AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

Digitalitza el teu negoci
Fes-lo cibersegur

L'**Agència de Ciberseguretat de Catalunya**, com a impulsora de la seguretat TIC a Catalunya, té com objectiu garantir una societat de la informació segura per a tothom.

L'Agència rep la missió d'ajudar les empreses a tenir negocis cibersegurs, gràcies a la prevenció de les noves ciberamenaces i la minimització dels danys produïts per un ciberatac. I això només és possible amb actuacions de sensibilització, conscienciació i formació en matèria de ciberseguretat.

L'Agència presenta la campanya ***Negociber-segur*** adreçada al teixit empresarial, als nous emprenedors i emprenedores i les professionals de les TIC, per tal d'impulsar la transformació digital de totes les empreses de Catalunya i, així, permetre recuperar ràpidament l'activitat econòmica en un context com l'actual.

Els objectius estratègics de la campanya:

- Sensibilitzar i formar les empreses en ciberseguretat.
- Conscienciar emprenedors i emprenedores i empreses joves en la cultura de ciberseguretat.
- Promoure certificacions d'especialització en ciberseguretat per a professionals de les TIC.

Arran de la pandèmia causada per la covid-19, la ciberseguretat en l'entorn empresarial s'ha convertit en un assumpte més crític que mai. Les empreses fan un ús intensiu de les tecnologies i xarxes IT com a element fonamental per possibilitar el teletreball: l'ús d'equips fora de la infraestructura empresarial (sovint els domèstics), la forta activitat via correu electrònic, la incorporació accelerada de connexions VPN, l'obertura de ports RDP, la proliferació d'*apps* de videoconferència...

Les empreses estan més exposades que mai als ciberatacs i, per això, també han d'estar més ben preparades que mai.

NEGOCIBERSEGUR, NEGOCI PROTEGIT

La ciberseguretat és un fonament bàsic de l'estructura digital d'un negoci, d'una empresa, de la imatge de marca que es projecta enfora. La ciberseguretat es pot gestionar des de moltes perspectives. És per això que és de vital importància tenir una visió polièdrica per no deixar cap escletxa oberta que ens pugui fer trontollar l'edifici.

Totes aquestes perspectives constitueixen els fonaments bàsics de l'edifici de la ciberseguretat en l'entorn empresarial i de negoci.

Protegeix-te del programari maliciós

El programari maliciós es concep específicament per prendre el control d'un sistema informàtic, interferir en el funcionament, desestabilitzar-lo i malmetre'l. Cada vegada és més avançat, complex, més multifuncional i a vegades polimòrfic. I en definitiva, és més complicat de fer-hi front.

Mantenir tots els programes actualitzats, tenir un antivirus que alerti de possibles amenaces i aplicar una política de contrasenyes amb caducitat variable, és una bona combinació per lluitar contra els atacs de *malware*. També és important la formació del personal per prevenir els errors.

Ransomware Restringeix totalment o parcialment l'accés als fitxers d'un sistema fins que no es paga una determinada quantitat de diners.

Troià Amb una funció aparentment útil, accedeix al sistema i el fa vulnerable.

Botnet Controla tots els dispositius infectats de forma remota per perpetrar activitats criminals.

+ 475% d'increment en les deteccions de *malware* arran de la crisi de la covid-19

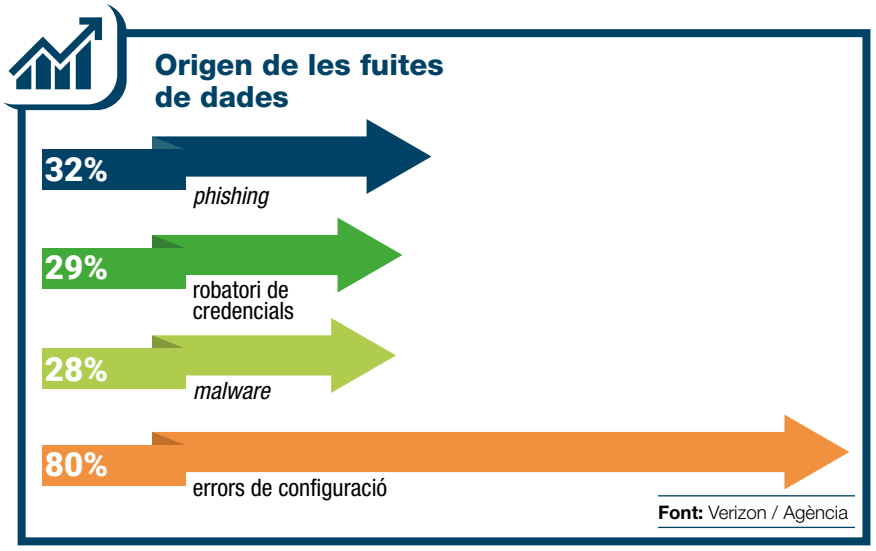
Font: Bitdefender

***Rootkit, backdoor*, RAT, cuc, *cryptojacker, spyware, keylogger, adware*...**

La informació a l'empresa: un tresor a protegir

Les dades personals i els fitxers confidencials són un dels valors més preuats del negoci, i cal vetllar perquè aquesta informació clau estigui ben custodiada i protegida.

Protegir les dades i els fitxers és seguir la legislació vigent en matèria de privacitat i en l'aprovisionament de serveis i productes. Fer-ho ens reportarà beneficis pel que fa al nostre valor de marca.



