

Nous models de salut en la societat de la informació: salut electrònica

Luis Fernández-Luque
Elia Gabarrón
Francisco Sánchez Laguna

PID_00206811



Els textos i imatges publicats en aquesta obra estan subjectes –llevat que s'indiqui el contrari– a una llicència de Reconeixement-NoComercial-SenseObraDerivada (BY-NC-ND) v.3.0 Espanya de Creative Commons. Podeu copiar-los, distribuir-los i transmetre'ls públicament sempre que en citeu l'autor i la font (FUOC. Fundació per a la Universitat Oberta de Catalunya), no en feu un ús comercial i no en feu obra derivada. La llicència completa es pot consultar a <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca>

Índex

Introducció	7
Objectius	10
1. Intel·ligència artificial	11
1.1. Algorismes genètics	12
1.1.1. Principis bàsics dels algorismes genètics	13
1.2. Xarxes neuronals	14
1.2.1. El perceptró	15
1.3. Aplicacions pràctiques de la intel·ligència artificial	16
2. Estàndards i interoperabilitat	18
2.1. SNOMED CT	18
2.2. HL7	20
2.3. DICOM	22
2.4. Interoperabilitat	22
2.4.1. Interoperabilitat tècnica	23
2.4.2. Interoperabilitat sintàctica	23
2.4.3. Interoperabilitat semàntica	24
3. Salut ubiqua	25
3.1. Salut mòbil	25
3.2. La Internet dels objectes	27
4. Pacients i medicina participativa	31
4.1. Els e-pacients	31
4.2. Medicina participativa	34
4.3. Comunitats de pacients	35
5. eHealth literacy	39
5.1. eHealth literacy i els seus components	39
5.2. Alfabetització en salut. Entrevista al Dr. Ignacio Basagoiti	40
6. Eines 2.0 utilitzades en salut	43
6.1. Facebook	44
6.2. Twitter	45
6.3. YouTube	45
6.4. Viquipèdia	46
6.5. Altres eines 2.0 en salut	46
7. e-Salut pública i jocs per a la salut	48

7.1.	e-Salut pública	48
7.1.1.	Els avantatges	48
7.1.2.	Els inconvenients	49
7.2.	Jocs i ludificació per a la salut	50
8.	La LOPD i el Web 2.0.....	53
8.1.	Introducció	53
8.1.1.	Les dades personals tenen valor econòmic	53
8.1.2.	El negoci de les xarxes socials són les dades personals	53
8.1.3.	No hi ha oportunitat sense risc	53
8.1.4.	En general, les xarxes socials presenten els mateixos riscos que qualsevol altre servei de tecnologies de la informació	54
8.1.5.	Hi ha riscos particulars de les xarxes socials	54
8.1.6.	El risc zero no existeix	54
8.1.7.	La decisió sobre el risc es pren en el més alt nivell	55
8.1.8.	Eficàcia relacionada amb els objectius de l'organització	55
8.2.	Àrees de risc	55
8.3.	Drets 2.0	57
8.3.1.	La llibertat d'expressió en el Web 2.0	58
8.3.2.	La llibertat d'informació en el Web 2.0	58
8.3.3.	La intimitat, privadesa i imatge pròpia en el Web 2.0 ...	58
8.3.4.	La protecció de dades en el Web 2.0	58
8.3.5.	La propietat intel·lectual en el Web 2.0	59
8.4.	Obligacions i responsabilitats	60
8.4.1.	Usuaris	60
8.4.2.	Administradors i moderadors	61
8.4.3.	Empreses prestadores de serveis	62
8.5.	Recomanacions	62
8.5.1.	Usuaris	62
8.5.2.	Administradors i moderadors	63
8.5.3.	Mecanismes perquè els usuaris puguin denunciar	64
8.6.	Les administracions públiques 2.0	64
8.6.1.	Motivació	64
8.6.2.	Normativa	64
8.6.3.	Serveis no aplicables	64
8.6.4.	Serveis aplicables	65
8.6.5.	Responsabilitats	66
8.6.6.	Altres riscos	67
8.6.7.	Conclusió	69
9.	Seguretat de la informació.....	70
9.1.	Introducció a la seguretat de la informació en salut i marc legal	70
9.1.1.	La confidencialitat	70

9.1.2.	L'informe ENEAS 2005	70
9.1.3.	Objectius de seguretat 2011 de la Joint Comission	71
9.1.4.	Cas real: la Comissió de Seguretat del Pacient d'un hospital terciari	72
9.1.5.	Conseqüències de la manca de confidencialitat per al pacient	72
9.1.6.	Conseqüències de la manca de confidencialitat per al professional	72
9.2.	De la confidencialitat a la seguretat de la informació. Dimensions de la seguretat	73
9.2.1.	La disponibilitat	73
9.2.2.	Exemple de falta de disponibilitat	74
9.2.3.	La integritat	74
9.2.4.	Exemple de falta d'integritat	75
9.3.	Eines per a la seguretat de la informació	76
9.3.1.	Alineació	76
9.3.2.	Polítiques	77
9.3.3.	Conscienciació	77
9.3.4.	Formació (específica i dirigida)	77
9.3.5.	Infraestructura organitzativa	78
9.3.6.	Supervisió (auditories)	79
9.3.7.	Programes de seguretat de la informació	80
9.3.8.	Gestió de riscos	80
9.4.	Confidencialitat a la Xarxa	81
9.5.	Conclusions	83
	Bibliografia	85

Introducció

El concepte d'*e-salut* està de moda en els últims anys. Són molts els qui en parlen, però no és senzill definir-la, la qual cosa queda patent en la revisió sistemàtica efectuada el 2005 pel Centre for Global eHealth Innovation del Canadà.

Van trobar cinquanta-una definicions úniques que no van mostrar un consens clar. N'hem extret dues, perquè ens semblen de les més completes:

“L'ús de tecnologies emergents de la informació i la comunicació, especialment Internet, per a millorar o desenvolupar la salut i l'atenció sanitària i permetre d'aquesta manera connexions més fortes i eficaces entre pacients, metges, hospitals, asseguradores, laboratoris, farmàcies i proveïdors.”

“Promoure i facilitar la salut i el benestar dels individus i les seves famílies, i també millorar la pràctica professional gràcies a l'ús de les tecnologies de la informació i la comunicació.”

També és digne d'esment el treball de Gunther Eysenbach, que afirma que la *e* d'*e-salut* ha de significar alguna cosa més que *electrònic*. Això queda patent en el que denomina les deu *e* d'*e-salut*:

- 1) Eficiència.
- 2) (*Enhance*). Millorar la qualitat de les atencions.
- 3) Basat en l'evidència.
- 4) (*Empowerment*). Apoderament dels pacients.
- 5) (*Encourage*). Estimular un nou tipus de relació entre pacients i professionals sanitaris.
- 6) Educació, tant dels ciutadans com dels professionals, gràcies als recursos que poden trobar a la Xarxa.
- 7) (*Enable*). Fer possible la comunicació i l'intercanvi d'informació d'una manera estandarditzada.
- 8) (*Extend*). Ampliar l'abast de l'assistència sanitària més enllà dels seus límits convencionals.

9) El repte ètic que comporta aquesta nova manera d'interactuar entre pacients i professionals.

10) Equitat, ja que no hem de deixar que la bretxa digital converteixi l'e-salut en un element diferenciador de classes.

Posteriorment, afegiu unes altres *e*: facilitat d'ús (*easy-to-use*), entretingut (ja que ningú no fa servir una cosa avorrida a llarg termini), emocionant i... que existeixi!

L'impacte que tenen els avenços tecnològics en les nostres vides és impressionant i la salut, un dels nostres béns més preuats, no en queda al marge.

És molt destacable el fet que tothom tingui més accés a la informació i a la tecnologia ha coincidit (i segurament hi ha influït d'una manera decisiva) amb un canvi de paradigma de com les persones s'impliquen en l'atenció a la salut. Hem passat d'un model paternalista, en el qual el metge tenia tota la responsabilitat i el poder de decisió, a un model multidisciplinari i de coresponsabilitat en el qual tots els professionals sanitaris proporcionen informació als pacients perquè ells prenguin les seves pròpies decisions sobre la seva salut. A més, els pacients utilitzaran les tecnologies de les quals disposen (com, per exemple, Internet) per obtenir informació per ells mateixos o interactuar amb altres pacients o professionals de la salut. Aquest fenomen es coneix com a *e-pacients*, i el nou model de participació compartida amb la resta dels actors es coneix com a *medicina participativa*.

En aquest manual, farem un repàs de diferents àrees relacionades amb la disciplina de l'e-salut. El primer bloc se centra en aspectes més tecnològics. Per començar, tractarem de l'apartat d'intel·ligència artificial a tall d'exemple sobre com els ordinadors poden ajudar a analitzar les quantitats ingents de dades que es generen en l'e-salut i, amb això, proveir serveis d'e-salut més intel·ligents. La intel·ligència artificial i l'e-salut no serien possibles sense la integració de les dades, i per aquest motiu en el segon apartat, "Estàndards i interoperabilitat", ens centrarem en com les dades s'integren utilitzant estàndards. La importància d'aquest apartat rau en el fet que, sense una integració de les dades, resulta impossible el flux d'informació i coneixements que és una pedra angular de l'e-salut. Actualment, l'e-salut no està limitada a l'ús d'ordinadors, sinó que podríem dir que ha passat a ser ubiqa mitjançant l'ús de sensors per a mesurar paràmetres fisiològics i dispositius mòbils. La salut mòbil i la Internet dels objectes s'estudien en l'apartat "Salut ubiqa".

El segon bloc d'apartats se centra en aspectes de l'e-salut més propers als usuaris, sia professionals o ciutadans. El cinquè apartat, sobre e-pacients i medicina participativa, tracta del fenomen dels e-pacients i com això ens condueix a una medicina més participativa. L'apartat "*eHealth literacy*" versa sobre una part imprescindible per a la transformació de l'e-salut, que consisteix en la formació en habilitats tecnològiques i de salut dels pacients. Actualment, l'e-

salut es troba en una fase de transformació ràpida amb la popularització de l'ús del Web 2.0. Per aquest motiu, en l'apartat "Eines 2.0 utilitzades en salut" fem un repàs de com el Web 2.0 s'utilitza en salut. Finalment, l'apartat "e-salut pública i jocs per a la salut" tracta sobre com l'e-salut i els jocs seriosos es poden convertir en aliats per a promoure la salut de la població.

Objectius

- 1.** La eSalud consisteix en l'aplicació de les tecnologies de la informació i la comunicació per a la millora de salut. Entre altres aspectes, la eSalud inclou l'ús de sistemes experts per a l'ajuda a la presa de decisions i Internet en totes les seves facetes (xarxes de pacients, objectius connectats).
- 2.** Aquesta obra té com a objectiu proporcionar una base teòrica de diversos aspectes de la eSalud, que sobre la base de la discussió de casos concrets proporcionen una guia sobre els aspectes més importants per al desenvolupament de la eSalud.

1. Intel·ligència artificial

El terme *intel·ligència artificial* fa referència a la intel·ligència en les màquines; a l'intent de fer-les raonar i solucionar problemes d'una manera semblant a un ésser humà. La seva aplicació en l'àmbit sanitari pot resultar tremendament beneficiosa, tant per als professionals que cuiden de la nostra salut (millorant els sistemes d'informació que usen en la pràctica clínica) com per als ciutadans (millorant els dispositius dels quals disposen per a la cura de la seva salut). Posem-ne alguns exemples:

- **Sistemes d'ajuda en la presa de decisions** basats en intel·ligència artificial. Serien capaços d'integrar la gran quantitat d'informació disponible per ajudar els professionals, d'aplicar sempre la màxima evidència científica i reduir la probabilitat d'errors.
- **Intel·ligència artificial aplicada a la formació** dels nostres professionals. S'aconsegueixen entorns de formació extremament realistes en fer que els simuladors es comportin com humans.
- **Dispositius intel·ligents.** Podrien ser molt beneficiosos perquè els ciutadans cuidin de la seva salut, en integrar tota la informació del nostre cos (monitoratge), el nostre entorn i la nostra història clínica per donar-nos el millor consell en cada moment. Al mateix temps, aquests dispositius podrien "treballar" amb els professionals sanitaris que cuiden de la nostra salut.

Exemple

MYCIN. Sistema d'ajuda en la presa de decisions en infeccions bacterianes, desenvolupat el 1975.

Exemple

Simuladors per a cirurgia robòtica.

Exemple

Omnipod comercialitza bombes d'insulina que analitzen dades de sensors de glucosa d'una manera automàtica per, així, ajustar dinàmicament les dosis de medicació.

Passem ara a un pla més teòric per enumerar algunes de les tècniques d'intel·ligència artificial més destacades (Sosa, 2006).

- **Sistemes experts:** son programes informàtics que recopilen el coneixement d'especialistes en una matèria. Els seus components principals són la **base de coneixement** (expressat en un llenguatge que entengui la màquina) i el **programa d'inferència** (el que obté la solució a un problema buscant a la base de coneixement).
- **Algorismes genètics:** aquests algorismes simulen la mecànica de la selecció natural i de la genètica, i utilitzen la informació històrica per trobar nous punts de cerca d'una solució òptima. Això permet obtenir solucions a problemes que, per la seva complexitat, no tenen cap mètode de solució precís.

- **Xarxes neuronals:** es tracta d'una tècnica de processament massiu i paral·lel de la informació que emula les característiques essencials de l'estructura neuronal del cervell biològic.
- **Lògica difusa:** es basa a comprendre els quantificadors del nostre llenguatge (per exemple, *molt*, *bastant*, *una mica*, etc.), i trobem una funció de pertinença a cada estat de cadascun dels seus elements. Es basa en regles heurístiques de la forma **si (antecedent) llavors (consegüent)**, en què l'antecedent i el consegüent són també conjunts difusos, purs o com a resultat d'operar-hi. Posem com a exemple el funcionament d'un termòstat: "si fa molta calor, **llavors** ha augmentat dràsticament la temperatura".

La naturalesa ha desenvolupat algunes maneres de solucionar problemes extraordinàriament eficients, encara que els principis del seu funcionament no s'entenen bé. Entendre com la intel·ligència artificial intenta imitar els principis biològics resulta fascinant. Per aquest motiu, explicarem amb més detall les dues tècniques més biologicistes de les enumerades anteriorment.

Acabarem l'apartat amb una secció dedicada a l'aplicació pràctica d'aquestes tècniques i posarem alguns articles científics com a exemple d'això.

1.1. Algorismes genètics

En l'evolució natural, els individus transfereixen les seves característiques a la seva descendència gràcies a la informació codificada en els seus gens. Cada pare contribueix amb un conjunt de característiques, i les combinacions d'aquests atributs poden aconseguir que els membres d'una generació estiguin millor adaptats a l'entorn que l'anterior.

Un algorisme genètic és una forma d'intel·ligència artificial que utilitza tècniques similars per proporcionar un mètode robust de resolució de problemes (Holland, 1992). Presenta l'avantatge que requereix poc coneixement específic del domini del problema per a implementar l'algorisme. Posteriorment, amb tècniques de selecció natural es busca una solució òptima i s'evoluciona.

Els algorismes genètics són molt útils per a treballar amb gran quantitat de dades, fins i tot amb les que tenen una estructura complexa. Són capaços de trobar solucions òptimes per a la presa de decisions, la classificació, l'optimització i la simulació d'escenaris reals.

1.1.1. Principis bàsics dels algorismes genètics

1) **Definició del problema.** Primer, hem de dissenyar una codificació adequada per a les possibles solucions: els cromosomes. L'exemple més simple de codificació és una representació binària (per a indicar la presència o absència d'un paràmetre, per exemple). Posteriorment, hem de crear una fórmula per avaluar la idoneïtat per resoldre el problema de cada membre d'una generació. D'aquesta manera, podem assignar a cadascun un valor discret que el representi i ens permeti comparar-los per identificar els millors.

2) **Avaluació.** Una vegada hem definit el problema com un algorisme genètic, es produirà una població inicial a l'atzar. S'aplicarà a cadascun la fórmula d'idoneïtat que hem descrit anteriorment, i s'assignarà un valor a cada membre de la població.

3) **Selecció dels pares.** L'objectiu d'aquesta fase és donar més oportunitats reproductives als membres més aptes en la solució del problema. Un dels procediments més populars per a fer-ho utilitza el concepte de la *ruleta de la fortuna*. La ruleta és un cercle que queda dividit en àrees proporcionals segons l'aptitud de cada membre (calculada amb la fórmula esmentada anteriorment) i imaginant que es llança la bola en aquesta ruleta. D'aquesta manera, els membres més aptes tenen més possibilitats de ser seleccionats, encara que hi hagi la possibilitat que membres menys aptes siguin seleccionats. En la pràctica, la bola de la ruleta se substitueix per un generador de nombres aleatoris.

4) **Entrecreuament.** En la naturalesa, durant la meiosi, es produeix l'entrecreuament de gens dels dos progenitors. D'aquesta manera, en els descendents podem observar característiques dels seus progenitors barrejades, la qual cosa pot resultar en una combinació més apta. Si apliquem aquest principi als algorismes genètics, podem arribar a solucions del problema de manera més ràpida. La tècnica més simple es denomina *entrecreuament en un punt*: se selecciona un punt a l'atzar que determina quina part anirà a cada descendent. Posem-ne un exemple.

Progenitor 1: a1 a2#a3 a4 Descendent 1: a1 a2 b3 b4

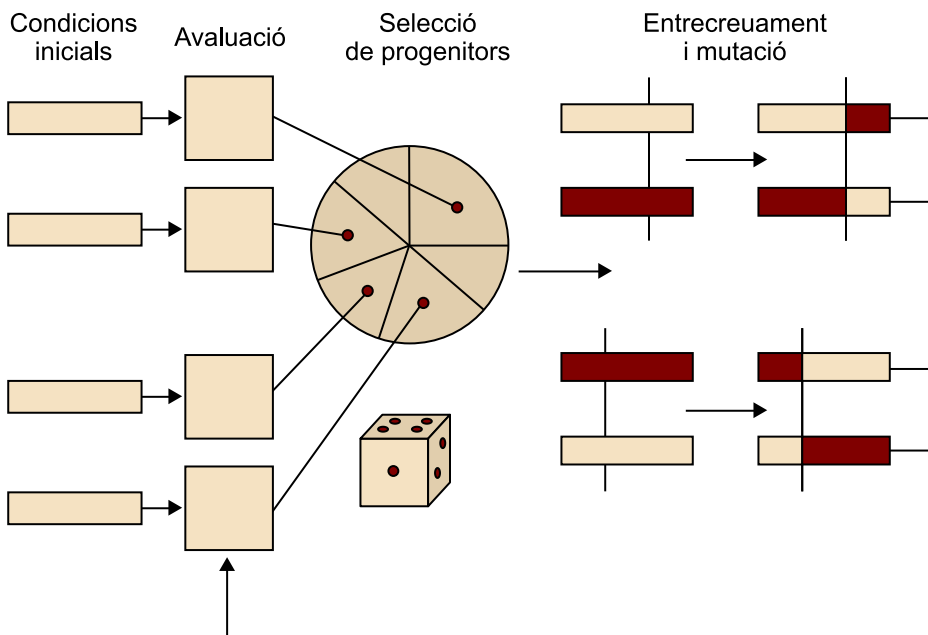
Progenitor 2: b1 b2#b3 b4 Descendent 2: b1 b2 a3 a4

5) **Mutació.** Es tracta d'un altre element important en la naturalesa que intervé d'una manera important en la nostra evolució. En el cas dels algorismes genètics, se sol introduir una probabilitat de mutació (usualment molt baixa, per exemple 0,008) que determina la modificació a l'atzar d'alguns dels elements. Les mutacions són molt importants, ja que permeten explorar tot un seguit de solucions noves a les quals no hauríem arribat d'una altra manera. A més, ajuden a prevenir el problema de convergència a una solució no òptima (l'equivalent en biologia a una línia successòria endogàmica).

A continuació, resumim els passos principals d'un algorisme genètic:

- 1) Definir els cromosomes i la fórmula que en mesurarà la idoneïtat.
- 2) Generar d'una manera aleatòria la primera generació.
- 3) Avaluar aquesta generació.
- 4) Seleccionar els progenitors següents i el punt d'entrecuament.
- 5) Dur a terme l'entrecuament.
- 6) Calcular la possibilitat de mutació.
- 7) Repetir els passos del 3 al 6 per a un nombre de generacions.
- 8) En finalitzar, el cromosoma més apte serà la solució.

Esquema de funcionament d'un algorisme genètic



1.2. Xarxes neuronals

Els ordinadors tenen un rendiment molt pobre quan es tracta de dur a terme tasques intuïtives, al contrari que el cervell. Això es deu al fet que el cervell manipula i processa la informació d'una manera diferent. La unitat funcional del cervell és la neurona. És una unitat de processament relativament senzilla, ja que (simplificant molt) només dona un senyal de sortida en funció de la suma de les entrades. No obstant això, la vertadera potència de la neurona està en les seves connexions: s'estima que el cervell té deu milions de neurones i, aproximadament, seixanta bilions de connexions entre elles. El cervell és lent en comparació d'un ordinador actual (mil·lisegons enfront de nanosegons), però ho compensa amb la seva capacitat de funcionament en paral·lel gràcies al nombre elevat de connexions interneuronals que fan. A més, aquestes connexions poden canviar (procés d'aprenentatge del cervell), característica que també imiten les xarxes neuronals artificials.

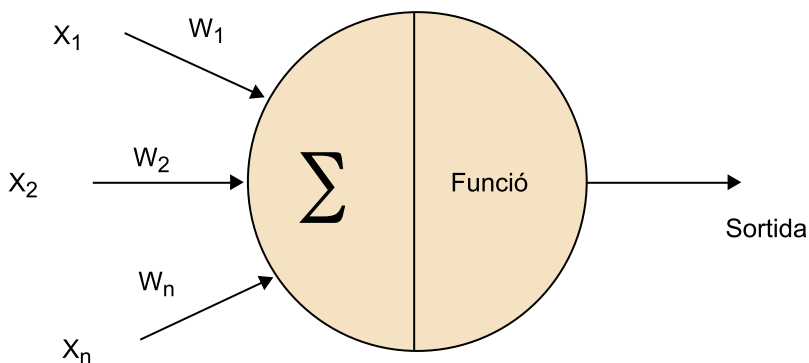
1.2.1. El perceptró

És un model utilitzable de la neurona (introduït per McCulloch i Pitts el 1943) que utilitza principis similars: suma, llindar d'acció i sortida. En lloc de concentracions químiques, el perceptró utilitza una funció matemàtica per establir el llindar d'acció.

En el diagrama següent, tenim un exemple bàsic de perceptró.

- X són els valors d'entrada.
- W són els coeficients que modulen cada entrada.
- Σ és la funció matemàtica que calcula la sortida del perceptró.

Exemple de percepció



L'atractiu més gran de les xarxes neuronals artificials és que es poden entrenar per a un problema particular. Això es fa mitjançant l'optimització dels coeficients que modifiquen les entrades del perceptró, assignats inicialment a l'atzar, per donar el mínim error possible en un conjunt de condicions d'entrada conegudes dins del domini del problema. Una vegada que la xarxa neuronal ha estat entrenada amb valors coneguts, es pot utilitzar per classificar les dades la sortida de les quals és desconeguda.

Hi ha múltiples algorismes d'entrenament. En posarem com a exemple un de senzill (a l'efecte docent), que en general es denomina *regla delta generalitzada* o *de Widrow-Hoff*.

Per a entrenar un perceptró, necessitarem un conjunt de dades de referència les entrades i sortides del qual siguin conegudes. Aquest es dividirà en dos subconjunts: l'un per a l'entrenament i l'altre per a comprovar el bon funcionament del perceptró.

