AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

Informe de tendències de ciberseguretat

2020

El sector sanitari en temps de pandèmia

El contingut d'aquest informe és titularitat de l'Agència de Ciberseguretat de Catalunya i resta subjecte a la llicència de Creative Commons BY-NC-ND.

L'autoria de l'obra es reconeixerà a través de la inclusió de la menció següent:

Obra titularitat de l'Agència de Ciberseguretat de Catalunya.
Llicenciada sota la llicència CC BY-NC-ND.
Aquest informe es publica sense cap garantia específica sobre el contingut.

Aquesta llicència té les particularitats següents:

Vostè és lliure de:

Copiar, distribuir i comunicar públicament l'obra.

Sota les condicions següents:

Reconeixement: S'ha de reconèixer l'autoria de l'obra de la manera especificada per l'autor o el llicenciador (en tot cas, no de manera que suggereixi que gaudeix del suport o que dona suport a la seva obra).

No comercial: No es pot emprar aquesta obra per a finalitats comercials o promocionals.

Sense obres derivades: No es pot alterar, transformar o generar una obra derivada a partir d'aquesta obra.

***Avís:** En reutilitzar o distribuir l'obra, cal que s'esmentin clarament els termes de la llicència d'aquesta obra.*

El text complet de la llicència es pot consultar a https://creativecommons.org/licenses/by-nc-nd/4.0/deed.ca

L'informe inclou recursos gràfics, com imatges i icones, subministrades des de plataformes de continguts gratuïts de lliure difusió. Menció específica a: https://www.iconfinder.com, https://pixabay.com.

Índex

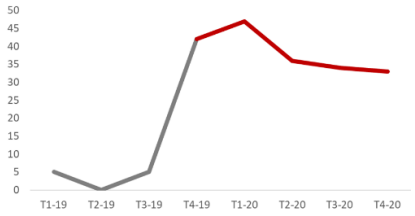
Aquest document és fruit del seguiment i de l'anàlisi de les tendències en relació amb les amenaces de ciberseguretat detectades durant l'any 2020 per part de l'Agència de Ciberseguretat de Catalunya.

Per a la realització d'aquest informe s'han tingut en compte l'activitat i la documentació pròpies generades per l'Agència de Ciberseguretat de Catalunya, així com diversos informes de referència i fonts qualificades d'entitats, fabricants, organismes i professionals del món de la ciberseguretat, tant de l'àmbit nacional com internacional.

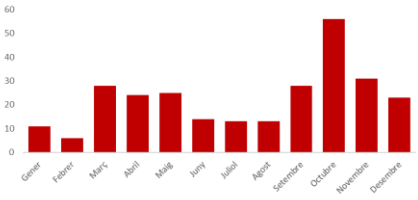
Resum

El sistema sanitari es digitalitza per combatre la pandèmia. Arran de la irrupció de la covid-19, el sistema sanitari català ha ampliat ràpidament instal·lacions, ha incorporat nous professionals, ha desplegat sistemes d'assistència a distància i plataformes de compartició de dades mèdiques... **La pandèmia ha impulsat la transformació digital del sector sanitari**, però aquest fet comporta nous **reptes en matèria de ciberseguretat i privacitat**. El **sector sanitari ha de fer front a ciberamenaces** creixents, de les quals destaquen el *phishing*, els atacs de *ransomware*, les fuites de dades i les vulnerabilitats de l'e-salut.

Els atacs de *phishing* exploten la pressió assistencial sobre el sector sanitari durant la pandèmia. El *phishing* és el principal mètode d'atac contra el sector sanitari i ha explotat la pressió assistencial **durant la pandèmia** i la manca de **conscienciació** en ciberseguretat dels professionals. El 2020, el **atacs de *phishing* contra el sector sanitari català** van experimentar un **increment del 198%** respecte del 2019. Amb l'*spear-phishing*, més elaborat i dirigit, la probabilitat d'èxit s'incrementa un 75%. L'objectiu habitual és el robatori de credencials, però també la infecció amb *malware* i els fraus de tipus BEC.



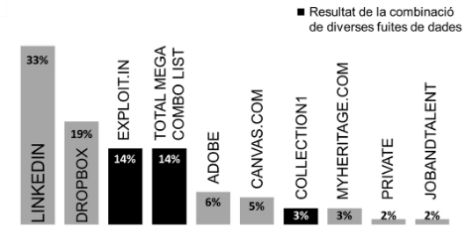
Incidents de phishing *detectats dirigits al sector sanitari públic de Catalunya*



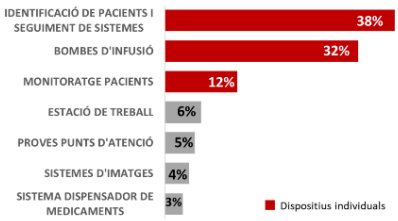
Incidents de ransomware *al sector sanitari identificats als mitjans*

El *ransomware* es dirigeix al sector sanitari perquè és especialment essencial durant la pandèmia. El 2020, el sector sanitari ha estat el principal objectiu del *ransomware* i **receptor del 17,9% d'aquests atacs**. Durant la **primera i segona onada** de la pandèmia, aproximadament **1 de cada 4 incidents** de *ransomware* publicats als mitjans especialitzats afectaven el sector sanitari. Els atacs incorporen la tècnica de la **doble extorsió**: al *ransomware* convencional s'hi afegeix el robatori d'informació sensible i l'amenaça de difondre-la públicament. El **70% dels atacs** es realitzen **a través de connexions RDP o VPN**, desplegades a bastament durant la pandèmia per poder teletreballar, i el **26% a través de correus de *phishing***. Amb la pressió sanitària provocada per la pandèmia, s'ha constatat que un incident en un hospital **pot posar vides humanes en risc**.

Les fuites de dades personals i de recerca del sector sanitari tenen l'origen en ciberatacs, motivats per l'alt valor d'aquestes, i errors causats pel factor humà. Les **dades personals de salut** són fàcilment **monetizables** al mercat negre, i les **dades de recerca sobre la covid-19** han esdevingut especialment **valuoses** per al ciberespionatge. Per això, el **67%** de les fuites està causat per **ciberatacs**, mentre que el **22%** es deu a **negligències o accions malintencionades**. L'**impacte econòmic** d'una fuita de dades personals és **més elevat en el sector sanitari** que en qualsevol altre sector i pot comportar importants **sancions**. En una **anàlisi de 201 fuites de dades**, es van identificar 12.581 comptes de correu electrònic de professionals del sector sanitari de Catalunya i el **58% de les entitats** havien estat afectades.



Origen de les credencials filtrades de comptes de correu electrònic del sector sanitari públic de Catalunya



Dispositius d'eSalut connectats més habituals

Les tecnologies d'e-salut proliferen i la ciberseguretat en el sector sanitari esdevé indispensable per garantir la salut dels pacients. La pandèmia ha impulsat les tecnologies d'e-salut, entre les quals s'hi troben l'IoHT i l'm-salut. L'**IoHT** destinat al **tractament individualitzat dels pacients** conforma el **82% de l'e-salut** i seguirà augmentant. Habitualment, les vulnerabilitats d'aquestes tecnologies tenen l'origen en la **manca d'actualitzacions**: mantenir actualitzat un parc de programaris tan divers i dispositius de diversos anys de vida esdevé molt complex. Les **conseqüències** d'una vulnerabilitat poden afectar les **dades de pacients**, la **qualitat d'un tractament** o ser l'**origen d'un ciberatac**. La **UE** ha establert un **paquet regulador** per als dispositius tecnològics sanitaris.

El sistema sanitari es digitalitza per combatre la pandèmia

Amb la irrupció de la covid-19, el sistema sanitari català ha ampliat instal·lacions i plantilles, ha promogut la teleassistència i la compartició de dades. L'aplicació d'aquestes tecnologies ha esdevingut un repte en matèria de ciberseguretat i privacitat. Així les coses, el sector sanitari ha hagut de fer front a la ciberamenaça del *phishing*, els atacs de *ransomware*, les fuites de dades i les vulnerabilitats de les tecnologies d'e-salut.

El desplegament accelerat de nous espais i la incorporació de professionals novells han permès entomar la crisi sanitària, però han incrementat el els actius i professionals a protegir a nivell cibernètic.

La pandèmia de la covid-19 ha impactat la societat a tots els nivells i ha suposat una autèntica prova per al sistema sanitari. De forma sobtada, els centres hospitalaris s'han vist desbordats per una **allau de pacients que ha portat al límit les seves capacitats assistencials**. En la primera onada, l'abril de 2020, es va arribar a la xifra de 1.528 pacients ingressats a les Unitats de Cures Intensives (UCI). Hem de recordar que, inicialment, Catalunya només disposava d'unes 600 places[1,2]. Davant d'aquest nombre de malalts sense precedents, es va constatar l'**escassedat de professionals i de llits**[3].

A arreu del món el sistema sanitari estava desbordat. A Catalunya, es va procedir a **adaptar nous espais** en hospitals, hotels i pavellons esportius per ubicar més llits i atendre els infectats de la covid-19[4,5]. En poques setmanes, es van **desplegar l'equipament i les instal·lacions** imprescindibles per tenir cura dels pacients i disposar de connectivitat als diferents espais. Però, des del punt de vista de la ciberseguretat, **irrompia sobtadament una nova infraestructura tecnològica que calia protegir**.

Pel que fa a la manca de professionals, es va procedir a **incorporar estudiants d'especialitats mèdiques** que feien el darrer curs, així com **professionals jubilats** amb menys de 71 anys i sense patologies de risc[6]. Si bé aquests professionals han estat d'altíssim valor per fer front a la crisi sanitària, la incorporació accelerada de nou personal comporta el **risc de fer-se sense la formació adequada en ciberseguretat**. Aquest fet pot suposar l'**incompliment** de bones pràctiques amb relació al **tractament de les dades personals dels pacients**.

[1] *https://dadescovid.cat/setmanal*
[2] *https://www.ccma.cat/324/un-75-dels-1-900-llits-duci-ocupats-per-pacients-amb-coronavirus/noticia/3002513/*
[3] *https://www.elnacional.cat/es/salud/coronavirus-se-colapsan-las-urgencias-criticos-intubados-no-solo-personas-mayores_482520_102.html*
[4] *https://www.ccma.cat/324/shabiliten-espais-en-hospitals-hotels-i-poliesportius-per-ampliar-el-nombre-de-llits/noticia/3000097/*
[5] *https://elpais.com/espana/catalunya/2020-05-16/cataluna-echa-el-cierre-a-los-hospitales-de-campana-de-la-covid-19.html*
[6] *https://www.lavanguardia.com/vida/20201102/49168618497/salut-reactiva-contratacion-estudiantes-covid.html*

S'han promogut tecnologies per reduir la mobilitat dels pacients als centres mèdics i s'ha procurat de mantenir unes condicions de ciberseguretat i privacitat adequades.

Les **noves tecnologies han estat un element clau** per tal que el sistema de salut pogués fer front a la crisi sanitària de la covid-19, però també han constituït un **repte per a la ciberseguretat**. De fet, aquestes noves tecnologies només podien reeixir si es guanyaven la **confiança de professionals i pacients**, per a la qual cosa la **ciberseguretat esdevenia un aspecte imprescindible**. Les noves tecnologies difícilment haguessin pogut generar confiança i ser exitoses si hi hagués hagut incidents, fuites d'informació o caigudes de servei.

A Catalunya, s'ha apostat per l'ús de la **tecnologia per donar resposta als pacients a distància**, amb l'objectiu de minimitzar el contacte físic i el desplaçament dels malalts de covid-19, així com alleugerir la càrrega dels professionals sanitaris. S'ha realitzat el **seguiment dels malats a través del telèfon, per correu electrònic o amb apps al mòbil**. Segons la Generalitat de Catalunya, mentre que abans de la pandèmia hi havia unes 135.000 visites presencials al CAP al dia (un 70% dels pacients), el mes d'abril de 2020 aquestes visites s'havien reduït a 18.000, és a dir, un 87% menys en poques setmanes. Per contra, **les visites telefòniques van créixer de 14.500 diàries a 87.000**, i **les e-consulta van passar de 1.000 a 17.000** diàries[7]. En aquesta línia, l'inici de la pandèmia coincidia amb el fet que la Generalitat de Catalunya publicava una licitació per posar en marxa una plataforma de telemedicina per a la telemonitorització, l'ús de la gamificació i la implementació de canals de comunicació entre professionals i pacients[8].

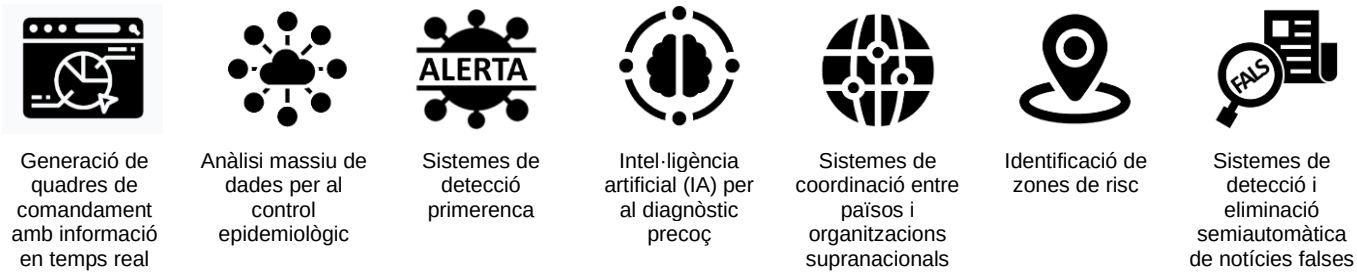
En pocs dies, el **Departament de Salut** va ser capaç de fer un salt endavant en matèria de **transformació digital per possibilitar el control i el diagnòstic de la covid-19 a distància**. En menys de 48 hores, es va desenvolupar una primera versió de l'**app STOP COVID-19 CAT.** Aquesta aplicació per a mòbil permetia als ciutadans autodiagnosticar-se, fer seguiment i vigilància dels símptomes de la malaltia i crear un mapa de calor sobre les àrees amb més infectats. La ciutadania va respondre positivament a l'ús d'aquesta app, amb més de **2,5 milions de descàrregues**, la realització de més de **21 milions de tests**, i la **derivació de 15.000 intervencions del Servei d'Emergències Mèdiques** (SEM)[9].

La recollida i compartició de dades massives dels malalts de covid-19 han permès combatre el virus, però comporten riscos en matèria de ciberseguretat i privacitat.

La ciència fa ús de **bases de dades massives per extreure tot tipus d'informació sobre el comportament de les malalties** amb l'objectiu de combatre-les més eficaçment. En el cas de la covid-19, una malaltia

[7] *https://el3devuit.cat/2020/04/25/78233/actualitat/salut-accelera-els-plans-de-transformacio-digital-per-la-crisi-sanitaria-de-la-covid-19/*
[8] *https://www.plantadoce.com/publico/la-generalitat-saca-a-concurso-la-telemedicina-en-plena-crisis-por-el-covid-19.html*
[9] *https://stopcovid19.cat/stop-covid19-cat/*

provocada pel coronavirus SARS-Cov-2, un virus nou i desconegut, **la recollida i compartició de dades dels malalts ha estat imprescindible** per tal d'aconseguir donar resposta a un conjunt de reptes d'importància cabdal (veure il·lustració 1).



Il·lustració 1. Fites a assolir mitjançant la compartició de dades mèdiques durant la pandèmia de la covid-19[10].

En aquesta línia, el mes d'abril de 2020, la **Comissió Europea** presentava la **Plataforma Europea de Dades sobre la covid-19** per tal que les dades d'investigació sobre la malaltia poguessin recopilar-se i compartir-se àgilment. L'objectiu: **entendre i diagnosticar millor la malaltia**[11]. Anàlogament, el Department of Economic and Social Affairs (DESA) de l'**Organització de les Nacions Unides** (ONU) va publicar una **central de dades** en què els països podien compartir dades en un entorn obert i cooperatiu[12]. Precisament, el grup HM Hospitales va col·laborar-hi amb la compartició de dades mèdiques de pacients degudament anonimitzades[13].

La recollida i la compartició de les dades dels pacients han ajudat a donar resposta a la pandèmia, però també han comportat un important increment dels **riscos** en matèria **ciberseguretat i privacitat**. El motiu és que les **dades personals mèdiques tenen valor al mercat negre** i constitueixen un objectiu suculent per als ciberdelinqüents.

La transformació digital que viu el sector sanitari impulsa la incorporació de tecnologies i bones pràctiques de ciberseguretat.

Un informe de Fenin (Federación Española de Empresas de Tecnología Sanitaria) anterior a la pandèmia, posava en evidència que **el nivell de transformació digital del sistema de salut de Catalunya era baix**. En alguns aspectes, però, es valorava un nivell de transformació digital alt: en la gestió de cites, l'accés a la història clínica electrònica per part dels professionals o la prescripció electrònica. En canvi, s'evidenciava la **necessitat de millorar** la **interacció no presencial** entre professionals i pacients, així com el **desplegament de solucions analítiques** basades en intel·ligència artificial per disposar de models predictius i prescriptius[14].

