) Quan la investigació forense s'hagi de presentar davant d'un jutjat s'han de prendre mesures especials. Una de les més importants és assegurar que l'evidència ha estat correctament recollida i documentar la cadena de custòdia, des de l'escena del delicte fins al jutjat per garantir d'aquesta manera la integritat de l'evidència digital.

Vegeu també

Ho podeu veure amb més detall en el mòdul «Fases i metodologia de l'anàlisi forense».

9) Dins de l'àmbit de la investigació de delictes, la informàtica forense hi serà present sempre que hi hagi elements digitals involucrats. Per tant, pot formar part de qualsevol investigació per delictes no relacionats amb les tecnologies

de la informació. Com a exemples, pot ser necessari en un robatori on s'hagin usat telèfons mòbils, en delictes on hi hagi correus electrònics o en robatori o falsificació d'informació en bases de dades.

La informàtica forense esdevé imprescindible des del moment en què gran part de la informació generada es troba emmagatzemada en suports digitals.

2.3. Principis de la informàtica forense

Com que la informàtica forense és una disciplina de la ciència forense, comparteix molts dels principis claus a l'hora d'examinar i manipular la informació. Aquests principis[9] són:

[(9)]Elaborats per l'Association of Chief Police Officers (ACPO) i seguits per la policia britànica.

- **Evitar la contaminació**: no es realitzarà cap acció que modifiqui les dades contingudes en un ordinador o dispositiu d'emmagatzematge. Per a poder obtenir una anàlisi veraç i precisa, la informació s'hauria d'emmagatzemar en un mitjà el més estèril possible.
  Amb l'evidència electrònica (imatges de discos i memòria, fitxers de dades i executables, etc.) la pràctica consisteix a obtenir *hashes* de la informació en el moment de l'obtenció, de manera que es pugui comprovar en qualsevol moment si l'evidència ha estat modificada.
  Els algoritmes de *hashing* acceptats com a estàndards són l'MD5 i l'SHA-1. Tot i que s'hi han descobert vulnerabilitats, segueixen utilitzant-se, ja que la possibilitat d'obtenir una col·lisió és infinitesimal.

- **Actuar metòdicament**: l'investigador ha de ser responsable dels seus procediments i del desenvolupament de la investigació, per tant, és important que es documentin clarament els processos, les eines i metodologies d'anàlisi emprats durant tot el procés.

- **Tenir control sobre l'evidència**: s'ha de mantenir en custòdia qualsevol evidència relacionada amb el cas, i documentar així mateix qualsevol esdeveniment que la pugui afectar: qui va lliurar l'evidència, com es va transportar, qui va tenir accés a l'evidència, etc. D'aquesta manera, un tercer analista independent hauria de ser capaç d'examinar aquests registres i assolir el mateix resultat.

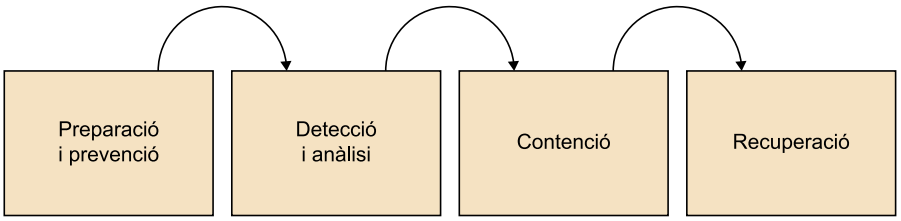
- **En circumstàncies excepcionals**: en cas que s'hagi d'accedir a les dades originals contingudes en un ordinador o dispositiu d'emmagatzematge, la persona ha de ser competent en aquesta pràctica, i explicar la rellevància i les implicacions de les seves accions.

2.4. La informàtica forense en les organitzacions

Actualment, la informàtica forense té una rellevància considerable dins de les organitzacions i hi juga un paper clau en la seguretat. Des del punt de vista de l'organització, la informàtica forense s'ha d'integrar dins de la seguretat global del sistema informàtic. Aquest, al seu torn, depèn del bon disseny de les mesures de prevenció, detecció, contenció i recuperació dels **incidents**[10] **informàtics**.

[10]Entendrem per incident qualsevol fet anòmal que afecti el funcionament del sistema. En propers apartats detallarem més el concepte.

Figura 2. Esquema bàsic de la gestió d'incidents



- **Mesures de prevenció**: aquestes mesures integren tots els aspectes relatius a evitar que es produeixi un incident o succés. La informàtica forense s'integra en aquesta etapa a través de les auditories i les seves corresponents tècniques com, per exemple, els anomenats *penetration tests*, i el *Black box*, *Gray box* o el *White box*, per a avaluar l'estat del sistema[11].

  Una de les mesures organitzatives fonamentals és el pla de prevenció de riscos. Per a preparar un pla de risc, el primer pas és identificar els riscos a què estem sotmesos. Per això, hem de determinar quins riscos ens poden provocar una fallada en el sistema i determinar quins són probables, quins són possibles i quins són crítics. Després, hem de determinar les prioritats d'aquests riscos basant-nos en l'entorn de la nostra empresa. És a dir, tot i que els riscos informàtics són semblants per a la majoria de les empreses, la prioritat que se'ls assigna depèn de l'ús informàtic que duu a terme l'empresa. Una vegada tenim identificats i prioritzats els riscos, hem de decidir quins generaran un pla de risc i quins no cal tenir implementats en un pla com aquest, a més de les característiques que ha de tenir aquest pla.

[11]No és objecte d'aquests materials detallar aquestes tècniques, les quals utilitzen la informàtica forense com un element més per a complir els seus objectius.

- **Mesures de detecció**: atès que és inevitable que l'incident succeeixi tard o d'hora, les mesures de detecció serveixen per a detectar violacions de la seguretat del sistema. La informàtica forense s'integra perfectament en eines com ara els analitzadors de trànsit, *honeypots* i *honeynets*, o els IDS[12].

[12]Un cop més, no és objecte d'aquests materials detallar aquestes tècniques.

- **Mesures de contenció**: un cop detectat i identificat l'incident, cal procurar per tots els mitjans restringir-ne l'expansió. Per a això, s'han de prendre mesures protocol·litzades. Les tècniques de *network forensics* ajuden a identificar l'origen de l'incident, i per tant a contenir i eliminar el problema.

- **Mesures de recuperació**: finalment, s'han de determinar l'origen de l'atac i els danys ocasionats (entre altres), i emprendre accions legals, si escau. Aquest és el camp de treball de la informàtica forense (en concret de l'anàlisi forense). Així mateix, també és de vital importància la recuperació de l'estat normal del sistema informàtic[13].

  En l'àmbit organitzatiu, el pla de contingència o recuperació és molt important, ja que ha de detallar els passos a seguir per a recuperar-nos de diferents situacions de crisi, i indicar clarament el que cal fer, el que no s'ha fer i qui és responsable de cada pas. És important també tenir present durant la recuperació el poder estar segurs que som capaços d'acumular els indicis i les dades que facilitaran les tasques d'informàtica forense i el posterior sanejament de la vulnerabilitat explotada.

[13] Forma part del pla de contingència o *Disaster Recovery Plan* (DRP), molt vinculat a les polítiques de còpia de seguretat.

3. Seguretat informàtica

El concepte *seguretat* en porta associat un altre que li dona sentit: *valor*. Només protegim allò que creiem que té un valor important per a nosaltres i, per tant, la seguretat va íntimament associada al valor que li donem a l'objecte o als objectes protegits.

Així doncs, si en el sistema informàtic ens preocupa tant la seguretat, què volem protegir?

3.1. El valor de la informació

Els tres elements bàsics que desitgem protegir en qualsevol sistema informàtic són el **programari**, el **maquinari** i les **dades** o la **informació**.

- Per **maquinari** entenem tots els elements físics d'un sistema informàtic, com servidors, estacions de treball, cablejat, cintes de còpia, DVD, etc.
- Per **programari** entenem tots els programes que fan funcional el maquinari, tant els sistemes operatius com les aplicacions.
- Per **dades** entenem el conjunt d'informació lògica que manegen tant el programari com el maquinari.

Dades i informació

Hi ha una diferència en aquests dos conceptes, tot i que sovint s'usen de manera indistinta.

Dades: conjunt discret de factors objectius sobre «alguna cosa». Pot ser un nombre, una lletra…

Informació: la reunificació i estructuració de les dades en un context que li dona sentit.

Exemple

Dada: 17,

Informació: En Joan té 17 anys. El nombre de persones a l'habitació és de 17…

En essència, el que més ens importa protegir, perquè és propi de l'organització, és la informació, ja que sens dubte constitueix un dels actius més grans de qualsevol organització. Per això, es destinen molts recursos a la protecció i al seu ús de forma controlada, ja que en molts casos, a més constitueix el seu coneixement[14].

[14] Saber fer en termes empresarials.

El problema més gran de la informació, per la seva naturalesa, és la dificultat de protegir-la, ja que no es pot protegir com els objectes materials, dipositant-la en un recinte custodiat. Això comporta que la informació sigui susceptible de còpia, robatori, destrucció, etc., amb les conseqüents pèrdues que pot suposar per a l'organització.

La informació és un dels béns més grans de l'organització.

La informació, tot i ser un dels béns que requereix més esforç quant a protecció, no és l'únic bé a protegir. En seguretat hem de considerar altres béns com ara els equips físics.

3.2. Què és la seguretat informàtica?

Encara que sigui de forma intuïtiva, tothom entén que un sistema informàtic es considerarà segur si es troba lliure de tot risc i dany. Tot i això, no és gens fàcil formalitzar el concepte de *seguretat informàtica*. L'entendrem com el conjunt constituït per les diverses metodologies, els documents, el programari i maquinari, que determinen que els accessos als recursos d'un sistema informàtic siguin emprats únicament pels elements autoritzats a fer-ho. Com que és totalment impossible garantir la seguretat o inviolabilitat d'un sistema informàtic, en lloc de l'inassolible concepte de *seguretat* és preferible emprar el terme de *fiabilitat*. Per tant, no podrem entendre la seguretat informàtica com un concepte tancat, conseqüència de l'aplicació de mètodes, sinó com un procés que es pot veure compromès en qualsevol moment de la manera més insospitada.

En general, doncs, direm que un sistema informàtic és fiable quan se satisfan les tres propietats següents:

- **Confidencialitat**: els recursos que integren el sistema només poden ser accedits pels elements autoritzats a fer-ho. Per recursos del sistema no només entendrem la informació, sinó també qualsevol recurs en general: impressores, processador, etc.

- **Integritat**: els recursos del sistema només poden ser modificats o alterats pels elements autoritzats a fer-ho. La modificació inclou diverses operacions, com l'esborrament i la creació, a més a més de totes les possibles alteracions que es puguin realitzar sobre un objecte.

- **Disponibilitat**: els recursos del sistema han de poder ser accessibles als elements autoritzats.

Triada CIA / CID

Les tres propietats juntes es coneixen com la tríada CID, per les inicials:
- **C**onfidencialitat
- **I**ntegritat
- **D**isponibilitat
- Aquestes mateixes sigles en anglès formen l'acrònim CIA.

Com podem imaginar, és molt difícil trobar un sistema informàtic que maximitzi les tres propietats. Normalment, i segons l'orientació del sistema, es prioritzarà algun dels tres components. Per exemple, en un sistema que emmagatzemi dades de caràcter personal, l'element a prioritzar és la confidencialitat

de la informació, tot i que també hem de tenir molt present el de la preservació (en la mesura que sigui possible) de la integritat i la disponibilitat. Observem que no serveix de res garantir la confidencialitat per mitjà d'algun mètode criptogràfic, si permetem que un intrús pugui esborrar fàcilment la informació emmagatzemada en el disc dur del servidor (atac contra la integritat).