L'algorisme d'entrenament consisteix a:

- 1) Assignar a l'atzar els coeficients que modulen cada entrada al perceptró (W).

2) Presentar al perceptró els valors d'entrada (X) coneguts i calcular-ne la sortida.

3) Si la sortida és correcta, tornar al pas 2 assignant a X el valor següent del conjunt de què disposem per a l'entrenament.

4) Si la sortida és incorrecta, ajustar els coeficients (W) per a cada línia d'entrada amb l'objectiu de minimitzar la diferència entre el que s'ha calculat i la sortida correcta coneguda.

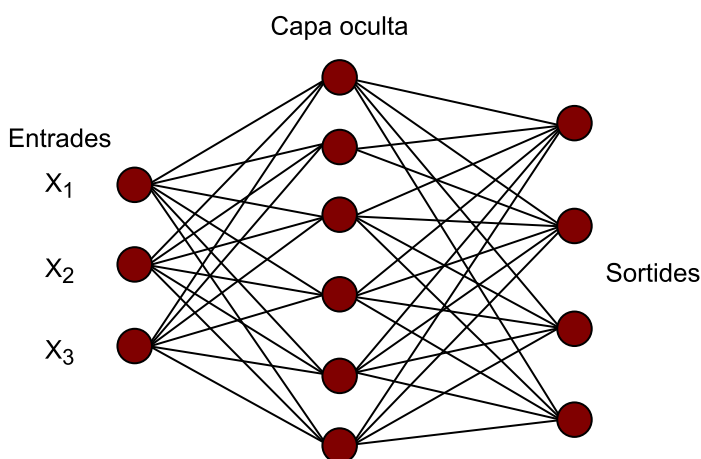
a) Si s'esperava 1 i el resultat és 0, s'augmentaran els coeficients en un valor δ predefinit ($W + \delta$).

b) Si s'esperava 0 i el resultat és 1, es reduiran els coeficients amb el mateix valor δ predefinit ($W - \delta$).

c) Repetir el procés amb cada patró d'entrenament.

Evidentment, aquest és un exemple molt simplificat de xarxa neuronal a l'efecte docent. Per a problemes més complexos, serà necessari complicar la xarxa mitjançant la introducció de més perceptrons i fins i tot capes intermèdies de perceptrons, denominades *capas ocultes*. Si observem el diagrama d'exemple que trobem sota aquestes paraules, ens podem fer una idea de la potència que pot adquirir una xarxa neuronal i la complexitat dels càlculs necessaris per a fer-la funcionar.

Exemple de xarxa neuronal complexa



1.3. Aplicacions pràctiques de la intel·ligència artificial

En aquest apartat, enunciarem alguns articles científics recents que utilitzen les tècniques explicades en problemes reals amb rellevància clínica.

Els algorismes genètics són bons en la caracterització de patrons. Per exemple, en l'optimització de l'anàlisi d'imatges: avaluació de les classes de cèl·lules sanguínies en imatges de microscopi o per a facilitar la planificació d'un tracta-

ment a partir de les imatges d'una ressonància magnètica. També es poden utilitzar per a la millora de productes farmacèutics; per exemple, augmentant-ne la capacitat antibacteriana en optimitzar-ne l'estructura tridimensional.

Una altra aplicació important és la seva capacitat per a millorar la precisió de les xarxes neuronals artificials (cosa que contribueix en el seu entrenament). La combinació d'algorismes genètics i xarxes neuronals artificials és un enfocament important per a millorar l'anàlisi de les dades mèdiques.

Alguns exemples de la bibliografia científica

- **Aplicació d'algorismes genètics:** utilitzant-los per processar imatges de la pell i identificar-hi característiques tumorals, cosa que ajuda en el diagnòstic de càncer de pell (H. Handels, 1999).
- **Aplicació de xarxes neuronals:** s'usen en el disseny de medicaments, en predir-ne l'activitat enzimàtica (M. Szaleniec, 2012).
- **Combinant algorismes genètics i xarxes neuronals:** utilitzant-los en la predicció de l'evolució de pacients crítics, la qual cosa resulta transcendental en la presa de decisions sobre el seu tractament (R. Dybowski, 1996).

Webs recomanats

En els enllaços següents, no solament trobarem una explicació de les tècniques d'intel·ligència artificial estudiades en aquest document. També aprendrem com portar-les a la pràctica, ja que ens ensenyen a programar el nostre propi sistema d'intel·ligència artificial.

- 1) Algorismes genètics
- 2) Xarxes neuronals
- 3) Revista Intel·ligència Artificial en Medicina

2. Estàndards i interoperabilitat

Els estàndards són conjunts de normes en els quals s'acorden criteris i processos per garantir quins elements dissenyats per diferents persones (o empreses) es poden acoblar i interactuar com si haguessin estat dissenyades per la mateixa persona. Fonamentalment, es persegueixen tres objectius.

- **Simplificació:** per quedar-se només amb els models més necessaris.
- **Unificació:** per permetre l'intercanvi en un àmbit internacional.
- **Especificació:** per evitar errors d'identificació i crear un llenguatge clar i precís.

Normalment, són coordinats per un organisme imparcial (tant nacional com internacional) amb la col·laboració de tots els actors (o la gran majoria) implicats en el procés. L'estandardització és un element crucial, com posen de manifest les elevades sumes de diners que els països desenvolupats inverteixen en els organismes normalitzadors.

Gràcies als estàndards podem parlar d'*interoperabilitat*, que consisteix en el fet que dos o més sistemes o components intercanviïn informació i la puguin utilitzar.

Per què això és important en l'àmbit de la sanitat? Perquè estableix les bases necessàries perquè els sistemes d'informació que alberguen la nostra informació clínica en diferents ubicacions (centres de salut, hospitals, clíniques, etc.) siguin capaços de compartir-la, de manera que deixin de ser sitges aïllades d'informació. Així, doncs, tots els professionals sanitaris que cuidin de la nostra salut podran tenir accés a la mateixa informació (com pretén el projecte d'història clínica electrònica nacional o europea) i, d'aquesta manera, evitar redundàncies innecessàries que facin perdre temps, reduir els errors i, en definitiva, augmentar la qualitat en la provisió de cures als ciutadans.

Aquest apartat no pretén ser una llista exhaustiva d'estàndards i tipus d'interoperabilitat. S'enumeraran els més habituals en la pràctica diària, tant en un àmbit professional (tècnic i sanitari) com directiu i polític i que, per tant, és molt recomanable conèixer.

2.1. SNOMED CT

SNOMED CT (*systematized nomenclature of medicine - clinical terms*, 'nomenclatura sistematitzada de medicina - termes clínics') sorgeix de la fusió entre SNOMED RT (*reference terminology*, 'terminologia de referència'), una terminologia

creada originalment pel Col·legi Americà de Patòlegs, i CTV3 (*clinical terms version 3*), desenvolupada per l'NHS (National Health Service, 'Servei Nacional de Salut') del Regne Unit.

SNOMED CT és una extensa terminologia clínica integral que permet als professionals de la salut de tot el món representar la informació clínica d'una manera precisa i inequívoca, en format multilingüe. Conté més de 311.000 conceptes amb significats únics organitzats en jerarquies. Es pot utilitzar per representar informació clínica rellevant d'una manera consistent, fiable i completa.

Actualment, és propietat d'IHTSDO (International Health Terminology Standards Development Organisation, 'Organització Internacional per al Desenvolupament d'Estàndards Terminològics de Salut'), una associació sense ànim de lucre que la manté i distribueix.

Podem destacar les característiques següents de SNOMED CT:

- És un recurs integral i científicament validat.
- És essencial per als registres electrònics de salut.
- És una terminologia que es pot crear amb altres estàndards internacionals.
- Està molt estès, atès que ja s'utilitza en més de cinquanta països.

SNOMED CT conté els components següents.

1) Conceptes: representen ens clínics (com *abscess* o *zigot*).

a) Cadascun està identificat per un codi numèric únic.

b) S'organitzen en jerarquies, d'allò més general a allò més específic. Gràcies a això, encara que la informació es registri d'una manera molt detallada, sempre es podrà agregar d'una manera més general per facilitar-ne l'explotació.

2) Descripcions: enllacen definicions llegibles als conceptes. Un concepte pot tenir diverses descripcions associades, cadascuna de les quals representa un sinònim que descriu la mateixa idea clínica. Perquè ens en fem una idea, trobem prop d'un milió de descripcions en la versió internacional de SNOMED CT (en anglès). Cada traducció inclou un conjunt addicional de descripcions que vinculen els conceptes amb les seves correspondències en els diferents idiomes.

3) Relacions: associen conceptes amb un significat relacionat. Aquestes relacions doten els conceptes implicats de definicions formals i altres característiques.

a) Un tipus de relació és “és un”, que associa un concepte amb d'altres de més generals. Per exemple, el concepte *pneumònia viral* té un “és un” amb el concepte més general de *pneumònia*. Les relacions “és un” defineixen les jerarquies de conceptes de SNOMED CT.

b) Altres relacions representen altres aspectes de la definició d'un concepte. Per exemple, el concepte *pneumònia viral* té una relació tipus agent causal amb el concepte *virus*, i una altra del tipus lloc de la troballa amb el concepte *pulmó*.

c) Perquè ens fem una idea de la dimensió de les relacions, a SNOMED CT n'hi ha més d'un milió.

2.2. HL7

HL7 (Health Level 7, 'Nivell 7 en salut') és una organització que es va fundar el 1987 per produir un estàndard per als sistemes d'informació hospitalaris. El 1994, va ser acreditada per l'ANSI (American National Standards Institute, 'Institut Nacional Americà d'Estàndards'). HL7 desenvolupa diferents tipus d'estàndards.

- **Estàndards de conceptes** (per exemple, HL7 RIM, *reference information model*, 'model d'informació de referència').
- **Estàndards de documents** (per exemple, HL7 CDA, *clinical document architecture*, 'arquitectura del document clínic').
- **Estàndards d'aplicacions** (per exemple, HL7 CCOW, *clinical context object workgroup*, 'grup de treball dels objectes en el context clínic').
- **Estàndards de missatgeria** (per exemple, HL7 v2.x i v3.0).

El nom de *Health Level 7* és una referència a la setena capa del model de referència ISO OSI. El nom indica que HL7 se centra en els protocols de la capa d'aplicació per al domini de la cura de la salut, independent de les capes inferiors.

Model obert de referència per a la interconnexió de sistemes

7. Capa d'aplicació
6. Capa de presentació
5. Capa de sessió
4. Capa de transport
3. Capa de xarxa
2. Capa de dades
1. Capa física

La modelització d'objectes fonamenta la metodologia HL7 V3, que captura la informació i semàntica associades amb l'activitat assistencial. Aquesta metodologia utilitza elements clau del llenguatge unificat de modelització (UML).

HL7 RIM: és un model d'informació que constitueix una especificació estructurada de la informació dins de l'escenari de la salut. Utilitza UML (*unified modeling language*, 'llenguatge unificat de modelització') per representar gràficament un model de classes que permet contextualitzar qualsevol esdeveniment que ocorri dins de l'operació dels serveis de salut.

HL7 V3: és una especificació d'interoperabilitat per a transaccions entre sistemes d'informació i aplicacions de programari utilitzats en el sector de la salut, que permet l'intercanvi electrònic de dades i les comunicacions entre aquestes. HL7 V3 té les característiques següents.

- Es basa en HL7 RIM, a partir del qual es construeixen les especificacions de missatges específics per a diferents dominis de l'escenari de salut.
- Considera l'ús de sintaxi XML, seguint la tendència internacional d'ús d'XML com un llenguatge per a l'intercanvi d'informació estructurada entre diferents plataformes.
- Utilitza principis d'orientació a objectes (POO) i llenguatge unificat de modelització (UML), la qual cosa comporta més detall, claredat i precisió de les especificacions, i també un control més gran sobre els dissenys finals dels missatges.
- No es limita a la capa 7, ja que era necessari desenvolupar un estàndard comprensible que inclogués altres capes del model OSI: XML, seguretat, vocabulari, modelització, metodologia, etc.

- Posa un èmfasi especial en l'ús de vocabularis controlats: LOINC, CIE-10, Snomed CT, etc. De manera addicional, HL7 V3 proposa llistes de codificacions pròpies per a casos específics.

2.3. DICOM

És l'estàndard reconegut mundialment per a l'intercanvi d'imatges mèdiques. Proposat per l'ACR (American College of Radiology, 'Col·legi Americà de Radiologia') i la NEMA (National Electrical Manufacturers Association, 'Associació Nacional de Fabricants de Dispositius Elèctrics'), permet la interoperabilitat i integració d'escàners, servidors, estacions de treball, impressores i maquinari de xarxa de múltiples proveïdors dins d'un sistema d'emmagatzematge i comunicació d'imatges (PACS, *picture archiving and communication system*, 'sistema d'arxivament i comunicació d'imatges').

Es tracta d'un estàndard obert que estableix un llenguatge comú que garanteix que una imatge mèdica produïda en la màquina d'un proveïdor es podrà visualitzar en l'estació de treball d'un altre proveïdor. Els diferents dispositius han de declarar la seva conformitat DICOM, és a dir, delimitar amb claredat les classes que suporten.

HL7 V3 inclou un domini d'imatge diagnòstica (*imaging integration domain*, 'domini d'integració d'imatges') per a la integració amb DICOM. Aquest domini disposa de models, guies d'implementació i exemples de documents i imatges necessaris per a il·lustrar la transformació d'un informe estructurat DICOM a documents electrònics CDA R2 HL7, i també la creació d'informes CDA d'imatge diagnòstica.

2.4. Interoperabilitat

La necessitat de crear un marc d'interoperabilitat és determinada per l'existència de la gran varietat de tecnologies i sistemes d'informació d'un servei de salut, tots amb la necessitat d'intercanviar informació entre ells.

Desafortunadament, els esforços en matèria d'interoperabilitat estan molt fragmentats. La història clínica electrònica, terminologies, ontologies, missatges, tipus de dades, seguretat i arquitectura de sistemes estan evolucionant d'una manera aïllada i amb iniciatives divergents. Per a solucionar aquest problema, és necessari un fort compromís per a definir un marc d'interoperabilitat en sistemes de salut alineat amb les necessitats dels ciutadans i els proveïdors de prestacions mèdiques.

La interoperabilitat s'ha d'entendre com la gestió continuada del canvi, que no afecti solament el concepte tècnic o d'estandardització, sinó que es tracti d'un procés que ha d'incloure les decisions sobre la inversió, aspectes polítics, institucionals, impacte organitzatiu, jurídic i de mercat.

2.4.1. Interoperabilitat tècnica

Inclou les qüestions de connectivitat i ús dels sistemes, i també de les aplicacions de serveis. Els aspectes més rellevants són: interfícies, interconnexió de serveis, models intermedis, integració, presentació i intercanvi de dades i seguretat. Ens defineix l'escenari tècnic sobre el qual s'estableix la interoperabilitat mitjançant l'ús d'estàndards tècnics.

El repte de la interoperabilitat en els serveis de salut pública s'ha d'iniciar amb l'adaptació de la tecnologia a les necessitats dels professionals i usuaris. Els usuaris finals (ciutadans, empreses o altres organitzacions públiques) volen accedir a la informació pública; el canal d'accés respondrà als condicionaments de cada grup d'usuaris, però s'ha de partir de la generació de continguts i serveis potencialment interoperables.

Per què s'ha d'aconseguir?

La falta d'estàndards mínims en els serveis de l'Administració fa difícil que els ciutadans, les empreses i els mateixos funcionaris els utilitzin. Actualment, es considera que amb la utilització d'estàndards s'afavoreix la compartició de serveis i informació, la redifusió de continguts i el desenvolupament de serveis que funcionin en diferents plataformes. Els avenços en interoperabilitat contribueixen a una gestió eficient de tot tipus de recursos, humans, tècnics, informatius i econòmics.

La interoperabilitat és necessària perquè hi pugui haver connectivitat maquinari i programari entre dispositius i aplicacions. És necessària la creació de normes que continguin guies d'implementació i mecanismes de prova i certificació de sistemes, per a facilitar que les empreses els adoptin i implementin.

2.4.2. Interoperabilitat sintàctica

La interoperabilitat sintàctica permet a dos sistemes remots intercanviar informació. Si dos o més sistemes són capaços de comunicar-se entre ells i intercanviar dades, és gràcies a la interoperabilitat sintàctica. La interoperabilitat sintàctica té en compte els formats de dades i protocols utilitzats per intercanviar-les, però no el significat de la informació que cal intercanviar.

Per què s'ha d'aconseguir?

En primer lloc, la interoperabilitat sintàctica és el pas previ per a aconseguir qualsevol interoperabilitat en un àmbit superior. En segon lloc, es tracta del grau mínim que s'ha d'assegurar per possibilitar la distribució de la informació clínica d'un pacient entre sistemes de diferents proveïdors, organitzacions o simplement amb dissenys arquitectònics i tecnològics diferents.

Avui dia, la situació habitual és que la informació clínica estigui distribuïda en diverses localitzacions. Això es deu al fet que cada centre sanitari, sia un hospital, un centre d'atenció primària o una consulta privada, manté la seva pròpia. No obstant això, el personal sanitari que atén un pacient necessita accedir a informació com ara diagnòstics i tractaments previs, encara que siguin en localitzacions diferents i fins i tot en diferents organitzacions sanitàries. Actualment, la falta d'un marc d'interoperabilitat fiable es considera l'obstacle més gran per a l'intercanvi de registres sanitaris electrònics.

2.4.3. Interoperabilitat semàntica

Assegura que el sentit de la informació intercanviada és comprensible per qualsevol altra aplicació que no va ser inicialment desenvolupada per a aquesta finalitat, i es tracta del factor determinant per a la seguretat de la comunicació de les dades d'una persona. S'aconsegueix quan el significat de la informació intercanviada és entès per les aplicacions i serveis receptors. Avui dia, és un dels reptes més grans per a la integració dels sistemes d'informació.

Per què s'ha d'aconseguir?

Per tal de garantir l'intercanvi coherent de la informació d'una persona de manera automatitzada. Ha de ser transparent i unívoc, de manera que permeti l'anàlisi d'aquesta informació sense necessitat de preprocessament i sense perdre els conceptes de *seguretat* i *confidencialitat*, i també que les organitzacions confiïn en aquells amb qui comparteixen informació.

3. Salut ubiqua

La computació ubiqua s'entén com la integració de la informàtica a l'entorn de la persona. Això és possible ja que, avui dia, els dispositius informàtics poden estar integrats en telèfons mòbils o sensors de presència en edificis intel·ligents, i fins i tot la roba pot tenir sensors per a mesurar constants vitals. Tot això fa possible que la computació sigui ubiqua o, el que és el mateix, que els ordinadors siguin omnipresents. La salut ubiqua seria l'aplicació del paradigma de la computació ubiqua en el camp de la sanitat. Termes relacionats amb la salut ubiqua són *salut pervasiva* (en anglès, *pervasive computing*), que fa més èmfasi en sensors i actuadors; o *vida assistida per l'entorn* (*ambient assisted living*), que se centra en com sistemes de salut ubiqua poden ajudar persones amb necessitats especials, especialment ancians. Ja fora del camp de la salut hem de destacar *intel·ligència ambiental*, en la qual l'entorn (en gran manera informàtic) s'adapta a les necessitats de l'usuari. A continuació, farem una introducció breu als aspectes més importants de la salut ubiqua, que són la salut mòbil i la Internet dels objectes.

3.1. Salut mòbil

Vivim immersos en la revolució dels dispositius mòbils. El fenomen dels mòbils intel·ligents (també coneguts com a *smartphones*) és una de les tendències més ubíquies i dinàmiques en comunicació.

Qui es podia imaginar quan van sorgir els primers telèfons mòbils l'ús que els donaríem avui dia? Hem deixat de dependre de "grans" aparells ancorats a casa nostra per portar a la butxaca la nostra pròpia finestra al món. Avui dia, es pot fer gairebé qualsevol cosa amb el nostre mòbil; es podria dir que el límit està en la nostra imaginació. Perquè us feu una idea de la seva capacitat, el dispositiu mòbil que teniu supera amb escreix en capacitat de procés i emmagatzematge l'ordinador que va usar Neil Armstrong per arribar a la Lluna; fins i tot rivalitzaria amb els ordinadors del centre de control de la NASA per a aquella missió.

No és difícil d'imaginar el gran potencial que tenen en l'àmbit de la salut aquesta manera d'estar connectats i aquesta gran capacitat de processament. Avui dia, disposem de sensors capaços de monitorar gairebé qualsevol paràmetre vital del nostre cos i transmetre'ls als professionals que cuiden de la nostra salut en temps real. A més, aquesta informació pot ser aprofitada per sistemes intel·ligents que ens ajudin a cuidar-nos per nosaltres mateixos mitjançant consells i alertes.

Amb aquestes xarxes de sensors, podem crear espais de monitoratge a la llar (la denominada *vida quotidiana assistida, ambient assisted living, AAL*) que ens ofereixen possibilitats enormes quant al seguiment i tractament de les persones.

L'e-salut és un dels sectors amb més creixement en la indústria de la tecnologia, i el seu impacte en la medicina ha estat significatiu.

Sense cap mena de dubte, un dels fenòmens que més han popularitzat els dispositius mòbils són les aplicacions, fenomen que també ha arribat, per descomptat, a l'àmbit de la salut mòbil.

Hi ha molts tipus d'aplicacions i, encara que el boom actual ens faci pensar en els nostres mòbils quan en parlem, també hi ha aplicacions per a ordinadors. Algunes fins i tot s'han "independitzat" dels dispositius per traslladar-se al núvol (és a dir, executar-se des de la mateixa Internet, amb independència del dispositiu que utilitzem per fer-ho). A més, les aplicacions estan adquirint cada vegada més components socials, una altra de les últimes tendències en tecnologia, que inclou la integració amb servidors socials en el núvol com ara Facebook o Twitter.

Per aquest motiu, farem una classificació segons la manera com ens hi relacionem, de manera independent de la plataforma en la qual funcionin, però tenint-ne en compte els usuaris potencials.

1) Aplicacions que ens ajuden a gestionar coneixement i/o informació.

- Professionals: accés a informació actualitzada en tot moment.
- Ciutadans: informació sobre salut, com cuidar-la i augmentar el coneixement sobre les malalties que puguin patir.

2) Aplicacions que ens ajuden en la consecució de tasques.

- Professionals: faciliten l'execució de tasques complexes o repetitives i redueixen les possibilitats de cometre errors.
- Ciutadans: ens ajuden amb recordatoris sobre la nostra salut, ens ensenyen a dur a terme procediments d'autocura, ens motiven a fer activitats físiques, ens connecten amb altres pacients per promoure hàbits de salut, etc.

3) Aplicacions que afavoreixen la comunicació.

- Professionals: faciliten les consultes entre diferents professionals, i també la coordinació d'equips multidisciplinaris, sobretot els que no són a la mateixa ubicació.

- Ciutadans: sia la comunicació amb els professionals que cuiden de la nostra salut, sia amb altres persones que puguin tenir interessos comuns en matèria de salut.

4) Aplicacions que es comuniquen amb dispositius per monitorar paràmetres vitals.

- Professionals: poden contribuir al monitoratge dels seus pacients, sia de manera hospitalària o ambulatoria.
- Ciutadans: ens ajuden a conèixer i controlar millor la nostra salut.