[10] *https://www.coit.es/noticias/digitalizar-plenamente-el-sector-sanitario-para-enfrentarse-mejor-crisis-como-la-del-covid*
[11] *https://ec.europa.eu/commission/presscorner/detail/es/ip_20_680*
[12] *https://covid-19-data.unstatshub.org/*
[13] *https://healthcare-in-europe.com/en/news/covid-19-data-saves-lives-in-spain.html*
[14] *https://diarisanitat.cat/el-sistema-nacional-de-salut-presenta-un-index-baix-de-transformacio-digital/*

Irònicament, la pandèmia de **la covid-19 ha suposat un impuls per a la transformació digital del sistema sanitari català en els àmbits en els quals era més feble: l'atenció no presencial i de recollida i tractament analític de dades mèdiques**. Ara bé, això només ha estat el començament. El Departament de Salut preveu la construcció, en un temps rècord, de **cinc nous i innovadors hospitals**, com a mòduls de suport al costat d'altres centres existents[15]. També ha assignat una inversió de **5,5 M€ en tecnologies per enfortir i transformar l'atenció primària** amb l'objectiu de garantir una resposta ràpida i eficient a la ciutadania. Aquest pla inclou millorar les **centraletes, incorporar nous equips de telemedicina, desenvolupar apps per a mòbil**, etc[16]. I de ben segur que també caldrà estudiar altres desenvolupaments tecnològics, com el trasllat de recursos del sistema sanitari al **núvol**, el desenvolupament de plataformes per a la **compartició de dades mèdiques anonimitzades**, l'ús d'**intel·ligència artificial**, el desplegament de sistemes basats en la tecnologia ***blockchain*** per tal que el ciutadà sigui el propietari de les seves dades personals, etc.

Inevitablement, a mesura que les TIC adquireixin més rellevància en el sistema sanitari, creixerà la **preocupació per garantir un entorn segur i resilient**, des del punt de vista cibernètic. Per aquest motiu, les mesures de ciberseguretat integrades en els sistemes, processos i persones del sistema de salut esdevindran un element habitual i imprescindible. Així ho entén la Comissió Europea que, en el marc del programa **Horitzó 2020**, anunciava l'aportació de **38 milions d'euros a projectes innovadors en el camp de la protecció d'infraestructures crítiques**, entre les quals s'hi troben els hospitals, amb l'objectiu de fer-los més intel·ligents i segurs[17].

Els atacs de *phishing*, *ransomware*, les fuites de dades i la seguretat dels dispositius d'e-salut són els principals reptes de la ciberseguretat al sector de la salut.

La **ciberseguretat** ha viscut una **etapa convulsa** amb la pandèmia, tal i com hem constatat en els **informes** del **primer** i **segon** semestre de 2020 de l'**Agència de Ciberseguretat de Catalunya**. En aquest context i enmig de la transformació digital del sector de la salut, el sistema sanitari català ha hagut de fer front a un seguit d'amenaces especialment rellevants.

Primer, el ***phishing***: els atacs en contra el sistema sanitari català han experimentat un increment del 198% respecte del 2019. En segon terme, el ***ransomware***: el 3 de setembre, un grup ciberdelinqüent xifrava alguns sistemes del Consorci Sanitari Integral i l'Hospital Moisès Broggi. Tercer, les **fuites de dades**: en una anàlisi de 201 fuites de dades diferents, es van identificar 12.581 comptes de correu electrònic de professionals del sector sanitari de Catalunya, amb el 58% de les entitats, afectades. Quart, la **seguretat dels dispositius d'e-salut**: el desembre de 2020, l'Agència alertava d'una vulnerabilitat que afectava una llarga llista de sistemes d'imatges per TC, raigs X i ressonància magnètica.

El detall d'aquestes amenaces es desenvolupa a les pàgines següents.

[15] *https://www.ccma.cat/324/salut-construira-cinc-hospitals-expres-en-20-setmanes-per-a-malalts-de-la-covid/noticia/3044195/*
[16] *https://web.gencat.cat/ca/actualitat/detall/El-nou-Pla-denfortiment-i-transformacio-de-latencio-primaria-te-un-pressupost-de-gairebe-300-milions*
[17] *https://www.esmartcity.es/2020/06/19/ue-destinara-mas-38-millones-euros-proyectos-innovadores-ciberseguridad*

Els atacs de *phishing* exploten la pressió assistencial sobre el sector sanitari durant la pandèmia

El *phishing* és el principal mètode d'atac contra el sector sanitari i, durant la pandèmia, ha explotat la pressió assistencial i la manca de conscienciació en ciberseguretat dels professionals. L'*spear-phishing*, més elaborat i dirigit, incrementa un 75% la probabilitat d'èxit dels atacs. Habitualment, l'objectiu és el robatori de credencials, però també la infecció amb *malware* i els fraus de tipus BEC.

El 57% dels atacs cibernètics contra el sector sanitari a l'Estat espanyol utilitza correus de *phishing* per explotar les vulnerabilitats del factor humà, conseqüències de la pressió assistencial i la manca de conscienciació en ciberseguretat. Les possibilitats d'èxit són especialment elevades en una situació de pandèmia. Si, a més, l'atac de *phishing* està elaborat i va dirigit a una víctima determinada (*spear-phishing*), la probabilitat d'èxit creix un 75%. Durant els primers dies de pandèmia, el *phishing* va augmentar un 30% i l'*spear-phishing*, un 667%. S'usaven temàtiques relacionades amb la covid-19 com a reclam per atraure les víctimes.

El 60% dels casos de *phishing* tenen com a objectiu les credencials d'accés i contenen un enllaç a un web fraudulent, en el qual se sol·licita que la víctima introdueixi l'usuari i la contrasenya. En altres casos, els correus de *phishing* busquen infectar la víctima amb un programari maliciós. Si el programari maliciós és un troià amb capacitats de *dropper*, aquest permetrà forçar la instal·lació d'altres *malwares*, una tècnica que s'utilitza habitualment en atacs de *ransomware*. Els correus de *phishing* també s'utilitzen per perpetrar fraus de BEC, dels quals el sector sanitari n'és el segon sector més afectat.

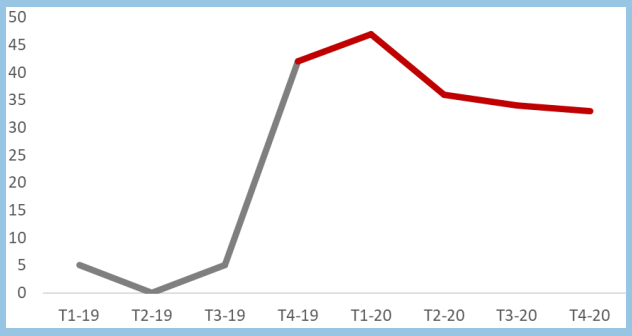
Aspectes clau:

- **El *phishing* és el mètode d'atac més utilitzat contra el sector sanitari per la seva efectivitat i senzillesa, així com pel fet que permet explotar l'efecte de la pressió assistencial sobre els professionals durant la pandèmia.**
- **El *phishing* al sector sanitari es dispara durant la pandèmia amb atacs especialment elaborats i dirigits.**
- **El *phishing* s'utilitza en el robatori de credencials, la difusió de programari maliciós (per robar informació o iniciar un atac de *ransomware*) i en fraus de BEC.**
- **Els ciberatacants fan ús del *phishing* i el *vishing* per atacar tot tipus de professionals, tant de centres sanitaris com proveïdors i pacients.**

Baròmetre

Augment del *phishing* al sistema sanitari de Catalunya durant el 2020

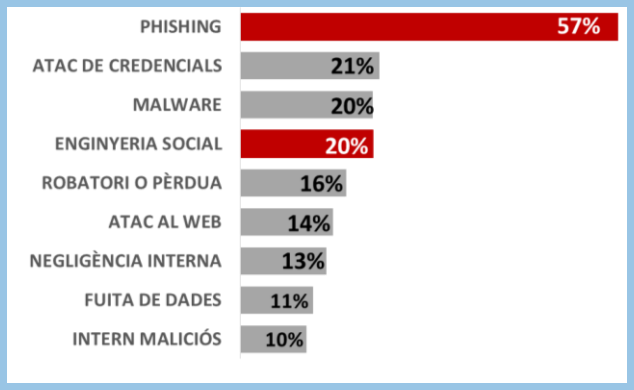
El 2020, els atacs de *phishing* contra el sistema sanitari català han vist un increment del 198% respecte del 2019. Han assolit el seu pic màxim el 1r trimestre de 2020, coincidint amb la declaració de pandèmia. No obstant això, l'onada de *phishing* ja va començar el 4t trimestre de 2019, quan es va identificar un increment del 950%. D'aleshores ençà i durant la pandèmia, els valors s'han mantingut alts.



Il·lustració 2. Incidents de phishing *detectats, dirigits al sistema sanitari de Catalunya (Font: Agència).*

El *phishing* és l'incident més habitual al sector sanitari

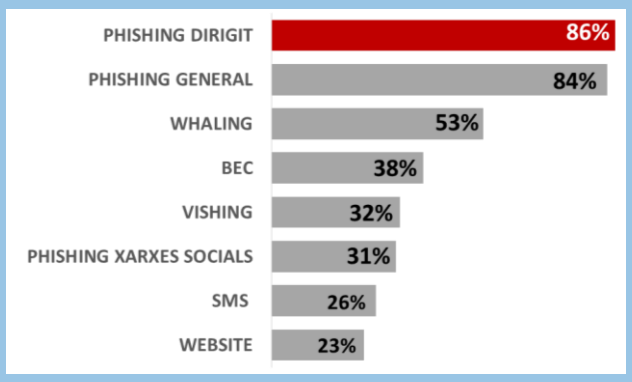
Una enquesta a professionals sanitaris constata que, en 12 mesos, el *phishing* ha estat l'incident de ciberseguretat més habitual que han experimentat: de fet, el 57% dels professionals n'ha experimentat algun. I destaca com el 20% ha experimentat incidents d'enginyeria social en un sentit més ampli.



Il·lustració 3. Percentatge de professionals que han experimentat diferents tipus d'incidents cibernètics al sector sanitari[18].

El *phishing* dirigit predomina al sector sanitari

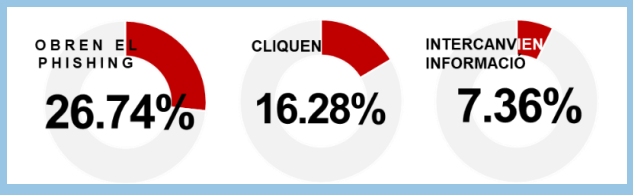
El 86% dels professionals sanitaris han experimentat atacs de *phishing* dirigit (*spear-phishing*), per sobre de qualsevol altra tipologia. Aquest fet evidencia com el sector sanitari és un objectiu d'interès per als ciberdelinqüents, els quals no dubten d'invertir esforços en l'elaboració dels atacs. També destaca com el 53% dels professionals han viscut atacs dirigits a responsables i alts càrrecs (*whaling*).



Il·lustració 4. Percentatge de professionals que han experimentat diferents tipus de phishing *al sector sanitari[19].*

Gairebé una quarta part dels professionals sanitaris obre, clica o dona dades en cas de *phishing*

En un estudi sobre el comportament dels professionals davant d'un atac de *phishing*, el sector sanitari obté la sisena millor puntuació d'entre 34 sectors. És una millora respecte d'altres estudis, però cal tenir en compte que la pandèmia ha provocat que el volum de correus electrònics s'hagi disparat en altres sectors i, així, ara els enganys són més difícils de distingir. Tanmateix, l'estudi indica que un de cada quatre professionals sanitaris obre un correu de *phishing*, un de cada sis clica l'enllaç maliciós i aproximadament un 7% arriba a donar informació.



Il·lustració 5. Resposta dels professionals sanitaris davant d'un atac de phishing*[20].*

[18] *https://www.himss.org/resources/himss-healthcare-cybersecurity-survey*
[19] *https://www.himss.org/resources/himss-healthcare-cybersecurity-survey*
[20] *https://cybernews.com/security/top-5-industries-that-fall-victim-to-phishing-scams/*

El phishing és una pràctica fraudulenta consistent a simular una identitat falsa, sovint per suplantació de la identitat d'una persona o un organisme determinats, sigui per correu electrònic, en una trucada o per altres mitjans, amb l'objectiu d'incitar les possibles víctimes a fer una acció que permeti robar-los dades personals, habitualment dades credencials o números de targeta de crèdit.

(font: Termcat)

Una vulnerabilitat és la feblesa d'un sistema informàtic davant de les amenaces a què està exposat.

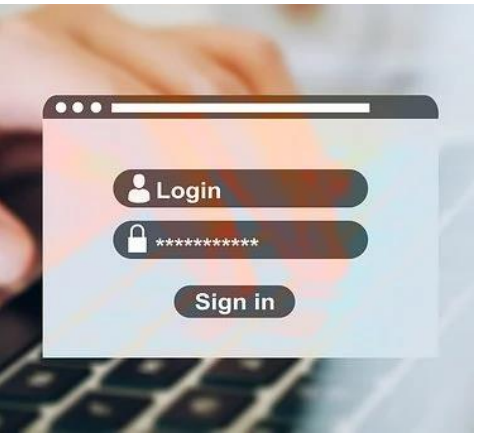
(font: Termcat)

El *phishing* és el mètode d'atac més utilitzat contra el sector sanitari per la seva efectivitat i senzillesa, així com pel fet que permet explotar l'efecte de la pressió assistencial sobre els professionals durant la pandèmia.

Els atacs de *phishing* tenen **poca complexitat: són fàcilment escalables i no requereixen un gran esforç**. Són escalables perquè permeten ampliar gairebé il·limitadament el nombre de destinataris sense cost afegit. Quant a l'esforç, els ciberdelinqüents disposen d'eines que els faciliten la tasca. Hi ha múltiples programaris per a la creació i difusió de campanyes de *phishing* que són a l'abast de qualsevol. No fa pas gaire que s'ha identificat l'oferta de més de 1.300 **kits de *phishing*** a la *dark web* que, per poc més de **20 euros** cada un, permetien suplantar llocs web i plataformes populars d'Internet amb l'objectiu de robar contrasenyes i comptes bancaris[21].

El *phishing* és el **mètode d'atac més utilitzat contra el sector sanitari**: a l'Estat espanyol, el **57% dels atacs cibernètics** contra aquest sector l'utilitzen[22]. El més preocupant és que, segons un estudi, aproximadament **una quarta part dels professionals sanitaris obre, clica o dona dades** (veure il·lustració 5). Si bé el percentatge que finalment **acaba intercanviant dades** és "només" d'un **7%**, cal ser conscient que **una única víctima pot significar el compromís de tota una organització**. I un **57% de professionals** informa que han estat **objectiu de *phishing*** (veure il·lustració 3). Un exemple: en pocs mesos, el sistema hospitalari més gran de Michigan (EUA) ha estat víctima de dos atacs de *phishing* que han provocat el robatori de les dades de milers de pacients[23].

Els atacs de *phishing* utilitzen **tècniques d'engany i persuasió per explotar** les vulnerabilitats del factor humà, com les **conseqüències de la pressió assistencial** i la **manca de conscienciació** en matèria de riscos cibernètics. La pandèmia de la **covid-19** i la corresponent crisi sanitària han generat un **context molt favorable** al *phishing*: en un sistema de salut saturat en el qual els professionals estan molt pressionats i esgotats, el risc cibernètic no figura entre les seves principals preocupacions. Per afegir llenya al foc, **els centres sanitaris no acostumen a dur a terme programes de conscienciació sobre ciberseguretat** als seus treballadors. Segons SANS Security Awareness, els motius més recurrents per no fer-ho són la manca de temps i l'escassedat de personal, però no pas la de pressupost[24].



El *phishing* al sector sanitari es dispara durant la pandèmia amb atacs especialment elaborats i dirigits.

Els cibercrim és conscient de la situació vulnerable dels professionals sanitaris, per la qual cosa són objectiu d'atacs de *phishing*. **A Catalunya, el *phishing* contra el sector sanitari ha experimentat un increment del 198%** respecte del 2019 (veure il·lustració 2). El *modus operandi* habitual dels atacants ha estat **suplantar personalitats o entitats de confiança**: un pretès professional del sector, un centre mèdic, una empresa farmacèutica, un ministeri o autoritat sanitària, l'agència de control de malalties infeccioses, les forces de l'ordre, organitzacions internacionals, etc. Ha estat especialment rellevant la suplantació de l'Organització Mundial de la Salut (OMS), fins al punt que l'organisme va difondre un missatge d'alerta per prevenir dels enganys que utilitzaven la seva imatge[25]. L'abril de 2020 s'alertava d'una campanya de *phishing* que suplantava l'OMS i es dirigia a empreses biomèdiques; s'oferien

[21] *https://www.redeszone.net/noticias/seguridad/kits-phishing-venta-internet/*
[22] *https://www.ituser.es/seguridad/2020/05/el-57-de-los-ataques-al-sistema-sanitario-son-de-phishing*
[23] *https://www.infosecurity-magazine.com/news/michigan-healthcare-provider/*
[24] *https://www.ituser.es/seguridad/2019/07/la-falta-de-tiempo-y-de-personal-lastra-la-concienciacion-en-ciberseguridad*
[25] *https://www.who.int/about/communications/cyber-security*

Un infostealer és un programari maliciós dissenyat per capturar informació (per exemple, credencials d'accés, números de targetes de pagament...) d'un sistema.

L'spear-phishing *o la pesca dirigida, és una tècnica de pesca en què s'intenta enganyar les víctimes, habitualment individus concrets o grups específics d'usuaris vinculats a empreses importants o a institucions governamentals, adreçant-s'hi d'una manera personalitzada, sovint per correu electrònic.*

(font: Termcat)

Un troià és programa maliciós amb una funció aparentment útil, però amb funcions addicionals amagades que faciliten l'accés no autoritzat a un sistema i el fan vulnerable.

(font: Termcat)

indicadors de l'evolució de la malaltia, però l'objectiu era infectar l'equip de la víctima amb l'*infostealer* Formbook inclòs en un fitxer adjunt[26].

Els atacs de *phishing* adaptats i dirigits a cada víctima han estat especialment rellevants. És el cas de l'*spear-phishing*. Només en els primers dies de pandèmia, el *phishing* va augmentar un 30%[27] i l'*spear-phishing* fins a un 667%[28] a nivell global. D'aquesta manera, el **86% dels professionals sanitaris han experimentat atacs** d'aquest tipus de *phishing* dirigit (veure il·lustració 4). En aquests atacs, fins i tot s'arriba a suplantar la identitat de **contactes reals i de confiança**, tal i com va passar al National Health Service (NHS) del Regne Unit: es van fer servir 113 bústies de correu compromeses per enviar correus maliciosos entre els seus professionals[29]. Amb l'*spear-phishing*, el ciberatacant arriba a menys objectius, però pot **millorar la probabilitat d'èxit un 75%** perquè és més creïble i difícil d'identificar[30]. Val a dir que cal estar molt alerta per identificar un correu electrònic fraudulent enviat des de la bústia d'un col·lega de professió.