Existeix alguna altra definició, que sense ser tan «informàtica», ens pot ser útil conèixer. Aquesta observa la seguretat informàtica en un entorn de treball.

La seguretat informàtica és el conjunt de regles, plans i accions encaminats a garantir tres objectius:

- La capacitat de treball (disponibilitat), és a dir, que el sistema sigui operatiu en tot moment, o hi hagi mecanismes de contingència que permetin un ritme de treball acceptable mentre se soluciona el problema.

- La integritat de la informació (consistència), de manera que la informació a disposició de l'usuari romangui inalterada.

- La confidencialitat de les dades (confidencialitat, control d'accés, autenticació), perquè cada usuari tingui accés només a la informació que li pertoca.

I per a protegir millor el nostre sistema cal que tinguem una bona idea de com se'l pot atacar, a fi de detectar-ne les vulnerabilitats, mirar de posar-hi solució i tenir plans de contingència detallats i provats per a una ràpida i satisfactòria solució de l'incident.

3.3. Conceptes bàsics de la seguretat

El primer pas en seguretat informàtica és tenir molt clar de què ens volem protegir i de què no volem, o no podem (cost, dificultat i/o impossibilitat) protegir-nos. La seguretat informàtica té diferents àmbits, entre els que destacarem l'accés físic als dispositius, cablejat o còpies de seguretat, els processos, les operacions i els permisos d'accés, l'arquitectura i la seguretat de la xarxa, la redundància del maquinari, la integritat de les dades, i els permisos dels usuaris. La seguretat ha de funcionar correctament en tots els diferents àmbits. El sistema és tan segur com el menys resistent dels seus elements. Vegem algunes definicions i conceptes bàsics.

Fortalesa de la seguretat

Un sistema informàtic és tan segur com ho és la seva baula més dèbil.

En altres paraules, el punt més feble de la seguretat serà el punt d'entrada.

3.3.1. Vulnerabilitat, amenaça i risc

- **Vulnerabilitat**: debilitat en qualsevol dels punts dels sistemes d'informació (accés, dades, subministraments, programes, maquinari, disseny, etc.) que podria ser explotada accidentalment o intencionadament, i que comportaria una violació de la política de seguretat de sistemes.

- **Amenaça**: indici pel qual es manifesta un perill.

- **Risc**: perill incert.

A tall d'exemple, podem dir que deixar el nostre terminal de treball sense estar protegit per una contrasenya és una vulnerabilitat que algú (amenaça) pot aprofitar i correm el risc que entri en el nostre compte i es faci passar per nosaltres o ens esborri o modifiqui fitxers.

3.4. Tipus de seguretat

Distingim dos tipus de seguretat, l'activa i la passiva.

La seguretat activa cerca protegir i evitar possibles danys en els sistemes informàtics, que comprenen les dades, el programari i el maquinari, és a dir, en els sistemes i les dades que emmagatzemem. Volem evitar els problemes abans no passin.

La seguretat passiva cerca minimitzar els impactes causats per *malware*, accidents (talls de corrent o xarxa, mal funcionament de dispositius crítics, etc.), usuaris (autoritzats o no autoritzats), i qualsevol altre possible agent pertorbador. Volem minimitzar les conseqüències un cop els accidents han passat i recuperar-nos-en al més ràpidament possible.

3.4.1. Activa

Amb la seguretat activa ens protegim de tots els possibles atacs maliciosos que ens puguin venir, bàsicament per la xarxa, i prenem consciència que cal implementar mesures addicionals perquè els intrusos no tinguin accés a la informació de l'organització.

Per a protegir-se de lectures no volgudes de la informació desada en un fitxer o de les dades que circulen per Internet, n'hi ha prou de xifrar els missatges o arxius amb un parell compost per una clau pública i una altra de privada, perquè ningú a qui no s'hagi donat permís exprés abans no pugui accedir a la informació.

D'altra banda, totes les aplicacions que s'han d'executar per a tenir l'accés mitjançant la xarxa les podem autenticar. És a dir, podem demanar que l'usuari s'autentiqui per a utilitzar aquestes aplicacions.

> Per exemple, en comptes d'utilitzar el protocol HTTP d'intercanvi de fitxers per Internet, es pot fer servir el protocol HTTPS, que ha d'autenticar l'usuari que intenta accedir al servidor web per baixar la informació.

Una altra manera d'assegurar-nos que no s'accedeixi a la informació privada són les extensions IPsec (seguretat del control d'Internet), canals segurs de la informació que viatja per Internet.

Una de les tasques d'un administrador de sistemes, a part d'aquestes que hem indicat, és el monitoratge de la xarxa. El trànsit d'informació de la xarxa dona molta informació de la manera com es pot accedir a les dades i qui ha accedit a cadascun dels recursos compartits.

3.4.2. Passiva

És un aspecte molt important que cal tenir en compte a l'hora d'administrar o instal·lar un equipament informàtic. En principi, una vegada configurades les polítiques de seguretat passiva, no cal que ens preocupem gaire del funcionament que tenen i, per tant, això fa que les oblidem fàcilment i si hi ha algun error o problema no ens n'adonem fins que molts cops és massa tard. No obstant això, el fet d'haver d'estar constantment pendents de la seguretat passiva significa que les decisions preses a l'hora de configurar-la han estat errònies i, per tant, realment no funciona correctament aquesta seguretat. Per exemple, un cas típic és la caiguda de fluid elèctric. Per a solucionar aquest problema es pot decidir entre instal·lar un sistema d'alimentació ininterrompuda (SAI) o contractar una doble companyia de subministrament elèctric (així, en cas que falli una companyia es pot utilitzar l'altra) i fins i tot instal·lar dues fonts d'alimentació o més (la majoria dels fabricants de servidors ja tenen aquesta doble font d'alimentació en els equips).

Alguns punts clau de la seguretat passiva són les polítiques de còpies de seguretat, els plans de prevenció de riscos i els plans de contingència a seguir davant diferents situacions. També els elements redundants (alimentació, xarxa, CPU, discos, etc.) ens ajudaran a recuperar ràpidament, i potser de manera automàtica, les funcionalitats del sistema en cas d'accident fortuït o deliberat.

Una de les mesures principals per a assegurar la continuïtat dels serveis és determinar els riscos a què ens enfrontem davant una fallada en el sistema. Això implica conèixer l'abast dels serveis crítics que hi estan involucrats, la incidència interna i externa que tenen i haver mesurat les possibles conseqüències d'una fallada. Per tant, cal preparar un conjunt d'accions que s'han de prendre en cas de fallada, tenint en compte que pot ser per un problema amb el maquinari o amb el programari (com virus, troians, atacs maliciosos, etc.). En això consisteix, precisament, un pla de risc.

4. Gestió d'incidents de seguretat

Malgrat tot el que fem per evitar que «passin coses» en un sistema informàtic, sempre existeix aquesta possibilitat i per tant incidents com un ciberatac per Internet, un tall de corrent o simplement que un ordinador s'espatlli són molt difícils de preveure (i moltes vegades el cost de fer-ho és massa elevat). Per tant, tota organització ha de tenir present com gestionar aquestes situacions.

4.1. Concepte de vulnerabilitat i incident

Entendrem per *incident* qualsevol fet anòmal que afecti el funcionament del sistema. Atès que els incidents són imprevisibles, l'única cosa que es pot fer és gestionar-los de la millor manera possible, ja que és impossible que no existeixin. Així doncs, la gestió d'un incident informàtic ha d'incloure el monitoratge i la detecció de l'incident, i la resposta davant d'aquest, que en general es pot considerar un incident de seguretat.

Actiu

Són els components indispensables per al correcte funcionament d'un sistema informàtic. En general, el maquinari, el programari i les dades.

Política de seguretat

Conjunt de regles, normes i protocols d'actuació que s'encarreguen de vetllar per la seguretat informàtica de l'organització.

Definició de vulnerabilitat d'un actiu

La potencialitat o possibilitat de la materialització d'una amenaça sobre aquest actiu. Es determina per dues mesures: freqüència i degradació causada.

Definició d'incident de seguretat informàtica

La violació o l'intent de violació de la política de seguretat.

Així, es converteix en essencial **la gestió de riscos i la planificació**. Partint del fet que l'incident serà inevitable, cal assegurar que els **plans de resposta** dissenyats en redueixen l'impacte en l'organització. La planificació de resposta d'incidents, globalment, està molt relacionada amb el coneixement de processos i amb el desenvolupament i l'aplicació de contramesures proactives de detecció, prevenció i reacció per a cada fallada potencial.

Els incidents que l'equip d'ajuda a l'usuari no pot resoldre ràpidament són assignats a un especialista de l'equip de suport tècnic. La resolució de l'incident ha de ser executada tan aviat com sigui possible per a restaurar el servei ràpidament. El procés habitual de gestió d'incidents és el següent:

- Detecció i registre de l'incident.
- Classificació i suport inicial.

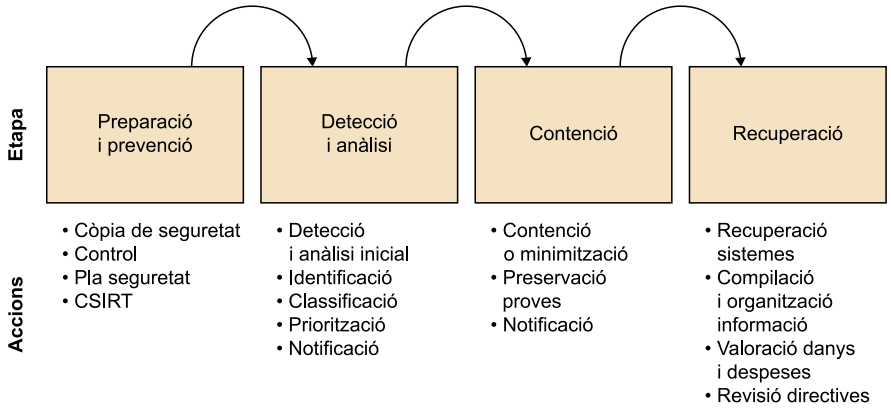
- Investigació i diagnòstic.
- Resolució i recuperació.
- Tancament de l'incident.
- Monitoratge, seguiment i comunicació de l'incident.

4.2. Cicle de vida de l'incident

Des del punt de vista de l'organització, la gestió de l'incident s'ha d'integrar dins de la seguretat global del sistema informàtic. Al seu torn, aquesta depèn del bon disseny de les mesures de prevenció, detecció i recuperació.

El cicle de vida general dels incidents de seguretat es pot veure en la figura 3.

Figura 3. Esquema detallat de les etapes en la gestió d'incidents



Cadascuna d'aquestes etapes conté un conjunt d'accions que s'han de portar a bon terme perquè el conjunt sigui efectiu.