Aplicació Fewtouch per al control de la diabetis



Font: Chomutare i d'altres (2011). Disponible en: <http://www.jmir.org/2011/3/e65/>

3.2. La Internet dels objectes

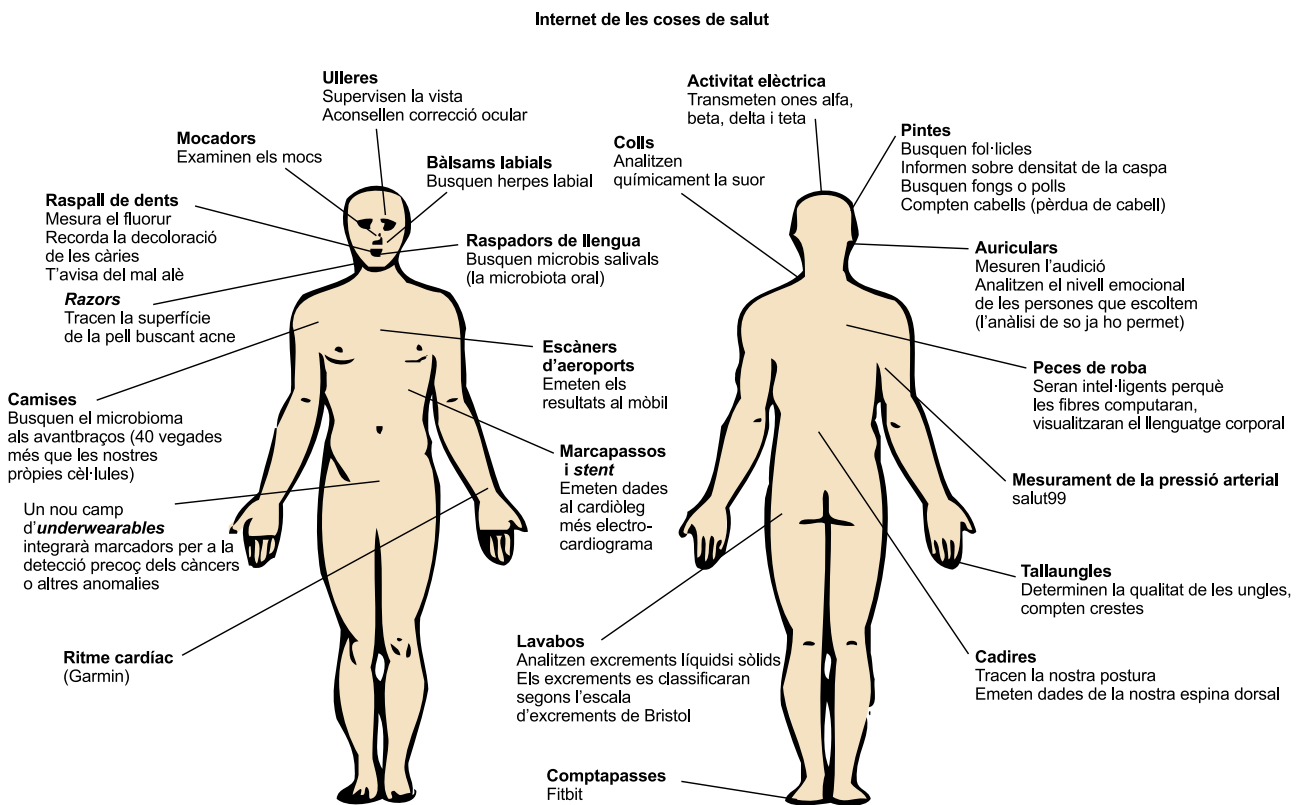
Cada vegada és més habitual que les persones tinguin diversos dispositius amb els quals es connecten a Internet: mòbil, tauleta, portàtil, ordinador de sobretaula, etc., i fins i tot molts electrodomèstics es connecten ja a Internet: consoles de videojocs, televisors, frigorífics, etc. Ningú no podia imaginar aquesta revolució quan Internet va ser dissenyada. Per aquest motiu, Internet es va començar a quedar sense connexions disponibles. Per resoldre-ho, es va evolucionar a un nou sistema de connexions denominat *IPv6*. No és l'objecte d'aquest text analitzar els detalls tècnics sobre aquesta transició, així que només donarem la dada següent: la nova Internet té una capacitat de $3,4 \times 10^{38}$ connexions. Per fer-nos una idea de la dimensió d'aquest nombre, podríem dir que la nova Internet té una connexió per cada estel de l'Univers.

Aquest avenç ens permetrà una comunicació més gran entre dispositius, la qual cosa millorarà el nostre entorn d'una manera substancial. Per exemple, mitjançant la creació de xarxes intel·ligents de dispositius que augmentin la

nostra capacitat de monitoratge, la qual cosa millorarà d'una manera significativa el seguiment i tractament de les persones. Això és el que denominem *vida assistida per l'entorn* o *ambient assisted living*.

També coneguda com a *health Internet of things*, la arribada d'aquesta nova Internet pot augmentar el potencial de les aplicacions sanitàries, però, si no es fan bé les coses, molt probablement crearem problemes nous. Per exemple, podríem passar del problema actual de no poder connectar la informació a un problema d'excés d'informació que no podrem manejar (i que, per tant, perjudicarà més que ajudarà).

Les xarxes de sensors intel·ligents ens poden ajudar a filtrar aquesta informació, i les aplicacions poden fer de recopiladors per alimentar un sistema que gestioni volums de dades enormes (també conegut com a *big data*).



Font: <http://quantifiedself.com/2011/02/hit-%E2%80%93-health-internet-of-things/>

Les aplicacions sanitàries també es podran integrar com a part de la nova Internet:

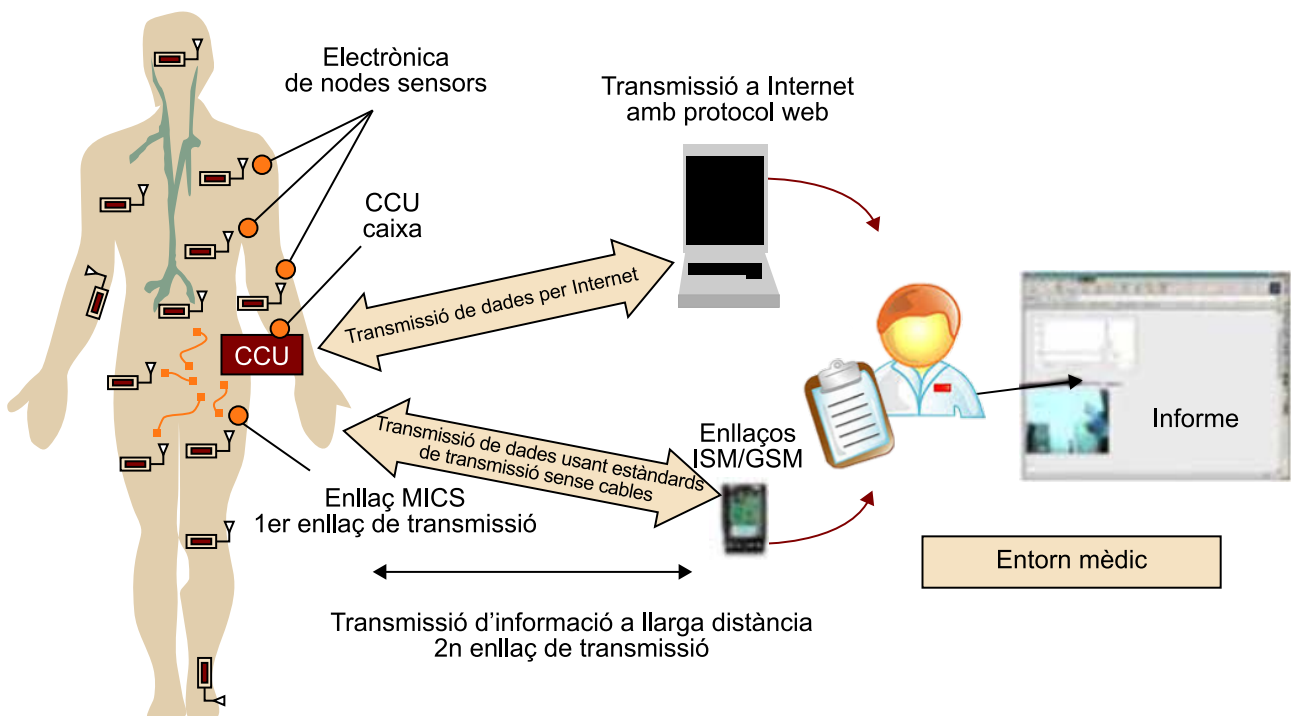
- Per recollir dades del context i recopilar la informació dels sensors. A més, podem afegir aspectes lúdics i d'oci (com hem vist anteriorment, la ludificació) amb l'objecte d'atreure el pacient en la cura de la seva salut.

- Per ajudar a processar l'enorme volum d'informació generat (*big data*), amb l'objectiu que ens resulti profitós en àmbits com el de la recerca, per exemple.
- Trobem aplicacions híbrides que, a més de gestionar i recopilar informació, ajudaran a filtrar-la i processar-la.

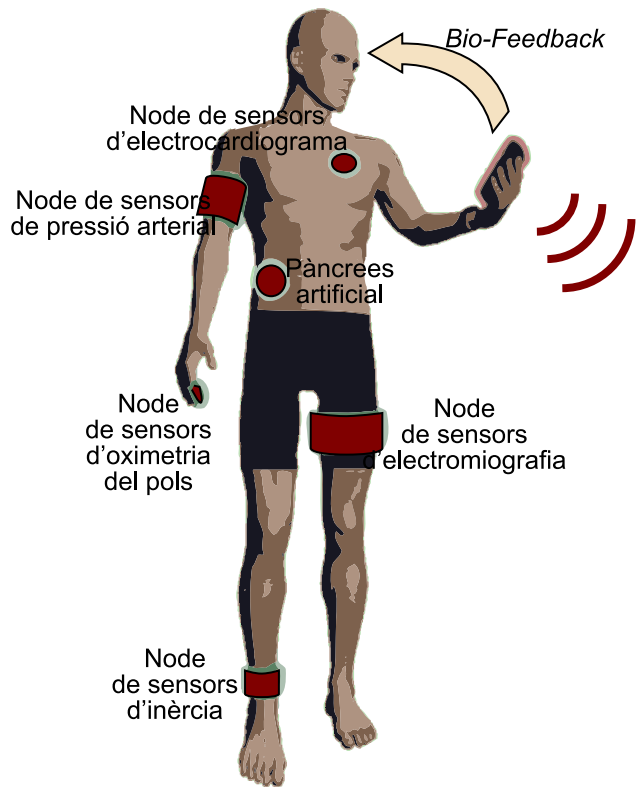
Com podem veure en les imatges següents, la tendència serà crear xarxes de sensors que mesurin multitud de paràmetres sobre l'estat de salut de les persones. Aquesta informació serà gestionada per aplicacions sanitàries per a profit dels diferents actors implicats: ciutadans, professionals, investigadors, etc., de manera que cobrirà les necessitats particulars de cadascú per ajudar al creixement global de tothom. Per exemple, la recerca d'aquestes dades redundarà en una cura millor per als ciutadans.

Per acabar, volem destacar el paper que tindrà aquesta tecnologia a les nostres llars. Les transformarà per convertir-les en part fonamental de la cura de la nostra salut, i també les dotarà d'una xarxa de sensors que transmetran informació essencial als professionals que cuiden de la nostra salut, i també d'aplicacions d'ús personal que portarem als nostres mòbils. Això és el que anteriorment hem denominat *vida assistida per l'entorn*.

Xarxa de sensors de salut



Xarxa de sensors corporals



Font: <http://rlpvlsci.ece.virginia.edu/body-sensor-network-bsn>

4. Pacients i medicina participativa

Fa diverses generacions, els professionals sanitaris, i els metges en particular, gaudien d'un gran prestigi i autoritat que els atorgava el poder de salvar vides i guarir malalts. Aquest prestigi era augmentat pels miracles continus de la medicina dels segles XIX i XX, que inclouen des de la invenció de l'anestèsia fins al descobriment dels antibiòtics o els trasplantaments de cor. El metge tenia la responsabilitat, gairebé en exclusiva, de la salut del pacient, des d'un punt de vista moltes vegades paternalista en el qual el pacient seguia les indicacions del metge cegament. No obstant això, aquest model no ha aconseguit el mateix grau d'efectivitat per a problemes de salut més relacionats amb els estils de vida o l'educació en autocures, com ara l'epidèmia d'obesitat o el control de pacients amb diverses malalties cròniques. Sia en prevenció sia en autocures, cal una gran implicació dels pacients i altres professionals sanitaris. Aquesta implicació no solament inclou un coneixement més gran, sinó un augment de responsabilitat per part del pacient.

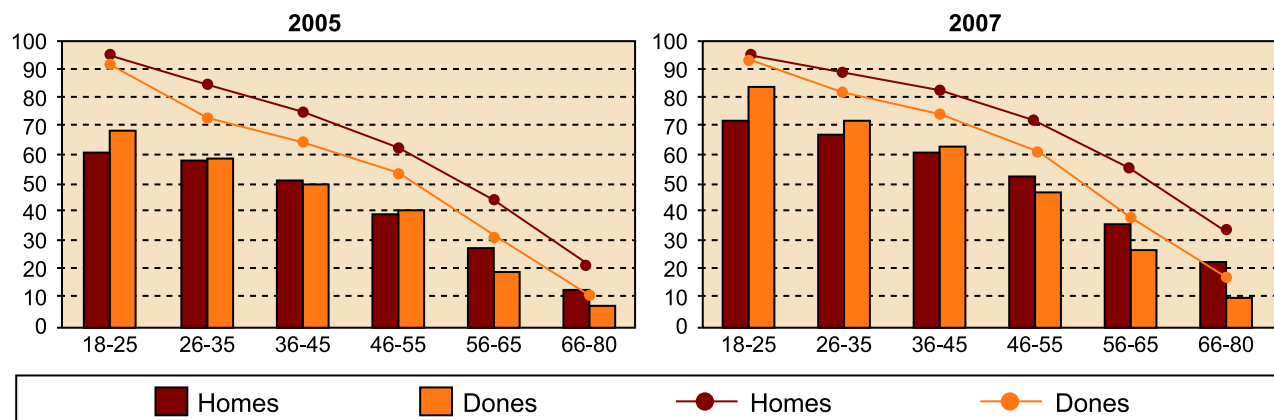
La implicació més gran dels pacients i ciutadans en la seva salut ha trobat en Internet una eina ideal, i s'ha arribat a l'extrem de definir un nou tipus de pacients, els e-pacients. Utilitzant una sèrie de casos d'estudi, en aquest apartat aprofundirem en el canvi que ha comportat Internet en la sanitat des del fenomen de l'e-pacient fins a la medicina participativa.

4.1. Els e-pacients

La definició més simple d'e-pacient consisteix en una persona que utilitza Internet per a temes relacionats amb la seva salut o la d'altres persones (per exemple, fills malalts). Tenint en compte aquesta definició, podem dir que la gran part dels espanyols i els europeus són ja e-pacients.

Avui dia, és relativament simple unir-se a grups de suport de malalties, accedir a informació sobre professionals sanitaris o hospitals, continguts educatius en línia o utilitzar aplicacions mòbils. A més, es comença a desenvolupar la possibilitat d'interactuar amb els serveis de salut via Internet (per exemple, cites prèvies o registre d'últimes voluntats).

Utilització d'Internet per a la salut a Europa entre el 2005 i el 2007



* Ús d'Internet com a línies, ús d'atenció mèdica per Internet com a barres

Font: <http://www.jmir.org/2008/4/e42/>

Hi ha una visió alternativa del fenomen de l'e-pacient, en la qual l'eina, en aquest cas Internet, no és l'important, sinó els canvis que comporta. Aquests e-pacients es converteixen en cogeneradors i participants de la seva salut, i ajuden en gran manera en l'ús de les tecnologies de la informació i la comunicació (TIC).

Explicació de l'apoderament del pacient per J. L. de la Serna, redactor en cap d'El Mundo Salut.

El paciente 'empoderado'



Font: <http://www.elmundo.es/elmundosalud/2012/05/07/codigosalud/1336389935.html>

Com a conseqüència d'aquest canvi de paradigma, es comença a parlar de medicina centrada en el pacient en contraposició amb la medicina tradicional, més centrada en les malalties. Un exemple clar d'això el tenim en pacients que comparteixen a xarxes socials les seves emocions i aspectes de la vida ordinària que són afectats en major o menor mesura per la seva malaltia.

Per exemple, S. Kerri escriu en el seu blog (sixuntilme.com) aspectes de la seva vida ordinària i la seva diabetis. Una de les entrades més populars del blog és una explicació sobre com es pot amagar la bomba d'insulina en un vestit de noces. Aquest nou rol d'un pacient coresponsable i cocreador de la seva salut s'ha denominat *pacient apoderat*. Segons el *Diccionari de la llengua catalana* de l'Institut d'Estudis Catalans (DIEC2), *apoderar* significa "atorgar poders (a algú)", que en aquest context significa donar més poder sobre la seva salut a l'individu, poder que representa una responsabilitat més gran.

Imatge del blog sixuntilme.com, en què s'explica com es pot amagar una bomba d'insulina en un vestit de noces.



El naixement de l'e-pacient Dave

Dave deBronkart era un enginyer amb una llarga carrera en màrqueting dins d'empreses tecnològiques. En una revisió rutinària, va comentar al metge certes molèsties a l'espatlla que atribuïa a jugar al tennis. La radiografia va revelar un escenari molt més ombrívol en descobrir unes taques que es corresponien amb un tumor. Tal com comenta en el seu llibre *Ríe, canta y come como un cerdo*, en un lapse de temps breu es va descobrir que la taca de la radiografia era un tumor metastàtic fruit d'un càncer de ronyó agressiu en fase molt avançada i amb molt poques esperances de curació. El seu metge de capçalera, uns dels fundadors del moviment de l'e-pacient, li va recomanar que consultés la comunitat de pacients ACOR. Dave deBronkart es va convertir en un e-pacient àvid disposat a lluitar contra la seva malaltia amb totes les eines disponibles.

Coneix l'e-pacient Dave

Dave deBronkart: Meet e-Patient Dave

FILMED APR 2011 • POSTED JUN 2011 • TEDxMaastricht



<> Embed Download Favorite Rate Show transcript

Font:http://www.ted.com/talks/dave_debronkart_meet_e_patient_dave.html

En la comunitat d'ACOR, es va unir a un grup de pacients amb el mateix tipus de càncer que s'ajudaven de manera mútua, especialment en la caça de tractaments experimentals, ja que eren l'única possibilitat de curació. Els membres d'aquesta comunitat el van informar sobre com podia entrar en un estudi experimental. A més, va penjar a Internet la seva història clínica per compartir-la lliurement amb metges de tot el món, per conèixer-ne les opinions i, d'aquesta manera, prendre la millor decisió sobre quin tractament havia de seguir. Els membres de la comunitat de pacients, entre altres consells, li van recomanar no començar un altre tractament convencional, ja que això li impediria unir-se al tractament experimental. Durant el tractament, Dave va optar per crear un blog en la plataforma <https://www.carepages.com/> per comentar la seva evolució, amb l'objectiu de mantenir informats els seus éssers estimats sense la necessitat d'estar tot el dia penjat al telèfon. Tal com comenta en el vídeo recomanat anteriorment, el blog es va convertir en una eina clau per a animar-lo, ja que va rebre multitud de comentaris positius fins i tot d'amics que feia dècades que no hi parlaven.

Una vegada guarit de la malaltia, va prendre la decisió de dedicar-se de ple a fomentar la participació dels ciutadans en la seva salut, amb un èmfasi especial en l'accés a les dades de la seva història clínica electrònica, en gran manera arran de descobrir que al seu hospital havien alterat la seva història clínica electrònica amb l'objectiu d'obtenir més ingressos de la seva assegurança mèdica. Avui dia, l'e-pacient Dave és convidat a fer xerrades magistrals en multitud de conferències en les quals comparteix la seva visió d'una medicina més participativa.

4.2. Medicina participativa

El fenomen dels e-pacients s'engloba dins d'un de més gran que es denomina *medicina participativa*. Aquesta, entre altres postulats, defensa que el pacient és un recurs infrautilitzat i pot ser la clau per a la "cura" del sistema sanitari. La medicina participativa no és possible sense una implicació dels professionals sanitaris i no pot ser entesa com una emancipació total del pacient. El pacient passa a interactuar amb un equip de professionals que li faciliten la cura de la seva salut. Els professionals passen a treballar en equips centrats en el pacient, i no en compartiments estancs entre els diferents nivells de l'Administració sanitària.

La transformació de la medicina participativa i els e-pacients no és un fruit de la revolució sociotecnològica d'Internet, sinó que Internet ha estat un element catalitzador i multiplicador del fenomen. Tal com veurem en els exemples següents, Internet ha estat una eina vital per a molts e-pacients en la cerca de respostes als seus problemes de salut. Entre altres aspectes, Internet ha comportat millorar l'accés a persones amb els mateixos interessos i una quantitat ingent d'informació. La participació engloba tant professionals com pacients i cuidadors informals.

El manifest d'Abla

El 2010, una sèrie de professionals i pacients es van reunir al poble d'Abla (a Almeria, Estat espanyol) per discutir com es podien aplicar els principis participatius del Web 2.0 per millorar la sanitat. D'aquesta reunió, va sorgir la iniciativa de crear un manifest que guiés la transformació de la sanitat cap a un model més sostenible i democràtic, amb l'objectiu d'aconseguir una sanitat més accessible i propera, que inclou un canvi en la cultura organitzacional basat en una concepció horitzontal i col·laborativa, enfront de la visió tradicional piramidal i jerarquitzada. Aquest manifest es troba publicat en el capítol 3.6 del llibre *El ePaciente y las redes sociales* (vegeu la bibliografia).

Aquest document es va elaborar utilitzant l'eina col·laborativa Google Docs, i es va comptar amb la participació de més de cinquanta persones en l'edició del document. Al document s'han adherit multitud de societats científiques i particulars. A continuació, proporcionem un resum dels principals aspectes del manifest, que es divideix en dues àrees: ciutadans i professionals sanitaris.

Els pacients passen a ser coresponsables de la seva salut, amb una participació activa tant en la millora de la seva salut com del sistema sociosanitari. Aquest punt es basa en la Llei d'autonomia del pacient. L'autonomia no és solament individual, sinó que ha d'incloure el foment de l'autoorganització ciutadana en comunitats en xarxa. A més, aquesta coresponsabilitat ha d'incloure la participació activa de la ciutadania en la millora del sistema sociosanitari, inclòs l'ús d'opinions en xarxa per a la millora dels serveis sociosanitaris. Un aspecte clau és la formació de la ciutadania per a evitar l'exclusió d'aquells amb dificultats físiques o econòmiques per a l'accés a les noves tecnologies. A més, cal exigir solucions simples, manejables i desenvolupades, tenint en compte les necessitats i opinions de la ciutadania. Les comunitats locals han de ser la font de la innovació i el lloc on es provin solucions abans de generalitzar serveis.

Els professionals són una part clau del canvi de model sanitari, i per aquest motiu cal garantir una sèrie de principis. S'ha de facilitar, i no controlar ni frenar, la col·laboració i l'intercanvi de coneixements entre professionals mitjançant l'ús de les xarxes professionals. Això es basa en la capacitat d'autoorganització dels professionals, incloent-hi el desenvolupament d'iniciatives locals que liderin el canvi. S'ha d'evitar la censura, i el debat entre professionals s'ha de considerar una oportunitat per a millorar el sistema sociosanitari. L'ús de les noves tecnologies és catalitzador del canvi i la millora, per la qual cosa se n'ha de fomentar l'ús sense restriccions degudes a falses excuses de seguretat, rols professionals, localització, etc. La formació sobre noves tecnologies és un dret i una obligació de tots els professionals. Finalment, però no menys important, Internet s'ha de considerar una eina per a la millora de la relació entre els ciutadans i els professionals que respecti l'autonomia, l'honor i la intimitat de professionals i ciutadans.

