1 ASIX

**MÒDUL 2: GESTIÓ DE BASE DE DADES**

ACTIVITAT 25: Seguretat de les dades

línea horizontal

# 



**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Alex Marin

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

**ÍNDEX**

[**EXERCICI 1 – Concepte de seguretat de les dades 3**](#_r1t74ixqluvj)

[CAS 1 3](#_kdciglb1us8d)

[CAS 2 3](#_jjfeo5joxbj)

[CAS 3 4](#_9vn75o93h7g5)

[CAS 4 4](#_sahtrtvi2zyx)

[CAS 5 5](#_hqq6hvtvqqws)

[CAS 6 5](#_xa93sjb3q3rt)

[**EXERCICI 2 – NORMATIVA VIGENT SOBRE LES DADES 7**](#_v059ptiqf9vc)

[Segons la LOPD, en quins nivells classifiquem les dades, segons el seu contingut? Posa exemples. 7](#_i4g7zcppexm2)

[Quines mesures marca la LOPD que s’han de prendre en funció del nivell de la informació tractada? 7](#_h76sr5uninbq)

[Fes una proposta de les mesures a AFEGEIX a nivell ORGANITZATIU i TÈCNIC per cobrir els requeriments del RGPD? 8](#_t3akyshys5n1)

# EXERCICI 1 – Concepte de seguretat de les dades

Digues, dels següents casos exposats a continuació, quines de les propietats (confidencialitat, disponibilitat i integritat) que formen part de la seguretat de la informació s’han vist afectades

### CAS 1

Al març de 2011, l'Administració Nacional d'Aeronàutica i de l'Espai d'Estats Units (NASA) va perdre un ordinador personal en el qual hi havia informació confidencial molt valuosa. En concret, el dispositiu emmagatzemava, entre altres dades sensibles els algorismes necessaris per manejar l'Estació Espacial Internacional (ISS) de forma remota.

La propietat afectada de la seguretat de la informació és la confidencialitat.

L'ordinador personal que contenia informació confidencial va ser perdut i, per tant, la informació sensible que hi havia a dins va quedar exposada.

Això implica que la informació podria ser llegida, copiada o mal utilitzada per persones no autoritzades, posant en perill les operacions de la ISS i la seguretat de les dades emmagatzemades.

### CAS 2

Múltiples serveis de Microsoft han estat sense accés durant prop d'una hora de la tarda d'avui, com EL MUNDO ha pogut comprovar en intentar accedir a Hotmail, Outlook, Skype i Xbox Live. Encara que la companyia no ha reconegut el problema públicament, molts usuaris ho han assenyalat en xarxes socials i en Internet.

La propietat afectada de la seguretat de la informació és la disponibilitat. Els serveis de Microsoft com Hotmail, Outlook, Skype i Xbox Live no estaven disponibles durant prop d'una hora, el que significa que els usuaris no podien accedir als seus comptes i dades, i no podien utilitzar els serveis proporcionats per aquestes plataformes. Això implica una interrupció en la disponibilitat dels serveis, el que podria tenir un impacte negatiu en els usuaris i en el negoci de Microsoft.

### CAS 3

Laura García, és una secretària de la clínica MOLT FUTUR S. A. Cada dia vénen a la clínica una mitjana d'entre 50 i 80 pacients per passar consulta amb el seu metge.

A primera hora del matí, han arribat diversos pacients amb la mateixa hora de visita per al metge Jorge Clemente fet que ha desencadenat una mica de descontrol en secretària.

La Laura ha consultat les fitxes dels pacients un a un per comprovar que havia succeït. A part de verificar que, efectivament el programari de gestió havia permès introduir pacients amb la mateixa hora de consulta per a un mateix metge, també observa que la informació d'alguns dels pacients tampoc és correcta. Com és el cas de la pacient Marta Vela la que, segons la seva fitxa, té 223 anys o com el cas de Rodrigo Estrada que en la seva fitxa apareix un DNI amb dues lletres.

Les propietats afectades de la seguretat de la informació són la integritat i la disponibilitat. La informació dels pacients no és correcta, com el cas de la pacient Marta Vela que té una edat impossible o Rodrigo Estrada que té un DNI amb dues lletres. Això indica que la integritat de la informació ha estat compromesa i que la informació no està exacta, completa i coherent. D'altra banda, la disponibilitat també ha estat afectada, ja que els pacients no han pogut passar consulta al seu metge degut al descontrol generat per la coincidència d'hores, el que ha afectat la disponibilitat del servei proporcionat per la clínica.