La seguretat global d'un sistema informàtic depèn, en gran mesura, del disseny detallat de les etapes següents:

- **Prevenció o preparació**. L'objectiu consisteix a intentar eliminar les causes que poden ocasionar els incidents. Per això, es parla d'anàlisi i gestió de riscos. Aquesta etapa inclou tant la prevenció dels atacs com la preparació per a respondre-hi correctament. Per a minimitzar el dany potencial d'un atac es requereix estar preparat i seguir unes pràctiques, com fer còpies de seguretat de les dades crítiques de manera periòdica, controlar i actualitzar el programari periòdicament, i tenir implementada i documentada una política de seguretat. Les polítiques de còpia de seguretat fetes amb regularitat minimitzen la pèrdua potencial de dades. El control amb els proveïdors, llocs web de seguretat i les llistes de distribució és una manera d'estar al dia sobre l'estat del programari i els pedaços de seguretat. És necessari actualitzar el programari per a corregir les vulnerabilitats que es van descobrint. També és vital actualitzar el programari antivirus per a mantenir la protecció del sistema actualitzada.

- **Detecció i anàlisi**. Atès que el risc és imprevisible, hi ha moltes probabilitats que tard o d'hora es materialitzi, de manera que l'escenari més adequat és la gestió dels incidents. El primer pas en la gestió d'incidents és identificar-los. S'han d'identificar diverses característiques d'un atac abans que es pugui contenir correctament: determinar que realment s'està produint un atac, els seus efectes sobre la xarxa (local i remota si n'hi hagués), el possible dany als sistemes i d'on s'origina.

- **Contenció**. Amb l'atac identificat, s'han de considerar els passos necessaris per a minimitzar-ne els efectes. La contenció permet protegir altres sistemes i xarxes de l'atac i limitar el dany. En aquesta fase, es fan els passos necessaris per a aturar l'atac. Una vegada s'ha contingut l'atac, la fase final és la recuperació.

- **Recuperació**. Finalment, quan l'incident ha tingut lloc, cal respondre-hi. De manera que cal recuperar el sistema a un estat segur, aplicar accions correctives i reunir les proves de l'incident. Cal valorar el dany, quina informació s'ha perdut. Per què s'ha produït? S'ha controlat immediatament i correctament? Es podria haver controlat millor? La fase d'anàlisi permet als administradors determinar la raó de l'atac i les accions correctives per a protegir-se contra atacs futurs.

La seguretat es pot veure com la gestió del risc.

4.3. Classificació dels atacs

Qualsevol equip connectat a una xarxa informàtica pot ser vulnerable a un atac. Per tant, hi ha multitud d'atacs diferents, i és molt important poder-los classificar d'alguna manera. Els podem agrupar segons la motivació, la manera d'actuar o en funció de qui els origina.

La protecció d'un sistema informàtic s'ha de dirigir al maquinari, al programari i de manera molt especial a les dades, tant aquelles que es trobin circulant a través de la xarxa, com les que estan emmagatzemades en discos durs o altres suports de similars propòsits. Observem que si bé és possible reemplaçar els components del maquinari i del programari d'un sistema informàtic, les dades no tenen substitut possible en cas de pèrdua definitiva.

4.3.1. Motius darrere d'un atac

Els motius existents darrere d'un atac són molts i molt diversos com ara:

- Obtenir accés al sistema.
- Robar informació, secrets industrials o propietat intel·lectual.
- Recopilar informació personal sobre algú (un usuari).

- Obtenir informació de comptes bancaris.
- Obtenir informació d'una organització (la companyia de l'usuari, etc.).
- Afectar el funcionament normal d'un servei o un sistema informàtic.
- Utilitzar el sistema d'un usuari com un «trampolí» per a un atac a un altre lloc.
- Suplantació d'identitat.
- Guany econòmic.
- Usar els recursos del sistema de la víctima per a fins diversos, en particular quan la xarxa en la qual es localitza el sistema atacat té un ample de banda considerable.
- Antic treballador d'una organització.

4.3.2. Segons com actua

Els atacs que poden patir el maquinari, el programari i, d'una manera molt especial, les dades, es classifiquen en quatre grans grups:

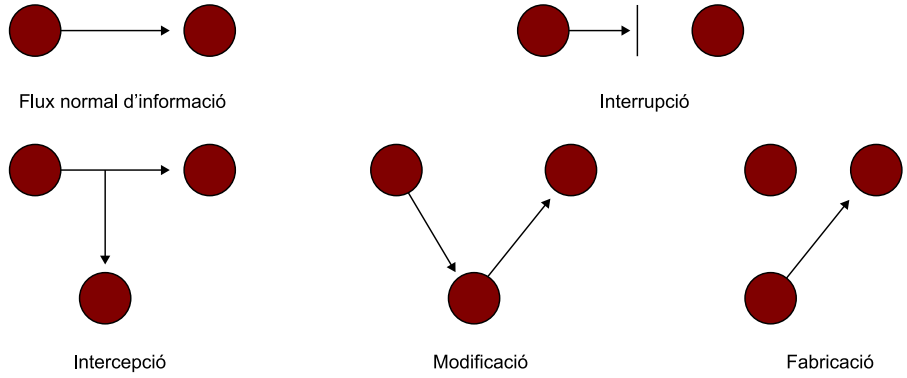
- **Interrupció**. Atac contra la **disponibilitat**, en el qual es destrueix un recurs del sistema o queda no disponible. Un exemple d'atac d'interrupció és tallar una línia de comunicació o deshabilitar el sistema de fitxers del servidor. Un altre exemple és un atac de denegació de servei.

- **Intercepció**. Atac contra la **confidencialitat**, en el qual un element no autoritzat aconsegueix accedir a un recurs. En aquest tipus d'atac no ens referim únicament a possibles usuaris que actuïn com a espies en la comunicació entre emissor i receptor. Per exemple, un procés que s'executa subreptíciament en un ordinador i que emmagatzema en un fitxer les tecles que prem l'usuari que utilitza el terminal constituiria un atac d'intercepció.

- **Modificació**. Atac contra la **integritat**, en el qual, a més d'aconseguir accedir de manera no autoritzada a un recurs, també s'aconsegueix modificar-lo, esborrar-lo o alterar-lo de qualsevol manera. Els atacs són fets pels intrusos. Esborrament de bases de dades, alteració de pàgines web, etc. són exemples típics d'aquesta modalitat d'atac.

- **Fabricació**. Atac contra la integritat, en el qual un element aconsegueix crear o inserir objectes falsificats en el sistema. Un exemple d'atac de fabricació és afegir, d'una manera no autoritzada, un nou usuari i la contrasenya corresponent en el fitxer de contrasenyes.

Figura 4. Representació dels diferents tipus d'atacs que pot patir la comunicació entre un emissor i un receptor



4.3.3. Segons qui l'origina

Poden ser una o diverses persones les que, amb diferents objectius, originen un atac a un sistema informàtic amb la finalitat d'intentar accedir a informació confidencial, destruir-la o simplement aconseguir el control absolut del sistema atacat. Conèixer els objectius dels atacants i les seves motivacions resulta, doncs, essencial per a prevenir i detectar les accions.

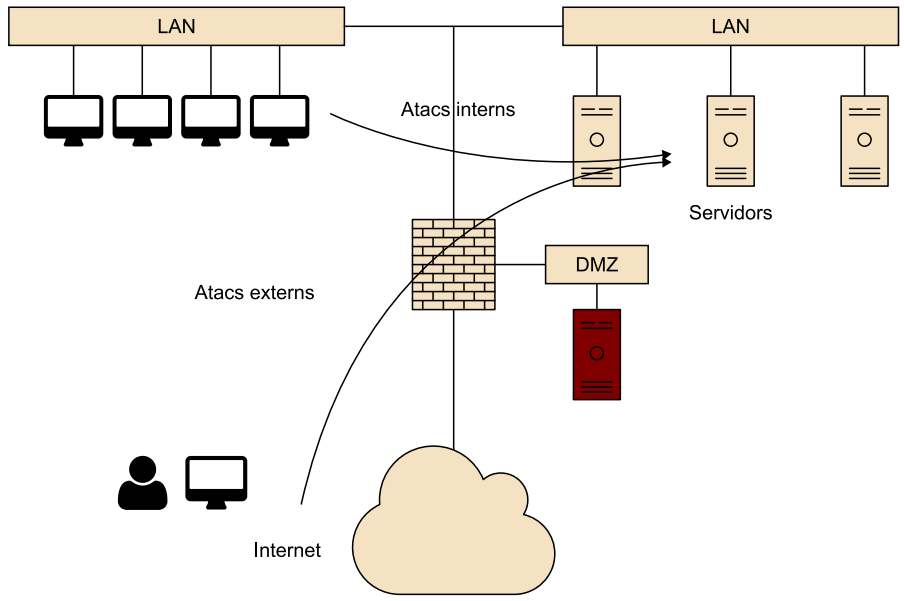
Els atacs provinents de persones es poden classificar en dos grans grups, atacs passius i atacs actius:

- **Atacs passius**. L'atacant no modifica ni destrueix cap recurs del sistema informàtic, simplement l'observa, normalment amb la finalitat d'obtenir alguna informació confidencial. Sovint, aquest atac es produeix sobre la informació que circula per una xarxa. L'atacant no altera la comunicació, sinó que senzillament l'escolta i obté la informació que es transmet entre l'emissor i el receptor. Com que la informació que es transmet no resulta alterada, la detecció d'aquest tipus d'atac no és una tasca senzilla, perquè l'escolta no té cap efecte sobre la informació que circula. Una solució molt eficaç, que permet resoldre aquest tipus de problema, consisteix en l'ús de tècniques criptogràfiques per a fer que la informació no es transmeti neta i no sigui comprensible per als espies.

- **Atacs actius**. En una acció d'aquest tipus, l'atacant altera o destrueix algun recurs del sistema. Exemples d'atacs actius són la suplantació d'identitat, la degradació fraudulenta del servei o la modificació de missatges.

Com ja s'ha indicat prèviament, conèixer les motivacions que poden tenir les persones per a atacar els sistemes informàtics pot ser vital a l'hora de prevenir tot tipus d'intrusions. Cal tenir present que un atac pot provenir tant de l'interior de la xarxa (*insiders*) com de l'exterior (*outsiders*).

Figura 5. Atacs interns i externs (*insiders* i *outsiders*)



Vegem, doncs, el perfil dels possibles atacants d'un sistema informàtic:

- **Antics treballadors.** Una part molt important dels atacs a sistemes informàtics són els que duen a terme antics treballadors que, abans de deixar l'organització, instal·len tot tipus de programari destructiu com, per exemple, virus o bombes lògiques que s'activen en absència del treballador que, acomiadat o descontent per les condicions de treball, ha decidit canviar d'ocupació. La presència d'aquest tipus de programari no sempre és fàcil de detectar, però almenys sí que es poden evitar els atacs que l'antic treballador pot dur a terme des de fora amb el nom d'usuari i la contrasenya de què disposava quan encara treballava a l'organització. Per tant, com a norma general, cal donar de baixa tots els comptes de l'extreballador i canviar les contrasenyes d'accés al sistema com més aviat millor.

- **Personal de la mateixa organització.** Encara que per defecte el personal intern gaudeix de la confiança de l'organització, cal tenir en compte que alguns atacs es poden produir des de dins mateix de la institució. Sovint, no cal que aquests atacs siguin intencionats (encara que, quan ho són, són els més devastadors que es poden produir); poden ser accidents provocats pel desconeixement del personal (per exemple, la formatació accidental d'un disc dur).