4.3. Comunitats de pacients

El poder de la comunitat i les xarxes socials és una cosa que transcendeix el món de la tecnologia i salut, ja que forma part de la condició humana. Trobem estudis que han demostrat que conductes humanes com el tabaquisme es transmeten d'una manera social. Fins i tot s'ha arribat a demostrar que

L'obesitat es transmet socialment, ja que ens influenciem els uns als altres. Tots aquests casos s'inclouen en el llibre *Conectados: el sorprendente poder de las redes sociales y cómo afectan a nuestras vidas* (N. A. Christakis, 2010).

Les comunitats de pacients no són un fenomen nou. Des de fa dècades, els pacients s'han unit per defensar els seus interessos comuns, incloent-hi des del suport a la recerca fins a cobrir les necessitats socials d'afectats o la prevenció. Un exemple el tenim en l'Associació Espanyola Contra el Càncer, que va néixer el 1953.

Internet representa una eina revolucionària per a l'associacionisme i la col·laboració entre pacients, el màxim exponent de la qual són les comunitats en línia de pacients. La tecnologia ha permès que qualsevol pacient es pugui comunicar amb els seus iguals independentment de la seva localització, la qual cosa ha augmentat enormement les possibilitats de comunicació. El cas més clar el tenim en les comunitats de persones afectades per malalties rares, que al món fora de línia tenen molt poques possibilitats reals d'interactuar amb altres afectats.

El fenomen de les comunitats en línia de pacients sorgeix en la dècada de 1990, encara que no d'una manera generalitzada. Un dels primers exemples va néixer l'any 1995 amb la comunitat ACOR, que consisteix en un conjunt de llistes de correus en què pacients fan consultes sobre determinats tipus de càncer, especialment càncers rars la informació dels quals és molt escassa. D'una manera gradual, aquestes comunitats van anar migrant a tecnologies més avançades com els fòrums en línia. Actualment, som davant una explosió de diferents tipus de comunitats centrades en continguts multimèdia, com ara les comunitats que sorgeixen en la plataforma de vídeos YouTube. A més, tal com expliquem en el cas següent de TuDiabetes, les comunitats passen a ser estructures molt més complexes en les quals s'integren diferents tecnologies com ara vídeos, aplicacions mòbils i jocs, juntament amb els fòrums i blogs tradicionals.

Les comunitats en línia de pacients proporcionen un suport emocional i informatiu als usuaris, i això n'explica en gran part la popularitat. Alguns estudis demostren que les comunitats de pacients poden ser de gran utilitat per a controlar la qualitat de la informació que es difon a Internet (Esquivel, 2006). En certa manera, estem parlant d'una intel·ligència col·lectiva que ajuda els pacients a cuidar millor de la seva salut. Aquesta intel·ligència col·lectiva pot ser també usada per científics per aprendre més sobre malalties i fins i tot sobre recerca genètica. L'empresa 23andme.com proporciona kits per a l'estudi de factors de risc genètic, i a més proveeix una sèrie de comunitats en línia en les quals els usuaris poden compartir dades de la seva salut i els seus gens. La informació generada en la comunitat en línia es combina amb les dades genètiques per, d'aquesta manera, facilitar la recerca genètica, i la informació de les comunitats es considera informació dels fenotips dels usuaris.

TuDiabetes i Carmen Termina

TuDiabetes és una comunitat de persones afectades per diabetis liderada per l'ONG Diabetes Hands Foundation. La comunitat va ser fundada l'any 2007 per Manny Hernández, un veneçolà establert als Estats Units. El principal motiu que va fer que Manny Hernández creés la comunitat en línia va ser la dificultat que va experimentar per trobar persones amb el mateix tipus de problemes que ell va tenir amb el seu diagnòstic de diabetis i l'ús de bombes d'insulina. La comunitat va tenir un gran èxit i el 2012 disposava ja de dues versions, en espanyol i en anglès, amb més de 40.000 usuaris, milers de vídeos i centenars de grups i blogs.

La comunitat es basa en la plataforma Ning, que proveeix un servei de creació de comunitats en línia que integra blogs, vídeos, xat, grups, aplicacions, etc. Bàsicament, es tracta de la mateixa funcionalitat de xarxes socials com Facebook, però els creadors poden controlar i personalitzar la comunitat. L'administració de comunitats tan àmplies no és una tasca fàcil, i en el cas de TuDiabetes l'administració la porten una sèrie de voluntaris que s'encarreguen d'ajudar membres nous i moderar usuaris i continguts. Dins de TuDiabetes, hi ha una sèrie de programes innovadors que la fan un referent internacional. Entre altres iniciatives, en destaquem les següents (més informació en <http://www.diabeteshandsfoundation.org>).

- **TuAnalyze:** aplicació a la xarxa social desenvolupada per la Universitat de Harvard, que permet als usuaris cedir dades personals per a recerca clínica en diabetis.
- **BigBlue Test:** programa per a la conscienciació sobre la importància de l'exercici. Es basa en l'ús de vídeos en xarxes socials i recopilació d'experiències personals sobre la importància de l'exercici físic per al control glucèmic.
- **HealthSeeker:** joc de Facebook dut a terme en col·laboració amb el Joslin Diabetes Center, per a l'educació en diabetis tipus 2.
- **Videoxat amb associacions mèdiques:** videoxats setmanals en www.estudiabetes.org, amb professionals sanitaris de la Societat Mexicana de la Diabetis.
- **La veu a la teva mà:** programa de conscienciació que es basa en fotografies de mans d'usuaris on han escrit com se senten respecte a la diabetis.

A continuació, presentem una entrevista a Carmen Termina, que és una usuària d'EsTuDiabetes. Nascuda el 1958, Carmen Termina és una dona valenciana que treballa en una empresa d'instal·lació d'aires condicionats, mestressa de casa i mare de dos fills. Carmen és, a més, diabètica tipus 2 des de fa catorze anys.

–Què et va motivar a unir-te a TuDiabetes? Com et vas assabentar d'aquesta xarxa?

–Fa tres anys, quan el metge em va aconsellar ampliar el meu tractament i injectar-me insulina, estava bastant perduda i buscant per la Xarxa, vaig trobar EsTuDiabetes.

–El teu metge i infermeres saben que uses TuDiabetes? Quina en va ser la reacció?

–Sí, ho saben, però no hi donen importància. Jo els recomano que l'aconsellin a altres pacients, però sense gaire èxit. Tinc la sensació que sembla que els fes por quedar-se sense clients-pacients, o que pensen que la gent no sap distingir entre una bona informació i una altra que no ho és.

–Què t'aporta TuDiabetes que no trobes en una associació tradicional de pacients?

–M'aporta proximitat amb persones de tot arreu. Persones com jo, que tenen les mateixes pors, les mateixes experiències i coses noves que aprendre i ensenyar cada dia. Són persones amb qui puc parlar a qualsevol hora, just quan se m'ocorri qualsevol cosa. En EsTuDiabetes sempre hi ha algú a l'altre costat, per exemple metges altruistes i mares de nens que expliquen les seves experiències perquè altres famílies s'eduquin. També és més amè perquè podem penjar-hi fotos, poesies, en fi, més divertit al mateix temps.

–Tens alguna anècdota (si pot ser una de bona i una altra de dolenta) fruit del teu ús de TuDiabetes?

–Explicaria que gràcies a EsTuDiabetes he conegut gent de l'Argentina, de Veneçuela, dels Estats Units, etc. que m'han vingut a visitar, i tinc una segona família a la República Dominicana, on vaig anar a portar material de diabètics a unes nenes que no tenien es. El costat negatiu és descobrir tants diabètics pel món que no tenen el necessari per a portar bé el control de la malaltia.

–Com t'ajuda Internet en el control de la diabetis?

–Crec que Internet en general pot servir de molt, si se sap triar la informació adequada, una cosa que la gent sap fer. A més, concretament EsTuDiabetes dóna suport als qui no s'atreveixen a parlar amb el metge i explicar-li el que fan realment. Els deu sonar allò de “no sé què passa, doctor, perquè jo sí que faig la meua dieta, exercici, etc.”. No obstant això, amb altres persones “amigues” a la Xarxa sí que ho fas, i això penso que és molt important. Jo haig de dir que des que estic en aquest tipus de xarxes socials entenc millor la meua condició, aprenc i ensenyo a qui puc i m'ajuden i estic molt millor. Sé moltes coses bones i dolentes per a mi que abans no sabia, o bé perquè el meu metge no té temps o perquè potser no li ha donat importància. Per exemple, hi ha nutricionistes que ens passen receptes. En fi, és com una gran família per la Xarxa. És, com jo dic, un Facebook de diabètics.

5. *eHealth literacy*

Hem vist que les eines en línia per a la salut de què disposem actualment estan adquirint una gran rellevància, i permeten que els usuaris coneguin més coses sobre les seves malalties, que estableixin contacte amb persones en la mateixa situació o amb els mateixos interessos de qualsevol part del món, o que intercanviïn els seus coneixements i experiències personals. No obstant això, perquè aquestes eines en línia siguin útils de debò per als usuaris és necessari que tinguin una sèrie d'habilitats per a utilitzar-les eficaçment, és a dir, que el seu nivell d'alfabetització en salut, també conegut com a *eHealth literacy*, sigui adequat.

5.1. *eHealth literacy* i els seus components

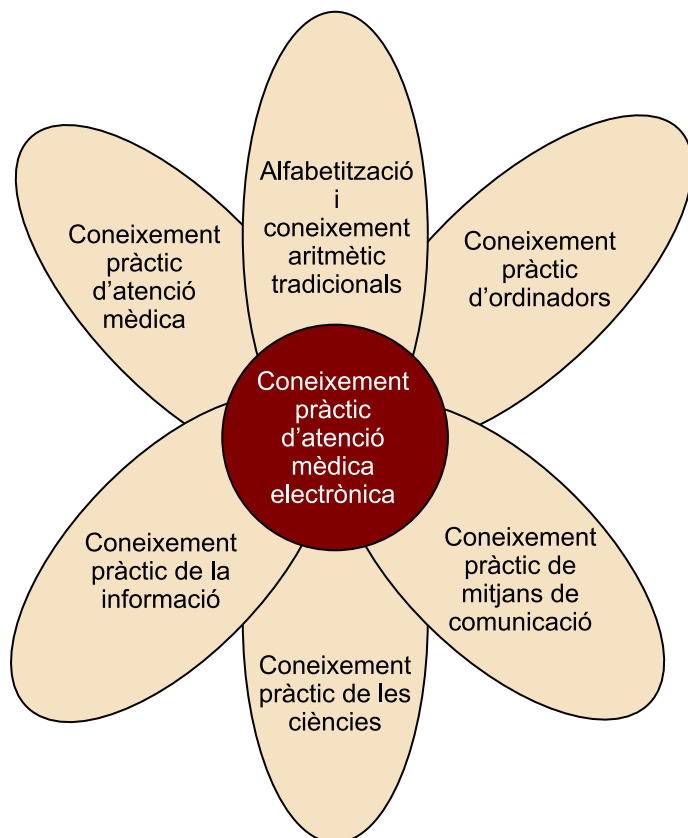
El concepte d'*eHealth literacy* o 'alfabetització en salut' va ser introduït pels canadencs Cameron D. Norman i Harvey A. Skinner en una publicació del 2006, i el van definir com "l'habilitat per a buscar, trobar, comprendre i valorar la informació sobre salut procedent de fonts electròniques, i aplicar els coneixements adquirits per abordar o resoldre un problema de salut".

Hi ha múltiples factors que afecten el nivell d'alfabetització en salut. Alguns d'aquests factors fan referència a característiques pròpies de l'individu com ara la capacitat de lectura i comprensió, les barreres lingüístiques o el nivell cultural. Per contra, altres factors rauen en la manera com es presenta la informació, per exemple el mitjà en el qual es presenta, el format i estil, les estructures gramaticals, l'ús o no d'imatges o il·lustracions aclaridores o el grau d'interactivitat amb la informació presentada. En el model d'*eHealth literacy* proposat per Norman i Skinner, es presenten els sis components o factors que, combinats, explicarien l'alfabetització en temes de salut dels individus.

- **Alfabetització tradicional (*traditional literacy*):** és la capacitat de l'individu per a llegir, comprendre, parlar i escriure un llenguatge coherent.
- **Alfabetització de la informació (*information literacy*):** fa referència a la capacitat de l'individu per a organitzar la informació, saber on buscar-la i com utilitzar-la.
- **Alfabetització mediàtica (*media literacy*):** es refereix a la capacitat de valorar d'una manera crítica els continguts.

- **Alfabetització en salut (*health literacy*):** serien les habilitats necessàries per a interactuar amb el sistema de salut i participar en les autocures pròpies.
- **Alfabetització informàtica (*computer literacy*):** és l'habilitat per a utilitzar els ordinadors per resoldre problemes.
- **Alfabetització científica (*scientific literacy*):** faria referència a la capacitat per a comprendre la naturalesa, els objectius, la metodologia, les aplicacions i les limitacions dels continguts.

Components d'eHealth literacy



Font: Norman & Skinner (2006). *JMIR* (núm. 8, vol. 2, pàg. 9).

Els mateixos autors, Norman i Skinner, són els creadors, a més, de l'eina *eHeals literacy scale*, una escala per a avaluar el grau de confort dels individus i les seves habilitats per a usar les tecnologies de la informació per a temes de salut.

5.2. Alfabetització en salut. Entrevista al Dr. Ignacio Basagoiti

Ja a l'Estat espanyol, Ignacio Basagoiti és metge d'atenció primària i investigador de l'institut ITACA de la Universitat Politècnica de València, i des de fa més de quinze anys compagina la seva tasca assistencial amb el desenvolupament de projectes en els camps de l'e-salut, salut 2.0, envelliment actiu i medicina participativa. Ha liderat la iniciativa per escriure el llibre *Alfabetización en salud. Comunicación, información y capacitación del paciente*.

Aquest llibre és el primer monogràfic publicat en espanyol dedicat de manera exclusiva a aquest tema. Es tracta d'una obra col·laborativa elaborada per més de quaranta autors de diferents perfils professionals, en la qual s'aborden temes com la comunicació en salut, els actors d'aquesta comunicació, els diferents tipus d'informació i els seus canals o els catalitzadors i les barreres per al futur. Està previst que aquest treball surti a la llum el desembre del 2012, i sota llicència Creative Commons podrà ser descarregat lliurement al web www.salupedia.org. A continuació, presentem l'entrevista efectuada al Dr. Basagoiti amb motiu d'aquest treball, per aprofundir més en el tema.

–Què és l'alfabetització en salut?

–En trobem desenes de definicions, depenent de l'àrea de coneixement que la considera. Hi ha hagut alguns intents d'oferir una definició integradora, però el resultat és complex i extens. Penso que un bon punt de partida és adoptar la definició de l'OMS de 1998: "les habilitats socials i cognitives que determinen el nivell de motivació i la capacitat d'una persona per a accedir, entendre i utilitzar la informació de manera que li permeti promoure i mantenir una bona salut". Hi podríem afegir que li permetin l'autocura, l'autogestió de la salut i la malaltia, l'apoderament i la presa de decisions i, fins i tot, la militància per mitjà de l'associacionisme (entesa com la conscienciació, la demanda legítima de millores i l'adopció dels punts de vista dels pacients per les administracions públiques i la societat en general).

–Per què un llibre d'alfabetització en salut?

–A ITACA-TSB fa més de deu anys que desenvolupem projectes dirigits a l'educació sanitària (Campusalud, Educarensalud, etc.). En els últims anys, a més, hem experimentat la necessitat d'introduir aspectes de l'alfabetització en salut en projectes de manera originària tenien un enfocament més tecnològic. Mitjançant Salupedia.org, intentem utilitzar el potencial de les eines col·laboratives a l'hora d'oferir al ciutadà informació sanitària de qualitat. Per mitjà d'aquest projecte, plantejem que, malgrat l'emergència del tema, i una demanda creixent d'eines per a quantificar i utilitzar la informació i la comunicació en el procés d'alfabetització en salut, encara no disposàvem d'un text que donés resposta a les múltiples preguntes que planteja un tema tan complex. D'aquesta manera, vam proposar a un bon nombre d'autors que col·laboressin en la creació de materials que aportessin les diferents perspectives, sensibilitats i àrees de coneixement implicades en l'alfabetització en salut. La resposta va ser impressionant. Quaranta-vuit autors han participat d'una manera desinteressada en l'elaboració de trenta-sis capítols que, organitzats en set seccions, aborden aspectes com la informació, la comunicació (tipus, canals, actors), codis, catalitzadors, barreres, etc. D'aquesta manera, metges, infermers, psicòlegs, pedagogs, documentalistes, periodistes, advocats i enginyers ofereixen la seva pròpia visió del tema des de diferents perspectives que intenten oferir una visió holística i gairebé sense zones d'ombra. Aquest text, gairebé de caràcter enciclopèdic, representarà una obra de referència que, probablement, servirà per a impulsar la recerca sobre l'alfabetització en salut en el nostre àmbit.

–Qui està implicat en l'alfabetització en salut?

–Com hem vist, l'alfabetització en salut és un tema complex. Concerneix, en primer lloc, els ciutadans, que en són els veritables protagonistes, en el sentit que sobre ells recauen les estratègies que els conduiran a l'autonomia personal i el guany en salut i qualitat de vida. D'altra banda, els professionals de disciplines molt diferents, des de la medicina fins al màrqueting, passant per les eines tecnològiques i educatives o els aspectes ètics i legals. Finalment, un actor que no hem d'oblidar són les mateixes administracions públiques interessades a obtenir beneficis en els ciutadans i la sostenibilitat dels sistemes sanitaris, però que, al seu torn, han de possibilitar els canvis que integrin la promoció de la salut, la prevenció de la malaltia, l'autocura i l'apoderament dels pacients, de manera transversal, en totes les organitzacions, i de manera efectiva i real perquè puguin oferir resultats.

–Com i on es produeix l'alfabetització en salut?

–La salut engloba i concerneix totes i cadascuna de les nostres activitats com a ciutadans. L'alfabetització en salut, igual que ocorre amb l'alfabetització en general, disposa d'intervencions i estratègies formals des de les escoles, les organitzacions sanità-

ries i les administracions quant a les campanyes de conscienciació i de salut pública. No obstant això, no solament aquest és el seu àmbit. Els mitjans de comunicació, les empreses, les associacions i els mateixos ciutadans en el seu entorn familiar, social o laboral són capaços de generar coneixements i habilitats en salut. Utilitzar el potencial de tots aquests àmbits és un repte, però amb uns resultats de transcendència enorme i indubtablement efectius pel que fa al cost.

-Quin podria ser el seu impacte en la sanitat del futur?

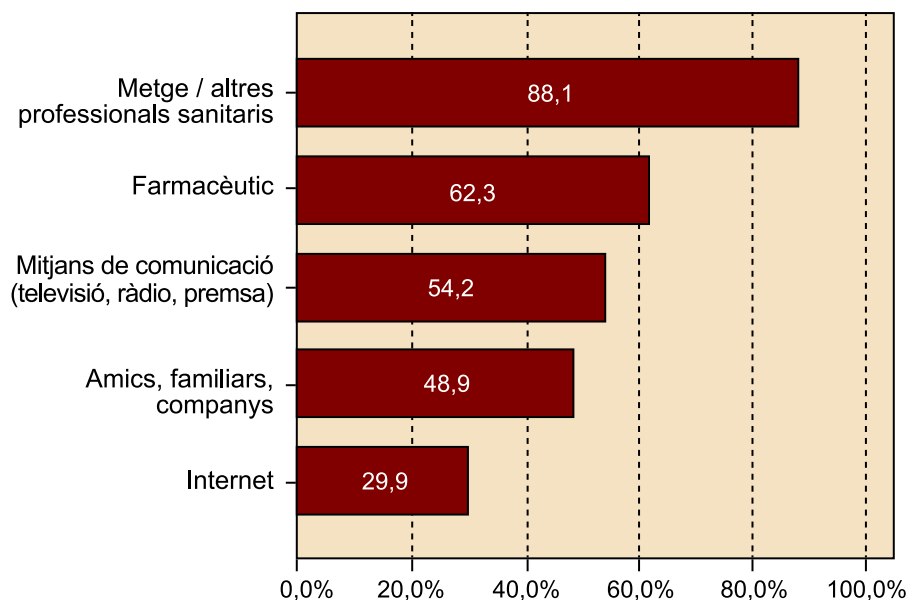
-Com hem dit abans, la sanitat està tendint a adoptar nous paradigmes en els quals el ciutadà i el seu entorn passen a ocupar el centre dels esforços i les estratègies. Els canvis són radicals i, per tant, el canvi real està resultant lent. El pas de malalties a pacients, d'estructures organitzatives tancades i sordes a serveis descentralitzats, d'assistència a col·laboració i participació ciutadanes... Aquestes tendències responen, sens dubte, a una demanda ciutadana: la participació activa en tots els aspectes de la societat. Això té com a condicionant -i de manera paradoxal, també com a motor- l'alfabetització. La general, la informacional, la tecnològica i l'alfabetització en salut. Només es poden prendre decisions lliurement a partir del coneixement i l'adquisició de destreses. D'aquesta manera, un ciutadà alfabetitzat serà el vertader motor de canvi dels sistemes sanitaris: demanarà una medicina basada en evidències, promourà polítiques saludables, utilitzarà els serveis de manera més eficient, demanarà una atenció més ajustada a les seves pròpies necessitats. En definitiva, el ciutadà formarà part de les mateixes organitzacions sanitàries i aquestes formaran part de l'entorn social dels ciutadans. Aquesta transversalitat de la sanitat del futur no comportarà una medicalització de la vida. Al contrari, serà capaç d'incloure les sensibilitats dels diferents grups i les necessitats dels individus, la qual cosa els permetrà la llibertat de decidir sense haver d'optar entre ser dins o fora del sistema. Per a això, necessitem alfabetitzar-nos, saber alfabetitzar i permetre que aquesta tasca doni fruits. Sembla que ens comencem a moure. Confiam que aquest llibre sigui un granet de sorra en aquest camí que concerneix a tothom.

6. Eines 2.0 utilitzades en salut

Internet s'ha convertit en una oportunitat sense precedents per a accedir a qualsevol informació relacionada amb la salut des de qualsevol part del món. Abans de l'aparició d'Internet, els coneixements sobre salut estaven bàsicament en mans de professionals sanitaris i científics, encara que avui dia qualsevol persona interessada a conèixer més sobre una malaltia o sobre com pot mantenir la seva salut es pot dirigir a la Xarxa i, després d'uns segons, accedir a continguts mitjançant milers de pàgines web en format 1.0 i 2.0. Mentre que en el primer tipus de web (1.0) l'usuari únicament podia llegir continguts, el Web 2.0 està concebut perquè els continguts siguin generats pels mateixos usuaris, la qual cosa facilita que es comparteixi informació i la interacció. Els webs 2.0 o xarxes socials no sols estan sent utilitzats per pacients, cuidadors i consumidors en general, sinó que a més s'han convertit en una eina d'intercanvi de coneixements per als professionals o de comunicació per part d'organismes oficials. A més, els nous telèfons i dispositius mòbils (*smartphones* i tauletes) i les aplicacions específiques (*apps*) han facilitat que aquestes xarxes socials siguin cada vegada més populars i s'usin amb més freqüència.

Amb relació a la salut, Internet i les xarxes socials són ja el mitjà pel qual accedir a informació per al 29,9% dels internautes espanyols.

Fonts d'informació de salut utilitzades pels espanyols.