El *phishing* s'utilitza en el robatori de credencials, la difusió de programari maliciós (per robar informació o iniciar un atac de *ransomware*) i en fraus de BEC.

Normalment, els correus de *phishing* s'utilitzen per obtenir credencials, dades personals o informació restringida. En un **60%** dels casos de *phishing*, l'**objectiu són les credencials d'accés**[31], habitualment mitjançant un enllaç a un web fraudulent en què se sol·licita que la víctima introdueixi un usuari i una contrasenya. Aquest web pot suplantar **Zoom, Google, Office 365 o, fins i tot, la intranet corporativa o el correu electrònic professional**. El risc que això succeeixi no és menor: el sector sanitari, juntament amb el financer, les agències governamentals i la indústria tecnològica, és un **objectiu preferent** per a aquest tipus d'atacs[32].

Només que un treballador caigui en el parany i faciliti les **credencials d'accés al seu correu electrònic**, les conseqüències poden ser greus, ja que estarà **cedint el control a la bústia i a tot el contingut**. Precisament, el juliol de 2020, el National Cardiovascular Partners (EUA) va notificar que les dades de 78.070 pacients havien estat compromeses després que un ciberatacant obtingués l'accés a la bústia de correu d'una víctima gràcies a un atac de *phishing*[33]. En el cas que les credencials filtrades pertanyin a un **administrador de sistemes** amb accessos privilegiats, les **conseqüències** poden ser encara més **funestes**, atès que estarà cedint l'**accés a la xarxa corporativa** a un atacant. El mes de setembre de 2020, després que un treballador filtrés les seves credencials d'accés remot amb Citrix en un atac de *phishing,* l'hospital de Nova Jersey va veure com un atac de *ransomware* aconseguia xifrar la informació dels seus servidors i es veia obligat a pagar un rescat per tal de recuperar-la[34].

El *phishing* també pot tenir com a objectiu **infectar la víctima amb un programari maliciós** de tipus *troià*, inserit en un document adjunt o que es descarrega a partir d'un enllaç. En funció de la naturalesa del programari maliciós, les **conseqüències poden ser diverses**. En el cas d'un troià

[26] *https://cyware.com/news/formbook-campaign-now-leveraging-covid-19-themes-92325530/?web_view=true*
[27] *https://www.mimecast.com/globalassets/cyber-resilience-content/the_state_of_email_security_report_2020.pdf?utm_source=pr&utm_medium=pr&utm_campaign=7013l000001N4dRAAS*
[28] *https://www.securitymagazine.com/articles/92157-coronavirus-related-spear-phishing-attacks-see-667-increase-in-march-2020*
[29] *https://digital.nhs.uk/news-and-events/news/nhs-digital-statement-on-nhsmail-phishing-incident*
[30] *https://www.mimecast.com/globalassets/cyber-resilience-content/the_state_of_email_security_report_2020.pdf?utm_source=pr&utm_medium=pr&utm_campaign=7013l000001N4dRAAS*
[31] *https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf*
[32] *https://healthitsecurity.com/news/credential-theft-via-spoofed-login-pages-increase-healthcare-top-target*
[33] *https://healthitsecurity.com/news/national-cardiovascular-partners-email-hack-impacts-78k-patients*
[34] *https://blog.elhacker.net/2020/10/hospital-de-nueva-jersey-pago-670-mil-dolares-rescate-para-evitar-fuga-datos-pacientes-ataque-ransomware.html*

Un troià d'accés remot, o RAT, és un programari maliciós que infecta la víctima fent-se passar per un programari lícit i que estableix una connexió amb el ciberdelinqüent, *al qual li atorga el control sobre el dispositiu de la víctima.*

El dropper és és un troià que ha estat dissenyat per forçar la instal·lació d'un altre programari maliciós, codi dels qual ja està inclòs en el mateix troià o cal ésser descarregat d'Internet, a un sistema d'informació sense ser detectat i sense el consentiment de l'usuari.

El Business Email Compromise *(BEC) és un atac d'enginyeria social en què se suplanta el correu electrònic d'un professional per sol·licitar a la víctima una transferència econòmica en favor de l'atacant a través d'algun tipus d'engany.*

Els dominis homogràfics s'utilitzen per suplantar dominis legítims fent ús de caràcters similars als originals.

infostealer, aquest s'instal·larà a l'equip del professional sanitari amb l'objectiu de **capturar dades i enviar-les al ciberdelinqüent**. La finalitat és robar credencials d'accés i dades bancàries, les quals poden vendre's al mercat negre o ser utilitzades en noves accions malicioses. En altres casos, els troians poden incorporar funcions de RAT (*Remote Access Tool*), que permeten al ciberatacant **accedir a l'equip infectat de la víctima a través d'una connexió remota** i, a partir d'aquí, tractar d'infiltrar-se i moure's per la xarxa del centre hospitalari. En aquets casos, quan l'atacant ha aconseguit el coneixement adequat de la xarxa, pot robar informació i, fins i tot, executar un *ransomware* allà on pugui causar més danys. Precisament, durant el 2020, organismes sanitaris de tot el món han estat víctimes d'una campanya de correus que oferien equipament mèdic i que incorporaven el troià *infostealer* i RAT anomenat Agent Tesla[35]. Quan els troians inclouen funcions de *dropper* permeten **forçar la instal·lació d'altres *malwares* en el sistema**. El mes de març, en ple brot del coronavirus, una campanya de *phishing* va arribar a hospitals de l'Estat espanyol després d'haver afectat diversos centres mèdics d'arreu del món. Amb el cimbell d'informació sobre la covid-19, quan l'usuari obria el fitxer adjunt s'infectava amb un *dropper* que forçava la descàrrega del *ransomware* Netwalker que xifrava la informació de l'equip de la víctima i exigia el pagament d'uns 1.000 € per recuperar-la[36, 37].

Il·lustració 6. Programaris maliciosos difosos pels ciberatacants entre el sector sanitari via phishing.

Per últim, el *phishing* també és un mitjà per a la **distribució de fraus**. Precisament, durant el brot de covid-19, en els moments de més gran confusió i necessitat de productes sanitaris, el *phishing* es va utilitzar per difondre **ofertes enganyoses de subministrament de productes quirúrgics** com ara mascaretes, equips de protecció individual (EPI), *kits* de diagnòstic, etc. Així ho va alertar la Interpol[38].

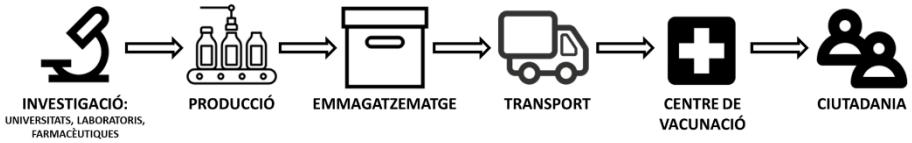
En matèria de frau via *phishing*, cal fer una menció especial als atacs de BEC, ja que **el sector sanitari és el segon més afectat després del sector industrial**[39]. Aquests atacs comencen quan el cibercriminal obté les credencials i el control de la bústia de correu electrònic d'un professional (per exemple, un càrrec directiu, un responsable de compres o un proveïdor). Des d'aquesta bústia, el ciberdelinqüent enviarà un **correu als responsables de finances o compres** i els instarà a fer el **pagament urgent d'una factura** amb la particularitat que el compte bancari del **beneficiari és el del cibercriminal**. Ho farà sense gaires problemes, ja que els correus enviats des d'una bústia legítima superen els filtres de correu brossa (*spam*) sense aixecar alertes. En altres casos, l'atacant crea una adreça de correu homogràfica. En qualsevol cas, l'atacant prèviament haurà **investigat** les relacions comercials de la víctima per tal que la **forma i el contingut dels correus de BEC no despertin cap sospita**. L'FBI alertava que, aprofitant la confusió causada per manca d'equipament mèdic durant les primeres fases pandèmiques, es van identificar diversos atacs de BEC que acabaven amb l'enviament de transferències econòmiques fora de la jurisdicció de les autoritats nord-americanes[40].

[35] *https://healthitsecurity.com/news/4-sophisticated-phishing-campaigns-impacting-the-healthcare-sector*
[36] *https://www.computing.es/seguridad/noticias/1117559002501/ransomware-netwalker-pone-jaque-todos-hospitales-espanoles.1.html*
[37] *https://www.incibe-cert.es/blog/ransomware-netwalker-analisis-y-medidas-preventivas*
[38] *https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/INTERPOL-avisa-de-una-estafa-relacionada-con-la-COVID-19*
[39] *https://www.trendmicro.com/en_us/research/20/j/french-companies-under-attack-from-clever-bec-scam.html*
[40] *https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic*

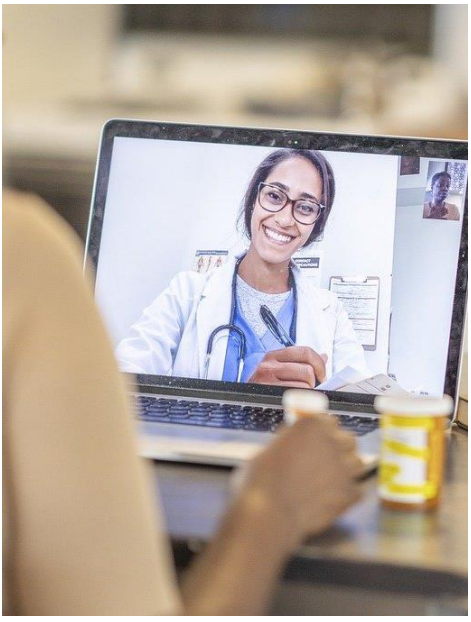
Els ciberatacants fan ús del *phishing* i del *vishing* per atacar tot tipus de professionals, tant de centres sanitaris com proveïdors i pacients.

El sector sanitari és un objectiu especialment suculent per al cibercrim: és una **font de dades personals sensibles** (veure capítol sobre fuites de dades personals) i un **objectiu prioritari dels atacs de *ransomware*** (veure capítol sobre *ransomware*). És important destacar que això no només implica els centres mèdics, també inclou **tota la cadena de subministrament: laboratoris d'investigació, productors de material i equipament, companyies farmacèutiques, asseguradores, etc**. Així ho alertava l'FBI en un missatge difós durant el mes d'abril[41].

Els actors maliciosos han dirigit les seves campanyes de ***phishing* a tota la cadena de subministrament sanitària** fent ús dels **reclams adequats** als diferents **moments de la crisi sanitària**. A l'inici de la pandèmia, el reclam del *phishing* explotava l'elevada demanda de material sanitari: els correus es dirigien als **proveïdors** que, amb l'excusa de demanar informació sobre **productes de protecció i desinfecció**, adjuntaven un fitxer maliciós amb el detall de la consulta[42]. Més recentment, coincidint amb la campanya de la vacunació, es va descobrir una campanya de *phishing* dirigida a **entitats, tant privades com públiques, implicades en el procés de distribució de les vacunes de la covid-19** de sis països diferents. Els correus suplantaven l'empresa Haier Biomedical, un fabricant xinès de dispositius per mantenir la cadena de fred de les vacunes, i adjuntaven arxius maliciosos, en format *html*, que induïen els destinataris a introduir les seves credencials[43].



Il·lustració 7. Cadena de producció i distribució de la vacuna objectiu de ciberatacs.



Qualsevol tipus d'organització del sector sanitari ha d'estar alerta contra l'amenaça del *phishing*, però també n'han d'estar **tots els professionals: des d'administratius, tècnics, investigadors, metges i infermeres fins als càrrecs directius**. Ningú està exempt de caure en un parany dissenyat de manera acurada. De fet, en el context actual, tots els **teletreballadors**, amb el **suport informàtic menys present** i **sense la protecció de la seguretat pròpia de la xarxa corporativa**, encara estan **més exposats**. És el cas, per exemple, d'una campanya de *phishing* dirigida als metges i francament difícil d'identificar: a partir d'un compte de correu compromès del *College of Family Physicians of Canada* es va enviar un missatge als professionals col·legiats convidant a fer un pagament a càrrec dels serveis subministrats[44].

Fins i tot els **pacients** són objectiu de campanyes de *phishing* en què se suplanten autoritats sanitàries o professionals mèdics. A l'Estat espanyol, una campanya d'aquestes característiques va suplantar el *Ministerio de Sanidad*, amb correus electrònics que informaven les víctimes que havien estat denunciades pels veïns per no portar mascareta. En el correu hi havia un enllaç per descarregar la suposada notificació de la denúncia però, en realitat, s'induïa a la descàrrega d'un troià per robar dades bancàries[45].

[41] *https://www.aha.org/system/files/media/file/2020/04/fbi-alert-tlp-white-covid-19-email-phishing-against-us-healthcare-providers-4-21-2020.pdf*
[42] *https://www.fortinet.com/blog/threat-research/scammers-using-covid-19-coronavirus-lure-to-target-medical-suppliers*
[43] *https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/*
[44] *https://ca.news.yahoo.com/phishing-scam-targets-doctors-emails-110000465.html?guccounter=1*
[45] *https://www.lavanguardia.com/tecnologia/20200609/481697889864/suplantan-pagina-web-ministerio-sanidad-phishing.html*

El vishing, o pesca per veu, és una tècnica de pesca en què s'intenta enganyar les víctimes telefònicament, mitjançant la veu per IP.

(font: Termcat)

Ara bé, els atacs de *phishing* no només han pres la forma de correus electrònics: l'anomenat *vishing* també ha estat especialment actiu en el sector sanitari. Destaca l'estafa de suport tècnic, en la **qual l'atacant es fa passar per tècnic d'una companyia de programari o de serveis informàtics** (habitualment Microsoft) que es posa en contacta amb un professional sanitari i li ofereix suport per solucionar un suposat problema en el seu equip[46]. A la fi, l'atacant acaba sol·licitant credencials o demana instal·lar un programari que, a la fi, resultarà maliciós. El *vishing* també s'utilitza **contra els pacients**: els clients de l'Spectrum Health System (EUA), una organització que integra múltiples entitats sanitàries de West Michigan, van rebre trucades telefòniques que suplantaven els professionals del centre amb l'objectiu d'obtenir informació confidencial[47].

Recomanacions

- **Els professionals no han de revelar credencials a tercers, ni de forma escrita (en el cas del *phishing*) ni de forma oral (en el cas del *vishing*).**
- **Els professionals han d'ignorar els correus electrònics amb remitent desconegut, en especial quan sol·licitin credencials o incloguin un fitxer adjunt.**
- **Els professionals, davant d'un correu sospitós, han de validar l'autenticitat de l'adreça del remitent, consultar directament amb el remitent per un altre mitjà o consultar amb el servei tècnic.**
- **Els professionals han de tenir desactivades les macros que permetin executar codi maliciós en arxius Office (.docxm/.xlsxm...) i abstenir-se d'obrir fitxers executables (.exe/.js/.jar/.py/.VBscript...) o imatges de disc (.ISO/.IMG...), fins i tot en carpetes comprimides (.zip/.rar/.arj...).**
- **Els responsables de TI han de vetllar per mantenir actualitzats els sistemes operatius i el programari, així com els *anti-malware* o antivirus amb els darrers patrons de codi maliciós.**
- **Les organitzacions han de realitzar campanyes de conscienciació contra el *phishing* entre els empleats en general, i contra el BEC, especialment entre els treballadors d'àrees de compres i finances.**
- **Les organitzacions han d'utilitzar proveïdors de serveis de correu electrònic que implementin tecnologies *anti-spam* i *anti-phishing*.**
- **Les organitzacions han compartir i informar-se de les amenaces i campanyes de *phishing* més actuals per alertar els treballadors.**

[46] *https://support.microsoft.com/en-us/help/4013405/windows-protect-from-tech-support-scams*
[47] *https://www.beckershospitalreview.com/cybersecurity/scammers-posing-as-spectrum-health-employees-are-calling-patients-to-steal-their-phi-health-system-warns.html#:~:text=Spectrum%20Health%20said%20the%20scam,a%20Spectrum%20Health%20phone%20number.*

El *ransomware* es dirigeix al sector sanitari perquè és especialment essencial durant la pandèmia

El 2020, el sector sanitari ha estat el principal objectiu del *ransomware* i el receptor del 17,9% dels atacs. El *ransomware* s'especialitza i incorpora la doble extorsió. El 70% dels atacs es realitzen a través de connexions RDP o VPN, tan desplegades durant la pandèmia per al teletreball, i el 26% a través de correus de *phishing*. S'ha constatat com un incident en un hospital pot posar vides humanes en risc.

Les entitats sanitàries duen a terme un servei essencial i, en cas d'un incident de *ransomware*, poden veure's forçades a pagar el rescat per mantenir l'activitat. Així, el nombre d'atacs de *ransomware* contra hospitals va pujar un 60% quan va esclatar la pandèmia, i el 2020, el sector sanitari n'ha estat el principal receptor, amb un 17,9% dels atacs.

El *ransomware* evoluciona i el model *Ransomware-as-a-Service* facilita el repartiment de feines i l'especialització. A finals de 2020, el 70% dels atacs de *ransomware* ja incorporaven la doble extorsió: al *ransomware* tradicional s'hi suma el robatori de dades i l'amenaça de fer-les públiques si la víctima no paga.

El 70,3% dels atacs de *ransomware* es realitza a través de les connexions RDP i VPN, àmpliament desplegades per al teletreball durant la pandèmia, i el 26,3% via *phishing*.

El cost mitjà que té un incident de *ransomware* en un hospital és de 760.000 €, sense comptar l'import del rescat i el perjudici des del punt de vista de la reputació. Fins i tot podria posar en risc la vida dels pacients.