- ***Crackers*** (intrusos informàtics). Normalment, aquestes persones duran a terme atacs passius orientats a obtenir informació confidencial (per exemple, un examen d'un curs universitari), o simplement amb la finalitat de posar-se a prova per a obtenir el control del sistema atacat. A més, si l'atacant és prou hàbil, fins i tot podria esborrar les traces de les seves accions en els fitxers que les registren (anomenats genèricament fitxers de registre o fitxers log). Com que aquest tipus d'accions no produeixen cap efecte «visible», no es detecten fàcilment. Els intrusos solen aprofitar la

vulnerabilitat coneguda de sistemes operatius i de programari per a aconseguir el control de tot el sistema informàtic. Per a dur a terme aquest tipus d'accions, n'hi ha prou d'executar diversos programaris que es poden obtenir a Internet i que automatitzen els atacs als sistemes informàtics sense que l'intrús necessiti disposar de molts coneixements tècnics.

Hackers* i *crackers

Cal ser curosos a l'hora d'emprar certs termes informàtics com aquests.

Tot i que popularment s'ha consolidat el concepte de *hacker* com el de pirata informàtic, aquest anglicisme seria l'equivalent a expert informàtic.

Per un altre cantó, el terme **cracker** seria l'equivalent a pirata informàtic.

- **Intrusos remunerats**. La ciberdelinqüència creix a un ritme molt ràpid, i apareixen constantment noves tendències. Les organitzacions delictives utilitzen Internet cada cop més amb l'objectiu de facilitar les seves activitats il·lícites i maximitzar els beneficis en el menor temps possible. En aquest cas, els intrusos estan perfectament organitzats (fins i tot poden ser en diferents llocs geogràfics) i ataquen d'una manera conjunta el sistema d'una organització determinada. Disposen de molts mitjans tècnics i reben remuneracions molt elevades de l'organització rival que dirigeix l'atac, sovint amb l'ànim d'accedir a informació confidencial (un nou disseny, un nou programari, etc.) o bé amb la intenció de provocar un dany important en la imatge de l'organització atacada (un banc).

5. Informàtica i ciències forenses

La generalització de l'ús de les tecnologies de la informació en la societat ha incrementat el valor de la informació digital i ha creat, al seu torn, la necessitat de protegir-la davant els atacs malintencionats o atribuïbles al desconeixement d'aquestes noves tecnologies. En tots dos casos, els rastres o les traces que podrien revelar l'execució d'un fet (tant si és constitutiu de delicte com no) estan emmagatzemats en suports digitals i es denominen genèricament *proves digitals*.

La prova digital presenta, a grans trets, les propietats següents:

- Es pot modificar o eliminar fàcilment.
- És possible obtenir una còpia exacta d'un fitxer sense deixar cap rastre.
- L'adquisició de la prova pot comportar l'alteració dels suports digitals originals.

L'anàlisi forense va sorgir de la necessitat de poder aportar elements rellevants en els processos judicials, en els quals les noves tecnologies es trobaven presents, o bé com a objectiu (per exemple, una intrusió que comporti danys en un sistema informàtic), o bé com a mitjà (per exemple, l'enviament de correus electrònics amenaçadors a un personatge públic). En qualsevol cas, la prova digital és essencial per a trobar les respostes a les preguntes habituals que es plantegen en qualsevol investigació:

Preguntes clau

- Què s'ha comès?
- Quan s'ha fet?
- On s'ha comès?
- Qui ho ha fet?
- Com s'ha dut a terme?
- Per què s'ha comès?

5.1. Principi d'intercanvi de Locard

Un principi fonamental en ciència forense, que usarem contínuament per a relacionar els autors amb els fets que han dut a terme, és el principi d'intercanvi o transferència de Locard.

Edmund Locard (1877-1966) va elevar a la categoria d'imprescindibles una sèrie de proves forenses que abans es consideraven inútils o fins i tot s'ignoraven. El principi d'intercanvi de Locard es pot resumir en la frase «cada contacte deixa un rastre», que significa que, en la majoria de les accions quotidianes, hi ha un intercanvi.

> Per exemple, el trencament d'un vidre per un cop de puny deixa restes de sang en l'escenari i fragments de vidre en la persona. De la mateixa manera, una trepitjada deixarà una petjada sobre el terreny i rastres de terra a la sola. El principi de Locard ens assegura que, en la gran majoria de situacions, hi ha un intercanvi. Només cal tenir la ment desperta i buscar-lo.

En el món digital, el principi s'aplica perquè qualsevol interacció amb un ordinador n'afecta l'operativa, l'estat de la memòria, i fins i tot el que s'escriu en el disc dur. De manera que un expert pot trobar traces de la interacció, i fins i tot detalls que permeten reconstruir els fets i identificar-ne els autors. Si bé és cert que les proves informàtiques (o evidències digitals) poden ser fràgils, això no vol dir que no existeixin i, per tant, que no es puguin obtenir proves definitives, verificables i irrefutables.

5.2. Ciberdelicte

El delicte informàtic no apareix explícitament definit en l'actual Codi Penal (1995), ni en les reformes posteriors.

> Es parla de delicte informàtic o ciberdelicte quan el sistema informàtic és l'objectiu o bé un mitjà de comissió d'un delicte.

En definitiva, la majoria de delictes informàtics són els delictes habituals (amenaces, estafes, etc.), en el quals el sistema informàtic és utilitzat com a mitjà de comissió. Evidentment, des del punt de vista informàtic, els que seran més interessants per a nosaltres seran aquells que tinguin el sistema informàtic com a objectiu. Amb aquesta característica només tenim, pràcticament, dos tipus de delictes: les intrusions i els danys (DoS, *defacements*, etc.) en sistemes informàtics.

El cas de la intrusió (accés no autoritzat, encara que es realitzi sense trencar cap contrasenya) és molt curiós, ja que, com a conseqüència de no tenir definit un capítol específic per als delictes informàtics, la intrusió apareixerà recollida en el delictes contra la intimitat (des de l'any 2010).

5.3. Exemples de delictes informàtics

5.3.1. Conrad Murray

És un dels casos més destacats dels darrers anys. Conrad Murray era el metge de Michael Jackson. Malgrat que la informàtica forense no va ser decisiva per al cas, no va ajudar gens que els investigadors forenses trobessin documentació mèdica en el seu ordinador que mostrava que autoritzava quantitats mortals de propofol per a l'estrella del pop.

5.3.2. BTK Killer

Aquest és probablement l'ús més famós de la informàtica forense per a la resolució d'un cas. Durant més de 30 anys, la policia va intentar utilitzar tècniques tradicionals per a localitzar la persona que havia estrangulat diverses dones durant un període de 16 anys, de 1974 a 1991. Es va conèixer amb les sigles BTK (*Bind, Torture and Kill*, és a dir, «lligar, torturar i matar»). Sovint es burlava de la policia amb lletres i poemes que enviava a la premsa. Després de 10 anys de silenci, va enviar un avís a la premsa l'any 2004 en un disquet amb un document de Word. En poques hores, els experts en informàtica forense van descobrir metadades al disc que el van connectar a un home anomenat Dennis, relacionat amb la Christ Lutheran Church. Finalment, es va detenir un home anomenat Dennis Rader, el qual, més tard, va admetre haver comès els crims.

5.3.3. Krenar Lusha

Quan la policia va entrar a casa seva van comissar, entre altres coses, un ordinador portàtil. Quan els experts en informàtica forense van examinar aquest ordinador, van descobrir que havia descarregat instruccions sobre com construir cinturons suïcides i altres tipus d'explosius. També solia tenir converses en directe amb persones, amb les quals s'havia identificat com a terrorista i havia dit que volia veure nord-americans i jueus assassinats. Tot això va provocar una recerca en el seu apartament, on els oficials van trobar equips de fabricació de bombes i altres armes.

5.3.4. Matt Baker

Malgrat no ser un cas famós, constata que quan s'utilitza un ordinador per al delicte, l'evidència no s'esvaeix ràpidament amb el temps. La història va començar quan la dona del senyor Baker va morir de sobredosi de pastilles per a dormir, i va deixar una nota de suïcidi. Tothom va acceptar que s'havia suïcidat, però després de quatre anys d'investigació i l'anàlisi forense de l'ordinador del senyor Baker, es va descobrir que aquest havia estat cercant a Internet in-

formació sobre sobredosis de pastilles per a dormir i que havia visitat diversos llocs web farmacèutics, poc abans del «suïcidi» de la seva dona. Matt Baker va ser sentenciat a 65 anys de presó.

5.3.5. L'ocultació d'evidències és pitjor que el delicte

A diferència dels casos anteriors, en aquest es comprova com la manca d'evidències també pot conduir a conclusions en relació als delictes comesos.

Harold Einstein i Jennifer Boyd van realitzar una compra d'una propietat (per una quantitat important de diners) en una transacció en què The Corcoran Group actuava com a agent. Després de la compra, es va determinar que hi havia greus deficiències a la propietat, les quals no havien estat notificades als compradors. El cas es va encarregar a un expert en informàtica forense, a fi de trobar les evidències d'aquesta operació de compra. Tot i que no es va trobar cap evidència, la conclusió a la qual es va arribar, va ser tant o més interessant: els correus electrònics i altres fitxers que haurien d'haver estat en els dispositius examinats, havien desaparegut. Malgrat que no es va poder demostrar que els acusats havien eliminat els correus electrònics rellevants, el jutge va dictaminar que intentaven ocultar intencionadament les proves i enganyaven el tribunal. La sentència va ser molt dura, ja que es va considerar que els acusats eren coneixedors dels problemes de la propietat i que, per tant, havien eliminat les evidències electròniques.

5.3.6. L'assassí de Craigslist

Una dona va ser assassinada i una altra va ser atacada després d'emprar un servei per a conèixer persones anomenat Craigslist. La policia va tenir el seu sospitós una setmana després de l'assassinat, gràcies a la investigació forense digital. Els investigadors van rastrejar l'adreça IP dels correus electrònics utilitzats a la correspondència de Craigslist, i les evidències van portar-los ràpidament cap a un sospitós: un estudiant de medicina de 23 anys anomenat Philip Markoff.

5.3.7. Suplantació d'identitats per a obtenir informació

Moltes entitats (en especial els bancs) pateixen sovint casos de *phising* (suplantació d'identitats). El gener del 2018 una coneguda entitat bancària suposadament es va posar en contacte amb els seus usuaris, advertint-los que hi havia una nova «onada de frau» en la qual els ciberdelinqüents falsificaven la marca de l'entitat, a fi d'obtenir les dades personals i la informació bancària diversa. Els atacants enviaven un correu electrònic amb la imatge del banc i demanaven als usuaris que els facilitessin dades privades.

5.3.8. Ashley Madison

El 2015 un grup de ciberdelinqüents autodenominat The Impact Team va assegurar haver robat les dades dels més de 37 milions de clients del web de cites Ashley Madison. Van amenaçar amb publicar tota la informació si la pàgina no tancava immediatament. Ashley Madison va seguir funcionant però, i els *crackers* van publicar 10 gigabytes d'informació, amb els noms, cognoms i transaccions bancàries de més de 32 milions d'usuaris del web. Les primeres anàlisis de les dades, realitzades per una empresa especialitzada en seguretat, CSO, varen assenyalar que hi havia desenes de milers d'adreces de correu electrònic pertanyents a organismes públics, molt probablement falses la majoria. Ashley Madison considera que no és un acte de *hacktivisme* sinó un acte criminal.

5.3.9. Equifax

Equifax, una empresa de crèdit nord-americana, va revelar que havia patit un ciberatac durant diversos mesos. Detectat al juliol del 2017, la fuita d'informació contenia les dades personals (noms, dates de naixement, números de la Seguretat Social, números de permisos de conduir) de 143 milions de clients nord-americans, canadencs i britànics, així com 200.000 números de targetes de crèdit. Els atacants van usar una vulnerabilitat coneguda del servidor web Apache Struts. Sospitosament, diversos executius de l'empresa van vendre accions pocs dies abans que es fes pública la violació de la seguretat.