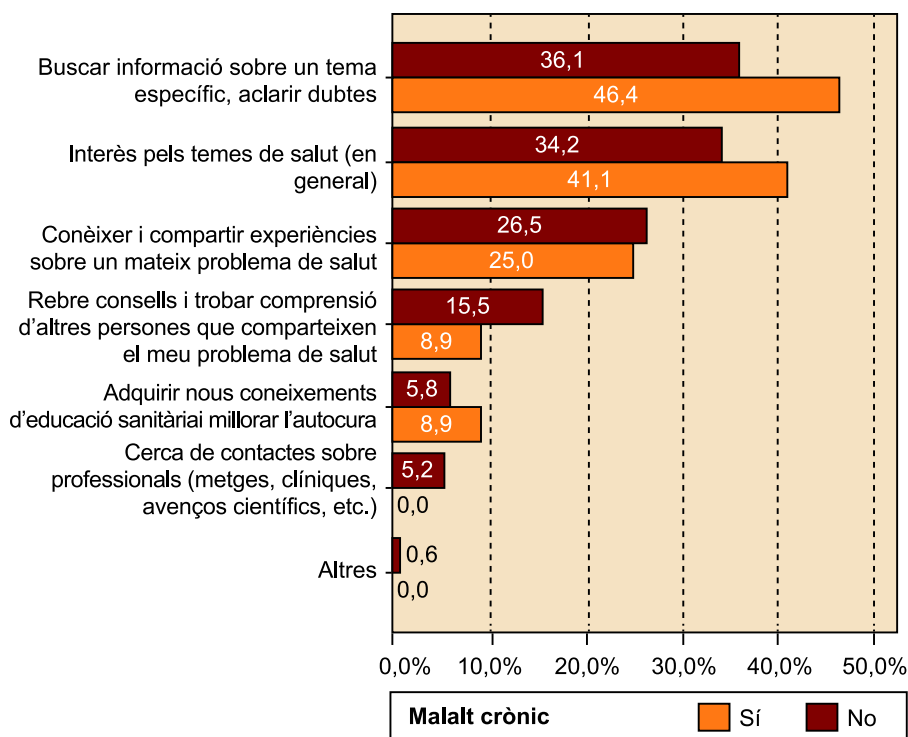
*Base N = 5.500 individus

Font: ONTSI (2012). Los ciudadanos ante la eSanidad

D'aquestes persones que recorren a les xarxes socials a la recerca d'informació sobre la salut, un informe de l'Observatori Nacional de Telecomunicacions del 2012 mostra que el 72% consulta la Viquipèdia, un 35% Facebook, el 30%

YouTube i un 13% Twitter. L'èxit i l'augment d'aquestes eines 2.0 com a font d'informació en salut rau precisament en això: l'aspecte social. Els pacients hi recorren per conèixer més coses sobre la seva malaltia i compartir experiències sobre un problema d'una manera personal i directa, i trobar persones que tinguin el seu mateix problema mèdic.

Motius pels quals internautes espanyols utilitzen les xarxes socials per a temes de salut.



*Nota: resultats calculats sobre $n = 211$ individus. Usuaris de xarxes socials

Font: ONTSI (2012). Los ciudadanos ante la eSanidad.

Cada vegada més professionals sanitaris i pacients tenen el seu propi blog, en què comparteixen informació i experiències. Fins i tot tenen les seves pròpies pàgines a Facebook, canals a YouTube o comptes a Twitter. També institucions, hospitals, centres de recerca o associacions de pacients són ja presents a la Xarxa. I és que tres de cada quatre pacients donaria suport a la idea que el seu metge tingués un blog o un web amb informació i consells de salut.

6.1. Facebook

Amb més de 900 milions d'usuaris, Facebook és la xarxa social més utilitzada a tot el món, i això la converteix en una de les eines en les quals, diàriament, a més d'informació lúdica, fotos o esdeveniments socials, es comparteix un volum més gran d'informació sobre salut. Facebook és una empresa creada per Mark Zuckerberg, i actualment cotitza a la borsa. Qualsevol usuari que s'hi registri pot crear un perfil, una pàgina o un grup dedicat a qualsevol tema i publicar-hi coses, i també fer que aquests continguts siguin d'accés privat o públic. El volum d'usuaris, pàgines, grups o causes de Facebook dedicats únicament a temes de salut ha anat augmentant al llarg del temps, i actualment hi podem trobar des d'associacions de pacients que comparteixen informació

amb els seus associats (per exemple, l'Associació Espanyola d'Al·lèrgics a Aliments i Làtex, AEPNAA), fins a associacions mèdiques professionals (per exemple, la Societat Espanyola de Cardiologia), entitats públiques sanitàries (el Ministeri de Sanitat), organitzacions sense ànim de lucre (Metges sense Fronteres), mitjans de comunicació especialitzats en salut (*Diario Médico*) o hospitals (per exemple, l'Hospital Sant Joan de Déu); sense esmentar, entre d'altres, els milers de professionals sanitaris que disposen de pàgines específiques en les quals divulguen, comparteixen i intercanvien continguts de salut amb els pacients o amb qualsevol persona interessada. Qualsevol que vulgui accedir a informació que s'està compartint en aquesta xarxa social sobre un tema de salut concret, o bé que vulgui conèixer altres usuaris amb problemes similars, únicament s'ha de dirigir al cercador de Facebook i introduir-hi el que està buscant. D'una manera automàtica, el cercador li oferirà una llista de pàgines, grups, aplicacions i persones que inclouen en el nom les paraules buscades.

6.2. Twitter

Twitter és un servei de microblogs que actualment té prop de 400 milions de comptes d'usuaris creats. Aquests, sota pseudònims reals o ficticis, o els denominats *comptes verificats*, publiquen i comparteixen qualsevol tipus d'informació per mitjà dels denominats *tuits*. Els tuits són frases que, amb un màxim de 140 caràcters, permeten tenir una idea general ràpida del que s'està comunicant; habitualment també inclouen un enllaç a una altra font d'informació en la qual es poden ampliar coneixements. De la mateixa manera que Facebook, aquesta xarxa social està sent aprofitada per intercanviar coneixements i compartir informació sobre salut. Tant usuaris particulars, pacients (@NataliaBem) i professionals de la salut (@lamamapediatra), com mitjans de comunicació generals (@LaVanguardia) o especialitzats en salut (@RedaccionMedica), revistes científiques (@GacetaSanitaria), associacions de pacients (@InmunitasVera), societats sanitàries professionals (@semfyc), grups d'investigadors (@CesaAlergia), hospitals (@HSJDBCN) o organitzacions oficials (@SalutCat) estan divulgant, compartint i intercanviant informació sobre salut amb altres usuaris. La manera d'accedir a aquesta informació compartida és similar a altres xarxes socials, encara que a més d'un cercador que dirigeix l'usuari cap a comptes que inclouen en el nom la paraula buscada, o cap a altres usuaris que han inclòs en els seus tuits aquesta paraula, també ofereix la possibilitat de crear llistes i/o seguir usuaris que comparteixen informació d'interès o que inclouen una etiqueta determinada (paraula clau precedida pel caràcter #). D'aquesta manera, es facilita l'accés immediat a infinitat de continguts i usuaris interessats en el mateix tema.

6.3. YouTube

YouTube és una xarxa social de vídeos en la qual qualsevol usuari pot publicar, reproduir, compartir o comentar vídeos. Amb més de cent milions de vídeos publicats, es tracta d'un recurs d'informació valuós també en temes de salut. En l'origen, la majoria dels vídeos relacionats amb temes de salut de YouTube

havien estat creats pels mateixos usuaris i mostraven experiències personals o donaven consells a altres pacients, però actualment cada vegada es troben més vídeos i canals que pertanyen a professionals de la salut i a institucions sanitàries oficials que fan servir aquest mitjà per divulgar informació i comunicar-se amb els usuaris. Alguns exemples en serien el Ministeri de Sanitat, Serveis Socials i Igualtat, l'Hospital Sant Joan de Déu de Barcelona o l'Hospital La Fe de València. Per tenir accés a continguts de salut, l'usuari ha d'utilitzar el cercador de YouTube, que el redirigirà a canals que incloguin aquestes paraules en el nom o a vídeos que les continguin en el títol o descripció.

6.4. Viquipèdia

La Viquipèdia és una enciclopèdia lliure escrita d'una manera col·laborativa per voluntaris de qualsevol país, per la qual cosa els continguts es poden trobar en diferents idiomes. La Viquipèdia s'ha convertit en un dels webs més visitats del món, i una de les principals fonts en línia d'informació en salut. De la mateixa manera que altres eines 2.0, no solament la fan servir pacients i usuaris en general, sinó que també la consulten professionals de la salut. De fet, els estudis mostren que un 70% dels metges de família júnior busquen informació sobre salut en aquest wiki. Gràcies a la denominada *intel·ligència col·lectiva*, els continguts de la Viquipèdia es consideren de bona o molt bona qualitat, fins al punt que algunes de les seves referències estan sent citades en publicacions científiques.

6.5. Altres eines 2.0 en salut

Amb l'excepció d'aquelles eines 2.0 que tenen una finalitat concreta, com podria ser compartir música o pel·lícules, pràcticament a qualsevol xarxa social en línia accessible al públic en general es comparteixen i es comenten continguts sobre salut. Alguns exemples d'això són MySpace, Google+, SlideShare, LinkedIn o SecondLife. Trobem, no obstant això, altres xarxes socials dirigides d'una manera específica a l'intercanvi d'informació, coneixements o anàlisi de casos clínics entre professionals de la salut i organitzacions mèdiques, com, per exemple, Medting.

Medting és una iniciativa espanyola dissenyada com una eina web per a l'intercanvi mèdic en línia de casos clínics i multimèdia. Les organitzacions sanitàries i els metges poden dur a terme recerca en un àmbit internacional, poden implementar serveis de telemedicina i segona opinió i fins i tot dissenyar la seva pròpia xarxa social o el seu propi portal d'aprenentatge electrònic clínic. La plataforma disposa de components tecnològics potents, sobretot en un àmbit multimèdia i d'imatges.

Els exemples presentats són tan sols això, exemples de com les eines 2.0 s'estan emprant avui en dia amb relació a temes de salut, encara que, a més de les esmentades, moltes més xarxes socials estan sent utilitzades amb aquesta finalitat, i probablement n'apareixeran altres de noves.

7. e-Salut pública i jocs per a la salut

7.1. e-Salut pública

Si la salut pública es defineix com “la ciència i l’art de prevenir les malalties, perllongar la vida i la promoció de la salut per mitjà dels esforços organitzats i decisions amb coneixement de la societat, les organitzacions, públiques i privades, comunitats i individus”, l’e-salut pública faria referència a aquesta mateixa ciència de promoció de la salut i prevenció, però per mitjà d’Internet i les TIC en general.

7.1.1. Els avantatges

La difusió d’informació amb l’objectiu d’educar sobre salut, promoure-la i prevenir el desenvolupament de malalties o les seves complicacions per mitjà de les TIC presenta avantatges indiscutibles per als organismes de salut pública. Exemples d’aquests avantatges són el baix cost que té, l’enorme potencial per a fer arribar la informació d’una manera ràpida a amplis sectors de la població o el fet de facilitar la interacció amb i entre els usuaris.

Cada vegada són més els professionals de la salut, gestors sanitaris, institucions públiques i organismes oficials que estan reconeixent el potencial enorme de les TIC en general, i d’Internet i les xarxes socials en particular, per estar al corrent del tipus d’informació que circula per la Xarxa amb relació a un tema concret. D’aquesta manera, volen estar preparats davant possibles preguntes, dubtes o consultes dels usuaris, però també divulgar informació sanitària i/o ser els primers a comunicar o donar respostes a temes de salut.

Grans institucions internacionals de salut pública de prestigi reconegut, a més de tenir els seus propis webs en què ofereixen quantitats enormes d’informació, estan utilitzant xarxes socials per comunicar-se amb pacients i usuaris, entre les quals podem destacar la Food and Drugs Administration (FDA), que utilitza els canals de comunicació de Facebook, Twitter, YouTube i Flickr, i els Centers for Control and Prevention of Diseases (CDC), que es comuniquen mitjançant Facebook, Twitter i YouTube. Aquests dos organismes sanitaris americans, FDA i CDC, s’han unit diverses vegades per mostrar per mitjà de les xarxes socials dades d’interès públic, com quan van publicar continguts per mitjà de la Xarxa amb relació als productes que havien estat retirats del mercat durant un brot de salmonel·la; o com quan es van unir per informar durant la pandèmia del virus de la grip A (H1N1) de fa uns anys. Altres organismes de prestigi reconegut com el National Health Service (NHS)

del Regne Unit, el Ministeri de Sanitat i Política Social a l'Estat espanyol o grans hospitals i fundacions estan fent servir Facebook, Twitter i YouTube amb aquestes finalitats.

Les TIC, per tant, s'han convertit ja en un magnífic mitjà per divulgar temes sanitaris d'interès general i educar els usuaris, tot i que les grans institucions i els organismes sanitaris encara tenen molta feina per fer respecte a donar respostes en temes de salut i obrir vies de comunicació més directes amb els usuaris.

7.1.2. Els inconvenients

Nombroses publicacions mostren les enormes possibilitats de promoure la salut a favor de la prevenció per mitjà de les TIC. Tot i així, no tota la informació sobre promoció de la salut o prevenció disponible en línia és de la mateixa qualitat o té les mateixes intencions. No és estrany trobar webs, blogs o comentaris sobre salut a xarxes socials en les quals no es pot conèixer l'entitat de les persones que hi ha al darrere, no s'esmenten les fonts d'informació, es presenten opinions com si es tractessin de fets científics o es poden entreveure altres interessos que no són o no són solament sanitaris.

Una publicació recent va analitzar publicacions científiques sobre salut a YouTube, i es va centrar en els possibles perills o riscos per a la seguretat dels usuaris d'aquests continguts. Es van detectar cinc tipus de perills per a la salut:

- 1) Continguts nocius dirigits directament als usuaris (per exemple, publicitat de medicaments o altres productes).
- 2) Presentació pública de conductes poc o gens saludables (gent que s'autolesionava o promocionava l'anorèxia).
- 3) Publicacions que desprestigien autoritats sanitàries (per exemple, continguts en contra de missatges emesos per entitats de salut pública).
- 4) Impacte psicològic dels usuaris que accedeixen a informacions inadequades, ofensives o esbiaixades sobre salut (per exemple, continguts en els quals tan sols s'esmenten els beneficis d'un procediment mèdic, o només se'n presenten els problemes).
- 5) Ús de la xarxa social per a divulgar continguts amb altres intencions (per exemple, interessos polítics).

Els resultats d'aquest treball, encara que centrat en YouTube, són generalitzables al que està succeint actualment en altres xarxes socials, fòrums i comunitats en línia i Internet en general.

7.2. Jocs i ludificació per a la salut

Quan es parla d'educar en temes de salut i promoure la prevenció per mitjà de les TIC, no es fa referència únicament a diferents webs centrats en temes sanitaris o a xarxes socials en les quals es difon, comparteix i comenta informació sobre salut o malalties. Des de fa uns anys, s'està aprofitant el poder lúdic amb aquestes finalitats, ja que hi ha un gran problema en l'adherència a les intervencions en salut pública utilitzant eines en línia. Molts usuaris perden l'interès en l'ús de les eines d'e-salut i, amb això, se'n redueix l'efecte. Retenir els usuaris es converteix en peça clau de l'e-salut.

Jugar és un dels principals mecanismes que els humans tenen per a aprendre, sobretot a edats molt primerenques. Els jocs educatius (també denominats *jocs seriosos*) poden ser dissenyats per educar en salut tant pacients com professionals. Tal com expliquem en la subsecció següent, partint d'una sèrie d'objectius educacionals, es dissenyen fases, missions i mecanismes per estimular l'usuari. A tall d'exemple, destaquem el videojoc Didget per a educació en diabetis que integra un glucòmetre amb la consola de joc Nintendo DS. L'objectiu del joc és educar els menors afectats i, sobretot, estimular que facin un bon control de la glucèmia mitjançant l'ús correcte del glucòmetre. En un àmbit professional, també trobem jocs per educar professionals, per exemple, en la interpretació d'electrocardiogrames (disponible en http://www.m2hnursing.com/flash/ecg_activity.html).

Joc per a diabetis *Didget*



Font: <http://www.bayerdidget.ca/>

La ludificació consisteix en la utilització de tècniques de disseny de jocs, i també l'ús de la seva mecànica, en contextos aliens als jocs (per exemple, en la cura de la salut). L'objectiu és convertir les tasques avorrides (com pot ser el control de la glucosa en sang) en divertides, i fomentar que adoptem actituds saludables, aprofitant la predisposició psicològica dels éssers humans per a participar en jocs, a més d'altres elements de la motivació humana. D'aquesta manera, obtenim beneficis per a la nostra salut gairebé sense adonar-nos-en.

Un exemple és el portal d'educació sexual <http://www.sjekkdeg.no/>, en què s'han incorporat elements de ludificació per atreure la població adolescent. Entre altres aspectes de ludificació, els usuaris podran guanyar punts per completar exercicis educacionals que els permetran comprar educació per als seus avatars.

Sistema de punts del portal sjekkdeg.no.

The screenshot shows a user's 'Avatar' page on the website sjekkdeg.no. The page has a blue header with a navigation menu, the user's name 'Avatar', and social media sharing buttons for Facebook and Twitter. Below the header, there are three tabs: 'Forandre avatar', 'Mine resultater', and 'Send unilink på nytt'. The main content area displays three achievement items, each with an icon, a title, a description, a price, and a lock icon indicating it is not yet earned.

Icon	Title	Description	Price	Lock Icon
	Nummer 1	Gjennomføre undersøkelsen	Price: Få nummer 1 medalje	
	Kitty bell krage	Les alle de vanlige spørsmålene	Price: En fin kitty bell krage	
	Best resultater i Nord Norge	Besvart alle spørsmålene perfekt	Price: Få de riktige svarene på alle spørsmålene i Skolen	

Font: <http://www.sjekkdeg.no/>

La ludificació està cridada a ser una de les tendències més importants en tecnologia. Segons un informe efectuat el 2011 per Gartner, el 2015 més del 50% de les organitzacions que gestionen processos d'innovació els ludificaran. Podem veure l'interès creixent per la ludificació en el gràfic següent de Google, que ens mostra com han anat evolucionant les cerques del terme *gamification* des del setembre del 2010 fins al setembre del 2012.

Google Trends: *gamification*

Interés a lo largo del tiempo ?

El número 100 representa el pico en el volumen de búsquedas

Titulares de noticias Previsión ?



Font: <http://www.google.es/trends/explore#q=gamification&date=9%2F2010%2025m&cmpt=q>

A més de la diversió, una altra manera d'incentivar poden ser les recompenses. Posem-ne alguns exemples.

- **Recol·lecció d'insígnies:** per exemple, x temps amb control acceptable de glucosa en sang.
- **Punts** que ens puguin situar en una taula de classificació, de manera que s'estimuli el nostre costat més competitiu.
- **Retroalimentació** amb informació segons els nostres assoliments.
- **Moneda virtual**, per a intercanviar per articles dins de la plataforma del joc: punts, insígnies, millores, etc. També es podrien comprar articles d'altres plataformes. Per exemple, si un nen aconsegueix un mes de bons controls glucèmics, podria obtenir un crèdit a l'iTunes per comprar una cançó o aplicació per al mòbil.

8. La LOPD i el Web 2.0

8.1. Introducció

Començarem exposant alguns conceptes fonamentals; premisses que no s'han de perdre de vista pel que fa a l'ús de les xarxes socials per part dels organismes públics.

8.1.1. Les dades personals tenen valor econòmic

Avui dia, ningú no qüestiona ja que les dades de caràcter personal constitueixen un gran negoci des de la dècada de 1980. Es compren i es venen com qualsevol altra mercaderia. El 1992, la LORTAD va intentar pal·liar els excessos de les empreses que comercialitzaven lliurement amb les nostres dades. Poc després, el 1999, també ho va fer la LOPD, acompanyada del Reial decret 1720/2007 que regula la LOPD i estableix les mesures de seguretat de la informació mínimes exigibles.

8.1.2. El negoci de les xarxes socials són les dades personals

Amb el temps, i gràcies a la legislació per a la protecció de dades personals, s'ha fet més i més difícil obtenir dades personals per a finalitats comercials. Llavors, apareixen les xarxes socials, com a formes d'oferir serveis "gratuïts" a les persones a canvi de les seves dades personals, i el negoci principal de les quals és vendre aquestes dades a tercers o utilitzar-les per a finalitats comercials.

Quan el servei és "gratuït", la mercaderia són les dades personals.

8.1.3. No hi ha oportunitat sense risc

Tota activitat comporta un cert risc. Som conscients que conduir implica un determinat risc d'accident. Per disminuir aquests riscos, conduïm amb més precaució, més a poc a poc, seguint les normes de circulació. Per disminuir l'impacte, s'incorporen als cotxes coixins de seguretat, ABS, cristalls especials, etc.

Igualment, en la pràctica clínica trobem riscos inherents. Per exemple, les transfusions sanguínies comporten un cert risc d'infecció: hepatitis o VIH. També hi ha el risc de transfondre sang d'un grup o Rh equivocat i provocar un xoc anafilàctic.

No obstant això, fem transfusions de sang en moltes intervencions, malgrat que sabem que han causat centenars de milers de morts a Occident, com indiquen alguns informes sobre seguretat del pacient de l'Organització Mundial de la Salut (OMS). En tot cas, es continuen salvant milions de vides.

8.1.4. En general, les xarxes socials presenten els mateixos riscos que qualsevol altre servei de tecnologies de la informació

En molts centres sanitaris hi ha moltes reticències a utilitzar les xarxes socials, i s'al·leguen arguments poc precisos. Cal ser prudents, per descomptat, però no a qualsevol preu, com veurem més endavant.

De vegades, la decisió de “ tancar ” l'ús de les xarxes socials no és una decisió meditada. De vegades prové del que podem denominar la *informàtica defensiva*. És a dir, es practica la seguretat “per si de cas”: si tanco, no tinc problemes.

Aquesta actitud pot estar limitant o fins i tot impeding objectius de l'organització i, en qualsevol cas, aquesta decisió ha d'estar basada en una anàlisi de riscos. En realitat, cessar l'activitat que pot causar el risc és una manera de gestionar-lo. No obstant això, la informàtica defensiva és una mala interpretació d'aquesta manera de gestionar-lo. Cessar una activitat necessària no és una manera de gestionar el risc.

Igual que conduir o fer una transfusió de sang, l'ús de les xarxes socials també presenta riscos inherents. Aquestes zones de risc són similars a d'altres de provocades per l'ús de les tecnologies de la informació, com ara la ineficiència, una inversió errònia, eficàcia insuficient, etc. Més endavant les comentarem.

8.1.5. Hi ha riscos particulars de les xarxes socials

No obstant això, les xarxes socials presenten algunes àrees de risc que podrien tenir un impacte més gran a causa del seu ús. Per exemple, **danys en la imatge pública** a causa de comentaris o missatges negatius i el **risc de velocitat d'expansió** que comentarem una mica més endavant.

8.1.6. El risc zero no existeix

Amb el risc, podem fer diverses coses:

- Evitar-lo cessant l'activitat. Mal entès, és el més fàcil, una forma d'informàtica defensiva; ben entès, pot representar una reenginyeria de processos.
- Reduir la probabilitat que ocorri.
- Reduir les conseqüències quan ocorri.

- Transferir-lo.
- Acceptar-lo.

L'única cosa que no es pot fer amb el risc és ignorar-lo.