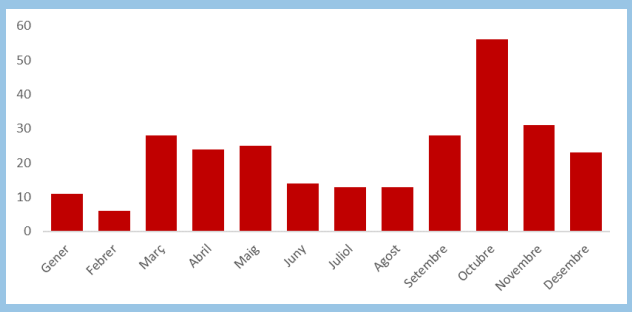
Aspectes clau:

- **Un incident de *ransomware* en un centre sanitari pot provocar el cessament de l'activitat assistencial, amb un risc per la vida dels pacients i costos econòmics.**
- **El cibercrim ha focalitzat els atacs de *ransomware* cap al sector sanitari ràpidament, però han trigat més per guanyar efectivitat.**
- **El conjunt de la cadena de subministrament del sector sanitari ha estat essencial durant la pandèmia. I un objectiu prioritari del *ransomware*.**
- **La doble extorsió contra el sector sanitari es consolida, impulsada per la sensibilitat de les dades personals de pacients i la informació de recerca de la vacuna.**
- **Les connexions RDP i VPN, àmpliament desplegades per fer possible el teletreball durant la pandèmia, són la principal entrada del *ransomware* al sector sanitari.**
- **El programari maliciós distribuït a través de *phishing* és la segona via d'entrada del *ransomware* al sector sanitari**

Baròmetre

El sector sanitari és l'objectiu del *ransomware* en el pitjors moments de la pandèmia

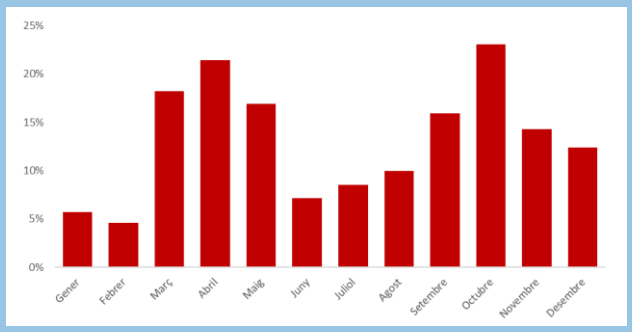
El nombre d'incidents de *ransomware* contra el sector sanitari ha augmentat significativament en els pitjors moments de la pandèmia, coincidint amb la primera onada (març) i la segona (octubre). Ara bé, la quantitat d'incidents al pic de la segona onada gairebé van doblar la primera. Les etapes més baixes en quant a nombre d'incidents van coincidir amb la fase més relaxada de la pandèmia, durant el període de vacances de l'estiu.



Il·lustració 8. Incidents de ransomware *al sector sanitari identificats als mitjans (Font: Agència).*

Els atacs de *ransomware* se centren en el sector sanitari

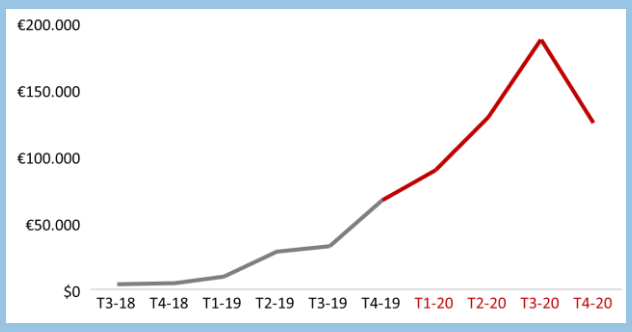
El cibercrim ha centrat els esforços a dirigir atacs de *ransomware* contra el sector sanitari. El percentatge d'incidents de *ransomware* al sector sanitari ha mantingut una tendència a l'alça durant el 2020, amb pics coincidint amb els pitjors moments de la pandèmia i les etapes de més saturació del sistema sanitari. Durant la primera i segona onada, pràcticament un de cada quatre incidents de *ransomware* afectava el sector sanitari.



Il·lustració 9. Percentatge d'incidents de ransomware *al sector sanitari identificats als mitjans (Font: Agència).*

Preus dels rescats a l'alça

L'import mitjà dels rescats sol·licitats en els incidents de *ransomware* ha crescut sostingudament fins el 4t trimestre de 2020, quan ha experimentat un descens. Així, el cibercrim es dedica a buscar noves formes d'extorsió per poder mantenir alt l'import dels rescats i forçar-ne el pagament. És el cas del robatori de dades sensibles i l'amenaça de publicar-les, un aspecte crític quan afecta dades personals de salut.



Il·lustració 10. Augment l'import mitjà dels rescats de ransomware[48].

La doble extorsió força el pagament de rescats elevats a les entitats sanitàries

La tècnica de la doble extorsió ha forçat algunes entitats sanitàries a pagar rescats elevats per evitar la publicació de les dades robades. Quan les dades robades són sensibles, la probabilitat que la víctima pagui creix. Per tant, l'amenaça és especialment crítica en el sector sanitari, on s'hi troben dades personals mèdiques i informació de recerca. Els dos rescats més grans pagats en el sector sanitari corresponien a víctimes de doble extorsió. Destaca el cas de l'Escola de Medicina de la Universitat de Califòrnia (EUA), que va pagar un rescat de pràcticament 1 M$ després de ser víctima d'un atac de *ransomware* amb doble extorsió.

Il·lustració 11. Ranking de pagaments de rescat.

[48] https://www.coveware.com/blog/q3-ransomware-marketplace-report

El ransomware, o programari de segrest, és un programari maliciós que restringeix totalment o parcialment l'accés als fitxers d'un dispositiu fins que no es paga una determinada quantitat de diners.

(font: Termcat)

La Directiva NIS és una legislació que entrà en vigor l'agost de 2016 per millorar la seguretat en xarxes i sistemes d'informació (en anglès, Network and Information Security) pels Estats de la Unió Europea. Principalment, aquesta legislació estableix cinc mesures concretes que han d'assolir tots els estats membres: una estratègia nacional, un grup de cooperació entre els estats membres, una xarxa CSIRT, unes condicions de seguretat per a operadors de serveis essencials i proveïdors de serveis digitals, i unes obligacions de ciberseguretat per a les autoritats nacionals.

L'RGPD és un reglament europeu d'obligat compliment a partir del 25 de maig de 2018 que, a Espanya, substitueix a la Llei Orgànica de Protecció de Dades (LOPD).

Aquest reglament estableix canvis importants amb relació a la normativa precedent: la responsabilitat proactiva de l'encarregat de tractar les dades i l'enfocament de la seguretat orientada a risc.

Un incident de *ransomware* en un centre sanitari pot provocar el cessament de l'activitat assistencial, amb un risc per la vida dels pacients i costos econòmics.

Un incident de *ransomware* en un centre hospitalari pot causar un **impacte alarmant: endarreriment de l'atenció als pacients, impossibilitat d'accedir als registres mèdics temporalment o irreversiblement, problemes en la gestió del parc d'ambulàncies...** La dependència de la xarxa informàtica i dels sistemes d'informació és tan gran que són molt nombrosos els hospitals víctimes d'un incident de *ransomware* que s'han vist obligats a **cessar alguns dels seus serveis**. El DCH Health System d'Alabama (EUA) es va veure obligat a tancar tres dels seus hospitals perquè no podia registrar nous pacients[49]. L'Hospital de Brno (República Txeca) es va veure obligat a apagar tots els sistemes d'informació, treballar amb paper i bolígraf i, en conseqüència, ajornar intervencions crítiques i traslladar pacients a altres hospitals pròxims[50]. L'Hospital del Districte de Rangely (EUA) va quedar-se sense accés als registres dels pacients i va perdre cinc anys d'informació[51]. Aquests només són alguns exemples, però n'hi ha molts més.

L'aturada de serveis assistencials a causa d'un *ransomware* pot **posar en perill la vida dels pacients**. A l'Hospital Universitari de Düsseldorf (Alemanya), un incident de *ransomware* va provocar l'aturada de les cirurgies i dels nous ingressos. Una pacient que necessitava tractament urgent no va poder ser atesa i va haver de ser traslladada a una altre centre situat a 30 km de distància[52]. Durant el trajecte, la pacient va morir i, si bé la policia alemanya no veu provat que el *ransomware* fos la causa de la mort, ja que el seu estat de salut era molt delicat, es tracta d'una alerta seriosa del que podria arribar a succeir[53].

Els incidents de *ransomware* també tenen **un impacte de caire econòmic**. De fet, es calcula que les pèrdues econòmiques provocades pel temps d'inactivitat i per les tasques de recuperació dels sistemes afectats poden ser de, **com a mínim, 760.000 €** (suposant que no es paga cap rescat). Addicionalment, pot comportar costos en concepte de **sancions derivades de l'incompliment de la regulació en matèria de ciberseguretat**. A la UE, per exemple, els hospitals són instal·lacions crítiques que estan sotmeses a la Directiva NIS[54] i a l'RGPD[55], a més a més de la normativa complementària de cada estat, que poden comportar importants multes.

El cibercrim ha focalitzat els atacs de *ransomware* cap al sector sanitari ràpidament, però han trigat més per guanyar efectivitat.

Amb la pandèmia, ràpidament, el cibercrim es va adonar de com d'essencial era el sector sanitari i que esdevenia un objectiu especialment interessant pels atacs de *ransomware*. Tot just amb l'**esclat de la crisi sanitària**, el març de 2020, el nombre d'**atacs de *ransomware* contra hospitals va augmentar un 60%**. Afortunadament, el percentatge d'**atacs bloquejats també va créixer un 73%** respecte del mes amb més bloquejos de 2019. D'aquesta manera es va evitar una allau d'incidents[56]. Les mesures de seguretat van funcionar i es va evidenciar que **el cibercrim no estava gaire preparat** per aprofitar una situació

[49] *https://www.alreporter.com/2019/10/01/dch-health-system-closes-three-hospitals-to-al-but-critical-patients-after-ransomware-attack/*
[50] *https://digilience.org/cyber-news/hospital-hit-cyberattack-cancels-surgeries*
[51] *https://www.healthcareitnews.com/news/ransomware-attack-leaves-5-years-patient-records-inaccessible-co-hospital*
[52] *https://www.xataka.com/seguridad/ataque-ransomware-a-hospital-alemania-pudo-ser-causante-muerte-paciente*
[53] *https://www.wired.co.uk/article/ransomware-hospital-death-germany*
[54] *https://www.dsn.gob.es/es/actualidad/sala-prensa/publicacion-directiva-nis*
[55] *https://www.boe.es/boe_catalan/dias/2018/12/06/pdfs/BOE-A-2018-16673-C.pdf*
[56] *https://securityboulevard.com/2020/05/global-ransomware-and-cyberattacks-on-healthcare-spike-during-pandemic/*

imprevista com la pandèmia[57]: amb les presses, els atacs no aconseguien traspassar les **barreres *anti-ransomware***[58]. Ara bé, poc a poc, els atacs de *ransomware* **guanyaven efectivitat** i el nombre d'**incidents** va anar **a l'alça** (veure il·lustració 8). Així, en els moments més greus de la pandèmia, pràcticament **un de cada quatre incidents** de *ransomware* tenia lloc en el **sector sanitari** (veure il·lustració 9).

A l'Estat espanyol, el setembre de 2020, **el nombre d'atacs de *ransomware*** contra les entitats del **sector sanitari** va créixer un **160%,** per sobre de països com ara Alemanya (145%), el Regne Unit (80%) o França (36%)[59]. Nombrosos atacs aconseguien impactar severament hospitals i proveïdors. A Catalunya, per exemple, el setembre, un atac de *ransomware* va afectar els 14 centres del **Consorci Sanitari Integral**, incloent el seu **Hospital Moisès Broggi**, on els professionals es van veure obligats a treballar amb registres en paper[60].

Les xifres d'atacs han estat altes tot i que alguns **operadors de *ransomware* van anunciar que no atacarien el sector sanitari mentre no s'estabilitzés la situació**[61]. Tanmateix, aquesta mesura aparentment solidària amagava la voluntat d'**autoprotecció**, ja que si un ciberatac causava la pèrdua de vides humanes podria ser el detonant d'una **persecució internacional**[62].

El conjunt de la cadena de subministrament del sector sanitari ha estat un element essencial durant la pandèmia. I un objectiu prioritari del *ransomware*.

Al 2020, el sector sanitari ha estat el **sector més atacat amb *ransomware***, amb el **17,9% dels atacs** (el 2019 fou el segon sector)[63]. Però no només els hospitals són objectiu: **tot el sector sanitari està amenaçat**. El motiu és que, durant la pandèmia, un **incident** de *ransomware* en algun dels elements de la **cadena de subministrament** del sector sanitari **afecta la resta** i es magnifica el seu **impacte**.

Els incidents de *ransomware* han afectat tot tipus d'entitats i proveïdors de l'àmbit sanitari: **els laboratoris on es fan les proves per detectar pacients amb covid-19, les farmacèutiques que investiguen la malaltia, els fabricants de productes sanitaris, les empreses de logística encarregades de la distribució, etc**[64]. Així, al març de 2020, el centre d'investigació mèdica Hammersmith Medicine Research (Londres), era impactat amb el *ransomware* Maze en plena recerca d'una vacuna contra la covid-19, i, com que no es va fer efectiu el pagament del rescat, les dades de 2.300 pacients van ser publicades[65]. Poc després, al maig, el grup Fresenius, proveïdor de productes i serveis altament consumits i imprescindibles durant la pandèmia, i titular dels principals hospitals privats d'Europa, entre els quals QuironSalud, va ser víctima del *ransomware* Snake. Els ordinadors de diferents seus es van veure afectats, tot i que la companyia va afirmar que l'incident únicament va limitar algunes operacions[66].

[57] *https://healthitsecurity.com/news/ransomware-success-declines-amid-covid-19-but-resurgence-is-likely*
[58] *https://securityboulevard.com/2020/05/global-ransomware-and-cyberattacks-on-healthcare-spike-during-pandemic/*
[59] *https://www.itdigitalsecurity.es/actualidad/2020/10/aumentan-un-160-los-ataques-de-ransomware-en-espana-en-el-tercer-trimestre*
[60] *https://www.ccma.cat/324/el-ciberatac-contra-lhospital-moises-broggi-afecta-13-centres-sanitaris-mes/noticia/3044998/*
[61] *https://www.virsec.com/blog/maze-and-other-ransomware-groups-say-they-wont-attack-hospitals-during-covid19-outbreak-but-how-trustworthy-is-their-word*
[62] *https://www.forbes.com/sites/daveywinder/2020/03/19/coronavirus-pandemic-self-preservation-not-altruism-behind-no-more-healthcare-cyber-attacks-during-covid-19-crisis-promise/?sh=47b5206252be*
[63] *https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020*
[64] *https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus/*
[65] *https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus*
[66] *https://www.cybersecurity-insiders.com/fresenius-europe-hit-by-ransomware/*

La doble extorsió es tracta d'un ciberatac que constitueix el resultat de la combinació de dues modalitats: ciberatac de segrest de dades i la fuita o publicació de les dades.

L'RDP (Remote Desktop Protocol) és un protocol propietari desenvolupat per Microsoft que permet la comunicació en l'execució d'una aplicació entre una terminal i un servidor de qualsevol tecnologia. La configuració per defecte utilitza el port 3389 per a comunicar els terminals amb el servidor de destinació.

Una VPN (Virtual Private Network), o xarxa privada virtual, és una xarxa privada que s'estén, mitjançant un procés d'encapsulació, i en algun cas d'encriptació, dels paquets a diferents punts remots, fent ús d'infraestructures públiques de transport.

(font: Termcat)

La doble extorsió contra el sector sanitari es consolida, impulsada per la sensibilitat de les dades personals de pacients i la informació de recerca de la vacuna.

En els darrers anys, la **ciberdelinqüència** ha demostrat una gran capacitat d'**adaptació** a cada context, i aquest fet s'evidencia en els atacs de *ransomware*. El cas és que, després d'una tendència a l'alça continuada, l'**import mitjà dels rescats** de les víctimes de *ransomware* va començar a **baixar el darrer trimestre de 2020**, probablement per la negativa de les víctimes a pagar (veure il·lustració 10). Així, en resposta a aquesta circumstància, el cibercrim ha estat capaç de **trobar nous arguments de coacció** i ha nascut la tècnica d'atac anomenada doble extorsió: a més de xifrar els sistemes d'informació i exigir un rescat per recuperar-los, també **es roben dades i s'amenaça de fer-les públiques**. Sovint, per demostrar que l'amenaça de fer pública la informació robada és seriosa, se'n filtra una part per incrementar el nivell d'intimidació i de pressió.

El primer atac que va utilitzar la **doble extorsió** va ser el 2019 i, a final de 2020, aquesta tècnica ja ha format part del **70% dels atacs** de *ransomware*[67]. Aquesta tècnica és especialment **efectiva** en les **institucions sanitàries**, ja que disposen d'**informació confidencial** que no pot ser revelada, com **dades mèdiques dels pacients o informació de recerca** (per exemple, d'un tractament o vacuna per a la covid-19)[68]. Sense anar més lluny, la Universitat de Califòrnia (EUA), dedicada a la recerca de tractaments per a la covid-19, va ser atacada amb el *ransomware* Netwalker i va decidir realitzar el pagament d'1,14 M$ en *bitcoins* per poder recuperar les dades xifrades i evitar-ne la difusió pública[69] (veure il·lustració 10).

Els incidents amb doble extorsió han estat molt nombrosos. Només durant el setembre de 2020, diversos atacs de *ransomware* perpetrats per grups diferents van permetre robar dades de cinc entitats sanitàries dels EUA i Canadà. Com que no es van pagar els rescats, les dades dels pacients van acabar publicades a la *dark web*, a les webs dels ciberdelinqüents i a Twitter, i incloïen expedients mèdics, anàlisis, factures, etc[70].