5.3.10. Marriott Hotels

La informació d'uns 500 milions d'usuaris del grup hoteler Starwood de Marriott fou compromesa, incloses les dades bancàries. La informació robada incloïa informació de pagament, noms, adreces de correu, números de telèfon, adreces de correu electrònic, números de passaport i, fins i tot, detalls sobre el compte Starwood Preferred Guest (SPG), una targeta de gamma alta emesa per l'emissor de targetes de crèdit American Express per a viatgers habituals.

5.3.11. Robatori de paraules de pas

L'agost del 2014, la companyia de seguretat informàtica Hold Security va revelar que uns pirates informàtics russos havien robat 1.200 milions de connexions i contrasenyes a 420.000 llocs web de tot el món. Això podria haver permès al grup de pirates informàtics CyberVor accedir a 500 milions de comptes de correu electrònic. Els *crackers* van utilitzar xarxes de zombis programades per a visitar llocs i realitzar proves de vulnerabilitat per tal d'explotar les vulnerabilitats d'injecció SQL i accedir a bases de dades. Tot i que l'atac és important per la seva escala, en última instància, no ha tingut conseqüències impor-

tants. Segons l'FBI, la informació només s'ha utilitzat en una gran campanya de correu brossa (*spam*) a les xarxes socials. La intenció real d'aquest robatori continua sent un misteri.

5.3.12. Facebook

Facebook ha reconegut en una nota que un atac informàtic ha compromès informació de 30 milions d'usuaris, sobretot dades personals i de contacte.

Els ciberdelinqüents van controlar uns 400.000 comptes a través d'una «vulnerabilitat» del codi de la plataforma que va afectar la funcionalitat *Veure com* (una eina que permet als usuaris veure el seu perfil com si fossin altres persones) d'uns 400.000 comptes i, des d'aquí, van arribar a 30 milions d'usuaris.

Dels 30 milions d'usuaris afectats, 15 milions van veure exposats els seus noms i les seves dades de contacte (número de telèfon, correu electrònic, o tots dos, segons el perfil de l'usuari). A 14 milions els van ser sostretes, a més, dades que tenien en el seu perfil de Facebook, com ara el seu nom d'usuari, sexe, idioma, religió, data de naixement, lloc de naixement, etc. Els pirates informàtics també es van apropiar d'informació relacionada amb els últims 10 llocs que aquests internautes havien visitat a la xarxa social, així com les seves últimes 15 recerques, els dispositius des dels quals es connectaven a Facebook i les pàgines que seguien.

5.3.13. Sexting

El maig del 2019, V.R. es va suïcidar arran de la difusió de diversos vídeos sexuals en els quals hi apareixia. En pocs dies aquests vídeos s'havien difós a través de missatges privats i grups de WhatsApp dins de l'empresa on treballava. Això va provocar en la dona, de 32 anys, una situació de pressió i angoixa. La dona temia que les imatges, enregistrades abans de casar-se, arribessin al seu marit, fet que, pel que sembla, es va produir. La policia tenia a la seva disposició el telèfon mòbil de la dona morta i se'n va realitzar l'anàlisi forense per a tractar d'esbrinar si també va poder patir assetjament per part d'algun company, tal com apuntaven cercles propers a la víctima.

5.3.14. Ciberassetjament

La policia va poder evitar el suïcidi d'un menor d'edat que estava sent assetjat sexualment a través d'Internet. Els dos arrestats contactaven amb els menors a través d'Internet, des de Guatemala i, després de guanyar-se la seva confiança, els sol·licitaven material pornogràfic d'ells mateixos. Aquest és el resultat d'una operació internacional entre agents espanyols, el departament Homeland Security Investigation (HSI) dels Estats Units i la policia de Guatemala. Després de les investigacions i de seguir el rastre digital dels assetjadors, es va

procedir a l'entrada i perquisició del domicili dels presumptes assetjadors. En el registre de l'habitatge es va descobrir l'existència de diverses desenes de víctimes en diversos països del món. Finalment es va decretar el seu ingrés a presó.

5.3.15. Abraham Abdallah

El cas d'Abraham Abdallah té tots els ingredients per ser un dels més extravagants dins dels fraus amb targeta de crèdit. Aquest ajudant de cambrer va agafar directament la llista de les persones més riques i amb una combinació de cerques a Internet i d'enginyeria social es va dedicar a recopilar números de la Seguretat Social, dates de naixement, adreces i fins i tot números de targetes de crèdit. Posteriorment, va utilitzar els números de les targetes de persones com Oprah Winfrey, Steven Spielberg i Warren Buffett. L'increïble de l'assumpte és que, avui dia, encara es desconeixen totes les compres i els càrrecs que realment va poder acabar fent. Es coneixen els que no va poder fer, però es parla fins i tot de la compra de propietats amb aquestes suplantacions de personalitat.

5.3.16. El problema de ser famós

Majerczyk i Ryan Collins s'han declarat culpables d'invasió de la intimitat i divulgació de contingut privat. Sense estar relacionats, ambdós aconseguien fotografies íntimes d'actrius i cantants famosos. Més de 1.000 celebritats van veure publicades per tota la xarxa imatges privades seves despullades o amb molt poca roba. El mètode consistia en accedir als comptes de Gmail i Apple iCloud de les víctimes. Per a dur-ho a terme, primer enviaven correus als seus objectius en nom d'iCloud, demanant-los les contrasenyes com a part d'un procés de seguretat. Un cop obtingudes, tenien via lliure per entrar al sistema d'emmagatzematge en el núvol.

Ara, tant Collins com Majerczyk faran front a una possible condemna per un delicte que atempta contra la privadesa i la imatge de totes les víctimes. La privadesa està prevista en la Declaració Universal dels Drets Humans, a l'article 12. Si bé el Departament de Justícia dels Estat Units no va trobar proves que els vinculessin amb la filtració de les imatges íntimes, tots dos *crackers* es van declarar culpables.

5.3.17. Campanya política de Macron

Es va dir que la campanya presidencial d'Emmanuel Macron del 2017 havia estat «víctima d'un atac pirata massiu i coordinat». Es van fer públics més de 20.000 correus relatius a la campanya presidencial un dia abans que els votants francesos anessin a les urnes.

Uns 9 gigabytes de dades van ser publicats per un usuari anomenat EMLEAKS a Pastebin, un lloc web per compartir documents que permet la publicació anònima. Mai ha quedat clar qui era el responsable de publicar les dades o si els correus electrònics eren genuïns. Ningú sap tampoc l'impacte que ha tingut aquest atac en el resultat de les eleccions.

5.4. Nous delictes informàtics

En ple 2019 ja s'està avisant dels perills dels nous dispositius mèdics connectats a la xarxa o que s'hi poden comunicar.

Marcapassos i monitors de ritme cardíac

El Departament de Seguretat Nacional Americà, que supervisa la seguretat en infraestructures crítiques dels Estats Units, incloent dispositius mèdics, va emetre una alerta perquè hi ha 750.000 marcapassos Medtronic vulnerables a la pirateria informàtica.

La primera vulnerabilitat, identificada com a CVE-2019-6538, és que el protocol sense fils de Conexus no té autenticació ni autorització, fet que significa que quan la ràdio del dispositiu està activada, els atacants poden prendre el control de la comunicació. Un cop fet això, no hi ha res que els impedeixi reconfigurar el dispositiu mèdic amb configuracions potencialment mortals.

La segona vulnerabilitat, identificada com a CVE-2019-6540, és que el protocol Conexus no utilitza cap tipus de xifratge sense fils, de manera que els atacants propers poden extreure les dades sensibles durant la comunicació del dispositiu.

Bombes d'infusió

El 2017 es van identificar problemes amb diverses bombes d'infusió als hospitals dels EUA. Es van trobar un total de vuit vulnerabilitats de seguretat a la bomba d'infusió Medfusion 4000, fabricada pel fabricant de dispositius mèdics Smiths Medical. Els dispositius en qüestió s'utilitzen a tot el món per al lliurament de petites dosis de medicaments en el context d'una atenció crítica aguda, incloses les cures intensives neonatals, les cures intensives pediàtriques i els procediments de quiròfans. L'amenaça per a la seguretat detectada podria permetre a un atacant remot obtenir accés no autoritzat i afectar l'operació prevista de la bomba, inclosa l'administració de sobredosis mortals. Els problemes de seguretat identificats són:

- Ús d'usuaris i contrasenyes codificats per a establir automàticament una connexió sense fils si no s'ha modificat la configuració per defecte.

- Un error de desbordament de la memòria intermèdia que es podria explotar per a l'execució remota de codi maliciós al dispositiu mèdic de destinació.

- Manca d'autenticació quan es va configurar la bomba per a permetre connexions FTP.

- Presència de credencials codificades per al servidor FTP de la bomba.

- La manca de validació adequada del certificat de l'amfitrió deixa la bomba vulnerable a atacs del tipus Man-in-the-middle (MiTM).

Sistemes de ressonància magnètica

Un sistema de ressonància magnètica de Bayer Medrad ha estat el primer dispositiu a ser *hackejat* als Estats Units. El dispositiu en qüestió s'utilitza per a controlar el que es coneix com a injector de potència, que ajuda a lliurar un agent de contrast als pacients de l'hospital. Aquests agents químics estan dissenyats per a millorar la qualitat de les exploracions de ressonància magnètica (MRI), que s'utilitzen per a detectar des de traumes fins a tumors del cervell i de la columna vertebral. Tot i que aquest atac no amenaça necessàriament la seguretat dels pacients, va provocar la parada de les màquines durant un període prolongat. Aquest problema, indirectament, podria desencadenar diversos errors clínics.

Xarxes informàtiques de sistemes de salut (hospitals...)

L'amenaça més gran per a la seguretat mèdica està a les xarxes hospitalàries senceres. En lloc de centrar-se en els pacients individuals i els seus dispositius implantats, els pirates informàtics tenen més probabilitats d'atacar sistemes hospitalaris sencers. Durant els darrers anys, s'han produït nombrosos atacs de virus *ransomware* als proveïdors de salut, incloent l'atac del *malware* WannaCry, que va devastar el Servei Nacional de Salut dels Estats Units (NHS) i nombrosos hospitals. Aquests atacs, que van aprofitar forats de seguretat dels sistemes operatius de Microsoft, van posar en evidència el fet que els hospitals encara no estan preparats per a resoldre aquests tipus d'incidències. Quan les xarxes hospitalàries són atacades, potencialment també es podrien comprometre els historials mèdics de pacients de tota la xarxa. També es podrien arribar a modificar aquests historials amb conseqüències mortals. Fins i tot l'accés a aquestes xarxes podria tenir com a objectiu el control de dispositius mèdics connectats a la xarxa.

6. Marc normatiu associat a la informàtica i als ciberdelictes

El marc normatiu associat a la informàtica, en general, és molt divers. Cal tenir en compte que hi ha un marc civil destinat a protegir la informació i les persones en l'àmbit digital, i especialment a Internet, que conté sancions en el seu incompliment. El marc penal s'associa als delictes informàtics i pot arribar a comportar fins i tot penes privatives de llibertat.