No obstant això, fem el que fem, **el risc zero no existeix**. El risc és interactiu: si hi ha el risc de dur a terme una activitat, també hi ha riscos per no dur-la a terme. Si es mitiga un risc, és molt probable que s'incrementi algun altre risc relacionat.

Per tant, si esperem a **eliminar el risc** per dur a terme una activitat, no podrem fer-ho mai.

8.1.7. La decisió sobre el risc es pren en el més alt nivell

Acceptar un risc o, per contra, evitar-lo, reduir-lo o transferir-lo comporta uns costos. És raonable reduir un risc fins que el cost de continuar fent-lo superi l'impacte que ocasionaria si es produís.

Una opció com cessar l'activitat que el podria provocar també té uns costos. L'organització es pot permetre cessar una de les seves activitats? Ens plantegem deixar de fer transfusions sanguínies pel risc d'infecció, o per contra redefinim processos i perfeccionem els controls sobre la sang?

Per què pel que fa a l'ús de les xarxes socials s'opta per aquesta manera de gestionar el risc mal entesa? No cal oblidar que les xarxes socials no són més que eines per a dur a terme activitats relacionades amb la missió o els objectius de l'organització. No són una finalitat en si mateixa.

En qualsevol cas, la decisió sobre cessar una activitat organitzativa correspon, com no pot ser d'una altra manera, a la més alta direcció, i en cap cas al personal tècnic. I per descomptat, després d'una anàlisi dels riscos.

8.1.8. Eficàcia relacionada amb els objectius de l'organització

L'ús de les xarxes socials n'hauria de demostrar l'eficàcia d'una manera mesurable, ja que es troba relacionada amb els objectius i l'estratègia de l'organització.

8.2. Àrees de risc

Les estadístiques mostren que, pel que fa als empleats que utilitzen les xarxes socials a la feina, hi ha un risc considerable més enllà del risc de pèrdua de productivitat (podeu veure la taula següent).

Riscos de les xarxes socials associats amb els empleats

El 64% de les persones que utilitzen les xarxes socials fa clic en els enllaços sense saber cap a on els portaran.

Més del 50% dels usuaris deixa les seves credencials d'accés als seus amics.

El 47% dels usuaris de les xarxes socials ha estat víctima de programari maliciós.

El 26% dels usuaris de les xarxes socials comparteix arxius personals en les xarxes socials.

El 21% dels usuaris de les xarxes socials accepta ofertes de contactes per part de desconeguts.

El 20% dels usuaris de les xarxes socials ha patit un robatori d'identitat.

Font: Protiviti. "Managing Privacy Risks in Social Media-Driven Society" [en línia]. <<http://www.protiviti.com>>

El 64% de les persones que fan servir les xarxes socials fan clic als enllaços, fins i tot sense saber cap a on portarà l'enllaç. Podem imaginar que qui ho fa a les xarxes socials ho farà igualment mentre navega o usant el correu electrònic. El mateix ocorre amb els usuaris víctimes del programari maliciós. Caldria preguntar-se: quants usuaris que no usen les xarxes socials han estat víctimes del programari maliciós? Quants usuaris comparteixen arxius per correu electrònic?

Vegem, a continuació, les amenaces que afecten l'ús de les xarxes socials.

Àrees de risc de les xarxes socials

Risc	Imatge pública	Efectivitat
Abús dels empleats		X
Publicacions negatives	X	
Falta de control adequat de continguts	X	X
Enteniment cultural inapropiat	X	X
Violacions potencials de la confidencialitat d'organització	X	X
Expansió (velocitat d'expansió d'esdeveniments adversos)	X	X
Mal ús (programari maliciós, usuaris compartits, ignorància)	X	X
Robatori d'identitat, enginyeria social	X	X
Pèrdua d'informació / dades sensibles	X	X
Violacions al compliment (legals i regulatòries)	X	X
Pèrdues financeres		

Font: Protiviti. "Managing Privacy Risks in Social Media-Driven Society" [en línia]. <www.protiviti.com>

Risc	Imatge pública	Efectivitat
Pèrdua de seguretat (per exemple, a causa de l'exposició d'informació sobre viatges o desplaçaments)		
Ús ineficient dels recursos de xarxa		X
Imatge corporativa inconsistent		X
Interrupció dels serveis		X
Usurpació de comptes d'usuari, <i>defacing</i> i difamació	X	X

Font: Protiviti. "Managing Privacy Risks in Social Media-Driven Society" [en línia]. <www.protiviti.com>

Com es pot comprovar, moltes de les àrees de risc operacional afecten l'efectivitat, i si ocorren és bastant probable que ocasionin, a més, un dany a la reputació i imatge pública de l'organització.

Aquestes zones de risc són probablement més elevades i amb més impacte que les que n'afecten només una.

Una de les coses que fan que els riscos de les xarxes socials siguin diferents d'altres riscos de les tecnologies de la informació (TI) és el **risc de la velocitat d'expansió**. És a dir, la informació es difon d'una manera molt ràpida a través de les xarxes socials, i la transició als mitjans de comunicació convencionals, en alguns casos, pot ocórrer tan sols en uns minuts des que s'ha produït una declaració polèmica o uns comentaris inadequats. En altres camps, el ritme no és tan ràpid ni tan ampli. És el que es descriu com una **transmissió viral**.

És important tenir en compte aquest fet en l'avaluació de riscos de les xarxes socials de l'organització per a la construcció posterior dels controls i les contramesures.

8.3. Drets 2.0

Fem un repàs breu als drets 2.0. Es tracta dels drets que tenen els usuaris de les xarxes socials. És important conèixer-los per a plantejar les nostres responsabilitats com a "fabricants" de productes 2.0, tant des d'àmbits personals i professionals com des de les organitzacions sanitàries.

8.3.1. La llibertat d'expressió en el Web 2.0

Poc cal dir sobre el dret que tenim tots a la **llibertat d'expressió**. Està inclòs en l'article 20 de la Constitució espanyola i ens permet "expressar i difondre lliurement els pensaments, idees i opinions mitjançant la paraula, l'escrit o qualsevol altre mitjà de reproducció i comunicar o rebre lliurement informació veraç per qualsevol mitjà de difusió".

8.3.2. La llibertat d'informació en el Web 2.0

Juntament amb la llibertat d'expressió, destaca d'una manera connexa un segon dret, el de la **llibertat d'informació**. No obstant això, es diferencia de l'anterior en el fet que presenta uns requisits objectius.

- Que la informació sigui veraç, és a dir, exigeix una base en fets objectius i reals.
- Que la informació tingui rellevància pública, i no tenen aquesta rellevància els fets que afecten persones privades en actuacions o fets quotidians.

El fet de comentar les intimitats d'una persona propera que no té el caràcter de personatge públic no quedaria emparat sota la protecció del dret de llibertat d'informació i, en funció dels comentaris efectuats, podria traspasar els límits del dret a la llibertat d'expressió.

El dret a la **llibertat d'informació** estableix dues condicions: la informació ha de ser veraç i, a més, tenir rellevància pública. És a dir, els fets que els succeeixen a les persones en la seva vida privada excedeixen el dret de llibertat d'informació.

8.3.3. La intimitat, privadesa i imatge pròpia en el Web 2.0

El **dret a la intimitat, privadesa i la imatge pròpia** limita el dret de llibertat d'informació. Possiblement, es tracta del que s'envaeix amb més facilitat, per exemple, mitjançant la divulgació d'insults o calúmnies contra persones identificables en fòrums, o el costum ja tan estès de publicar fotos de tercers a les xarxes socials més enllà del cercle d'amics.

8.3.4. La protecció de dades en el Web 2.0

El dret a la protecció de dades és un dret fonamental. En la mesura que cada internauta pot ser protagonista, editar la seva pàgina personal, participar en wikis, crear el seu web o mantenir el seu blog, assumeix una responsabilitat jurídica.

Els usuaris de les xarxes socials tenen **dret al fet que es respectin les seves dades personals**, a estar informats de quines activitats s'hi duran a terme i que se'ls sol·liciti el consentiment per utilitzar-les.

Hem de tenir en compte que funcionalitats com la geolocalització, imatges, vídeos, enregistraments de veu, etc. són dades de caràcter personal si poden identificar l'usuari i, per tant, serà necessari el seu consentiment per a publicar-los.

Els responsables de webs i blogs assumeixen una responsabilitat jurídica sobre el que es publica en els seus llocs.

8.3.5. La propietat intel·lectual en el Web 2.0

La propietat intel·lectual és el dret que tenen les persones sobre les creacions o obres pròpies. Sempre que es vulgui utilitzar una obra (textos, fotografies, vídeos, etc.) allotjada en la Xarxa, s'ha de comprovar que està permès reproduir-la i que l'obra no està protegida per la propietat intel·lectual.

L'Institut Nacional de Tecnologies de la Comunicació (INTECO), en la seva *Guía de introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas*, diu que en el context del Web 2.0, els usuaris podran utilitzar en plataformes col·laboratives:

- Qualsevol obra que hagin creat (sempre que no hagin cedit els drets d'explotació a uns altres).
- Obres amb autorització dels seus titulars de drets, sia d'una manera directa o per mitjà de qualsevol de les llicències que hi ha actualment (Creative Commons, GPL, etc.).
- Obres caigudes en el domini públic.
- Obres exposades d'una manera permanent en la via pública (cartells, escultures, etc.).
- Discursos o conferències pronunciats en públic, sempre que tinguin una finalitat informativa (i no merament comercial).
- Treballs sobre temes d'actualitat, en la mesura descrita anteriorment.

8.4. Obligacions i responsabilitats

Per descomptat, atès que els usuaris de les xarxes socials tenen uns drets, d'altra banda tant usuaris com generadors de continguts (administradors) tenen unes responsabilitats.

8.4.1. Usuaris

En primer lloc, com a usuaris, hem de respectar els drets 2.0 dels altres, i fer un ús responsable del dret a la llibertat d'expressió.

L'Institut Nacional de Tecnologies de la Comunicació (INTECO), en la *Guía de introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas*, exposa que excedeixen les funcions de l'usuari i, per tant, són conductes il·lícites:

- Cometre el delictes d'injúries o calúmnies en efectuar una imputació falsa d'un delictes a una altra persona o manifestar expressions que atemptin contra el dret a l'honor, a la imatge pròpia i a la intimitat personal.
- Incórrer en violacions a la Llei de la propietat intel·lectual (drets d'autor) en publicar qualsevol obra protegida que no tingui l'autorització expressa del titular o quan no es faci un ús correcte del dret de citació, sia sobre textos (articles, llibres, notes, etc.) sia continguts multimèdia (música, àudio, vídeo, programari, etc.).
- Violar drets de marca, de disseny, secrets comercials o drets industrials (com patents).
- Atemptar contra el dret a la protecció de dades publicant informació privada de tercers (publicar un correu electrònic personal).
- Cometre delictes de pornografia infantil, en publicar qualsevol representació d'un menor de divuit anys dedicat a activitats sexuals explícites o tota representació de les seves parts genitals amb finalitats predominantment sexuals.

En tot cas, la responsabilitat serà de la persona que cometi el fet delictiu. No obstant això, aquesta responsabilitat es pot ampliar a altres persones per la falta d'una vigilància correcta de la plataforma, com es veurà en l'apartat següent.

Per exemple, publicar un vídeo d'una altra persona que no ha atorgat el seu consentiment exprés perquè es fes aquesta difusió, i fins i tot perquè es gravés aquest vídeo, representa un atemptat contra el seu honor i la seva intimitat personal.

8.4.2. Administradors i moderadors

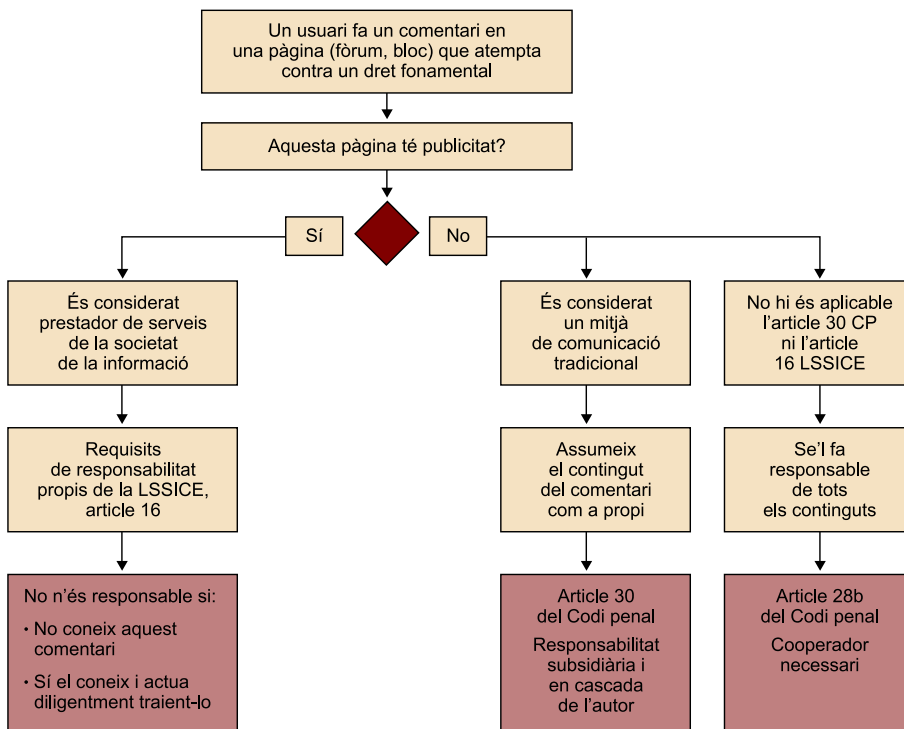
Els administradors i moderadors tenen l'obligació de fer que es respectin tots els drets dels usuaris i garantir un ús de la plataforma. Encara que els comentaris puguin ser anònims, l'administrador en continua sent responsable.

És una bona pràctica que l'administrador d'un fòrum inclogui en la seva pàgina una política de publicació, per evitar entrades inadequades dels usuaris i la possibilitat que altres usuaris denunciïn aquestes situacions i es pugui dur a terme un control posterior més efectiu.

És important destacar l'**existència de mecanismes efectius que permetin als usuaris denunciar** situacions que atemptin contra algun dels drets esmentats (per mitjà d'un correu electrònic o un formulari, per exemple). D'aquesta manera, qui és responsable dels comentaris escrits en un blog?

Encara que sembli una mica estrany, l'existència de publicitat determina la llei que és aplicable per a l'assignació de responsabilitat. Per tant, si el blog conté publicitat, el propietari és considerat un prestador de serveis, i hi és aplicable l'article 16 de la LSSICE. En canvi, si el blog no té publicitat, el propietari es pot considerar un mitjà tradicional o col·laborador necessari, i hi és aplicable el Codi penal.

El diagrama següent esquematitza el procés de determinació de responsabilitat.



Font: elaboració pròpia

8.4.3. Empreses prestadores de serveis

Finalment, la tercera figura participant de les xarxes socials són els proveïdors de serveis (Facebook, Twitter, LinkedIn, etc.). Aquests també tenen les seves obligacions i responsabilitats enfront dels usuaris.

Novament, en trobem un bon resum en la *Guía de introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas*. Els prestadors de serveis d'allotjament de pàgines web, serveis web 2.0, serveis d'allotjament de dades, els proveïdors d'accés i els operadors de telecomunicacions tenen les obligacions següents.

- Informar els clients sobre les principals dades com a prestadors de serveis (identificació i correu electrònic), els serveis prestats i els termes de la prestació, la política de protecció de dades i els mitjans tècnics que augmentin la seguretat dels usuaris.
- Col·laborar amb els organismes públics per a execucions que no es puguin dur a terme sense la seva ajuda.
- Són responsables dels continguts si tenen coneixement efectiu que l'activitat o la informació a la qual remeten és il·lícita o que lesiona béns o drets d'un tercer susceptibles d'indemnització.
- Són responsables pel que fa a les dades de caràcter personal que es tracten en els cercadors de perfils o en les campanyes de publicitat personalitzada.

8.5. Recomanacions

Aquestes recomanacions estan extretes de la *Guía de introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas*, en la qual podreu trobar a més algunes bones pràctiques tant per a usuaris com per a administradors.

8.5.1. Usuaris

- En el Web 2.0 els usuaris han de respectar unes normes de privadesa, tant quant a dades pròpies com a informació de tercers.
- Els usuaris han de protegir la informació. Per aquest motiu, és necessari llegir les polítiques de privadesa i establir uns límits sobre qui pot o no accedir a la informació publicada.
- Una bona pràctica és recórrer a l'ús de pseudònims o *nicks* personals que li permetin disposar d'una "identitat digital".

- No s'ha de publicar informació excessiva de la vida personal i familiar, és a dir, informació que no es difondria en entorns no tan propers.
- És necessari tenir una cura especial en publicar continguts audiovisuals i gràfics, sobretot si es tracta d'imatges relatives a terceres persones.
- Abans de publicar una foto, és recomanable considerar si és adequat penjar-la o si aquesta acció pot comportar conseqüències i involucrar gent de la feina, escola, universitat o de l'entorn proper o personal.
- Si es vol utilitzar o reproduir qualsevol obra a la Xarxa (gràfica o no), s'ha de recórrer a l'avís legal de la pàgina web en què es trobi i veure'n les condicions de reproducció.
- S'ha de recórrer a l'Agència de Protecció de Dades, AEPD, per exercir els drets que atorga la LOPD amb relació a la protecció de les dades de caràcter personal. En el lloc de l'AEPD es pot descarregar un model de reclamació.

8.5.2. Administradors i moderadors

Segons s'estableix en la LOPD, tota persona que tracti dades de caràcter personal (associades a cercadors, perfils, etc.) ha de complir unes obligacions i atendre els afectats d'aquest tractament. Entre altres requisits, hi ha d'haver un titular que dugui a terme un tractament de dades.

- Ha d'inscriure el fitxer en el registre de l'AEPD i adequar els fitxers a la normativa vigent (LOPD i Reglament de desenvolupament).
- Està obligat a informar els usuaris sobre la política de privacitat de la pàgina web, i també de la finalitat per a la qual es recaptin dades de caràcter personal, el responsable del tractament i els drets de què disposa l'usuari.
- Ha de recaptar el consentiment inequívoc de l'afectat per difondre'n les dades.
- Ha de permetre als usuaris l'exercici dels seus drets d'accés, rectificació, cancel·lació i oposició.
- No ha d'incloure publicitat.
- Ha d'incloure la política de publicació.

8.5.3. Mecanismes perquè els usuaris puguin denunciar

És important exercir d'una manera efectiva les tasques de supervisió i control, sobre els participants i les seves informacions. Davant comentaris o informacions incorrectes o il·lícits, cal intervenir en el debat i/o eliminar-ne els comentaris.

Cal implementar mesures tecnològiques que permetin conèixer l'edat dels usuaris, com ara l'ús de certificats reconeguts de signatura electrònica o d'aplicacions que detectin el tipus de lloc web visitat i els serveis més demanats.

És un deure col·laborar amb les forces i els cossos de seguretat de l'Estat per identificar usuaris que cometen fets il·lícits.

8.6. Les administracions públiques 2.0

8.6.1. Motivació

Al portal d'Administració electrònica, podem trobar la afirmació següent: “els mitjans i xarxes socials són un lloc de trobada en el qual els usuaris d'Internet consumeixen un temps cada vegada més gran. Els organismes i ministeris hi han iniciat un acostament, i surten a l'encontre dels ciutadans allí on els ciutadans es troben”.

Això indica una estratègia clara de l'Administració pública per arribar a la ciutadania a partir dels nous mitjans. Podem dir, llavors, que l'ús de les noves tecnologies està perfectament justificat amb unes finalitats concretes. No obstant això, és necessari tenir en compte les regulacions aplicables.

8.6.2. Normativa

La Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics (LAECSP) regula les condicions per a la prestació de serveis a la ciutadania.

La LAECSP reconeix el dret dels ciutadans a relacionar-se amb les administracions públiques espanyoles amb mitjans electrònics, i regula la utilització de les tecnologies de la informació o TIC perquè els drets dels ciutadans quedin garantits quan siguin atesos per aquesta via (art. 3 LAECSP).

8.6.3. Serveis no aplicables

Segons l'estudi *Redes sociales en Internet 2011* (Observatori Nacional de les Telecomunicacions i la Societat de la Informació), els principals riscos derivats de l'ús d'aquests serveis estan relacionats amb la suplantació d'identitat, la possibilitat que puguin saber el que es fa o diu en la Xarxa i l'ús delictiu

de la informació que conté. Els serveis de xarxa social presenten problemes d'identificació i autenticació, i també de seguretat, integritat i confidencialitat de la informació, requisits tots exigits per la LAECSP (art. 1.2) per a la utilització de les tecnologies de la informació en les relacions de l'Administració amb la ciutadania.

Prestació de serveis

Sembla que en aquestes condicions no és gaire adequada la prestació de serveis públics o mantenir relacions administratives amb els ciutadans per mitjà de les xarxes socials. L'Administració pública no podria garantir d'una manera adequada el servei, i a més no té la possibilitat d'actuar de cap manera per millorar-lo, ja que per a això depèn completament del prestador de serveis (Facebook, Twitter, Twenti, etc.).

Per a la prestació de serveis electrònics a la ciutadania, s'ha d'habilitar un canal segur que garanteixi les condicions adequades per a la prestació del servei. Aquest canal és la seu electrònica.

Comunicació d'actes administratius

Les xarxes socials tampoc no són un mecanisme adequat per a la comunicació d'actes administratius amb un ciutadà en particular. Novament, la LAECSP estableix en l'article 27.3 el següent.

“Secció 2a. De les comunicacions i les notificacions electròniques.

Article 27. Comunicacions electròniques.

3. Les comunicacions per mitjans electrònics són vàlides sempre que hi hagi constància de la transmissió i recepció de les dates, del contingut íntegre de les comunicacions i s'identifiqui d'una manera fidedigna el seu remitent i el seu destinatari.”

8.6.4. Serveis aplicables

Activitat informativa

El Reial decret 208/1996, de 9 de febrer, pel qual es regulen els serveis d'informació administrativa i atenció a la ciutadania en l'àmbit de l'AGE2 08/1996, de 9 de febrer (per la qual es regulen els serveis d'informació administrativa i atenció a la ciutadania en l'àmbit de l'AGE), permet utilitzar per a la difusió d'informació administrativa de tipus general el mitjà que resulti més adequat segons les circumstàncies. S'inclou “qualsevol forma de comunicació que els avenços tecnològics permetin” (art. 1.4).

Comunicació institucional

“Segons la Llei 29/2005, de 29 de desembre, de publicitat i comunicació institucional, una campanya institucional de publicitat és qualsevol activitat orientada i ordenada a la difusió d'un missatge o objectiu comú, dirigida a una pluralitat de destinataris, que utilitzi un suport publicitari pagat o cedit i que sigui promoguda o contractada per algun dels subjectes enunciats en l'article 1, és a dir, per qualsevol de les administracions públiques espanyoles. Campanya de comunicació és quan s'utilitzin formes de comunicació diferents de les publicitàries.

En l'exposició de motius d'aquesta norma es pot apreciar que no solament es recomana, sinó que s'ordena, la utilització dels mitjans de comunicació que garanteixin millor la difusió del missatge. Per això diem que l'entorn xarxa social arriba a ser, en aquest cas concret, molt apropiat per les característiques que ja s'han descrit amb anterioritat.”

Govern obert

Les xarxes socials representen un canal excel·lent per a escoltar les opinions i reaccions de la ciutadania davant les actuacions de les administracions, de manera que es converteixen en una eina excel·lent per a la participació de la ciutadania en l'Administració pública.