### CAS 4

Marc García i Gemma Capdevila són dos estudiants brillants de l'escola Jaume Viladoms. Encara que han suspès diverses assignatures per no lliurar les pràctiques i per faltes d'assistència, han demostrat tenir una capacitat excel·lent en tots els temes relacionats amb la seguretat dels sistemes informàtics.

Un dia, entre bromes, la Gemma comenta amb el Marc que creu que la plataforma clickEdu de l'escola és vulnerable i que seria molt fàcil accedir a la informació de la base de dades.

Com el Marc sent curiositat per veure fins a quin punt té raó la Gemma, li proposa treballar conjuntament per comprovar si realment la plataforma és tan vulnerable com ella diu.

La mateixa tarda, després d'unes hores de recerca i uns quants intents, aconsegueixen accedir a la base de dades en la qual s'allotja la plataforma clickEdu. De les múltiples taules que hi ha en la base de dades, en Marc i la Gemma se centren en la de "Notes". En veure tota aquesta informació i saber que són capaços de modificar-la, en Marc i la Gemma arriben a l'acord de canviar les notes de les assignatures en les quals han suspès per un 10 com a premi de la seva gran gesta.

Les propietats de confidencialitat i integritat s'han vist afectades. Pel que fa a la confidencialitat, el fet que el Marc i la Gemma hagin accedit a la base de dades de la plataforma clickEdu implica que han accedit a informació que no estava destinada per a ells i que podria ser confidencial per a altres usuaris de la plataforma. Pel que fa a la integritat, el fet que hagin modificat les notes dels seus propis exàmens posa en qüestió la veracitat de la informació i la fidelitat dels registres en la plataforma. A més, el fet que hagin modificat les notes de manera no autoritzada també posa en qüestió la integritat de la informació. La disponibilitat, en aquest cas, no sembla haver estat afectada directament.

### CAS 5

Al març de 2011 es va saber que un empleat de la companyia British Petroleum (BP) havia perdut un ordinador portàtil que contenia dades personals de 13.000 ciutadans de Louisiana que van presentar reclamacions d'indemnització després de l'abocament de petroli en el Golf de Mèxic, segons va publicar el diari The Guardian. El portàtil va ser robat durant un viatge de negocis, segons va afirmar Curtis Thomas, un portaveu de la companyia.

La propietat afectada és la confidencialitat de les dades personals dels ciutadans de Louisiana. La pèrdua del portàtil i el robatori de les dades que contenia van fer que aquesta informació confidencial arribés a mans no autoritzades, posant en risc la privacitat dels afectats.

### CAS 6

La setmana passada, Amazon va ser la protagonista d'un important error que va deixar sense servei a moltes plataformes i aplicacions d'Internet, com Slack o Imgur. L'origen del problema es va conèixer ràpid i es va fer públic per esclarir qualsevol dubte: un empleat havia introduït una errata en un codi de programació.

La propietat afectada de la seguretat de la informació és la disponibilitat, ja que el servei va quedar inoperable per moltes plataformes i aplicacions d'Internet a causa de l'error introduït en el codi de programació. Això va afectar la capacitat d'aquestes plataformes i aplicacions per mantenir el servei accessible i en línia per als seus usuaris.

### 

# EXERCICI 2 – NORMATIVA VIGENT SOBRE LES DADES

Busca informació i respon a les següents preguntes:

### Segons la LOPD, en quins nivells classifiquem les dades, segons el seu contingut? Posa exemples.

Segons la LOPD (Llei Orgànica de Protecció de Dades), les dades es classifiquen en tres nivells segons el seu contingut i el grau de sensibilitat:

* Dades de caràcter personal: són aquelles que permeten identificar a una persona física, com el nom, cognoms, DNI, adreça, número de telèfon, adreça de correu electrònic, etc.
  + Exemple: Dades dels clients d'una empresa, amb les seves dades personals per a la gestió de les comandes.
* Dades de caràcter protegit: són aquelles que, a més de permetre identificar a una persona física, contenen informació relacionada amb la salut, l'origen racial o ètnic, l'orientació sexual, les creences religioses, etc.
  + Exemple: Històrial mèdic dels pacients d'un centre sanitari.
* Dades de caràcter altament protegit: són aquelles que, a més de permetre identificar a una persona física, contenen informació relacionada amb infraccions penals, condemnes i mesures de seguretat.
  + Exemple: Registres penals d'una comissaria de policia.