Les connexions RDP i VPN, àmpliament desplegades per fer possible el teletreball durant la pandèmia, són la principal entrada del *ransomware* al sector sanitari.

El **70,3% dels atacs de *ransomware*** es realitza fent ús de **credencials d'accés obtingudes il·lícitament** i l'**explotació de vulnerabilitats** en les tecnologies de connexió remota RDP i VPN[71]. Aquest fet és molt rellevant, atès que la pandèmia ha impulsat el **teletreball** i el desplegament d'aquest tipus de connexions, sovint de manera **accelerada i sense fer ús de les mesures de seguretat adequades**. En aquests atacs, dirigits i orquestrats manualment, l'atacant penetra en els sistemes de les organitzacions per desplegar el *ransomware* i causar el més gran impacte possible.

Els ciberatacants ataquen les connexions RDP o VPN no actualitzades. En el cas dels **RDP**, exploten **vulnerabilitats** antigues com la BlueKeep (CVE-2019-0708[72]) o altres de més recents que permeten aconseguir l'accés mitjançant

[67] *https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020*
[68] *https://www.economiadehoy.es/el-ransomware-de-doble-extorsion-llega-a-los-hospitales-para-aprovecharse-del-covid19*
[69] *https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/#15e739d818a8*
[70] *https://healthitsecurity.com/news/ransomware-hacking-groups-post-data-from-5-healthcare-entities*
[71] *https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate*
[72] *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708*

Un atac de força bruta és un atac d'autenticació que consisteix a intentar totes les entrades possibles a un sistema fins a trobar la que desbloqueja l'accés..

(font: Termcat)

l'enviament de paquets elaborats (CVE-2020-0609[73] i CVE-2020-0610[74]), entre d'altres. En el cas de les **VPN**, s'explota un gran nombre de vulnerabilitats, de les quals cal destacar la que permet l'execució de codi en portals VPN de Citrix (CVE-2019-19781[75]) o l'obtenció de les contrasenyes en servidors VPN Pulse Secure (CVE-2019-11510[76]).

En altres casos, els ciberatacants fan ús de **credencials d'accés** obtingudes a través de ***phishing*** o atacs de força bruta[77]. Val a dir, però, que és habitual que els ciberdelinqüents que obtenen les credencials d'accés no siguin els que acaben realitzant l'atac de *ransomware*. Així, aquests ciberdelinqüents, una vegada han obtingut l'accés, n'ofereixen les **credencials al mercat negre**. Les credencials d'accés **RDP**, **Citrix** i **VPN** tenen un preu mitjà de **2.600 €**, però poden arribar fins als **116.000 €**, en funció de la víctima[78]. Tanmateix, cal destacar que el preu dels accessos RDP ha caigut fins a uns 13-20 € els darrers mesos. És un mal senyal, conseqüència de la gran quantitat de credencials RDP a la venda. L'explicació cal buscar-la en la proliferació del teletreball i les mesures més aviat pobres de ciberseguretat existents[79].

El programari maliciós distribuït a través de *phishing* és la segona via d'entrada del *ransomware* al sector sanitari.

En el **26,3% dels atacs de *ransomware***, es fa ús dels **correus de *phishing***[80] que, precisament, han augmentat de manera espectacular durant la pandèmia (veure capítol sobre *phishing*). En funció de la variant de *ransomware*, l'atac es desenvolupa d'una manera particular.

Per exemple, en les variants NetWalker i Avaddon, quan la víctima obre el fitxer adjunt maliciós, **es xifra el disc de l'equip** i rep el **missatge de reclam del rescat**[81]. En altres casos, com en les variants Mr. Robot o Philadelphia, **es convida la víctima a descarregar el fitxer maliciós a través d'un enllaç**. En aquest tipus d'atacs de *ransomware*, les quantitats reclamades com a rescat són sensiblement baixes i poden arribar a uns **700 €**[82]. El motiu és que, en principi, la infecció només **afecta l'ordinador de la víctima**, sempre i quan no aconsegueixi propagar-se a altres dispositius de la xarxa.

Altres atacs de via *phishing* comencen amb la **descàrrega d'un troià** que permet a l'atacant **comprometre la xarxa** de la víctima, moure's, guanyar privilegis i, finalment, desplegar el ***ransomware* allà on pugui causar més estralls**. En aquests atacs el cost del rescat és més elevat i supera **els 100 mil euros** de mitjana. Cal destacar el cas del **troià Emotet**, el qual ha estat el més difós entre els equips informàtics del sistema de salut del món, utilitzat com a porta d'entrada de diferents variants de *ransomware* com Ryuk, MegaCortex i BitPaymer, entre d'altres[83]. Afortunadament, el grup ciberdelinqüent que operava Emotet ha estat detingut gràcies a una operació policial internacional realitzada el gener de 2021. Tot apunta, doncs, que ja no podrà participar en la difusió de *ransomware* o qualsevol altre *malware*. Ara bé, l'amenaça persisteix, ja que hi ha altres troians similars, com Qbot, Trickbot o Dridex[84].

[73] *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0609*
[74] *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0610*
[75] *https://support.citrix.com/article/CTX267027*
[76] *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510*
[77] *https://threatpost.com/millions-brute-force-attacks-rdp/155324/*
[78] *https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover*
[79] *https://www.zdnet.com/article/the-price-of-stolen-remote-login-passwords-is-dropping-thats-a-bad-sign/*
[80] *https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate*
[81] *https://healthitsecurity.com/news/ransomware-attacks-delivered-via-phishing-campaigns-on-the-rise*
[82] *https://www.zdnet.com/article/ransomware-attacks-that-start-with-phishing-emails-are-suddenly-back-in-fashion-again/*
[83] *https://www.spamhaus.org/news/article/806/emotet-is-disrupted-but-the-malware-it-installed-lives-on*
[84] *https://www.zdnet.com/article/cybersecurity-this-costly-and-destructive-malware-is-the-most-prolific-threat-to-your-network/*

Recomanacions

- **Els responsables de TI han de vetllar per mantenir actualitzats els sistemes operatius i el programari, així com els *anti-malware* o antivirus amb els darrers patrons de codi maliciós.**
- **Els responsables de TI han de procurar dotar els terminals dels professionals de les millors eines de protecció, com EDR (*Endpoint and Response System*) per a la monitorització continuada d'amenaces cibernètiques.**
- **Els responsables de TI han de mantenir actualitzats i avaluar la seguretat dels accessos remots, en especial RDP, VPN i Citrix.**
- **Els administradors de sistemes, i si és possible tota la resta d'usuaris, han de disposar d'accessos amb doble factor d'autenticació.**
- **Les organitzacions han de disposar de còpies de seguretat actualitzades i fora de línia, per evitar que puguin ser xifrades per un *ransomware*.**
- **Les organitzacions han d'emmagatzemar les dades personals amb un xifratge segur per evitar que un intrús pugui robar-les en text pla.**
- **Les organitzacions han d'elaborar anàlisis de riscos identificant, especialment, els actius crítics i desplegant mesures de prevenció, protecció i resposta proporcionals**
- **Les organitzacions han de disposar d'un pla de continuïtat del negoci i un pla de recuperació de desastres, i han de validar que s'ha verificat el simulacre per a atacs *ransomware*.**
- **Les organitzacions han d'aproximar models de confiança zero amb la segregació dels serveis interns de la xarxa empresarial i disposar de protecció perimetral.**

Les fuites de dades personals i de recerca del sector sanitari tenen l'origen en ciberatacs, motivats per l'alt valor d'aquestes, i errors causats pel factor humà

Les dades personals de salut són fàcilment monetitzables al mercat negre i les dades de recerca sobre la covid-19 han esdevingut valuoses per al ciberespionatge. Així, el 67% de les fuites es deuen a ciberatacs i el 22%, a errors humans o accions malintencionades. L'impacte econòmic d'una fuita és més elevat en el sector sanitari que en qualsevol altre, i pot comportar importants sancions.

La diversitat de centres de salut, el desplegament de noves tecnologies i la creixent connectivitat fan que augmenti el risc d'exposició de dades. Així, el nombre d'incidents amb fuita de dades al sector sanitari creix any rere any, tot i que, el 2020, el volum d'informació personal exposada ha estat menor.

La informació del sector sanitari és valuosa: un perfil sanitari complet d'un pacient pot vendre's per un import d'entre 200 i 830 €, i les dades de recerca o propietat intel·lectual són un bé molt preuat pel ciberespionatge. En aquest sentit, la pandèmia ha disparat l'interès per la informació relacionada amb la recerca d'un tractament o una vacuna per a la covid-19.

El 2020, el 67% de les fuites de dades del sector sanitari han tingut l'origen en ciberatacs i, concretament, el 46%, en atacs de *ransomware*. El 22% de les fuites les han provocat errors humans i accions malintencionades dels propis treballadors.

El sector sanitari encara és el sector en què les fuites de dades tenen un major impacte econòmic. El 2020, cada fuita ha implicat un cost mitjà de 5,9 M€, un 10% més que el 2019. A més, les entitats s'arrisquen a fer front a sancions molt importants.

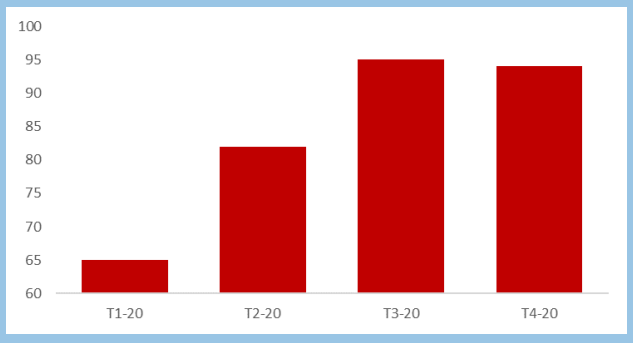
Aspectes clau:

- **La complexitat de l'ecosistema sanitari i la transformació digital comporten més informació digitalitzada, més connectivitat i un major risc de fuita de dades.**
- **Els ciberatacants busquen robar informació fàcilment monetitzable, com ara les dades personals mèdiques i les de recerca sobre la covid-19.**
- **Dues terceres parts de les fuites de dades al sector sanitari són causades per ciberatacs, entre els quals destaquen el *ransomware* amb doble extorsió i el *phishing*.**
- **Una de cada cinc fuites de dades al sector sanitari és fruit d'errors humans dels treballadors i poden combatre's amb plans de conscienciació.**
- **En una fuita de dades personals, les entitats del sector sanitari s'enfronten a costos milionaris en concepte de despeses de recuperació, pèrdua d'ingressos i sancions.**

Baròmetre

El nombre de fuites de dades s'incrementa arran de la declaració de la pandèmia

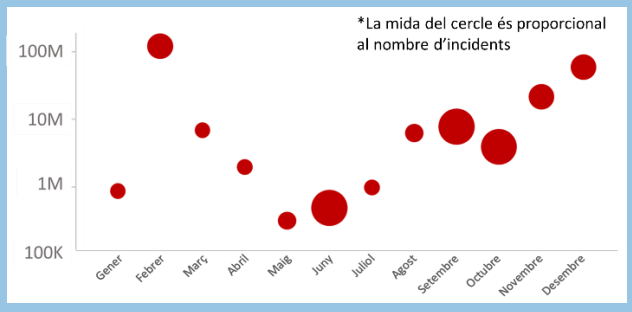
Amb l'inici de la pandèmia, el nombre d'incidents de fuita de dades al sector sanitari va créixer. El 2n trimestre de 2020, el nombre d'incidents ha resultat ser un 30% superior al 1r trimestre.



Il·lustració 12. Incidents de fuita de dades identificats als mitjans (Font: Agència).

Més fuites menors i alguns casos de rècord

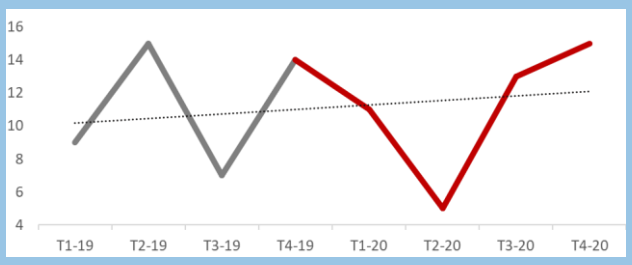
El 2020 hi ha hagut més fuites però menys registres de dades personals filtrats que no pas el 2019. No obstant això s'han donat algunes fuites de massives. Destaca, al febrer, l'exposició de 120 milions d'imatges mèdiques a l'Índia.



Il·lustració 13. Registres exposats al sector sanitari el 2020 (Font: Agència).

Dispositius perduts: un mal freqüent

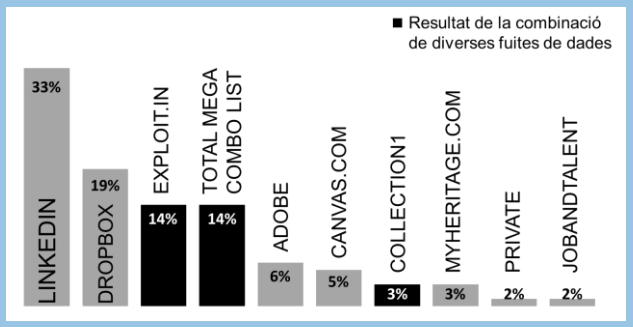
La pèrdua i el robatori dels dispositius dels professionals és una causa habitual dels incidents de fuita de dades al sector sanitari. A Catalunya, en el sistema sanitari públic, s'han perdut o robat de mitjana gairebé quatre dispositius cada mes. El nombre d'incidents va decaure coincidint amb període de confinament més intens durant el 2n trimestre de 2020.



Il·lustració 14. Incidents per pèrdua o robatori de dispositiu (Font: Agència)

L'origen de les credencials del sistema sanitari català, a la venda

L'abril de 2020, en una anàlisi de 201 fuites de dades diferents realitzat per l'Agència, s'identificaven 12.581 comptes corresponents a professionals del sector sanitari de Catalunya, amb un 58% de les entitats afectades. D'aquests comptes, un 40% feien ús de la mateixa contrasenya en diferents serveis, i el 26% venien acompanyats de la seva contrasenya corresponent en text pla. La fuita de LinkedIn va ser la que va tenir un major impacte, amb una tercera part de tots els comptes filtrats.



Il·lustració 15. Fuites de dades personals amb comptes de professionals del sector sanitari públic de Catalunya (Font: Agència).

Sancions econòmiques

Les tres sancions per RGPD més elevades a la UE estan relacionades amb la manca de mesures de protecció en les xarxes i sistemes d'informació. A l'Estat espanyol destaca la sanció al grup *HM Hospitales*, amb tres centres a Barcelona, pel fet de tractar les dades sense el consentiment dels pacients.

Il·lustració 16. Principals sancions a la UE per incompliment normatiu

Un registre és un conjunt de camps que contenen informació relativa a una persona o entitat.

La dark web, o web fosc, és la part del web profund allotjat en xarxes xifrades, superposades a Internet, que utilitzen l'anonimat per a l'intercanvi d'informació.

(font: Termcat)

La complexitat de l'ecosistema sanitari i la transformació digital comporten més informació digitalitzada, més connectivitat i un major risc de fuita de dades.

El **sistema sanitari** català és **heterogeni i complex**. Més de 70 centres hospitalaris, gairebé 400 equips d'atenció primària, un centenar de centres d'internament sociosanitari, quasi 40 centres de salut mental, 400 recursos de transport sanitari urgent i altres serveis sanitaris... Són, a més a més, de titularitat diversa: entitats de dret públic, societats mercantils, consorcis, fundacions, etc.

Per si aquesta complexitat no fos poca, el sector sanitari viu una **transformació digital accelerada**. Aquest fet impacta directament en un creixement del volum d'**informació mèdica digitalitzada** que és consultada per professionals de la salut i pacients. A més, precisament durant la pandèmia, la **compartició** de dades mèdiques s'ha accentuat, ja que l'RGPD flexibilitza el tractament de dades personals de salut sense el consentiment de l'interessat en situacions d'interès públic, com és la lluita contra la propagació del virus[85].

La diversitat d'entitats al sistema de salut, el volum de dades digitalitzades i l'elevada connectivitat eleven, cada vegada més, el risc de fuites de dades. En aquesta línia, a nivell global, any rere any, **el nombre de fuites d'informació va en augment**, i així **també** ha succeït **el 2020** (veure il·lustració 12). Segons les dades disponibles dels EUA, l'any 2020, el nombre de fuites d'informació notificades a les autoritats va ser un **25% superior respecte del 2019**, i un 100% respecte de 2014.

En canvi, el 2020, el **volum mitjà** de registres exposats per cada incident **s'ha reduït**[86]. El motiu es pot trobar en el fet que, arran de la situació generada per la covid-19, els ciberatacants han dedicat els seus esforços a buscar mecanismes d'atac més profitosos, com el *ransomware*, i això ha minvat la capacitat d'obtenir grans volums de dades.

No obstant això, el 2020 hi ha hagut **fuites de dades massives** (veure il·lustració 13). El febrer, a la Índia, s'identificava la fuita d'imatges mèdiques (ressonàncies magnètiques, raigs X, fotografies...) de **120 milions de pacients** a causa d'un servidor PACS (*Picture Archiving and Communications Systems*) insegur[87]. També, cal destacar la fuita de dades originada a partir d'un atac de *ransomware* contra Blackbaud, un proveïdor d'informàtica al núvol. Tot i que es va aconseguir aturar el xifratge de la informació, no es va evitar que els ciberatacants robessin les dades de **10 milions de pacients** de més d'una vintena d'entitats sanitàries dels EUA[88].

Els ciberatacants busquen robar informació fàcilment monetitzable, com les dades personals mèdiques i les de recerca sobre la covid-19.