El govern obert (*open Government*) és un govern que entaula una conversa constant amb els ciutadans per escoltar el que diuen i sol·liciten, que pren decisions basades en les seves necessitats i preferències, que facilita la col·laboració dels ciutadans i funcionaris en el desenvolupament dels serveis que presta i que comunica tot el que decideix i fa d'una manera transparent i oberta (Calderón i Lorenzo, 2010).

8.6.5. Responsabilitats

Encara que les xarxes socials són productes oferts i controlats pels seus proveïdors de serveis respectius, la seva utilització per part de les administracions públiques, que actuen com un simple usuari, no està exempta de responsabilitats.

L'Administració ha de mostrar una actitud activa en la implementació i en el maneig de les seves xarxes socials, i també configurar i actualitzar d'una manera adequada les opcions de seguretat que ofereixen.

D'altra banda, cal considerar la responsabilitat patrimonial de l'Administració.

Segons declara la nostra norma bàsica i fonamental en l'article 106.2, "els particulars, en els termes establerts per la llei, tenen dret a ser indemnitzats per tota lesió que sofreixin en qualsevol dels seus béns i drets, excepte en els casos de força major, sempre que la lesió sigui conseqüència del funcionament dels serveis públics".

Encara que aquesta responsabilitat és present, el risc que es causi dany als drets dels usuaris a causa d'activitats informatives o de comunicació institucional sembla molt baix.

8.6.6. Altres riscos

Identitat institucional

Un dels riscos inherents a l'ús de les xarxes socials per part de qualsevol organització és la inconsistència de la imatge institucional. Altres amenaces, com la suplantació d'identitat o *defacing*, poden desembocar en situacions semblants.

D'altra banda, sempre es corre el risc que apareguin pàgines no oficials que imiten els perfils institucionals. No obstant això, en la nostra opinió, l'impacte d'aquesta amenaça és encara més gran si l'Administració no és present a les xarxes socials per contrarestar aquesta "imitació".

El risc d'inconsistència en la imatge institucional es pot salvar amb la publicació de guies d'estil i formació específica per als usuaris autoritzats per actuar en nom de l'organització per mitjà de les xarxes socials.

Pel que fa a la suplantació d'identitat, es pot limitar gairebé completament amb una configuració adequada de les opcions de privadesa, utilitzant claus d'usuari fortes (combinacions de lletres majúscules i minúscules amb nombres i símbols de més de vuit caràcters) i canviant les contrasenyes d'una manera periòdica.

El *defacing* (atac en el qual es modifica el web i s'hi fan aparèixer missatges, normalment reivindicatius de part de l'atacant) i l'aparició de pàgines d'imitació es poden limitar amb una actitud activa per part de l'organització, si es denuncien ràpidament aquests comportaments davant el prestador de serveis oportú.

Propietat intel·lectual

Com tots sabem, l'ús de les xarxes socials comporta l'acceptació de les condicions imposades pel prestador de serveis corresponent, que sol incloure clàusules abusives relatives a la propietat intel·lectual del material allotjat en la Xarxa i que representen una cessió de drets al seu favor. Això també succeeix per a l'Administració.

El problema consisteix que l'Administració pública no pot cedir els seus drets de propietat intel·lectual en favor de tercers, segons s'inclou en la Llei 33/2003, de 3 de novembre, del patrimoni de les administracions públiques.

Es corre el risc que algun usuari autoritzat publiqui o comparteixi documentació sotmesa a propietat intel·lectual per mitjà de les xarxes socials.

Una vegada més, una bona tasca de conscienciació i formació entre els usuaris autoritzats serà la manera més efectiva de limitar el risc que ocorri aquesta amenaça.

D'altra banda, una tasca de supervisió activa dels continguts per part de l'Administració hi ajudarà. Aquesta supervisió no s'ha de confondre amb formes de control o censura que limitarien l'eficàcia d'aquestes eines en les seves comeses.

I les dades de caràcter personal?

Es tracta d'una de les grans preocupacions de les administracions, que limiten l'ús de les xarxes socials com a mitjans de comunicació institucionals.

En aquells casos en els quals un usuari de les xarxes socials actua en nom d'una empresa o associació o utilitza les xarxes socials amb finalitats comercials, polítiques o socials, es considera que no està actuant en l'àmbit personal i, per tant, estarà plenament sotmès a la LOPD.

Una administració pública en l'ús de les xarxes socials es trobaria, per tant, en aquesta situació. No obstant això, encara que estaria sotmesa a la LOPD, si es fa un ús de les xarxes socials amb les finalitats esmentades anteriorment (activitat informativa i comunicació institucional), s'estarien tractant dades de caràcter personal?

Els proveïdors de serveis de les xarxes socials ofereixen la possibilitat d'utilitzar perfils d'empresa, organització i institució, que no permeten ni llançar ni acceptar sol·licituds d'amistat, amb la qual cosa no es generarà una base de dades d'amics que es considerarien un fitxer.

Novament, la formació i conscienciació dels usuaris autoritzats torna a ser molt important per a limitar aquest tipus de riscos.

La difusió del deure de secret i les conseqüències del seu incompliment entre els empleats autoritzats per representar l'organització per mitjà de les xarxes socials són el mecanisme més efectiu.

8.6.7. Conclusió

La participació de les administracions públiques a les xarxes socials és legalment possible i, dins dels límits explicats, fins i tot oportuna.

Encara que hi ha riscos, aquests es poden mitigar sense gaire dificultat.

I encara que aquesta participació no està exempta de certa complexitat, la formació adequada als implicats en l'ús de l'entorn tecnològic a què s'enfrontaran, en el marc legal aplicable i en les condicions per a l'ús d'aquestes eines, limita els riscos inherents.

Es tracta de formació sobre les seves responsabilitats i obligacions respecte de la informació que manegen i respecte dels ciutadans. Per a això, la creació i difusió adequades de guies d'estil i manuals d'ús ben elaborats constitueixen les millors eines.

Resulta molt recomanable una figura encarregada de supervisar el compliment d'aquestes normes. Això comporta la translació de la figura del gestor de comunitats (*community manager*) a l'àmbit de l'Administració pública.

En qualsevol cas, la manera com les administracions decideixin ser presents a les xarxes socials ha de ser fruit d'una anàlisi de riscos.

Una anàlisi seriosa sobre les amenaces i el seu impacte en l'organització ens donarà una idea més encertada sobre allò del que ens hem de preocupar i ens permetrà orientar-nos sobre les maneres de mitigar aquests riscos.

Senzillament, cessar l'activitat susceptible de risc no és una opció responsable sense una anàlisi rigorosa sobre les conseqüències. De vegades, cessar les activitats pròpies de l'organització no és possible ni viable, i fins i tot pot ser que introdueixi riscos més grans per a la seva imatge.

9. Seguretat de la informació

9.1. Introducció a la seguretat de la informació en salut i marc legal

9.1.1. La confidencialitat

La Llei orgànica de protecció de dades i el Reial decret 1720/2007 de mesures de seguretat han estat pilars fonamentals per al desenvolupament de les polítiques sobre seguretat de la informació.

Quan es parla de protecció de dades, se sol fer referència a la **confidencialitat**. S'ha establert un binomi protecció de dades - confidencialitat que s'ha estès entre els professionals i que ha repercutit en conscienciació i en actuacions relacionades amb el transport i la custòdia de les històries clíniques, per exemple.

No obstant això, veurem a continuació que la vertadera inquietud entre els professionals no és la confidencialitat, sinó la disponibilitat i, sobretot, la integritat de la informació.

Organismes com l'OMS han establert una relació directa entre **seguretat de la informació** i **seguretat del pacient**. Parlen en termes d'incidents de seguretat i esdeveniments adversos, però sobre aspectes directament relacionats amb la informació següent.

- Errors d'identificació del pacient.
- Errors de comunicació entre professional i professional.
- Errors de comunicació entre professional i pacient.

Termes com *identificació* i *comunicació* semblen més propers al món de les TI que a l'esfera de la sanitat.

9.1.2. L'informe ENEAS 2005

L'Estudi ENEAS 2005, *Estudio nacional sobre los efectos adversos ligados a la hospitalización*, inclou la definició següent.

Error per identificació deficient

Aquest error considera i inclou totes les actuacions efectuades a un malalt per al qual no estaven destinades com a conseqüència d'una identificació deficient (per exemple, transfusions a un malalt equivocat, errors en actuacions quirúrgiques, membre equivocat, etc.).

A més tipifica efectes adversos, com els següents:

- Retard en el diagnòstic per falta de proves pertinents (disponibilitat de la informació).
- Error d'identificació del pacient (integritat de la informació).
- Error d'etiquetes identificatives en els tubs d'hemograma (integritat de la informació).
- Transmissió incorrecta dels resultats de microbiologia (integritat de la informació).
- Cirurgia de lloc equivocat (integritat de la informació).
- Confusió de la història clínica (integritat de la informació).
- Lletra il·legible en l'informe d'alta (integritat de la informació).
- Informació deficient sobre tractament postalta (integritat de la informació).

9.1.3. Objectius de seguretat 2011 de la Joint Comission

D'altra banda, segons l'OMS, es calcula que als països desenvolupats un de cada deu pacients sofreix algun tipus de dany durant l'estada a l'hospital.

Una de les iniciatives més influents són els objectius per a la seguretat del pacient, que proposa anualment la Joint Comission, que mira de concentrar els esforços en els aspectes considerats més prioritaris per a la millora de la qualitat i seguretat dels centres sanitaris.

Entre els objectius proposats per al 2011, podem trobar els següents.

Objectiu 1: millorar la identificació del pacient (integritat de la informació)

- NPSG.01.01.01: utilitzar, almenys, dos identificadors del pacient quan es proporcionen serveis, tractaments i cures.
- NPSG.01.03.01: eliminar els errors en les transfusions relacionats amb la identificació del pacient.

Objectiu 2: millorar la comunicació efectiva entre cuidadors (disponibilitat de la informació)

- NPSG.02.03.01: informar a temps i de manera oportuna sobre els resultats crítics de proves diagnòstiques.

Objectiu 3: millorar l'ús segur dels medicaments (integritat de la informació)

- NPSG.03.04.01: etiquetar la medicació, els seus contenidors (xeringues, pots, etc.) i altres solucions.

Objectiu 4: assegurar la precisió de la medicació en les transicions assistencials (integritat i disponibilitat de la informació)

- NPSG.08.02.01: quan el pacient és transferit a un altre hospital o a atenció primària, la llista completa i conciliada de medicació es comunica al proveïdor següent.
- NPSG.08.03.01: quan el pacient abandona l'hospital, se li proporciona una llista completa i conciliada de la medicació, que s'explica al mateix pacient o a la família.

9.1.4. Cas real: la Comissió de Seguretat del Pacient d'un hospital terciari

En el Registre d'esdeveniments adversos del 2011, es van fer 409 declaracions.

- 2%: adhesius erronis en la història clínica (dins de la història clínica).
- 9%: mescla de documents.
- 4%: falta d'identificació.
- 6%: etiquetatge erroni.

Això fa un total d'un 21% d'incidents relacionats amb seguretat de la informació (integritat).

En l'arxiu d'històries clíniques s'han detectat uns vint mil duplicats, i un equip de set persones treballa per detectar i fusionar les històries clíniques duplicades detectades. No es tracta sols de la seguretat del pacient: aquest tipus d'errors té costos econòmics.

9.1.5. Conseqüències de la manca de confidencialitat per al pacient

Cas de filtració de situació de VIH entre els veïns d'un pacient. El pacient era el propietari d'un petit negoci familiar d'alimentació.

9.1.6. Conseqüències de la manca de confidencialitat per al professional

Troben morta la infermera de Kate Middleton, que va sofrir una broma radiofònica (<http://es.omg.yahoo.com/blogs/informaci%C3%B3n-confidencial/suplantant-isabel-ii-para-conseguir-datos-m%C3%A9dicos-kate-164715618.html>). Exemple clàssic d'atac d'enginyeria social.

Cas Pitiusa: ramificació Sanitària. Jordi, el detectiu i fals doctor. (http://politica.elpais.com/politica/2012/07/14/actualidad/1342302719_566857.html). Nou exemple d'atac d'enginyeria social.

La falta del deure de secret. Règim disciplinari dels serveis regionals de salut.

9.2. De la confidencialitat a la seguretat de la informació.

Dimensions de la seguretat

L'objectiu principal de la seguretat de la informació consisteix a garantir l'activitat de l'organització a la qual presta els seus serveis; en el nostre cas, la prestació dels serveis sanitaris als ciutadans. El compliment legal és un dels ítems que cal considerar, que, sens dubte, és obligatori i ni és negociable ni susceptible de prioritació.

No obstant això, en vista de les dades abans esmentades, sembla clar que la vertadera preocupació d'organitzacions i professionals sanitaris no sols és la protecció de dades en el sentit de privadesa o confidencialitat, ni el compliment legal, sinó la integritat i disponibilitat i la seguretat del pacient.

Hem de començar a canviar el nostre discurs i la manera de veure les coses, i no parlar tant del concepte de *protecció de dades*, que per a nosaltres és insuficient. No n'hi ha prou amb parlar solament de confidencialitat i privadesa: cal anar més enllà.

9.2.1. La disponibilitat

La disponibilitat agrupa les mesures de seguretat dirigides a garantir que la informació estarà disponible en el moment en què es necessiti i per a les persones autoritzades.

Recopilem les dades dels nostres pacients per proporcionar-los una assistència sanitària adequada. Aquesta assistència comporta altres tractaments, tant de tipus administratiu com de caràcter sanitari. Altres professionals hauran d'assignar al pacient cites, ingressos, tractaments i, per descomptat, deixar registre documental en la història clínica, segons exigeix la Llei d'autonomia del pacient.

És molt probable que al pacient no el tracti un sol especialista, sinó que sigui un equip de professionals qui dugui a terme l'assistència. Cada professional que reuneix informació del pacient ha de ser conscient que la aquesta informació haurà d'estar disponible per a la resta de l'equip de professionals que intervenen en el procés. No es tracta solament de l'obligació dels professionals

i les organitzacions, sinó també d'un dret dels pacients que la seva informació estigui disponible per als professionals que la necessitin per fer una assistència sanitària adequada i d'acord amb la realitat del pacient.

La mesura de seguretat més important relacionada amb la disponibilitat és un pla de contingències.

És habitual que els usuaris dels sistemes d'informació es resignin a les parades o fallades informàtiques que resulten en falta de disponibilitat. No obstant això, això no val per als responsables i ens referim a tots, no solament als de TI. La manca de disponibilitat no està justificada ni és assumible per a cap organització actual.

Sempre hi ha d'haver un pla B, ja que tots els sistemes informàtics tard o d'hora sofriran una parada. La funció d'un bon pla de contingències consisteix a minimitzar els efectes de la fallada i oferir, entre altres coses, alternatives perquè la marxa normal del negoci continuï endavant, fins i tot encara que sigui amb un cert nivell de pèrdua en les funcionalitats. El que no resulta admissible és que el metge no disposi de la informació que necessita a la seva consulta quan té el pacient al davant.

9.2.2. Exemple de falta de disponibilitat

La conseqüència més directa de la falta de disponibilitat de la informació és la impossibilitat de prestar els serveis que depenen d'aquesta informació. En el nostre cas, una possible suspensió de la consulta mèdica o una assistència de menys qualitat, la qual cosa obliga el pacient a tornar un altre dia i a omplir l'agenda amb consultes que no s'haurien d'haver produït.

Una altra conseqüència podria ser l'increment de les estades d'hospitalització pel retard en proves diagnòstiques, i fins i tot la necessitat de repetir-les.

A més de les conseqüències per a pacients i professionals, hem de tenir en compte les conseqüències econòmiques de tot això.

9.2.3. La integritat

El principi de qualitat de les dades inclòs en l'RD 1720/2007 estableix el següent:

“Les dades de caràcter personal han de ser exactes i s'han de posar al dia de manera que responguin amb veracitat a la situació actual de la persona afectada. Si les dades fossin incloses directament per la persona afectada, es consideren exactes les que ella mateixa faciliti.”

A la qual cosa la Llei d'autonomia del pacient afegeix el següent:

“Les administracions sanitàries estableixen els mecanismes que garanteixin l'autenticitat del contingut de la història clínica i dels canvis que experimenti, i també la possibilitat de la seva reproducció futura.”

El principi d'integritat de la informació intenta garantir que la informació sigui veraç, impedir-ne la manipulació o alteració per persones no autoritzades i la pèrdua accidental o intencionada de les dades.

Mantenir la integritat de la informació és la tasca més delicada i, potser, la més complicada. Actualment, la informació clínica es construeix pas a pas amb la participació d'un grup variat de professionals, administratius, professionals d'infermeria, metges, documentalistes, etc. Un error en qualsevol dels passos serà arrossegat per tot el procés, amb conseqüències que poden ser fatals.

Habitualment, quan es parla de protegir la integritat de la informació se sol fer referència a protecció contra atacs externs a la informació. No obstant això, els errors comesos pels mateixos professionals des de dins de l'organització constitueixen la causa més freqüent en la falta d'integritat.

Un error en el número de telèfon, el DNI o l'adreça del pacient són exemples d'errors en la integritat de les dades. No obstant això, potser l'error d'integritat més perillós per al pacient, el professional i l'organització el constitueixen els errors d'identificació del pacient.

9.2.4. Exemple de falta d'integritat

Un auxiliar administratiu que dona una cita o assigna els resultats d'una anàlisi a un pacient que es diu igual que el que cerca comença una sèrie d'errors en cadena que poden acabar amb conseqüències fatals per al pacient. Per no parlar dels problemes morals que es plantegen als professionals que han intervingut en el cas, a més dels problemes legals i, per descomptat, el cost d'imatge que un succés d'aquesta classe tindrà per al centre sanitari.

Un error d'aquesta classe pot fer que la vida del pacient no estigui a les mans del metge, sinó a les mans de l'auxiliar administratiu que en va mecanitzar les dades, la qual cosa pot acabar derivant en responsabilitats professionals.

En una entrevista a un comandant de les forces aèries nord-americanes, a qui van preguntar en què pensava quan va haver de saltar de l'avió en ser derrocat per l'enemic, va respondre: “resava perquè la persona que havia doblegat el paracaigudes hagués fet bé la seva feina”.

En la cadena de procés, tothom és importants i els uns depenen dels altres.

Dimiteix el director de l'Hospital Reina Sofía, on una dona va ser esterilitzada per error (<http://www.elmundo.es/elmundo/1998/agosto/17/sociedad/dimision.html>).

9.3. Eines per a la seguretat de la informació

Trobem la creença que la seguretat de la informació constitueix més una molèstia per al treball dels professionals que una cosa realment útil per al pacient o per als professionals. Se sol parlar de *compliment impossible* de la llei. Potser hàgim tingut l'oportunitat d'escoltar afirmacions com ara "si haguéssim de complir les lleis, caldria tancar l'hospital" per part d'algun directiu, o "si hagués de complir la llei, no treballaria" per part de més d'un professional.

Aquests professionals semblen pensar en la "seva" feina i en la "seva" manera de fer les coses, però és clar que no estan considerant per a res l'objecte fonamental de la feina que duen a terme i la raó de ser de tota organització sanitària: el pacient.

En primer lloc, i permeteu-nos l'analogia, "el codi de circulació no és opcional". Tothom coneix les possibles conseqüències quan algú no respecta el codi de circulació.

Per tant, el compliment legal respecte a la seguretat de la informació és una obligació de tots els centres, és responsabilitat de la direcció impulsar-lo i obligació dels professionals fer-lo una realitat. No és una cosa ni opcional ni negociable.

Dit això, volem afegir que el que estableixen les lleis aplicables és pur sentit comú. La informació és confidencial. Potser és possible un altre supòsit? La informació ha de ser exacta i actualitzada. Resulta admissible qualsevol altra opció? La informació ha d'estar disponible on es necessita, quan es necessita i per al professional que la necessita, de manera que es pugui atendre el pacient com és degut. Pot ser d'una altra manera?

Els professionals sanitaris són els més interessats que es compleixi la llei, almenys els qui es preocupen pels pacients. Són els professionals sanitaris els qui haurien de ser més exigents amb el compliment legal, com una garantia per a la seguretat del pacient, en primer lloc, i com una manera de garantia jurídica per al professional, en segon lloc.

Per a garantir la bona salut d'aquests tres pilars fonamentals, es tendeix a pensar en termes tecnològics i econòmics. Còpies de seguretat, tallafocs, contrasenyes, antivirus, servidors segurs, etc. No obstant això, tot això solament serà la materialització final resultat d'altres eines molt més importants.

9.3.1. Alineació

Totes les activitats dutes a terme en una organització, sense excepció, han de tenir com a objectiu aconseguir les metes proposades per aquesta organització. Han de ser metes marcades per les seves polítiques i pels seus objectius. No en són una excepció les tecnologies de la informació, la funció de les quals és,

no ho oblidem, contribuir a la consecució dels objectius marcats. Tampoc no n'és una excepció la funció de seguretat de la informació, amb la missió de garantir el funcionament de totes les activitats que depenen de la informació de la qual s'alimenten.

Serveis, tecnologies de la informació i seguretat de la informació han d'estar permanentment alineats, coherents entre ells i amb l'organització quant a les activitats que efectuen. Qualsevol de les activitats dutes a terme s'ha de poder rastrejar d'una manera directa fins a algun dels objectius marcats per l'organització.

Això, que sembla tan obvi, pot ser un problema greu. Alguns actors duen a terme activitats que no es corresponen amb els objectius. El resultat és que tecnologies de la informació poden estar donant suport a activitats que no són importants per a l'organització, o que seguretat de la informació intenti protegir actius d'informació que no aporten res.

9.3.2. Polítiques

Es tracta de la definició de les polítiques, de les normes i dels procediments corporatius que formen part del document de seguretat de la informació adaptat a cada centre. Les polítiques deriven dels objectius i els procediments de les polítiques, de manera que tots estiguin perfectament alineats.

9.3.3. Conscienciació

No tots els riscos inherents a la informació es resolen mitjançant la tecnologia. Un programa de conscienciació sobre seguretat de la informació pot reduir en gran manera els riscos de seguretat, en actuar incidint sobre la conducta dels professionals.

Plans de conscienciació continus destinats a tots els col·lectius professionals poden ser molt més efectius que qualsevol mesura de tipus tecnològic.

9.3.4. Formació (específica i dirigida)

Parlem de formació específica i dirigida a col·lectius concrets: professionals d'arxius d'històries clíniques, dels serveis d'atenció a la ciutadania, dels serveis d'admissió, investigadors, etc., de manera que s'estableixin procediments d'actuació similars d'una manera transversal en tota l'organització i es difonguin per igual les polítiques, les normes i els procediments corporatius a tots els col·lectius professionals.

9.3.5. Infraestructura organitzativa

Nomenaments

Per tenir un referent adequat que actuï com a assessor en l'organització, és necessària la figura del responsable de seguretat de la informació, figura, a més, obligatòria segons la Llei orgànica de protecció de dades.

No obstant això, no és suficient amb un nomenament formal. Per afegir un valor real a l'organització, el responsable de seguretat de la informació s'ha de dedicar a temps complet a aquesta funció i ser independent dels serveis de tecnologies de la informació que en limiten les funcions i un treball objectiu independent. El responsable de seguretat ha d'informar i assessorar la direcció, de manera directa o per mitjà d'una comissió de seguretat de la informació.

Tal com exigeixen tots els estàndards internacionals, i des del gener del 2010, l'Esquema Nacional de Seguretat, s'ha de mantenir el principi de separació de rols, de manera que les diferents figures que intervenen en el tractament i la seguretat de la informació es mantinguin independents.

Comissió de Seguretat de la Informació

La missió inicial de la Comissió de Seguretat de la Informació (CSI) consisteix a impulsar la seguretat del centre. No obstant això, les seves funcions van molt més enllà.