### Quines mesures marca la LOPD que s’han de prendre en funció del nivell de la informació tractada?

La LOPD (Llei Orgànica de Protecció de Dades) estableix que, en funció del nivell de protecció que requereixi la informació tractada, s'han de prendre diferents mesures per garantir la seva seguretat.

En general, la LOPD estableix que les mesures de seguretat han de ser proporcionals al risc que representa el tractament de les dades, i ha de tenir en compte la naturalesa de les dades, el volum de les dades, la complexitat del tractament, el nombre d'usuaris que tenen accés a les dades, etc.

* Nivell bàsic: aquest nivell s'aplica a les dades personals que són accessibles a través d'Internet, però que no contenen informació sensible (com ara dades de salut, ideologia, religió, etc.). En aquest cas, les mesures de seguretat que s'han de prendre són, com a mínim, les següents: identificació i autenticació dels usuaris, realització de còpies de seguretat de les dades i manteniment actualitzat del programari de seguretat.
* Nivell mitjà: aquest nivell s'aplica a les dades personals que contenen informació sensible, com ara dades de salut, ideologia, religió, etc. En aquest cas, les mesures de seguretat que s'han de prendre són més estrictes, com ara la identificació i autenticació reforçada dels usuaris, l'ús de xifrat de dades, la restricció d'accés només als usuaris que realment necessitin accedir a les dades, la realització de revisions periòdiques de les mesures de seguretat, etc.
* Nivell alt: aquest nivell s'aplica a les dades personals que poden afectar la llibertat, la privacitat o altres drets fonamentals de les persones. En aquest cas, les mesures de seguretat són les més estrictes i inclouen, entre d'altres: la identificació i autenticació reforçada dels usuaris, l'ús de xifrat de dades avançat, la restricció d'accés només als usuaris que realment necessitin accedir a les dades i amb un registre detallat de les seves accions, la realització de revisions periòdiques de les mesures de seguretat, la implementació de polítiques de gestió de contrasenyes, l'ús de protocols segurs de comunicació, etc.

### Fes una proposta de les mesures a AFEGEIX a nivell ORGANITZATIU i TÈCNIC per cobrir els requeriments del RGPD?

Per cobrir els requeriments del RGPD, a continuació, es detallen algunes mesures que es poden afegir a nivell organitzatiu i tècnic:

* Nivell Organitzatiu:

Establir un programa de formació i conscienciació en matèria de protecció de dades per a tot el personal que treballa amb dades personals.

Definir les funcions i responsabilitats de la figura del Delegat de Protecció de Dades (DPO).

Establir un pla de contingència en cas de violació de dades personals que incloui les mesures a prendre en cas de detecció d'una infracció.

Actualitzar les polítiques de privacitat i protecció de dades per assegurar que reflecteixen les pràctiques de tractament de dades.

Establir acords de confidencialitat amb terceres parts que puguin tenir accés a les dades personals.

* Nivell Tècnic:

Implementar mecanismes de xifrat i anonimització de les dades personals.

Establir polítiques de gestió de contrasenyes segures, així com protocols de gestió d'identitats i accessos per garantir que només els usuaris autoritzats puguin accedir a les dades personals.

Establir un sistema de monitoratge i auditoria per detectar qualsevol accés no autoritzat a les dades personals.

Implementar mesures de seguretat físiques, com ara controls d'accés als edificis i sales de servidors, per prevenir el robatori o la pèrdua de dades personals.

Realitzar una avaluació de riscos periòdica per identificar possibles vulnerabilitats en el tractament de dades i establir mesures preventives per mitigar-les.

Aquestes són només algunes de les mesures que es poden implementar per cobrir els requeriments del RGPD. Cada organització ha de realitzar una avaluació de riscos pròpia per determinar quines són les mesures més adequades segons les seves necessitats i el nivell de protecció requerit per a les dades que tracta.