La principal motivació del cibercrim és la cerca d'ingressos i, precisament, el robatori de **dades mèdiques** pot ser una activitat profitosa perquè aquestes poden ser **monetitzades** fàcilment. Aquestes dades poden consistir en **dades personals, expedients mèdics, registres sanitaris, resultats de proves de laboratori, diagnòstics, factures mèdiques, dades d'assegurances, comptes bancaris, assegurances, radiografies,** etc. Aquestes dades són

[85] *https://www.redaccionmedica.com/secciones/sanidad-hoy/coronavirus-la-proteccion-de-datos-supeditada-al-interes-de-parar-al-virus-6284*
[86] *https://www.hipaajournal.com/healthcare-data-breach-statistics/*
[87] *https://thelogicalindian.com/news/maharashtra-medical-data-leak-19603*
[88] *https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020*

L'EINSA és una agència de la Unió Europea creada amb l'objectiu de millorar les xarxes i la seguretat de la informació i contribuir al desenvolupament d'una cultura de xarxa i seguretat de la informació per al benefici dels ciutadans, consumidors, empreses i organitzacions del sector públic de la Unió Europea (EU).

posades a la venda a la *dark web*: un perfil sanitari complet pot arribar a costar **entre 200**[89] **i 830 euros**[90], unes **25 vegades més que el preu d'una targeta bancària**[91]. El motiu és que les dades mèdiques són especialment útils per perpetrar delictes de **suplantació d'identitat, frau financer o extorsió**, de manera que permeten l'obtenció d'importants beneficis. Un exemple: l'octubre de 2020, uns ciberdelinqüents van obtenir del centre de psicoteràpia Vastaamo (Finlàndia) les notes de les sessions d'uns 300 pacients, entre els quals s'hi trobaven personalitats polítiques (una política parlamentària) i menors d'edat. Els ciberdelinqüents van sol·licitar 450.000 euros a canvi de no publicar les dades robades però, com que el centre s'hi va negar, van procedir a extorsionar els pacients amb imports que anaven dels 200 als 500 euros per no fer pública la seva informació personal[92].

Els cibercriminals també van al darrere d'**informació de recerca, propietat intel·lectual o resultats de proves amb medicaments**, ja que poden tenir un gran **valor econòmic** i ser el resultat d'**anys de recerca i experiments costosos**. De fet, tot el món ha començat una carrera per trobar la resposta mèdica al virus SARS-CoV-2, i el cibercrim ha trobat un filó en el robatori i venda d'informació estratègica als estats. ENISA estima que, actualment, **el 38% dels actors cibercriminals estan connectats amb els estats**, i aquesta quantitat creix cada dia que passa[93]. Aquest fet es constata en la llarga relació d'**incidents i acusacions de ciberespionatge** que hi ha hagut durant la pandèmia, entre les quals destaca que el **CNI** va alertar d'atacs de ciberespionatge contra laboratoris de recerca sobre la covid-19[94]. Així mateix, el desembre de 2020, l'**Agència Europea del Medicament** (EMA) va confirmar que havia estat víctima d'un ciberatac. Els ciberdelinqüents havien tingut accés a un nombre limitat de documents amb informació de la vacuna desenvolupada per BioNTech i Pfizer. Es dona el cas que els ciberatacants van filtrar la informació robada, però abans la van manipular amb la intenció de generar desinformació i incentivar la desconfiança cap a les vacunes utilitzades a la UE i les seves institucions. Aquest fet va fer pensar que l'atac havia estat perpetrat per un grup de ciberdelinqüents patrocinat per un estat amb alguna rivalitat geopolítica amb la UE[95].

Poques vegades el **robatori d'informació sensible** té una motivació que no sigui econòmica. No obstant això, també es podria tractar d'un mecanisme per obtenir **visibilitat o emetre algun tipus de missatge polític**. En aquest sentit, en plena pandèmia de la covid-19, a Madrid es va detenir un noi de 16 anys per accedir a la base de dades sanitàries de la comunitat de Madrid. L'atacant va fer ostentació de la fita a les xarxes socials i va mostrar com un dels perfils als quals va tenir accés corresponia a un líder polític i parlamentari espanyol[96].

Dues terceres parts de les fuites de dades al sector sanitari són causades per ciberatacs, entre els quals destaquen el *ransomware* amb doble extorsió i el *phishing*.

El **67% de les fuites** de dades del 2020 al sector sanitari van estar causades per **ciberatacs**[97] i, concretament, el **46% per atacs de *ransomware***[98]. Tot i que la finalitat tradicional del *ransomware* és el xifrat de les dades, a finals de 2020,

[89] *https://www.securelink.com/blog/healthcare-data-new-prize-hackers/*
[90] *https://portswigger.net/daily-swig/coronavirus-fall-in-healthcare-data-breaches-could-be-due-to-pandemic-distraction*
[91] *https://www.rsa.com/en-us/blog/2020-08/diagnosing-the-cybersecurity-challenges-in-healthcare*
[92] *https://www.helpnetsecurity.com/2020/10/26/data-breach-psychotherapy-center/*
[93] *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage*
[94] *https://www.lavanguardia.com/politica/20200929/483759728569/cni-espera-mas-ciberataques-a-investigadores-de-la-covid-y-a-redes-domesticas.html*
[95] *https://www.infosecurity-magazine.com/news/leaked-covid19-vaccine-data/*
[96] *https://elpais.com/espana/2020-04-17/detenido-un-hacker-de-16-anos-que-pirateo-datos-medicos-de-un-politico-con-coronavirus.html*
[97] *https://www.hipaajournal.com/healthcare-data-breach-statistics/*
[98] *https://www.zdnet.com/article/ransomware-attacks-now-to-blame-for-half-of-healthcare-data-breaches/*

El còpia de seguretat, o backup, *és la còpia d'un fitxer o un conjunt de fitxers, generalment actualitzada periòdicament, que permet restaurar les dades originals en cas de pèrdua.*

(font: Termcat)

el robatori de dades i la **doble extorsió** eren utilitzats en un **70%** dels ciberatacs[99] (veure capítol sobre *ransomware*). Un dels casos més rellevants de 2020 fou l'atac de *ransomware* al centre sanitari Ventura Orthopedics (EUA) que, tot i que disposava de còpies de seguretat per recuperar la informació xifrada, va experimentar el greu robatori de les dades de 640.000 pacients[100]. Igual que li va passar a la companyia de serveis sanitaris Magellan Health[101] (EUA) que, en un atac de *ransomware*, va ser víctima del robatori dels registres de 365.000 pacients[102].

Els **atacs de *phishing*** també són l'origen de bona part de les fuites de dades del sector sanitari (veure capítol sobre *phishing*). Malauradament, **només cal que un empleat d'una organització introdueixi l'usuari i la contrasenya de correu electrònic en un lloc web de pesca de credencials** perquè el seu compte quedi compromès. Aleshores, l'atacant podrà accedir als correus electrònics, en els quals hi pot haver **dades sensibles**, o podrà fer ús de la bústia per **enviar *phishing*** a altres empleats de l'organització. En aquesta línia, la mútua assistencial Aetna (EUA) va viure una fuita dels registres sanitaris de prop de 500.000 clients perquè un treballador d'un soci comercial va ser víctima d'un atac de *phishing* i va lliurar les seves credencials a l'atacant. La conseqüència: una les fuites d'informació més grans de 2020 en el sector sanitari mundial[103].

Una de cada cinc fuites de dades al sector sanitari és fruit d'errors humans dels treballadors i poden combatre's amb plans de conscienciació.

El **22% de les fuites d'informació** tenen l'origen en accessos no autoritzats fruit d'**errors humans o de l'acció malintencionada de treballadors interns**[104]. No es tracta d'errors humans atribuïbles únicament als treballadors sanitaris. De fet, els responsables de sistemes i els mateixos proveïdors hi tenen una important responsabilitat.

Els casos de d'errors de ciberseguretat causats pel factor humà no són estranys entre els professionals sanitaris i constitueixen essencialment un símptoma d'una **manca de conscienciació**. Es tradueix en un conjunt de males pràctiques com ara el fet de **tractar les dades mèdiques de pacients fora dels sistemes d'informació centrals i sense xifrar**, amb el risc que per error puguin acabar en males mans. Si la informació s'emmagatzema en un dispositiu portàtil, aquest pot perdre's o ser robat, juntament amb totes les dades que contingui. A Catalunya, per exemple, el sistema sanitari públic experimenta **quatre incidents de pèrdua o robatori cada mes** (veure il·lustració 14).

Els errors humans també pot **ser responsabilitat d'un proveïdor** amb el qual hi hagi una col·laboració estreta. Destaca el cas del proveïdor de transport sanitari del Health Share (EUA), en el qual un treballador va ser víctima del robatori d'un ordinador amb dades personals de 654.000 pacients: el dispositiu no comptava amb un sistema de cadenat ni del xifratge de la informació del disc[105]. O és el cas de l'hospital Saint Josep Health i sis proveïdors de serveis sanitaris nord-americans, els quals van descobrir que part de la informació que s'havia encarregat de destruir de forma segura a un proveïdor extern es trobava

[99] *https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020*
[100] *https://www.databreaches.net/ventura-orthopedics-hit-by-ransomware-weeks-ago-some-patient-data-dumped/*
[101] *https://www.tfun.org/2020/05/13/ransomware-data-breach-follow-phishing-attack-at-magellan-health/*
[102] *https://healthitsecurity.com/news/magellan-health-data-breach-victim-tally-reaches-365k-patients*
[103] *https://www.spamtitan.com/blog/500000-record-healthcare-data-breach-highlights-risk-of-phishing-attacks/*
[104] *https://www.hipaajournal.com/healthcare-data-breach-statistics/*
[105] *https://www.zdnet.com/article/health-share-of-oregon-discloses-data-breach-theft-of-member-pii/*

L'amenaça interna és aquella que representen per a una entitat les persones que en formen part o que hi estan vinculades i que tenen accés a informació interna.

(font: Termcat)

en un abocador, a l'accés de qualsevol persona. Aquesta informació incloïa dades de pacients i treballadors des de 1995 fins a 2015[106].

En altres casos, la manca de conscienciació en ciberseguretat correspon als **responsables de TI**, que no configuren correctament **els accessos, el nivell de seguretat de les contrasenyes i la caducitat, el bloqueig automàtic de la sessió després d'un temps curt d'inactivitat de l'equip, el xifratge del disc dur dels ordinadors,** etc[107]. Precisament, a final de 2020, es van identificar 45 milions de fitxers amb radiografies i TAC emmagatzemades, accessibles des d'Internet, ja que es trobaven sense protecció en més de 2.000 servidors en 67 països diferents, inclosos alguns estats de la UE. Els servidors corresponien principalment a clíniques, però també professionals independents (dentistes, oftalmòlegs, etc.)[108,109]. En un altre exemple el Servei Públic de Gales, fruit d'un error humà, es va publicar un fitxer amb dades de més de 18.000 ciutadans que s'havien realitzat la prova de la covid-19. La informació permetia la identificació de les persones, va estar publicada 20 hores i va ser visualitzada 56 vegades[110]. També és destacable el cas de l'empresa Babylon Health, un proveïdor de consultes mèdiques a distància via missatges de text o vídeo que va admetre que alguns usuaris de la seva aplicació havien pogut accedir als vídeos enregistrats d'altres usuaris a causa d'un error de programació. Això sí, una vegada van identificar l'incident, es va resoldre en només dues hores[111].

Altres fuites d'informació són causades per **accions intencionades,** perpetrades per **treballadors interns** (la coneguda com amenaça interna). La condició privilegiada de què disposa un treballador intern representa una autèntica amenaça**: lliure mobilitat per àrees restringides, accés legítim que el fa invisible als sistemes de detecció d'intrusos, coneixement de la configuració de la xarxa i les seves vulnerabilitats,** etc. El treballador intern o *insider*, habitualment, mira de robar informació a través de **dispositius d'emmagatzematge extern, en fa una còpia al núvol** o **l'envia a un compte de correu particular**. Pel que fa al motiu pel qual un treballador intern pot decidir actuar contra la pròpia organització, novament, cal parlar de voluntat econòmica, ja que se li pot presentar la possibilitat de vendre aquestes dades. No obstant això, el motiu també pot ser la venjança: perquè la relació laboral no és bona, potser fruit d'un acomiadament. Això és el que li va passar a Stradis Healthcare, un proveïdor de material quirúrgic que, en el pic de la pandèmia i amb una alta demanda de producció, va descobrir com un alt càrrec directiu, després de ser acomiadat, va conservar un compte secret que va utilitzar per accedir, manipular i, fins i tot esborrar, dades dels enviaments[112].

En una fuita de dades personals, les entitats del sector sanitari s'enfronten a costos milionaris en concepte de despeses de recuperació, pèrdua d'ingressos i sancions.

El 2020, una **fuita de dades** en una entitat del sector sanitari ha tingut un cost mitjà de **5,9 M€**, en concepte de **despeses de recuperació i altres pèrdues d'ingressos que poden dilatar-se en el temps**. Representa un **10% d'increment** respecte del 2019 i significa que el sector sanitari segueix sent el sector on les fuites de dades tenen un major impacte econòmic[113].

[106] *https://www.beckershospitalreview.com/cybersecurity/saint-joseph-health-6-more-indiana-providers-report-improper-disposal-of-patient-records.html*
[107] *https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion_del_puesto_de_trabajo.pdf*
[108] *https://www.welivesecurity.com/2020/12/15/medical-scans-exposed-online/*
[109] *https://cybelangel.com/medical-data-breaches/*
[110] *https://www.digitalhealth.net/2020/09/public-health-wales-data-breach-covid-19/*
[111] *https://www.digitalhealth.net/2020/06/babylon-admits-software-error-led-to-data-breach-of-gp-at-hand/*
[112] *https://www.bankinfosecurity.com/prosecutors-insider-sabotaged-medical-equipment-shipments-a-14172*
[113] *https://www.fiercehealthcare.com/tech/average-cost-healthcare-data-breach-rises-to-7-1m-according-to-ibm-report*

Addicionalment, si es demostra que s'ha posat en risc la privadesa dels pacients, les entitats poden haver de fer front a **multes importants**. El fet és que l'**RGPD** obliga als centres de salut a fer una avaluació per **conèixer els riscos** als quals estan subjectes les dades personals i **adoptar mesures** de seguretat per a protegir-les. A més, la normativa és clara en establir que, en cas de produir-se un incident que pugui afectar els drets i llibertats de les persones, cal informar-ne les autoritats competents en un termini màxim de **72 hores**. Entre altres aspectes, exigeix als centres de salut comptar amb un **Delegat de Protecció de Dades** que ha d'informar i assessorar els responsables del tractament de les dades sobre les obligacions normatives[114].

A l'Estat espanyol, la **LOPDGDD** (*Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales*) complementa l'RGPD. Estableix sancions administratives que imposa l'*Agencia Española de Protección de Datos* (AEPD) que, per a les infraccions molt greus, poden arribar a ser de **fins a 20 M€** o, en el cas de les empreses, fins al **4% del volum de facturació anual**[115]. A l'Estat espanyol, aquest 2020, l'AEPD ha imposat una multa de 48.000 € a l'empresa HM Hospitales, amb tres centres a Barcelona, per no obtenir degudament el consentiment explícit d'un pacient a l'hora de tractar les seves dades personals[116] (veure il·lustració 16). En l'àmbit europeu, el 2018 hi va haver la primera multa per incompliment de l'RGPD a l'Hospital Barreiro de Portugal, el qual va ser sancionat amb 400.000 € per permetre als metges de l'hospital accedir a l'historial clínic dels pacients sense controls ni restriccions[117]. El 2019, l'Hospital Haga dels Països Baixos va ser sancionat amb 460.000 € per no tenir en ordre la seguretat dels registres dels pacients[118]. Tot i això, aquestes sancions encara estan per sota de les imposades als EUA per incompliment de l'HIPAA (*Health Insurance Portability and Accountability Act*); el 2020, la comunitat de centres de salut de LifeSpan Health System va rebre una multa d'1 M€ pel robatori d'un portàtil que contenia dades de 20.000 pacients[119].

Recomanacions

- **Els usuaris del sistema de salut han de ser conscients de les finalitats i en quines condicions es poden utilitzar les seves dades personals, i quins drets poden exercir (veure la Guia de protecció de dades per a pacients i persones usuàries dels serveis de salut de l'APDCAT).**
- **Els professionals sanitaris han d'evitar extreure les dades dels pacients dels sistemes centrals i emmagatzemar-les en altres suports, especialment sense xifratge.**
- **Els responsables de sistemes han de realitzar auditories de seguretat periòdiques quan es realitzin canvis en els sistemes o en l'arquitectura, per evitar la informació exposada per errors de configuració.**
- **Els responsables sistemes han garantir les bones pràctiques i les mesures de protecció de la informació al núvol (veure el document Ciberseguretat al núvol per a serveis sanitaris d'ENISA).**

[114] *https://apdcat.gencat.cat/web/.content/03-documentacio/documents/Guia-proteccio-de-dades-pacient.pdf*
[115] *https://www.ambit-bst.com/blog/todo-lo-que-necesitas-saber-para-cumplir-la-rgpd-en-el-sector-salud*
[116] *https://rgpdblog.com/la-agencia-espanola-de-proteccion-de-datos-aepd-impone-una-multa-de-48-000-euros-a-un-hospital-por-infraccion-del-rgpd/*
[117] *https://rgpdblog.com/primera-multa-por-infraccion-del-rgpd-en-portugal-400-000-euros/*
[118] *https://www.careersinfosecurity.asia/patient-record-snooping-incident-leads-to-gdpr-fine-a-12797*
[119] *https://www.careersinfosecurity.com/lifespan-health-system-hit-1-million-hipaa-fine-a-14714#:~:text=Federal%20regulators%20have%20slapped%20the,the%20data%20of%2020%2C000%20individuals.*

- **Les organitzacions han d'elaborar i desplegar un pla de compliment normatiu proactiu, identificant els marcs reguladors interns i externs aplicables, aplicant les directrius i normes emeses i avaluant periòdicament el nivell de compliment.**
- **Les organitzacions, en cas de produir-se un incident que pugui afectar els drets i les llibertats de les persones, han d'informar l'autoritat competent en un termini màxim de 72 hores.**
- **Les organitzacions han de realitzar un Estudi d'Impacte de Protecció de dades (EIPD), en el qual s'analitzin els riscos i s'estableixin mesures de protecció adequades per garantir al seguretat i la privacitat de les dades.**
- **Les organitzacions han d'emmagatzemar les dades personals amb xifratge segur per evitar que un intrús pugui robar la informació en text pla.**
- **Les organitzacions han de fer ús de la pseudonominització (veure Tècniques i millors pràctiques per a la pseudonominització d'ENISA).**
- **Els centres de salut han de comptar amb un Delegat de Protecció de Dades que, entre altres obligacions, ha d'informar i assessorar els responsables del tractament de les dades sobre les obligacions normatives.**
- **Les organitzacions han de considerar els conflictes d'interoperabilitat entre sistemes que puguin suposar problemes per a la seguretat de la informació.**
- **Les organitzacions han de disposar de protocols d'actuació en cas de pèrdua o robatori d'un dispositiu.**

Les tecnologies d'e-salut proliferen i la ciberseguretat en el sector sanitari esdevé indispensable per garantir la salut dels pacients

La pandèmia ha impulsat les tecnologies d'e-salut, entre elles l'IoHT i l'm-salut, les quals poden presentar vulnerabilitats a causa de la falta d'actualitzacions. Mantenir al dia la diversitat de programaris d'IoHT i els dispositius antics esdevé molt complex. Una vulnerabilitat pot afectar la privacitat de les dades dels pacients, la qualitat d'un tractament o ser l'origen d'un ciberatac. La UE ha establert un paquet regulador per als dispositius tecnològics sanitaris.