6.1. Legislació en l'àmbit digital i Internet

Llei 34/2002 de Serveis de la Societat de la Informació i de Comerç Electrònic (LSSICE). S'aplica al comerç electrònic i als altres serveis d'Internet quan siguin part d'una activitat econòmica. També regula el que fa referència a les obligacions i responsabilitats dels prestadors d'aquests serveis. El concepte de serveis de la LSSICE és ampli i engloba altres coses a més de la contractació de béns i serveis per via electrònica.

Entre d'altres, i sempre que representin una activitat econòmica, s'hi inclouen els següents:

- La contractació de béns o serveis per via electrònica.
- L'organització i gestió de subhastes per mitjans electrònics o de mercats i centres comercials virtuals.
- La gestió de compres a la xarxa per grups de persones.
- L'enviament de comunicacions comercials.
- El subministrament d'informació per via telemàtica.
- Les activitats d'intermediació relatives a la provisió d'accés a la xarxa.
- La realització d'una còpia temporal de les pàgines d'Internet sol·licitades pels usuaris.
- El vídeo sota demanda, com a servei en què l'usuari pot seleccionar a través de la xarxa, tant el programa desitjat com el moment del seu subministrament i recepció, i, en general, la distribució de continguts prèvia petició individual.

Llei 22/1987 de propietat intel·lectual. Aquesta llei ha sofert molts canvis, el darrer, el febrer de 2019 (Llei 2/2019). Malgrat això, l'esperit inicial es manté. Regula els drets d'autor i les seves creacions. Des del vessant tecnològic, l'augment progressiu de l'ús d'Internet fa necessari un estudi de la regulació que protegeix les creacions que es posen a la disposició dels usuaris a la xarxa i que es transmeten per mitjà d'aquesta. Si bé fa anys era molt car i complicat fer una còpia d'una obra, avui dia el panorama és molt diferent, ja que és enormement fàcil i barat reproduir i distribuir continguts. Aquest canvi (en les formes de reproducció i distribució de les obres) genera un desfasament entre les vies de tutela de la propietat intel·lectual (sorgides en un moment i en una realitat molt diferent de l'actual) i la necessitat de protecció que demanda la propietat intel·lectual actualment. En definitiva, aquest desfasament ha fet que la propietat intel·lectual es converteixi en un tema de controvèrsia i objecte d'un debat social molt intens.

A grans trets, des de la perspectiva informàtica, la informació que es protegeix és la creació d'una obra, inclosa aquesta en format digital, els programes d'ordinador, les bases de dades, obres multimèdia i llocs i pàgines web.

Llei 59/2003 de signatura electrònica. La impossibilitat d'emprar el document de paper i la signatura manuscrita en les transaccions electròniques determina que apareguin instruments que compleixin les funcions tradicionals que els primers exercien. La signatura manuscrita suposa la identificació de la persona i la seva vinculació amb el contingut del document. La signatura electrònica sorgeix com a tècnica substitutiva de la signatura manuscrita, que pretén cobrir les mateixes funcions:

- la determinació de la identitat de l'emissor del missatge i
- la comprovació que els termes dels missatges de dades enviades no han estat alterats.

Llei 3/2018 de protecció de dades personals i garantia dels drets digitals. Aquesta llei adapta la normativa europea del Reglament General de Protecció de Dades (GDPR). Es pretén «garantir i protegir, pel que fa al tractament de les dades personals, les llibertats públiques i els drets fonamentals de les persones físiques, i especialment del seu honor i intimitat personal i familiar». Per tant, la llei tracta de protegir la intimitat de les persones físiques enfront del tractament de les seves dades personals.

Nota

Tècnicament deroga la Llei de protecció de dades 15/1999 i el seu Reglament de desenvolupament 1720/2007.

El Reglament General de Protecció de Dades (GDPR) (UE 2016/679) és un reglament europeu mitjançant el qual l'Eurocambra, el Consell de la Unió Europea i la Comissió Europea pretenen enfortir i unificar la protecció de dades per a tots els països de la Unió Europea (UE), i controlar també la transferència de dades. Es va publicar el maig del 2016 i va entrar en vigor el passat 25 de maig de 2018.

6.2. Els delictes informàtics i el Codi Penal

Tot seguit, veurem amb una mica més detall alguns articles del Codi Penal (CP), relacionats amb els mal anomenats delictes informàtics (com ja hem vist, no existeixen definits com a tals):

- **Article 197 (delictes contra la intimitat)**

  1. El qui, per descobrir els secrets o vulnerar la intimitat d'altri, sense el seu consentiment, s'apoderi dels seus papers, cartes, missatges de correu electrònic o qualsevol altre document o efectes personals o intercepti les seves telecomunicacions o utilitzi artificis tècnics d'escolta, transmissió, gravació o reproducció del so o de la imatge, o de qualsevol altre senyal de comunicació, ha de ser castigat amb les penes de presó d'un a quatre anys i multa de dotze a vint-i-quatre mesos.

  3. El qui, per qualsevol mitjà o procediment i vulnerant les mesures de seguretat establertes per impedir-ho, accedeixi sense autorització a dades o programes informàtics continguts en un sistema informàtic o en part d'un sistema informàtic o es mantingui dins d'aquest en contra de la voluntat

de qui tingui el legítim dret a excloure'l, ha de ser castigat amb pena de presó de sis mesos a dos anys.

Per tant, són constitutives de delicte les conductes següents (sense consentiment de la persona afectada, ni autorització judicial motivada):

- L'apoderament de papers, cartes, missatges de correu electrònic o qualsevol altre document o efectes personals.
- La intercepció de les comunicacions.
- La intrusió en un sistema informàtic.

Per tant, NO es pot obrir un correu que no sigui el nostre personal, sense autorització. Aquesta qüestió és, des del punt de vista judicial, molt complexa, ja que, fins i tot en aquells casos en què el correu electrònic és considerat com una eina empresarial, obrir-ne el contingut podria comportar problemes legals.

- **Article 248 (estafa)**

  1. Cometen estafa els qui, amb ànim de lucre, utilitzin engany suficient per produir error en un altre, i l'indueixin a realitzar un acte de disposició en perjudici propi o d'altri.

  2. També es consideren reus d'estafa:

  a) Els que, amb ànim de lucre i valent-se d'alguna manipulació informàtica o artifici semblant, aconsegueixin una transferència no consentida de qualsevol actiu patrimonial en perjudici d'un altre.

  b) Els que fabriquin, introdueixin, posseeixin o facilitin programes informàtics específicament destinats a la comissió de les estafes que preveu aquest article.

  c) Els que utilitzant targetes de crèdit o dèbit, o xecs de viatge, o les dades que consten en qualsevol d'aquests, realitzin operacions de qualsevol classe en perjudici del seu titular o d'un tercer.

Article 248

Aquest article recull, entre altres, els fraus per *phising* informàtic.

- **Article 264 (delicte de danys)**

  1. El qui per qualsevol mitjà, sense autorització i de manera greu esborri, faci malbé, deteriori, alteri, suprimeixi, o faci inaccessibles dades, programes informàtics o documents electrònics aliens, quan el resultat produït sigui greu, ha de ser castigat amb la pena de presó de sis mesos a dos anys.

  2. El qui per qualsevol mitjà, sense estar autoritzat i de manera greu, obstaculitzi o interrompi el funcionament d'un sistema informàtic aliè, introduint, transmetent, fent malbé, esborrant, deteriorant, alterant, suprimint o fent inaccessibles dades informàtiques, quan el resultat produït sigui greu, ha de ser castigat, amb la pena de presó de sis mesos a tres anys.

Article 264

Aquest article contindria els atacs DoS, *defacements*, etc.

En definitiva, cal recordar:

- No tot allò que es tècnicament possible és legal.
- El desconeixement de les normes no exonera de responsabilitat a l'informàtic.
- Si una prova no s'ha obtingut amb prou garanties, pot ser invalidada.

La taula resum següent segueix la classificació que fa el Consell d'Europa, en el nostre Codi Penal, on hi ha reflectides les conductes delictives següents (font: Guàrdia Civil):

1r Delictes contra la confidencialitat, la integritat i la disponibilitat de les dades i dels sistemes informàtics

Article 197	Es tipifiquen en aquest article les conductes que duen a apoderar-se de missatges de correu electrònic aliens o que permetin l'accés a documents privats sense l'autorització dels seus titulars.
	La instal·lació de programaris del tipus ***sniffer***, ***keylogger*** o **troians** que permetin l'accés a dades reservades de caràcter personal, com ara missatges de correu electrònic. L'accés no autoritzat a sistemes informàtics aprofitant *bugs* (forats) de seguretat o altres tècniques de *hacking*. L'apoderament de dades reservades d'altres persones que es trobin en qualsevol suport informàtic.
Article 264.2 Article 278.3	Destrucció, alteració o dany de programes o documents continguts en ordinadors.
	La remissió o instal·lació en un ordinador aliè de virus, cucs o programaris maliciosos que alterin continguts o ocasionin danys. La destrucció de dades o producció de danys en sistemes informàtics després d'accessos no autoritzats.
Article 278.1	Apoderament o difusió de documents o dades electròniques d'empreses.
	La instal·lació de programaris del tipus ***sniffer***, ***keylogger*** o troians que permetin l'accés a dades d'empreses que permetin realitzar competència deslleial. L'accés no autoritzat a sistemes informàtics aprofitant *bugs* (forats) de seguretat o altres tècniques de *hacking* per a descobrir secrets d'empresa.

2n Delictes informàtics

Article 248.2	Estafes com a conseqüència d'alguna manipulació informàtica.
	Compres fraudulentes a través d'Internet. Vendes fraudulentes a través d'Internet. Fraus en banca electrònica usurpant la identitat de la víctima.
Article 256	Utilització no consentida d'un ordinador (sense l'autorització del seu propietari) que li causa un perjudici econòmic superior a 300,5 €.
	Comunicacions a Internet des de l'ordinador pont d'una altra persona, que ocasiona que a aquesta se li facturin per aquest fet més de 300,5 €.

Cal destacar que conductes tan habituals en aquesta Societat de la Informació, com són el correu brossa o el simple escaneig de ports, difícilment troben cabuda entre els delictes tipificats en el nostre Codi Penal, per la qual cosa no són perseguibles per via penal.

3r Delictes relacionats amb el contingut

Article 186	Distribució a menors d'edat de material pornogràfic.
	Enganys a xats específicament destinats a menors, fent-se passar per un d'ells, enviant-los fotografies pornogràfiques i proposant-los pràctiques abusives.
Article 189	Distribució de material de pornografia infantil a través d'Internet.
	Intercanviar o enviar fotografies de pornografia infantil a través de correu electrònic, xat o qualsevol altre programa que permeti la distribució de fitxers. Tenir aquest material per tal de distribuir-lo a través d'Internet.

4rt Delictes relacionats amb infraccions de la propietat intel·lectual i drets afins

Article 270	Còpia no autoritzada de programes d'ordinador o de música.
	Venda a través d'Internet de còpies de programaris o de CD de pel·lícules o música.
Article 270	Fabricació, distribució o tinença de programes que vulneren les mesures de protecció antipirateria dels programes.
	Creació, distribució o tinença de *cracks* que permeten saltar-se les limitacions amb què compten alguns programes.
Article 273	Comerç a través d'Internet de productes patentats sense autorització del titular de la patent.
	Venda a Internet de còpies il·legals o productes pirates.

7. Estàndards ISO/UNE i organismes internacionals

L'àmbit forense i la seguretat informàtica compten amb un conjunt de normatives i d'organismes internacionals a fi de tenir guies de bones pràctiques (com fer les coses), mètodes i mesures comunes.