- Donar suport als plans de seguretat nascuts de les successives auditories i impulsar-los.
- Assessorar la direcció gerencial del centre pel que fa a seguretat de la informació.
- Garantir l'alineació dels objectius de seguretat de la informació amb els objectius de l'organització (seguretat del pacient).
- Coordinar-se amb altres comissions relacionades, Comissió de Seguretat del Pacient i Comissió d'Històries Clíiques.

Comissió de Seguretat del Pacient

La participació del responsable de seguretat de la informació en la Comissió de Seguretat del Pacient mira de garantir l'alineació dels objectius de seguretat de la informació amb els objectius de seguretat del pacient i, per extensió, de l'organització, actualment una de les preocupacions dels centres sanitaris. No hem d'oblidar que la nostra raó de ser són els pacients i, per tant, qualsevol ac-

tivitat en matèria de seguretat de la informació ha d'estar directament relacionada amb la salut, per a la qual cosa es basarà, per descomptat, ens els seus pilars fonamentals: confidencialitat, integritat i disponibilitat de la informació.

9.3.6. Supervisió (auditories)

Res de l'anterior serà realment útil sense una supervisió periòdica. La llei estableix l'obligació de dur a terme auditories de seguretat de la informació cada dos anys. És el responsable de seguretat de la informació el responsable d'analitzar els resultats de les auditories i proposar els plans de seguretat resultants a la Comissió de Seguretat de la Informació que, al seu torn, els ha de comunicar a la direcció del centre.

Una auditoria comprèn almenys els aspectes següents.

Auditoria de compliment dels principis fonamentals inclosos en la Llei orgànica de protecció de dades de caràcter personal

- Identificació d'actius d'informació.
- Registre de fitxers.
- Informació i consentiment.
- Principis de protecció de dades (finalitat dels fitxers i deure de secret).
- Drets ARCO.

Auditoria de compliment de les mesures de seguretat establertes en el Reial decret 1720/2007 que regula la LOPD

- Encarregats del tractament (empreses externes).
- Prestació de serveis sense accés a dades.
- Delegació d'autoritzacions.
- Treball fora dels locals de l'empresa.
- Creació i gestió de fitxers temporals o còpies de documents.
- Funcions i obligacions del personal.
- Control d'accessos.
- Gestió de suports i documents.
- Identificació i autenticació.
- Còpies de seguretat i recuperació.
- Registre d'accessos.
- Accés a dades per mitjà de xarxes de telecomunicacions.
- Criteris d'arxivament.
- Emmagatzematge de la informació.
- Custòdia de suports.
- Revisió del document de seguretat.
- Registre d'incidències.
- Auditories periòdiques.

9.3.7. Programes de seguretat de la informació

Un programa de seguretat de la informació comprèn totes les activitats i els recursos que proporcionen serveis de seguretat de la informació a una organització. El programa de seguretat de la informació deriva d'una auditoria prèvia i estableix les estratègies per corregir les deficiències detectades durant l'auditoria.

En un programa de seguretat de la informació, s'han d'abordar actuacions relatives al següent:

- Circuit d'atenció a l'exercici de drets ARCO.
- Pla de conscienciació sobre la LOPD.
- Circuit per al consentiment per al tractament de dades de caràcter personal.
- Gestió d'accessos.
- Còpies de seguretat i recuperació.
- Tractament de documentació. Suport paper.
- Accés a la informació per tercers (empreses externes).
- Entrada i sortida d'informació. Gestió d'autoritzacions.
- Gestió d'incidències de seguretat.
- Gestió de suports amb dades de caràcter personal (**no paper**).
- Registre d'accessos.
- Adequació del CPD. Mesures físiques.
- Adequació del document de seguretat.

Tot i que encara ens queden assumptes pendents per millorar respecte al primer pla de seguretat, ja hem engegat el segon programa de seguretat de la informació 2012-2014.

9.3.8. Gestió de riscos

La seguretat de la informació, com a disciplina, existeix per a gestionar el risc relacionat amb la confidencialitat, la integritat i la disponibilitat. Proporciona nivells acceptables d'assegurament per a les activitats de l'organització. Sense la determinació i l'anàlisi dels riscos per a les activitats de l'organització, no és possible determinar el cost o l'impacte d'un esdeveniment advers i, per tant, no serà possible establir les mesures de seguretat apropiades.

L'eficàcia de la gestió de riscos dependrà del grau en què formi part de la cultura de l'organització i que cadascú assumeixi la seva responsabilitat.

Una gestió de riscos efectiva serveix per a reduir la incidència d'esdeveniments adversos significatius en tractar les amenaces, mitigar l'exposició i/o reduir la vulnerabilitat o l'impacte. En la mesura que això es compleix, la gestió de riscos proporciona un nivell de predicció que confirma la capacitat de l'organització per a operar d'una manera efectiva.

9.4. Confidencialitat a la Xarxa

L'encontre virtual professional entre sanitari i pacient ja és inqüestionable: cada dia, més pacients estan capacitats per a utilitzar còmodament les possibilitats que ofereixen les noves tecnologies. Constantment, ens arriben notícies sobre projectes i iniciatives en aquest sentit. Hello Health és un projecte per a la teleassistència nord-americà, en el qual metges ofereixen assistència en línia als pacients i aquests poden consultar els seus historials clínics o els resultats de les seves analítiques, per exemple. La iniciativa Icor és un projecte espanyol dut a terme d'una manera conjunta entre Telefónica i el Parc de Salut del Mar de Barcelona que ofereix el control a distància de pacients amb insuficiència cardíaca, la qual cosa redueix la mortalitat un 34% i els ingressos hospitalaris un 43%, o el projecte Rehabitic, en aquest mateix hospital, orientat a la rehabilitació dels pacients amb pròtesis de genoll. Medibaby és un sistema que, gràcies a la telemedicina, connecta la família o el centre escolar amb les urgències pediàtriques, la qual cosa permet a l'especialista establir una preavaluació a l'infant i que es prenguin les primeres decisions. Ja està funcionant en alguns centres escolars de la Comunitat de Madrid.

Una altra tendència en auge és l'*mHealth*, dirigida als usuaris mòbils i 2.0, com GoMeals de Sanofi, per a pacients diabètics i que permet un seguiment de les seves dietes (*Mobile Health Around the Globe: Healthcare Technology in the 21st Century*).

D'altra banda, la presència d'organitzacions sanitàries i hospitals a les xarxes socials s'està incrementant. Un 26% d'hospitals nord-americans té presència en Facebook i Twitter. Per descomptat, això també succeeix amb els professionals, amb una presència en fort creixement i ja molt consolidada.

Trobem també plataformes per a professionals que constitueixen punts de trobada per als especialistes (Esanum) i plataformes destinades als pacients (forumclinic), i també portals de les associacions de pacients (sospacientes).

Tot això, juntament amb una innovació constant en noves tecnologies, fa que el procés sigui imparabile. Els dispositius mèdics comencen a connectar amb els mòbils personals per recopilar informació i enviar-la als centres sanitaris per al seu seguiment, i es creen protocols específics per a això: *bluetooth health device profile* (HDP). Al mateix temps, les administracions públiques, incloses les sanitàries, comencen a traslladar els seus sistemes al núvol, la qual cosa facilitarà l'accés dels ciutadans.

Són clars els beneficis per a pacients i professionals. No obstant això, cal anar amb compte, ja que la informació que circula per la Xarxa és difícil de controlar i de protegir.

- TS desestima recurs del Govern contra una sanció a SCS després de publicar-se en Internet dades de pacients. <http://www.20minutos.es/noticia/1678633/0/>
- 4.000 històries clíniques d'avortaments es filtren a la Xarxa mitjançant eMule. http://elpais.com/diario/2008/04/25/sociedad/1209074403_850215.html
- El 94% dels hospitals pateix violacions de dades.

Una de les activitats que genera més dubtes en els professionals és la comunicació via correu electrònic amb els pacients. Podem utilitzar el correu electrònic per enviar informació de salut als pacients, resoldre dubtes, etc.?

És important que sapiguem una cosa sobre la Llei FISA 2012, o Llei de vigilància d'intel·ligència estrangera. En essència, a instàncies d'una ordre secreta del Govern dels Estats Units, les empreses nord-americanes que operen a la UE estan obligades a lliurar les dades dels ciutadans europeus. Text complet en: <http://actualidad.rt.com/actualidad/view/83293-tocar-controlando-nube-ley-eeuu-amenaza-gravemente-soberania-ue>

És a dir, quan enviem un informe clínic a Hotmail o Gmail, enviem també la informació de salut a les autoritats nord-americanes.

Davant aquest atropellament a l'estil Gran Germà, ja estan sorgint iniciatives que poden complicar una mica la intrusió en les nostres vides privades ("Mega: benvinguts a la Internet xifrada i distribuïda"). És molt possible que el futur vagi en aquesta direcció, perquè els ciutadans puguem "tenir vida privada".

Aquí trobareu una referència interessant sobre l'ús de dispositius mòbils: : *Guía de buenas prácticas en el uso corporativo de dispositivos móviles*, del CSIRT (Centre de Seguretat TIC de la Comunitat Valenciana).

Webs recomanats

La revolució digital del sector sanitari

<http://www.elconfidencial.com/tecnologia/blogs/directivo-digital/2013/01/14/la-revolucion-digital-del-sector-sanitario-4001/>

Els pacients al comandament de la seva pròpia salut: el futur digital de l'atenció sanitària

<http://www.hospitaldigital.com/2013/01/08/los-pacientes-al-mando-de-su-propia-salud-el-futuro-digital-de-la-atencion-sanitaria/>

9.5. Conclusions

Cal passar de parlar de protecció de dades al concepte més ampli de *seguretat de la informació* en el marc dels objectius de seguretat marcats per la seguretat del pacient, tenint molt en compte que qualsevol objectiu de seguretat de la informació s'ha de poder rastrejar d'una manera directa fins als objectius de l'organització.

En la mesura que siguem capaços d'alinejar les activitats de seguretat de la informació amb les de seguretat del pacient, serà més fàcil per a les organitzacions i els directius entendre la importància dels plans de seguretat de la informació; les conseqüències clíniques de descuidar la integritat, disponibilitat i confidencialitat de la informació, i el paper que tenen les lleis sobre protecció de dades i seguretat de la informació en la defensa de la prestació dels serveis sanitaris i de la salut dels ciutadans.

Bibliografia

Basagoiti, I. (coord.) (2012). *Alfabetización en salud. De la información a la acción* [en línia]. <<http://www.salupedia.org>>

Brox, E.; Fernández-Luque, L.; Tøllefsen, T. (2011). "Healthy Gaming – Video Game Design to promote Health". *Applied Clinical Informatics* (núm. 2, vol. 2, pàg. 128-142).

Buchanan, B. G.; Shortliffe, E. H. (1984). *Rule Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project*. Reading, MA: Addison-Wesley. ISBN 978-0-201-10172-0.

Chomutare, T.; Fernández-Luque, L.; Årsand, E.; Hartvigsen, G. (2011). "Features of Mobile Diabetes Applications: Review of the Literature and Analysis of Current Applications Compared Against Evidence-Based Guidelines" [article en línia]. *J. Med. Internet Res.* (núm. 3, vol. 3). <<http://www.jmir.org/2011/3/e65/>>

Christakis, N. A.; Fowler, J. H. (2012). *El sorprendente poder de las redes sociales y cómo afectan nuestras vidas*. Taurus («Taurus Pensamiento»). ISBN 9788430606887.

Coiera, E.; Aarts, J.; Kulikowski, C. (2012). "The dangerous decade". *Journal of the American Medical Informatics Association* (núm. 19).

CSO (2014). *Las diez principales amenazas del networking social* [en línia]. <<http://www.csospain.es/>>

DeShazo, J.; Harris, L.; Pratt, W. (2010). "Effective intervention or child's play? A review of video games for diabetes education". *Diabetes Technol. Ther.* (núm. 12, vol. 10, pàg. 815-822).

DICOM (2012). *Digital Imaging and Communications in Medicine* [en línia]. National Electrical Manufacturers Association. [Data de consulta: 5 de novembre de 2012]. <<http://medical.nema.org/>>

Donelle, L.; Booth, R. G. (2012). "Health tweets: an exploration of health promotion on twitter". *Online J. Issues Nurs.* (núm. 17, vol. 3, pàg. 4).

Dubose, C. (2011). "The social media revolution". *Radiol Technol.* (núm. 83, pàg. 112-119).

Dybowski, R. (1996). "Prediction of outcome in critically ill patients using artificial neural network synthesised by genetic algorithm". *Lancet* (núm. 347, pàg. 1146-1150).

Esquivel, A.; Meric-Bernstam, F.; Bernstam, E. V. (2006). "Accuracy and self correction of information received from an internet breast cancer list: content analysis". *BMJ* (núm. 332, vol. 7547, pàg. 939-942).

Eysenbach, G. (2001). "What is e-health?" [article en línia]. *J. Med. Internet Res.* (núm. 3, vol. 2). <<http://www.jmir.org/2001/2/e20/>>

Ferguson, T. i altres (2007). *Libro Blanco de los ePacientes* [en línia]. Sociedad de la Medicina Participativa. <<http://e-pacientes.net/u/2011/11/Libro-blanco-de-los-e-Pacientes.pdf>>

Gabarron, E.; Fernández-Luque, L. (2012). "eSalud y vídeos online para la promoción de la salud". *Gaceta Sanitaria* (núm. 26, vol. 3, pàg. 197-200).

Gartner Newsroom (2011). "Press releases: Gartner Says By 2015, More Than 50 Percent of Organizations That Manage Innovation Processes Will Gamify Those Processes" [en línia]. Egham, Regne Unit: Gartner, Inc. [Data de consulta: 6 de novembre de 2012]. <<http://www.gartner.com/it/page.jsp?id=1629214>>

Grupo de Interoperabilidad del Living Lab Salud Andalucía (2009). *Interoperabilidad: qué es y por qué debemos llegar a ella* [en línia]. Sevilla: Consejería de Innovación, Ciencia y Empresa y Consejería de Salud. <<http://livinglabsalud.es/inicio/files/2009/07/documento-interoperabilidad-v10.pdf>>

Grupo de trabajo sobre protección de datos del artículo 19 (2009). *Dictamen 5/2009 sobre las redes sociales en línea* [en línia]. <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf>

Handels, H. i altres (1999). "Feature selection for optimized skin tumor recognition using genetic algorithms". *Artif. Intell. Med.* (núm. 16, vol. 3, pàg. 283-297).

Hans, O. i altres (2005). "What Is eHealth: A Systematic Review of Published Definitions" [article en línia]. *J. Med. Internet Res.* (núm. 7, vol. 1). <<http://www.jmir.org/2005/1/e1/>>

Heilman, J. M.; Kemmann, E.; Bonert, M. i altres (2011). "Wikipedia: a key tool for global public health promotion". *J. Med. Internet Res.* (núm. 13, vol. 1).

Hernández, E.; Gómez-Zúniga, B. (coord.) (2007). "Intervención en salud en la Red" [en línia]. UOC Papers (núm. 4). UOC. <<http://www.uoc.edu/uocpapers/4/dt/esp/monografico.pdf>>. ISSN 1885-1541.

Holland, J. (1992). *Adaption in Natural and Artificial Systems*. MIT Press.

INTECO (2010). *Seguridad, Observatorio, Guías* [en línia]. <http://www.inteco.es/Seguridad/Observatorio/guias/guia_ayuda_redes_sociales>

ISACA (2011). *Volume 1. Chain Exploitation. Social Networks Malware* [en línia]. <<http://www.isaca.org/Journal/Past-Issues/2011/Volume-1/Documents/jpdf11v1-chain-exploitation.pdf>>

ISACA (2012). "What Every IT Auditor Should Know About Auditing Social Media" [article en línia]. *Isaca Journal* (vol. 5). <<http://www.isaca.org/Journal/Past-Issues/2012/Volume-5/Documents/12v5-What-Every-IT-Auditor.pdf>>

Kummervold, P. E.; Chronaki, C. E.; Lausen, B.; Prokosch, H. U.; Rasmussen, J.; Santana, S. i altres (2008). "eHealth trends in Europe 2005-2007: a population-based survey" [article en línia]. *J. Med. Internet Res.* (núm. 10, vol. 4). <<http://www.jmir.org/2008/4/e42/>>

Lands, N.; Bédard, J. R. (2012). *Gamification wiki* [en línia]. Gamify, Inc. [Data de consulta: 6 de novembre de 2012]. <<http://gamification.org/>>

Lau, A. Y. S.; Siek, K. A.; Fernández-Luque, L. i altres (2011). "The Role of Social Media for Patients and Consumer Health". *IMIA Yearbook 2011* (pàg. 131-138).

Lau, A.; Gabarron, E.; Fernández-Luque, L.; Armayones, M. (2012). "Social Media in health. What are the safety concerns for healthcare consumers?". *Health Information Management Journal* (núm. 41, vol. 2, pàg. 30-35).

Mike 2.0 (2012). *Big Data Definition* [en línia]. [Data de consulta: 6 de novembre de 2012]. <http://mike2.openmethodology.org/wiki/Big_Data_Definition>

Neter, E.; Brainin, E. (2012). "eHealth literacy: extending the digital divide to the realm of health information". *J. Med. Internet Res.* (núm. 14, vol. 1).

Norman, C. D. (2011). "eHealth literacy 2.0: problems and opportunities with an evolving concept". *J. Med. Internet Res.* (núm. 13, vol. 4).

Norman, C. D.; Skinner, H. A. (2006). "eHealth Literacy: Essential Skills for Consumer Health in a Networked World". *J. Med. Internet Res.* (núm. 8, vol. 9).

Norman, C. D.; Skinner, H. A. (2006). "eHEALS: The eHealth Literacy Scale". *J. Med. Internet Res.* (núm. 14, vol. 8).

Observatori Nacional de les Telecomunicacions i de la Societat de la Informació (2012). *Los ciudadanos ante la e-Sanidad* [en línia]. Ministeri d'Indústria, Energia i Turisme. <http://www.ontsi.red.es/ontsi/sites/default/files/informe_ciudadanos_esanidad.pdf>

PatientView (2012). *European Directory of Health Apps 2012* [en línia]. <http://www.patient-view.com/uploads/6/5/7/9/6579846/pv_appdirectory_final_web_300812.pdf>

Pereyra, T. (2012). "Las Administraciones públicas en las redes sociales" [article en línia]. *Datospersonales.org. La revista de la Agencia de Protección de Datos de la Comunidad de Madrid* (núm. 58). <<http://www.datospersonales.org/> septiembre 2012>

Protiviti (2011). *Managing Privacy Risks in Social Media-driven Society* [en línia]. <<http://www.protiviti.com>>

Ramos, V.; García, J.; Moreno, O.; Pozo, A. del; Carranza, N.; Blanco, P. (2009). *Investigación en tecnologías de inteligencia ambiental para la salud del futuro*. Instituto de Salud Carlos III.

Sosa Sierra, M. C. (2006). *Introducción a las técnicas de inteligencia artificial aplicadas a la gestión financiera empresarial* [en línia]. Màlaga: EUMEDNET. <<http://www.eumed.net/ce/2006/mcss.htm>>

Szaleniec, M. (2012). "Prediction of enzyme activity with neural network models based on electronic and geometrical features of substrates". *Pharmacol. Rep.* (núm. 64, vol. 4, pàg. 761-781).

Torre-Díez, I. de la; Díaz-Pernas, F. J.; Antón-Rodríguez, M. A (2012). "Content analysis of chronic diseases social groups on facebook and twitter". *Telemed. J. E. Health* (núm. 18, vol. 6, pàg. 404-408).

Traver, V.; Fernández Luque, L. (coord.) (2011). *El ePaciente y las Redes Sociales* [en línia]. Fundació Vodafone. <<http://www.salud20.es>>. ISBN 9788469441107.

Vance, K.; Howe, W.; Dellavalle, R. P. (2009). "Social internet sites as a source of public health information". *Dermatol. Clin.* (núm. 27, pàg. 133-136).

Vital Wave Consulting (2009). *mHealth for Development* [en línia]. Fundació de les Nacions Unides i Fundació Vodafone. <<http://www.unfoundation.org/>>

Documents web

5 consejos para mejorar nuestra privacidad en redes sociales. <http://www.taringa.net/posts/info/15371094/5-consejos-para-mejorar-nuestra-privacidad-en-redes-sociales.html>

5 maneras en que Facebook engaña a usuarios. <http://america.infobae.com/notas/57008-5-maneras-en-que-facebook-engana-a-usuarios>

7 de cada 10 CIO han bloqueado el acceso a Facebook este 2012. <http://blog.seguinfo.com.ar/2012/08/7-de-cada-10-cios-han-bloqueado-el.html?axzz27VIFilxr>

Al publicar fotos de las vacaciones en las redes sociales, ¿conoces tus derechos? http://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Post_veranoseguro_fotos

¿Cómo puedes proteger tu seguridad y privacidad en Facebook? https://www.osi.es/es/actualidad/blog/2012/06/26/%C2%BFcomo-puedes-proteger-tu-seguridad-y-privacidad-en-facebook?origen=rs_twitter

Cómo proteger tus fotos en Facebook para que no sean descargadas ni compartidas. http://www.socialblabla.com/como-proteger-tus-fotos-en-facebook-para-que-no-sean-descargadas-in-compartidas.html?utm_source=twitterfeed&utm_medium=twitter

Consejos para mantener mi privacidad en Facebook. <http://www.hijosdigitales.es/2012/07/consejos-para-mantener-mi-privacidad-en-facebook/>

Difuminado de caras: cuando la imagen requiere del anonimato. <http://googleespana.blogspot.com.es/2012/07/difuminado-de-caras-cuando-la-imagen.html>

El 63% de las apps de Facebook publican contenidos en nombre de los usuarios. <http://www.europapress.es/portaltic/socialmedia/noticia-63-apps-facebook-publican-contenidos-nombre-usuarios-20120905153041.html>

¿Es responsable un webmaster de los comentarios que se vierten en su web? <http://www.elconfidencial.com/tecnologia/2012/08/13/es-responsable-un-webmaster-de-los-comentarios-que-se-vierten-en-su-web-2950/>

Etiquetas en las imágenes de las redes sociales, un riesgo para la privacidad y la convivencia. http://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Post_veranoseguro_etiquetas

Facebook meterá publicidad en el muro de sus usuarios sin su consentimiento. <http://www.globbtv.com/2440/noticias/facebook-metera-publicidad-en-el-muro-de-sus-usuarios-sin-su-consentimiento>

Guía de introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas. <http://creativecommons.org/licenses/by-nc/2.5/es/>

Health Level Seven International. <http://www.hl7.org/>

No sé lo que quiero pero lo quiero ya. <http://www.solis.com.ve/no-se-lo-que-quiero-pero-lo-quiero-ya/>

¿Puedo colgar las fotografías de las vacaciones con mis amigos en redes sociales? <http://www.legaltoday.com/gestion-del-despacho/nuevas-tecnologias/articulos/puedo-colgar-las-fotografias-de-las-vacaciones-con-mis-amigos-en-redes-sociales>

Ministeri de Ciència i Innovació. <http://gesdoc.isciii.es/gesdoccontroller?action=download&id=14/09/2012-4e59449d32>

Recomendaciones para proteger su privacidad. <http://blog.segu-info.com.ar/2012/08/10-recomendaciones-para-proteger-su.html#axzz26q1XvIMk>

Snomed Clinical Terms. http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html

Social Networks and Privacy. Threats and Protection. <http://www.isaca.org/Journal/Past-Issues/2012/Volume-5/Pages/Social-Networks-and-Privacy-Threats-and-Protection.aspx>.