La pandèmia ha impulsat les tecnologies d'e-salut (*eHealth*) per a la telemedicina, la gestió unificada de la informació i el control eficient de la malaltia. Una de les amenaces més habituals en els dispositius d'e-salut és la manca d'actualitzacions que facilita l'aparició de vulnerabilitats.

Els IoHT (*Internet of Healthcare Things*) són el 8% dels dispositius connectats als centres mèdics, però mantenir actualitzat un parc de sistemes operatius tan variat és complex. Els dispositius més cars tendeixen a tenir una vida més llarga, però a partir dels 10 anys poden considerar-se obsolets perquè el proveïdor ja no en dona suport o no han rebut les actualitzacions pertinents. Les vulnerabilitats poden tenir conseqüències greus: afectar la privacitat de les dades sensibles dels pacients, degradar la qualitat d'un tractament i, fins i tot, ser explotades per dur a terme un ciberatac.

La UE té la voluntat de garantir que els dispositius sanitaris comercialitzats als estats membres siguin adequats per fer front als riscos de ciberseguretat. Les normes MDR i IVDR situen la ciberseguretat com un aspecte a tenir en compte durant tot el cicle de vida dels dispositius. La Directiva NIS i l'RGPD també són rellevants per a la ciberseguretat dels dispositius mèdics.

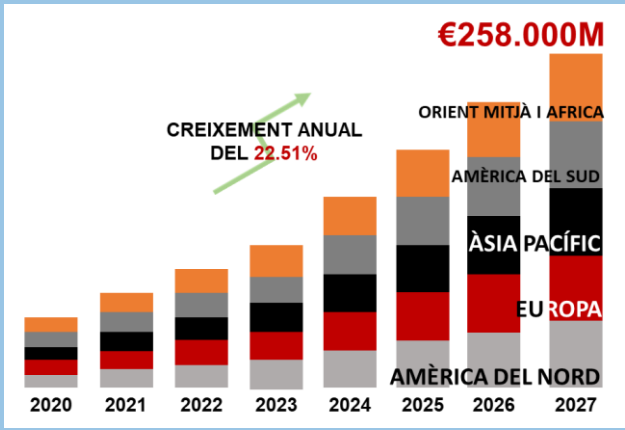
Aspectes clau:

- **La covid-19 impulsa les tecnologies d'e-salut en matèria d'assistència a distància, connectivitat per a l'atenció dels malalts i control de la pandèmia amb dispositius mòbils.**
- **La proliferació i la diversitat de dispositius mèdics amb connectivitat comporta dificultats d'actualització, un risc per a la ciberseguretat.**
- **Les vulnerabilitats d'e-salut poden permetre a un ciberatacant accedir a dades sensibles i afectar la qualitat dels tractaments. Cal resoldre-les tot garantint les funcionalitats.**
- **La UE prepara un espai comú en el qual el desplegament dels dispositius d'e-salut es realitzi respectant la ciberseguretat i la privacitat dels pacients.**

Baròmetre

El mercat de les tecnologies d'e-salut creix un 22,51% cada any

La transformació digital al sector sanitari es constata en l'evolució a l'alça del mercat de les tecnologies d'e-salut, el qual preveu un creixement anual del 22,51% i que arribi als 258.000 M€ (aproximadament un 10% superior al PIB de Catalunya) el 2027.



Il·lustració 17. Projecció del mercat dels dispositius mèdics[120].

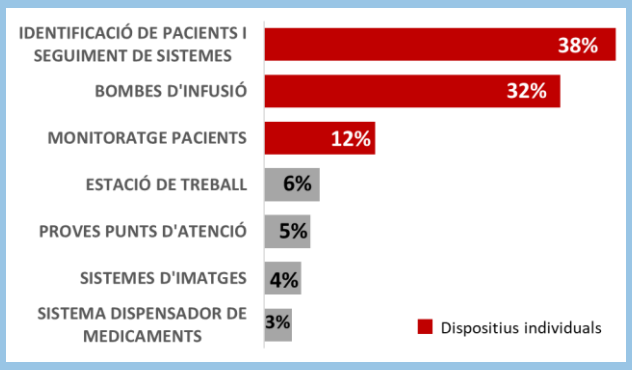
Els dispositius IoHT són imprescindibles pel futur del sector

La transformació digital del sector és imparable, un fet que s'evidencia en el desplegament de dispositius IoT sanitaris (IoHT). Un estudi indica que el 89% de les entitats sanitàries ja han adoptat algun IoHT. Un 87% d'aquestes entitats veu essencial la seva adopció per al futur del tractament dels pacients, tot i que només un 58% tenen previst incorporar nous IoHT durant els pròxims dos anys. En qualsevol cas, queda molt clar que l'adopció dels IoHT és una realitat present i futura que no genera dubtes.

Il·lustració 18. Estadístiques d'adopció d'IoHT a les entitats sanitàries[121].

Els dispositius IoHT individuals amb connectivitat són, amb escreix, els més nombrosos

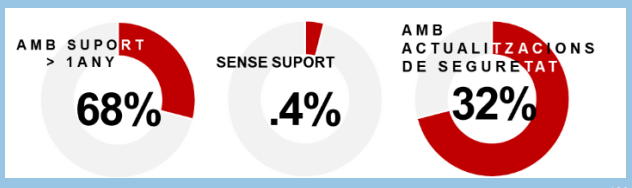
Els dispositius IoHT més nombrosos són aquells utilitzats en el tractament individual dels pacients. Són els dispositius d'identificació i seguiment, les bombes d'infusió i els dispositius per a la monitorització dels pacients, i conformen el 82% dels IoHT. La proporció d'aquests amb els pacients és 1:1 i seguiran proliferant.



Il·lustració 19. Tipus de dispositius d'e-salut connectats més habituals[122].

Els sistemes heretats (*legacy*) són un risc per a la seguretat

Un dels problemes més grans per a la ciberseguretat de l'e-salut és l'existència de sistemes heretats o *legacy*. Són sistemes en ús, però que es consideren obsolets perquè ja no reben un manteniment ni actualitzacions. Destaca el cas dels equips amb Windows (el sistema operatiu del 59% dels dispositius sanitaris). Mentre que el 68% tindrà suport garantit durant més d'un any, el 32% restant funciona amb versions de Windows antigues, amb actualitzacions excepcionals i ampliacions de seguretat (*Extended Security Updates*). Així, la tercera part dels dispositius amb Windows passaran a ser sistemes *legacy* ben aviat.



Il·lustració 20. Suport dels dispositius amb SO Windows[123]

[120] https://www.databridgemarketresearch.com/reports/global-ehealth-market
[121] https://www.forbes.com/sites/louiscolumbus/2020/10/12/10-insights-from-microsofts-latest-iot-signals-report/
[122] https://www.forescout.com/company/blog/device-security-is-critical-in-protecting-patient-data-and-keeping-patients-safe/
[123] https://www.forescout.com/connected-medical-device-security-report/

La e-salut, o eHealth*, és l'ús eficient i segur de tecnologies de la informació i comunicacions en l'activitat del sector sanitari, com els serveis d'atenció de la salut, la monitorització contínua, la vigilància, la documentació sanitària, l'educació, l'intercanvi de coneixement i la recerca. Engloba els sistemes d'història clínica electrònica i el* big data*, la telemedicina, les apps mòbils, els dispositius mòbils per a la monitorització, l'IoHT, les tecnologies d'estandardització i interoperabilitat entre tecnologies...*

La IoT o Internet de les coses és la xarxa formada per un conjunt d'objectes connectats a internet que es poden comunicar entre si i també amb humans, i així transmetre i tractar dades amb intervenció humana o sense.

(font: Termcat)

L'm-salut, o mHealth*, és l`ús de telèfons i tecnologia mòbil per pràctiques mediques i de salut publica per gestionar i monitorar la salut de les persones.*

La covid-19 impulsa les tecnologies d'e-salut en matèria d'assistència a distància, connectivitat per a l'atenció dels malalts i control de la pandèmia amb dispositius mòbils.

Cada vegada més, la medicina fa ús de **noves tecnologies i de comunicacions electròniques**; és el que s'anomena e-salut. S'estima que el seu mercat global **creixerà un 22,51%** anual fins al 2027 (veure figura 17), ja que, a mesura que la tecnologia ha anat avançant i ha crescut la consciència per a la salut de les persones, sorgeixen noves oportunitats per desenvolupar les solucions d'e-salut. Tot i això, **la pandèmia de la covid-19 ha esdevingut l'impuls definitiu**.

Els centres mèdics s'han vist obligats a fer ús de la **telemedicina** per atendre i fer **seguiment a distància** dels pacients per tal d'**evitar els desplaçaments** i el **col·lapse dels centres sanitaris**. A Catalunya, abans de la pandèmia, el 89% de les persones realitzaven les consultes a la sanitat pública de forma presencial i, el setembre de 2020, només un 30%[124]. Aquest fet ha estat possible gràcies a l'ús de sistemes d'atenció mèdica per mitjans com el telèfon, el WhatsApp o les videotrucades[125].

La tecnologia IoT, que aplicada a la salut s'anomena **IoHT** (*Internet of Health Things*), ha esdevingut clau en la **recollida de dades** dels pacients en **temps real** durant la ràpida evolució de la covid-19. De fet, a **cada llit d'hospital**, s'hi poden trobar instal·lats diversos **dispositius de control mèdic amb connectivitat de xarxa** (respiradors, control arterial, nivell d'oxigen a la sang, pressió de la sang, anticoagulants, etc.), un fet que permet l'**enfocament intel·ligent del servei** i la **presa de decisions** més precisa i eficaç. La UCI intel·ligent inaugurada a l'Hospital Universitari Vall d'Hebron n'és un exemple: està equipada amb la tecnologia més avançada i connectada a un programa que integra totes les dades clíniques i de seguretat del pacient. Fent ús d'un programari pioner a l'Estat espanyol, les dades clíniques que genera l'equipament mèdic (per exemple, la pressió arterial dels pacients) o que provenen de la història clínica (analítiques), es combinen amb les dades relatives a seguretat (informació del llit, respiradors) i s'integren, en temps real, a un sistema de control central[126].

L'm-salut (*mHealth*) ha demostrat un enorme potencial per **canviar la manera de proveir els serveis sanitaris** a través dels **dispositius mòbils**. Ja se sabia que era útil per a la **monitorització en temps real i remot** de malalties cròniques com la diabetis o les malalties cardíaques, l'atenció de persones que viuen en àrees aïllades o que pateixen problemes de mobilitat. Però la novetat és que, arran de la covid-19, han nascut de les ***apps* de rastreig de la malaltia per a dispositius mòbils**. Aquestes *apps* permeten que les autoritats puguin identificar i alertar quan algú ha estat a prop d'un malalt diagnosticat com a positiu i, al mateix temps, supervisar l'evolució de la propagació del virus. És el cas de l'*app* **STOP COVID19 CAT**, destinada a fer vigilància dels casos de coronavirus a partir de les dades enviades pel ciutadà i, si s'escau, activar els serveis del centre d'atenció primària o els serveis d'emergències mèdiques[127]. Molts països han publicat la seva pròpia *app*, però el fet que hagin estat elaborades i publicades a contrarellotge ha facilitat que, en alguns casos, no s'hagin avaluat adequadament des del punt de vista de la ciberseguretat. Sense anar gaire lluny, a les Illes Balears, es va publicar l'*app* CliniCovery per autoavaluar-se i recollir dades de salut, però s'hi va detectar una vulnerabilitat a

[124] *https://www.lavanguardia.com/vivo/lifestyle/20201013/483933849024/telemedicina-casos-tratar-distancia.html*
[125] *https://catsalut.gencat.cat/ca/serveis-sanitaris/atencio-telefonica-linia/*
[126] *https://www.lavanguardia.com/local/barcelones-nord/20180912/451781985346/lhospital-vall-dhebron-estrena-una-uci-intelligent-amb-56-boxes-la-mes-gran-de-lestat-espanyol.html*
[127] *https://canalsalut.gencat.cat/ca/salut-a-z/c/coronavirus-2019-ncov/stop-covid19-cat/*

La segmentació és una tècnica per la qual una xarxa se subdivideix en múltiples subxarxes amb l'objectiu de millorar la seguretat i evitar la propagació d'una amenaça.

Un pegat és un fitxer que conté una o diverses modificacions d'un programa destinades a corregir-ne un error, a incorporar-hi funcions noves o a actualitzar-lo.

(Font: Termcat)

través de la qual es podia accedir a les dades dels usuaris sense necessitat de coneixements excessivament avançats[128].

La proliferació i la diversitat de dispositius mèdics amb connectivitat comporta dificultats d'actualització, un risc per a la ciberseguretat.

En el sector sanitari, hi ha un gran nombre de **dispositius connectats**. Aproximadament, un 53% són equips informàtics com ara ordinadors personals, servidors, clients virtuals, etc. El 39% són dispositius IoT com ara telèfons VoIP, dispositius mòbils, tauletes, dispositius de videoconferències, càmeres, etc. El **8%** són **dispositius que garanteixen l'activitat dels centres sanitaris, com ara els IoHT, l'aire condicionat, generadors elèctrics, càmeres de seguretat**, etc[129]. A dia d'avui, es constata com els **IoHT** constitueixen una **part petita** de tots els equips connectats, però la **previsió és que cada vegada n'hi hagi més**. La tendència és que s'incorporin més IoHT de seguiment i control per a cada llit, amb l'objectiu de **millorar l'atenció a cada pacient**. En canvi, els dispositius mèdics d'ús compartit, com els de diagnòstic, proves de laboratori o imatge mèdica, tendiran a créixer menys (veure il·lustració 19).

La incorporació de **tecnologies amb connectivitat** en el sector sanitari aporta **avantatges** inqüestionables, però també planteja importants **reptes en l'àmbit de la ciberseguretat**. En un ecosistema sanitari que s'assembla cada vegada més a un entorn TI pel nombre de dispositius electrònics connectats, cal plantejar que els elements de l'e-salut s'administrin de forma similar. Així, cal que siguin **dissenyats, configurats i mantinguts** tenint en compte criteris de **ciberseguretat i la privacitat** dels pacients.

En la mateixa xarxa d'un centre sanitari s'hi poden trobar dispositius amb sistemes operatius Windows, distribucions de Linux o *firmwares* diversos, i **mantenir actualitzat un parc de programaris tan variat esdevé francament complex**. De fet, quan l'actualització dels sistemes no s'ha realitzat adequadament **apareixen els sistemes heretats (*legacy*)**, o sigui, sistemes que essencialment estan desactualitzats. Tot i que encara resultin ser operatius, suposen un problema en matèria de ciberseguretat, ja que poden ser **vulnerables**. Sovint, localitzar aquests dispositius heretats d'entre tots els elements connectats és una tasca inassolible, ja que alguns només s'activen esporàdicament. Per tant, cal assumir la necessitat de segmentar la xarxa dels centres hospitalaris per tal que els dispositius potencialment vulnerables no puguin interferir en les parts de la xarxa on hi ha els elements més crítics[130].

Els dispositius sanitaris cars i que tendeixen a tenir una vida llarga acaben quedant obsolets i esdevenen un risc per a la ciberseguretat.

Els **dispositius de diagnòstic, proves de laboratori o imatge mèdica són els dispositius més cars** i, per aquest motiu, tendeixen a tenir una **vida llarga**. Quan la seva vida ronda els **10 anys i segueixen funcionant**, es pot afirmar que s'han convertit en **dispositius heretats**, ja que compleixen la seva funció però són obsolets perquè probablement no disposin dels darrers pegats i actualitzacions del fabricant. En termes de ciberseguretat, és força preocupant

[128] *http://www.caib.es/pidip2front/jsp/es/ficha-convocatoria/strongspan-stylecolor1c697dcovid-19nbspspanstrongel-servicio-de-salud-pide-la-desactivacioacuten-de-la-app-de-covid-19-ofrecida-por-clinicovery*
[129] *https://www.forescout.com/wp-content/uploads/2019/05/forescout-healthcare-report.pdf*
[130] *https://www.opencloudfactory.com/segmentacion-red-respuesta-incidencias/?cn-reloaded=1*

constatar que **el nombre de dispositius de més de 10 anys d'antiguitat és força important**. A Catalunya, amb dades de 2019, el 54% dels equips de monitorització, el 51% dels equips de radiologia i el 39% dels equips de ressonància magnètica, eren dispositius amb més de 10 anys d'antiguitat[131].