7.1. Seguretat informàtica

Família ISO 27000. És un conjunt d'estàndards internacionals sobre la Seguretat de la Informació. La família ISO 27000 conté un conjunt de bones pràctiques per a l'establiment, implementació, manteniment i millora de Sistemes de Gestió de la Seguretat de la Informació (SGSI). Estan publicats per l'Organització Internacional per a l'Estandardització (ISO) i la Comissió Electrotècnica Internacional (IEC). SGSI és l'abreviatura utilitzada per referir-se a un Sistema de Gestió de la Seguretat de la Informació. ISMS és el concepte equivalent en anglès a les sigles de *Information Security Management System*.

La sèrie conté les millors pràctiques recomanades en Seguretat de la Informació per desenvolupar, implementar i mantenir especificacions per als SGSI. Les més rellevants per a nosaltres són:

- **ISO/IEC 27000**. Information security management systems - Overview and vocabulary[9]
- **ISO/IEC 27001**. Information technology - Security Techniques - Information security management Systems
- **ISO/IEC 27002**. Code of practice for information security controls - essentially a detailed catalog of information security controls that might be managed through the ISMS
- **ISO/IEC 27003**. Information security management system implementation guidance
- **ISO/IEC 27004**. Information security management - Monitoring, measurement, analysis and evaluation
- **ISO/IEC 27005**. Information security risk management
- **ISO/IEC 27006**. Requirements for bodies providing audit and certification of information security management systems
- **ISO/IEC 27017**. Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- **ISO/IEC 27031**. Guidelines for information and communication technology readiness for business continuity
- **ISO/IEC 27032**. Guideline for cybersecurity
- **ISO/IEC 27033-1**. Network security - Part 1: Overview and concepts
- **ISO/IEC 27033-2**. Network security - Part 2: Guidelines for the design and implementation of network security

- **ISO/IEC 27033-3**. Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
- **ISO/IEC 27039**. Intrusion prevention
- **ISO/IEC 27036-4**. Information security for supplier relationships - Part 4: Guidelines for security of cloud services

7.2. Anàlisi forense

La sèrie 27000 també conté diverses normes relacionades amb la gestió de les evidències digitals (27037) i l'anàlisi forense (27042).

ISO/IEC 27037. Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence

Gestió de les evidències digitals (apareixen les etapes prèvies a l'anàlisi de les evidències).

ISO/IEC 27040. Information technology - Security techniques - Storage security

Reuneix guies i recomanacions perquè l'emmagatzematge de les evidències digitals sigui segur. Ens presenta riscos existents en l'emmagatzematge i ens proveeix directrius o bones pràctiques incloent models d'auditories i revisions per a poder controlar l'emmagatzematge de les evidències i garantir que es faci de forma correcta i segura.

ISO/IEC 27041. Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative

ISO/IEC 27042. Information technology - Security techniques -Guidelines for the analysis and interpretation of digital evidence

Indicacions per a l'anàlisi i interpretació de l'evidència digital.

ISO/IEC 27043. Information technology - Security techniques - Incident investigation principles and processes

A més, de les normes anteriors, Espanya disposa de normes UNE específiques que no són una mera traducció de les anteriors. Aquestes normes, relatives a la gestió de l'evidència digital, l'anàlisi forense i els informes pericials, són les següents:

Família UNE 71505

UNE 71505-1. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales

UNE 71505-2. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas

UNE 71505-3. Tecnologías de la Información (TI). Sistemas de Gestión de Evidencias Electrónicas (SGEE). Parte 3: Formatos y mecanismos técnicos

UNE 71506. Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas

UNE 197010. Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)

Finalment, entre altres, també podem disposar de les guies RFC:

RFC 3227. Maneig i recol·lecció d'evidències. Aquest document ens indica les principals guies per a la recol·lecció i l'emmagatzematge d'evidències digitals. Aquesta RFC es considera un estàndard.

RFC 4810. Com preservar la informació a llarg termini. Aquesta RFC ens defineix un estàndard relacionat amb la preservació de la informació. Punt molt important per als informes pericials i les investigacions tecnològiques, ja que el treball sempre ha de poder ser comprovat per a validar-ne l'autenticitat i la veracitat. En aquesta RFC, entre d'altres, indica als perits com han de procedir per verificar una signatura digital després d'haver passat un gran espai de temps des de la generació de la mateixa.

7.3. Organismes internacionals

Els organismes internacionals són multidisciplinaris i estan integrats per experts de diferents disciplines, amb l'objectiu d'avançar en el coneixement de la ciència forense i la seva aplicació en l'àmbit judicial, fomentant la col·laboració per a la consecució d'acords mutus dins del camp. Aquests acords són de vital importància tant en el context científic com en el context del procés judicial, contextos en què sorgeixen debats de diferent índole.

- International Association of Computer Investigative Specialist (IACIS). Aquesta associació ofereix una certificació internacional (CFEC, Computer Forensic External), dirigida a analistes que no formin part dels cossos policials o judicials.

- International Organisation on Computer Evidence (IOCE).

- Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas (esCERT).

- American Academy of Forensic Sciences (AAFS). http://www.aafs.org/

- European Network of Forensic Science Institutes (ENFSI). http://enfsi.eu/

Resum

En aquest mòdul didàctic hem vist què és la informàtica forense, els seus orígens i com s'ha expandit molt més enllà d'aplegar evidències amb finalitats judicials. La informàtica forense pot ser vista com una disciplina forense on s'analitza un cas, se n'extreuen evidències i es formula una possible explicació de què ha passat. Aquesta visió està molt lligada a un peritatge judicial i, de retruc, al funcionament del sistema judicial.

Com que constitueix una disciplina consolidada, la seva vinculació amb estàndards internacionals i amb normativa legal és molt important. La normativa vigent pot ser civil, com ara la Llei de protecció de dades i la Llei de propietat intel·lectual o penal com la tipificació i les penes associades als ciberdelictes. Quant als estàndards, la trobem amb la seguretat de la informació i amb els mètodes i la recollida d'evidències que fan que tota la comunitat d'informàtica forense treballi de la mateixa manera.

A causa que la informàtica forense ha ampliat molt el seu camp d'us, s'ha plantejat la informàtica forense també com a element en les organitzacions dins de la seguretat informàtica i en la gestió d'incidents. Així doncs, pot ajudar a protegir la informació, actiu principal de les organitzacions.

La gestió d'incidents és molt important, ja que no és possible la seguretat absoluta. La informàtica forense esdevé una eina fonamental per a avaluar les anomalies en sistemes informàtics. Una correcta avaluació (informe forense) n'ha de permetre l'ús en seu judicial i a la vegada un document per a corregir les falles d'un sistema informàtic, a fi que no torni a succeir l'incident.

Malgrat que l'anàlisi forense es pot aplicar a les organitzacions per motius tècnics, de gestió del sistema, o per a la implantació de polítiques de seguretat, en els peritatges també s'ha de veure la seva intersecció amb el sistema legal, és a dir, que no es tracta únicament d'ordinadors, xarxes i documents electrònics, sinó també de processos legals, garanties en l'obtenció de les proves, informes clars i concisos, i fets que s'han de presentar de manera convenient i convincent.

La informàtica forense, per tant, constitueix la intersecció entre la seguretat de la informació, la gestió del incident, el peritatge i la normativa vigent.

Activitats

1. Busqueu per la xarxa informació addicional sobre Locard i compartiu-la al fòrum. Descobrireu que han canviat molts dels conceptes de la criminalística moderna. La ciència forense actual seria diferent sense el seu treball.

2. Busqueu una noticia vinculada a la delinqüència tecnològica i pugeu-la al fòrum de l'assignatura.

Exercicis d'autoavaluació

1. Què volen dir els acrònims següents?

LSSICE	
LPI	
CP	
GDPR / RGPD	
IDS	
LOPDGDD	
TIC	
ENFSI	
CID / CIA	

2. Quines d'aquestes frases respecte als peritatges són certes i quines falses?

a) Els peritatges s'orienten a l'avaluació de l'eficàcia i l'eficiència.
b) El seu objectiu és la constitució de proves mitjançant l'emissió d'un dictamen sobre fets concrets.
c) Només s'emeten conclusions sobre punts concrets.
d) La seva periodicitat és planificada o periòdica.
e) Es duen a terme per presumpció de delicte, dany o ineficàcia.
f) El perit és lliure de definir el seu àmbit d'actuació.

3. Relacioneu els termes següents:

Delicte informàtic		SGSI
Delicte d'intrusió		Qualsevol disciplina els principis científics de la qual s'utilitzin per a ajudar la justícia
ISO 27000		No està definit al Codi Penal
Ciències forenses		197bis del Codi Penal

4. Quins són els principis de la informatica forense?

5. És cert o fals que el principi de Locard diu que qualsevol rastre ha de provenir de dos o més contactes?

6. Quines d'aquestes frases són certes i quines falses?

a) La preparació és una etapa molt important per a minimitzar la quantitat i importància dels atacs al sistema.
b) La metodologia forense s'ha d'aplicar un cop contingut l'incident, ja que és quan hi ha les evidències digitals.
c) La informàtica forense i la recuperació del sistema s'han de ponderar per evitar la pèrdua d'evidència digital.
d) La contenció de l'incident es pot fer de forma automàtica.
e) Amb eines de gestió d'incidents no cal un equip de resposta d'incidents.

7. Quins són els articles del codi penal vinculats als ciberdelictes?

8. Com es defineix la informàtica forense?

a) Com un conjunt de recursos interconnectats per millorar el rendiment.
b) Com una ciència forense que s'encarrega de la preservació, identificació, extracció, documentació i interpretació de l'evidència digital, de manera que aquesta sigui acceptada en el protocol de seguretat.
c) Com una ciència forense que s'encarrega d'assegurar, identificar, preservar, analitzar i presentar l'evidència digital, de manera que aquesta sigui acceptada en un procés judicial.
d) Com una ciència o especialitat científica on els principis, mètodes i tècniques s'apliquen a la justícia, en qualsevol dels seus aspectes.

9. Relacioneu els temes amb les seves descripcions:

Detectar intrusió		Anticipar-se a l'incident
Locard		Detecció i anàlisi
Objectiu preventiu		Tenir control sobre l'evidència
Principi de la informàtica forense		IDS
Etapa de gestió d'incidents		Cada contacte deixa un rastre

10. Quines d'aquestes frases són certes i quines falses?

a) La informàtica forense es va iniciar a la Primera Guerra Mundial i com a conseqüència d'aquesta.
b) Els usos de les ciències forenses, i la informàtica forense no és una excepció, estan molt lligats als processos judicials.
c) La informàtica forense permet millorar la seguretat de l'organització.
d) L'evidència digital, afortunadament, no és volàtil, de manera que la seva adquisició és un procés factible.
e) La informàtica forense és un procés científic i gràcies a això podem assegurar que les proves són rigoroses.

Solucionari

Exercicis d'autoavaluació

1.

LSSICE	Llei de Serveis de la Societat de la Informació i de Comerç Electrònic.
LPI	Llei de propietat intel·lectual.
CP	Codi Penal.
GDPR / RGPD	Reglament General de Protecció de Dades (RGPD) o el seu equivalent anglès General Data Protection Rule (GDPR).
IDS	Intrusion Detection System. Sistema de detecció d'intrusos.
LOPDGDD	Llei orgànica de protecció de dades personals i garantia dels drets digitals.
TIC	Tecnologies de la Informació i la Comunicació.
ENFSI	European Network of Forensic Science Institutes.
CID / CIA	Confidencialitat, Integritat i Disponibilitat (CID) o l'equivalent en anglès Confidenciality, Integrity and Availability (CIA).

2. a) Fals
b) Cert
c) Cert
d) Fals
e) Cert
f) Fals

3.

Delicte informàtic	SGSI
Delicte d'intrusió	Qualsevol disciplina els principis científics de la qual s'utilitzin per a ajudar la justícia
ISO 27000	No està definit al Codi Penal
Ciències forenses	197bis del Codi Penal

4.
- Evitar la contaminació.
- Actuar metòdicament.
- Tenir control sobre l'evidència.

5. Fals.

6. a) Cert
b) Cert
c) Cert
d) Fals
e) Fals

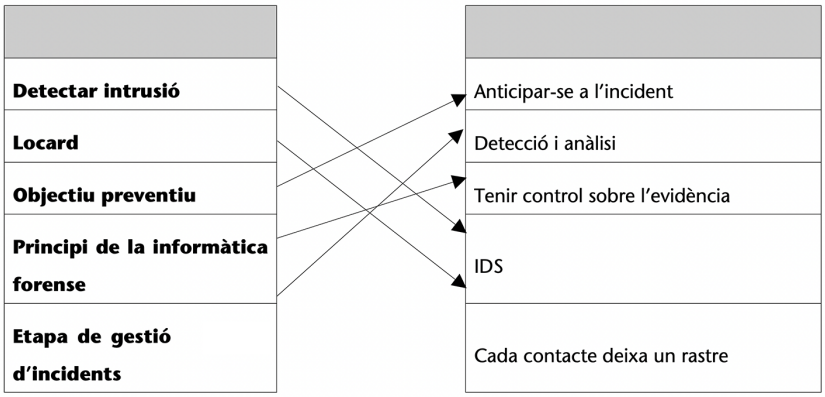
7. Articles del Codi Penal:

- 197
- 248

- 264

8. c

9.



10. a) Fals
b) Cert
c) Cert
d) Fals
e) Cert

Glossari

actiu *m* Són els components indispensables per al correcte funcionament d'un sistema informàtic. En general, el maquinari, el programari i les dades.

CART Computer Analysis and Response Team. L'equip de resposta d'anàlisi d'ordinadors de l'FBI ofereix ajuda en la recerca i adquisició de proves d'ordinador, així com exàmens forenses i suport tècnic per a investigacions.

ciència forense *f* L'aplicació de pràctiques científiques dins el procés legal. La ciència forense abasta tant la branca civil com la penal del dret.

cracking Accedir de manera il·legal a dades emmagatzemades en un ordinador o servidor.

dades *f pl* Conjunt discret de factors objectius sobre «alguna cosa». Pot ser un nombre, una lletra...

delicte d'intrusió informàtica *m* Accés a un sistema informàtic vulnerant la seguretat establerta. Apareix tipificat a l'article 197bis del Codi Penal.

demanda *f* Petició concreta, davant un òrgan d'una jurisdicció determinada, que inicia un procediment davant d'aquest. En aquesta demanda es narren els fets, s'adjunten documents i s'expressen fonaments de dret.

denúncia *f* Acció de posar en coneixement de l'autoritat competent una infracció penal o administrativa. En general, és obligatòria per a qui l'hagi presenciat o en tingui coneixement.

diligència *f* Actuació del secretari judicial en un procediment criminal o civil.

element material probatori *m* Objecte que serveix per provar uns fets com, per exemple, una pistola que és a l'escena del crim.

evidència *f* Qualsevol element que proporcioni informació de la qual es pugui inferir alguna conclusió o bé que constitueixi una troballa relacionada amb el fet que s'investiga.

FLECT Federal Law Enforcement Training Center. Centre d'entrenament federal per al compliment de la llei. És una organització de formació de compliment de la llei que entrena a més de 80 agències federals. El centre també proporciona servei a agències estatals i internacionals. Té la seva seu a Glynco. http://www.fletc.gov

IACIS International Association of Computer Investigative Specialists. Organització internacional d'especialistes en investigació informàtica. És un voluntariat internacional sense ànim de lucre compost per professionals dedicats a l'ensenyament en el camp de la informàtica forense. Els membres de l'IACIS representen a professionals d'àmbit nacional i internacional. http://www.iacis.com/

incident *m* Qualsevol fet anòmal que afecti el funcionament del sistema informàtic.

informació *f* La reunificació i estructuració de les dades en un context que li dona sentit.

informàtica forense *f* Ciència forense que s'ocupa de l'ús dels mètodes científics aplicables als sistemes informàtics. S'encarrega de la preservació, identificació, extracció, documentació i interpretació de l'evidència digital, de manera que aquesta sigui acceptada en un procés judicial.

insaculació *f* Selecció del perit per sorteig entre els membres de les llistes de perits o bé entre tres perits (terna) que s'hagin proposat al jutge.

IOCE International Organization on Computer Evidence. Organització internacional d'especialistes en evidència computacional. El seu propòsit és proveir un fòrum internacional per a l'intercanvi de la informació relacionada amb la investigació computacional i la informàtica forense.

jurisdicció *f* Conjunt d'òrgans jurisdiccionals ordinaris o especials. Als ordinaris, se'ls atribueix el coneixement i la resolució dels conflictes en general, mentre que els especials s'ocupen de matèries específiques com, per exemple, la militar.

jurisdicció ordinària *f* Jurisdicció separada en quatre ordres: civil, penal, contenciós administratiu i laboral o social.

màxima *f* Regla, principi o proposició generalment admesa pels qui professen una facultat o ciència.

ministeri fiscal *m* Òrgan integrat dins del poder judicial que actua amb autonomia en l'acompliment de les seves funcions, exerceix la seva missió per mitjà d'òrgans propis i actua de manera coordinada i unitària a tot el territori de l'Estat.

organització *f* Qualsevol entitat, institució o agrupació que necessiti o utilitzi una infraestructura informàtica per a dur a terme el seu objectiu.

política de seguretat *f* Conjunt de regles, normes i protocols d'actuació que s'encarreguen de vetllar per a la seguretat informàtica de l'organització. Es tracta d'un pla realitzat per a combatre tots els riscos als quals està exposada l'organització en el món digital.

provisió de fons *f* Quantitat de diners que la part o les parts lliuren a compte dels honoraris totals per a efectuar les proves pericials sol·licitades.

querella *f* Concepte similar a la denúncia, però en aquest cas el querellant manifesta la voluntat de formar part de la causa i s'han de complir alguns requisits addicionals. Es dirigeix a l'acció penal.

ransomware *m* Programari maliciós que requereix a la víctima un pagament per a poder accedir als fitxers que ha xifrat.

recurs d'apel·lació *m* Recurs enfront de la sentència definitiva dictada pel jutge penal.

signatura electrònica *f* Procediment que permet comprovar la identitat de l'emissor d'un missatge electrònic i la seva autenticitat. Perquè sigui equiparable a la signatura manuscrita ha de ser avançada, basada en un certificat reconegut i haver estat creada per un dispositiu segur de creació de signatura.

signatura electrònica avançada *f* Signatura que permet identificar el signatari i que es pot vincular, de manera única, tant al signatari com a les dades, i també permet detectar canvis posteriors de les dades.

sistema informàtic *m* Tot dispositiu físic o lògic utilitzat per a crear, generar, enviar, rebre, processar, comunicar o emmagatzemar, de qualsevol forma, missatges de dades.

Tecnologies de la Informació *f pl* Conjunt de tècniques per a processar informació en qualsevol format que pugui aparèixer. Amb això també s'inclou la informàtica.
sigla: **TI**

terna *f* Conjunt de tres persones perquè es designi entre elles la que ha d'exercir un càrrec o una ocupació.

TI Vegeu Tecnologies de la Informació.

Bibliografia

Abel Lluch, X. (2006). *Empresa y prueba informática*. Barcelona: Bosch.

Agencia Estatal BOE (1882). Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal (BOE núm. 260, de 17/09/1882). <http://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf>

Agencia Estatal BOE (1978). Constitución Española de 27 de diciembre de 1978 (BOE núm. 311, de 29 de diciembre de 1978). <http://www.parlament.cat/document/nom/ConstitucioConsolidat.pdf>

Agencia Estatal BOE (1995). Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (BOE núm. 281, de 24/11/1995). <http://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf>

Agencia Estatal BOE (1996). Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril (BOE núm. 53, de 2 de marzo de 2019). <http://www.boe.es/boe_catalan/dias/2019/03/02/pdfs/BOE-A-2019-2974-C.pdf>

Agencia Estatal BOE (2002). Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE núm. 166, de 12/07/2002). <http://www.boe.es/buscar/act.php?id=BOE-A-2002-13758>

Agencia Estatal BOE (2003). Ley 59/2003, de 19 de diciembre, de firma electrónica (BOE núm. 304, de 20/12/2003). http://www.boe.es/buscar/act.php?id=BOE-A-2003-23399

Agencia Estatal BOE (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 6 de diciembre de 2018, páginas 119.788 a 119.857). <http://www.boe.es/boe_catalan/dias/2018/12/06/pdfs/BOE-A-2018-16673-C.pdf>

Balagué Doménech, J. C. (2007). *La prueba pericial contable en las jurisdicciones civil, penal, contencioso-administrativa y laboral*. Barcelona: Bosch.

Colobran Huguet, M.; Arques Soldevila, J.; Marco Galindo, E. (2008). *Administració de sistemes operatius en xarxa*. Barcelona: Editorial UOC.

Colobran Huguet, M. (2015). *A General-Purpose Security Framework. PHD Thesis*. Universitat Autònoma de Barcelona. <http://www.tdx.cat/handle/10803/322814>

Colobran Huguet, M.; Arques Soldevila, J.; Guash Petit, A. (2012). *Anàlisi forense de sistemes d'informació. Investigació de la prova digital*. Barcelona: Editorial UOC.

Elias Baturones, J. J. (2008). *La prueba de documentos electrónicos en los tribunales de justicia*. València: Tirant lo Blanch.

Flores Prada, I. (2006). *La prueba pericial de parte en el proceso civil*. València: Tirant lo Blanch.

García Pañeda, X.; Melendi Palacio, D. (2008). *La peritación informática. Un enfoque práctico*. Oviedo: Colegio Oficial de Ingenieros en Informática del Principado de Asturias.

Guasch Petit, A. i altres (2008). *Auditoría, peritajes y aspectos legales para informáticos*. Barcelona: UOC.

Harris, S.; Harper A.; Eagle, C.; Ness, J.; Lester, M. (2005). *Hacking Etico / Gray Hat Hacking* (Hackers & Seguridad / Hackers and Security). Anaya Publishers.

Humero Martín, A. (2006). *Guía de actuación y responsabilidades del perito en los procedimientos: civiles, penales, contencioso-administrativos, tributarios, sancionadores de consumo, arbitrales*. Madrid: Dykinson.

Luzón Cuesta, J. M. (2000). *La prueba en el proceso penal derivada de la entrada y registro domiciliario*. Madrid: Cólex.

Scientific Working Group on Digital Evidence (2006). *Best Practices for Computer Forensics*. <http://www.swgde.org/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf>

Union Europea (2016). *General Data Protection Regulation (EU)* 2016/679. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL>

U.S. Department of Justice. Federal Bureu of Investigation. Laboratory Division (2007). Handbook of Forensic Services. EUA. <http://www.fbi.gov/file-repository/handbook-of-forensic-services-pdf.pdf/view>