L'**obsolescència** es pot deure al fet que **el proveïdor ha deixat de donar suport a les actualitzacions del programari**. És el cas dels dispositius que fan ús del sistema operatiu Windows, utilitzat en el 59% dels dispositius sanitaris, dels quals el 32% està funcionant amb actualitzacions de seguretat com a suport excepcional (veure il·lustració 20). Un cas particular és el **Windows 7**, que va néixer el 2009 i **el gener de 2020 Microsoft va deixar de donar-hi suport**. Aquest fet ha esdevingut especialment crític al sistema sanitari, ja que actualment **diversos sistemes** se sostenen sobre aquest sistema operatiu i han quedat **desactualitzats**. De fet, com a exemple, als EUA, el 83% de les màquines d'imatge mèdica han quedat sense suport o sense noves actualitzacions[132].

En altres casos, l'obsolescència té l'origen en el fet que **no s'han aplicat les actualitzacions** pertinents. Sovint, el motiu és que **alguns sistemes crítics o d'alt rendiment no es poden aturar** per tal de ser actualitzats o pel fet que, després d'una actualització, sempre hi ha el **risc que deixin de funcionar correctament**. En altres casos, **no es disposa d'un servei de manteniment del fabricant contractat** com a mesura d'estalvi, però el fet és que sovint no es pot realitzar l'actualització del programari per compte propi si no vol perdre la garantia del seu funcionament correcte.

La security-by-design és l'enfocament que promou la necessitat de tenir en compte els criteris de ciberseguretat i privacitat des del mateix moment que es dissenya un programari o maquinari.

La criptomineria furtiva és una pràctica fraudulenta consistent a utilitzar la capacitat de càlcul computacional d'un dispositiu aliè per a fer criptomineria sense el coneixement del propietari.

(Font: Termcat)

Les vulnerabilitats d'e-salut poden permetre a un ciberatacant accedir a dades sensibles i afectar la qualitat dels tractaments. Cal resoldre-les tot garantint-ne les funcionalitats.

Tradicionalment **la ciberseguretat no s'ha tingut en compte en el disseny dels dispositius sanitaris**. De fet, les vulnerabilitats més habituals en els dispositius d'e-salut es deuen a aspectes intrínsecs al seu disseny, com l'ús de **contrasenyes febles, l'ús de de protocols de comunicacions no segurs i la manca d'actualitzacions**. Tot i que els fabricants de dispositius sanitaris cada vegada tenen més en compte la producció amb criteris de *security-by-design*, contínuament apareixen **vulnerabilitats** que afecten milions de dispositius mèdics. Es tracta d'una qüestió essencial, ja que l'entorn sanitari és crític i que les vulnerabilitats en l'e-salut poden ser **explotades per un ciberatacant** i derivar en conseqüències especialment greus.

En un **centre hospitalari**, un ciberatacant podria **explotar la vulnerabilitat** d'un dispositiu per **obtenir-ne el control, modificar la configuració i alterar-ne el funcionament, capturar dades o modificar-les, desplegar un programari maliciós,** etc. Destaca el cas de la **vulnerabilitat Bluekeep** (CVE-2019-0708), identificada el 2019 i que afecta els sistemes operatius Windows 7 i altres versions més antigues, la qual permet a un ciberatacant executar codis maliciosos de forma remota. Segons un estudi, el **45% dels dispositius mèdics dels hospitals no han estat actualitzats** i serien vulnerables[133]. S'ha emprat, per exemple, per infectar els dispositius amb *malware* de criptomineria furtiva[134]. Val a dir, però, que no es tracta d'un cas aïllat. El desembre de 2020, l'Agència va emetre un butlletí de seguretat en què es feia ressò de la **vulnerabilitat**

[131] *https://www.fenin.es/documents/document/675*
[132] *https://www.wired.com/story/most-medical-imaging-devices-run-outdated-operating-systems/*
[133] *https://healthitsecurity.com/news/45-connected-medical-devices-vulnerable-to-bluekeep-exploit*
[134] *https://healthitsecurity.com/news/microsoft-warns-bluekeep-rdp-flaw-attacks-will-increase-urges-patch*

CVE-2020-25179, la qual afecta una **llarga llista de sistemes d'imatges per TC, raigs X i ressonància magnètica** fabricats per GE Healthcare. En aquest cas, les credencials codificades de GE per a l'administració remota es podien trobar en línia, de manera que un atacant podia utilitzar-les per capturar dades confidencials, afectar la disponibilitat del sistema o manipular-lo[135].

Més enllà de les **vulnerabilitats** dels dispositius dels centres hospitalaris, també cal destacar aquelles que es troben en els **dispositius mèdics personals**. La realitat és força diferent, ja que són dispositius **que el pacient porta a sobre** i als quals és ell mateix qui ha de **fer les actualitzacions pel seu compte** o fer-les **presencialment a un centre mèdic**. En aquest sentit, el 2020 es va notificar la vulnerabilitat en la comunicació *bluetooth* anomenada 'SweynTooth', que possibilitava l'**aturada o l'accés** a les funcions de dispositius com ara **marca-passos, monitors de glucosa o dispositius d'ultrasò, per part d'un ciberatacant**[136]. Així mateix, Medtronic, un proveïdor de dispositius sanitaris, a final de 2020, informava de diferents vulnerabilitats que permetien a un atacant **obtenir el control** d'un determinat aparell de **marcapassos** via *bluetooth* i, poc abans, el 2019, havia informat d'una vulnerabilitat similar en dues de les seves **bombes d'insulina**[137]. I un altre exemple és el cas del *firmware* i del portal web per a l'administració de les **bombes d'infusió** del fabricant BD, els quals presentaven una vulnerabilitat que permetia que un atacant pogués **instal·lar programari maliciós**[138].

A tot això, cal destacar que l'actualització dels dispositius sanitaris i la instal·lació de pegats no són l'única preocupació. Especialment en el sector sanitari, després de qualsevol actualització o pegat, cal **assegurar-se que els dispositius mantenen les especificacions** i que **no es produeix cap mal funcionament que pugui impactar en els pacients**.

La UE prepara un espai comú en què el desplegament de dispositius d'e-salut es realitzi respectant la ciberseguretat i la privacitat dels pacients.

El nombre de dispositius d'e-salut prolifera sense parar. Actualment, es calcula que hi ha més de **500.000 tipus de dispositius sanitaris al mercat de la UE**: màquines de raigs X, marcapassos, aplicacions de programari, mesuradors de sucre a la sang, etc[139]. Aquests dispositius mereixen una atenció acurada, ja que una fallada de ciberseguretat podria afectar la privacitat o la salut dels pacients.

En aquest sentit, la **UE** pretén garantir que els **dispositius sanitaris** que s'hi comercialitzen siguin **adequats per fer front als riscos de ciberseguretat dels nous reptes tecnològics**. Al mateix temps, té la voluntat d'establir un **marc comú** entre els països membres. Així, el 25 de maig de 2017, a la UE es van aprovar el **Reglaments 745/2017 (MDR)[140], sobre dispositius mèdics,** i el **Reglament 746/2017 (IVDR)[141], sobre dispositius mèdics in vitro**. Aquests reglaments són d'aplicació directa en els estats membres i deroguen tres directives de més de vint anys de vigència i les corresponents transposicions de l'Estat espanyol[142]. L'MDR serà d'aplicació obligada a partir del 26 de maig de 2021, i l'IVDR, a partir del 26 de maig de 2022[143]. Tot i que la transició als nous

[135] *https://ciberseguretat.gencat.cat/ca/detalls/noticia/Seguretat-GE-Healthcare-Desembre-2020*
[136] *https://cisomag.eccouncil.org/fda-reveals-potential-vulnerabilities-in-certain-medical-devices/*
[137] *https://www.healthcareitnews.com/news/fda-issues-new-alert-medtronic-insulin-pump-security*
[138] *https://www.prnewswire.com/news-releases/vulnerabilities-disclosed-by-cybermdx-allow-attackers-to-take-over-infusion-pumps-300867517.html*
[139] *https://ec.europa.eu/health/md_sector/overview_en*
[140] *https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02017R0745-20170505&from=EN*
[141] *https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017R0746&from=EN*
[142] *https://www.csvexperts.com/nuevos-reglamentos-productos-sanitarios/*
[143] *https://www.tecno-med.es/?p=32654*

reglaments serà progressiva, cal recordar la data del **26 de maig de 2024**, a partir de la **qual no es podrà introduir cap nou producte sanitari al mercat que no compleixi les normes**[144].

Ambdós reglaments estableixen **directrius rellevants amb relació als dispositius mèdics que incorporen sistemes informàtics**. Situen la **ciberseguretat** com un aspecte a tenir en compte **durant tot el cicle de vida dels dispositius**, des dels processos de disseny i fabricació fins a la seva retirada. Així, els **fabricants** són els encarregats de desenvolupar i fabricar els dispositius mèdics d'acord amb l'estat de la tecnologia, els principis de la gestió de riscos i les millors pràctiques en matèria de ciberseguretat[145]. I els **centres sanitaris** han d'adequar els seus processos per ajustar-se a aquestes millors pràctiques. També estableixen l'obligatorietat d'obtenir un **certificat (marcatge CE)** i seguir els requisits de ciberseguretat detallats a l'annex I dels Reglaments per poder subministrar dispositius als estats membres. El mecanisme d'obtenció d'aquest certificat no pot ser una autoavaluació, sinó que es necessita un laboratori (anomenat "organisme notificat"). També estableix la creació de la **base de dades EUDAMED** (*EUropean DAtabase on MEdical Devices*), a través de la qual es pretén centralitzar el seguiment de tots els productes sanitaris durant el seu cicle de vida. EUDAMED disposarà d'una part oberta al públic perquè qualsevol profà en la matèria pugui fer consultes.

Ara bé, aquesta no és l'única normativa a la qual s'han d'ajustar els dispositius d'e-salut a la UE. La **Directiva NIS 2016/1148** (amb les seves corresponents transposicions a l'Estat espanyol) i l'**RGPD 2016/679** (complementada amb la LOPDGDD) són especialment rellevants per a la **ciberseguretat** dels dispositius mèdics i per al **tractament de les dades personals sanitàries**, i han d'aplicar-se al mateix temps que les normes MDR i IVDR. També cal fer esment del **Reglament Cybersecurity Act 2019/881** que, precisament, introdueix un **marc de certificació de ciberseguretat** a tota la UE per a productes, serveis i processos TIC[146].

El conjunt de normes citades correspon a la UE, però la resta d'estats del món disposen de les seves pròpies, la qual cosa pot comportar desajustos o incompatibilitats entre regions. Per superar aquesta problemàtica, un grup de treball de l'*International Medical Device Regulators Forum* (IMDRF) treballa en una guia de ciberseguretat de dispositius mèdics amb l'objectiu de promoure un enfocament global i harmonitzat[147].

Més enllà de les normes amb afectació directa sobre els dispositius electrònics mèdics, cal recordar que la UE està treballant en nova normativa en matèria de ciberseguretat: la futures **Directiva NIS 2** i **Directiva sobre la resiliència d'entitats crítiques.** Així mateix, a l'Estat espanyol, es disposa de dues **transposicions per a la Directiva NIS**[148,149], de la **LOPDGDD**[150] que complementa el RGPD, així com de l'**ENS** (*Esquema Nacional de Seguridad*)[151] d'aplicació per a hospitals considerats com entitats de dret públic en les seves activitats fora del règim privat.

[144] *https://ticsalutsocial.cat/es/actualitat/nuevo-reglamento-de-productos-sanitarios/*
[145] *https://ec.europa.eu/docsroom/documents/41863*
[146] *https://www.emergobyul.com/blog/2020/01/new-guidance-published-medical-device-and-ivd-cybersecurity-under-mdr-and-ivdr-europe*
[147] *http://www.imdrf.org/workitems/wi-mdc-guide.asp*
[148] *https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257*
[149] *https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192*
[150] *https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf*
[151] *https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330*

*Els **logs*** o registres són enregistraments *seqüencials, en un fitxer o en una base de dades, de tots els esdeveniments que afecten a un procés particular, de manera que conforma una evidència del comportament del sistema (sistema operatiu, aplicació, activitat d'una xarxa informàtica, etc.)..*

Un Security Information and Event Management (*SIEM*) *és una eina que recol·lecta i emmagatzema centralitzadament els logs corresponents als esdeveniments de seguretat i a l'activitat d'una infraestructura TI. Possibilita la presentació de tota la informació a través d'una interfície única, de manera que permet una anàlisi global unificada que facilita la detecció d'incidents de seguretat.*

Recomanacions

- **Els responsables de sistemes han de disposar d'un inventari d'actius i de gestió de la seva configuració, en el qual s'estableixin, per exemple, mecanismes de control d'accés i comunicacions xifrades.**
- **Els responsables de sistemes han de disposar de plans per a l'actualització dels dispositius, així com els sistemes operatius o *firmwares*.**
- **Els responsables de sistemes han de disposar de processos per a la gestió de vulnerabilitats: monitorització, identificació i correcció, així com proves del correcte funcionament posterior.**
- **Les organitzacions han de contractar els sistemes i dispositius electrònics tenint en compte els criteris de ciberseguretat i les garanties de suport durant el cicle de vida (veure les Directrius per a la contractació cibersegura en hospitals i l'Eina de suport d'ENISA).**
- **Les organitzacions han de permetre la monitorització i auditoria dels dispositius electrònics amb connectivitat, així com la recollida de *logs* en un *SIEM*.**
- **Les organitzacions han de disposar de xarxes segmentades en les quals els sistemes i serveis crítics estiguin aïllats de la resta de dispositius.**
- **Les organitzacions han de realitzar proves de penetració, periòdicament o cada vegada que es realitza un canvi en l'arquitectura o els sistemes.**
- **Els fabricants de productes sanitaris, abans del 26 de maig de 2024, hauran d'obtenir un certificat en matèria de ciberseguretat (marcatge CE) per poder subministrar els dispositius als estats membres.**

Conclusions

La covid-19 pràcticament ha paralitzat el món. En canvi, arran de la crisi sanitària mundial, **el sector sanitari** s'ha vist carregat amb una **volum d'activitat i responsabilitat sense precedents i s'ha evidenciat imprescindible** i

Les **noves tecnologies han estat cabdals en el desenvolupament de l'activitat sanitària durant la pandèmia**. Han fet possible el tractament i el diagnòstic a distància, l'accés i correlació de les dades massives per definir formes d'actuar més eficients, la compartició d'informació per a la recerca, etc. Però, més enllà de la covid-19, **la transformació digital al sector sanitari ha de continuar** per poder donar resposta a futures catàstrofes en les millors condicions.

Així mateix, el futur digital del sistema sanitari ha d'assumir que ha d'estar **preparat per fer front a un incident cibernètic** que pugui impactar en el servei als pacients, especialment en un entorn tant convuls com l'actual en matèria de ciberseguretat, com ha constatat l'Agència de Ciberseguretat de Catalunya en els **informes de tendències** del **primer** i **segon** semestre de 2020. Així ho està entenent el sector: s'estima que un **73%** de les **organitzacions augmenta la inversió en ciberseguretat**[152]. Precisament, el president francès, Emmanuel Macron, recentment ha anunciat una inversió de 1.000 M€ per accelerar la protecció en ciberseguretat després de diversos incidents de *ransomware* a hospitals de França[153].

En aquesta línia, la **UE** ha començat a fixar les regles per garantir unes **condicions de ciberseguretat** adequades en tots els **països membres**. En aquest moment ja es disposa d'un conjunt regulador per mantenir uns sistemes amb un **nivell de protecció adequat** (Directiva NIS i les corresponents transposicions a l'Estat espanyol), per preservar la **privadesa de les dades dels pacients** (RGPD), per disposar d'un **marc de certificació de dispositius electrònics** (Cybersecurity Act) i per garantir unes **condicions de seguretat durant tot el cicle de vida** (MDR i IVDR). I estan en curs la Directiva NIS 2 i la Directiva sobre la resiliència d'entitats crítiques.

El **Govern de la Generalitat,** amb competències exclusives en matèria de sanitat i salut pública, se suma a la **transformació digital i cibersegura**. En aquest sentit, segons s'estableix a l'Estratègia de ciberseguretat de la Generalitat de Catalunya 2019-2022[154], l'Agència de Ciberseguretat de Catalunya col·labora amb el **Departament de Salut** en el **disseny i l'execució d'un programa de ciberseguretat**.

Es despleguen **plans de sensibilització i conscienciació** pels **professionals de la salut**. Per tal de protegir la infraestructura tecnològica, s'ha desenvolupat un **model de governança de la ciberseguretat**, en el qual s'identifiquen els **sistemes d'informació crítics** i es despleguen **mecanismes de protecció, revisió i ciberresiliència**. I, en cas d'incident, el **Catalonia-CERT** exerceix les funcions d'**equip de resposta a incidents** competent a Catalunya, previstes a la legislació vigent.

La **digitalització** és el **camí** i cal un esforç conjunt per recorre'l de forma **segura**.

[152] *https://www.economiadehoy.es/el-73-por-ciento-de-las-empresas-del-sector-salud-aumenta-su-inversion-en-ciberseguridad*
[153] *https://www.efe.com/efe/america/mundo/macron-defiende-una-mayor-inversion-para-proteger-hospitales-de-ciberataques/20000012-4468375#:~:text=El%20presidente%20franc%C3%A9s%2C%20Emmanuel%20Macron,piratas%20inform%C3%A1ticos%20que%20reclaman%20rescates.*
[154] *https://ciberseguretat.gencat.cat/web/.content/PDF/EstrategiaCiberseguretat-de-Catalunya-2019.2022.pdf*

AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

ciberseguretat.gencat.cat
@ Agència de Ciberseguretat de Catalunya
juliol de 2021