16,2 dies és la mitjana de temps que dura una aturada causada per un *ransomware*

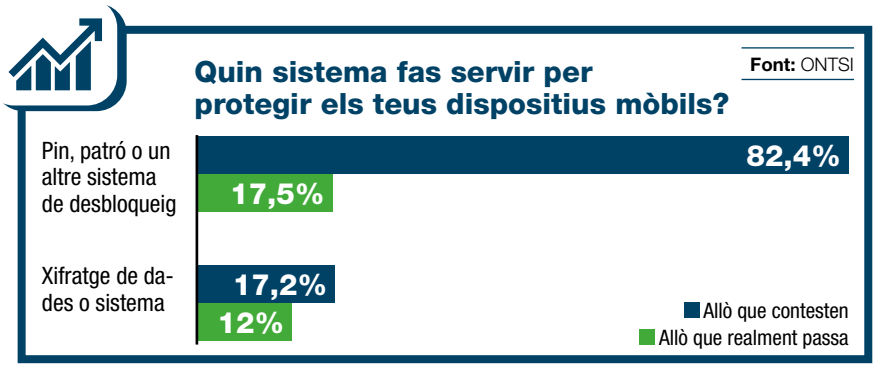
Font: Coveware

Dispositius de feina, a punt!

Els dispositius de feina que es mouen amb nosaltres sovint es poden veure exposats a causa d'*apps* malicioses, per configuracions errònies o males pràctiques en l'ús.

1 de cada 3 organitzacions ha experimentat fuites de dades derivades de dispositius mòbils

Font: Verizon



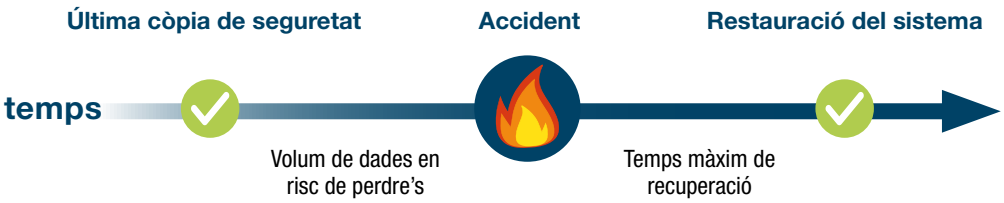
Els dispositius mòbils ens faciliten molt la feina, però poden comprometre informació sensible. Poden ser una porta d'entrada de programari maliciós i causar la pèrdua de dades del negoci que, en males mans, ens crearien molts maldecaps. Protegim-los amb antivirus i altres eines de protecció, amb contrasenya, i posem en pràctica polítiques que garanteixin una navegació segura (per exemple, evitar wifis insegures), un control d'accés, un protocol en cas de pèrdua o robatori...

Còpies de seguretat, el pla A

El nostre negoci és com la rotació de la Terra: mai no s'atura! Qualsevol tipus d'incident tècnic ens pot deixar fora de combat si no tenim les eines i els plans necessaris per assegurar que, en qüestió de minuts o hores, podrem recuperar la normalitat.

El 40% de les empreses no es recuperen després d'un desastre

Font: FEMA (govern EUA)



La continuïtat del negoci ha d'estar assegurada gràcies a les còpies de seguretat. Amb un bon pla d'emergència i de contingència, el temps sense servei serà petit i el nostre negoci (i la nostra reputació) no es veurà afectat. Aquests plans s'han d'haver testejat i saber-los aplicar convenientment.

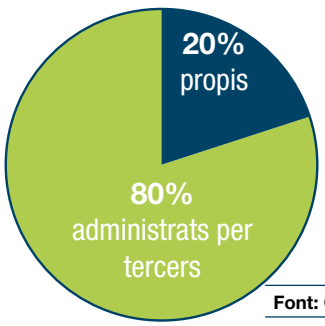
Ciberseguretat: sinònim de confiança

L'ús de les noves tecnologies ja no s'entén sense la ciberseguretat. Perquè la ciberseguretat és l'element que pot garantir les relacions de la cadena de subministrament i crea un clima de confiança potent.

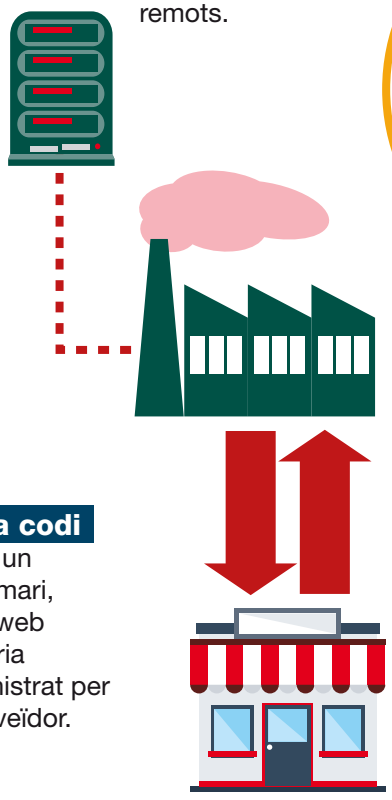
Treballar la ciberseguretat és treballar la confiança en l'ecosistema digital i en la fidelització de tots els actors implicats. L'ús de certificats de seguretat a la web, sistemes de pagament i facturació electrònica segurs, o mesures de protecció de la infraestructura tecnològica són cabdals per generar el clima de benestar necessari que blindi el nostre ecosistema.

14.000 atacs diaris al voltant de la covid-19, el **94%** dels quals en format *phishing*

Com són els actius TIC de l'empresa?



Font: Cycognito



***Hack* a l'accés**
Atac a un proveïdor vulnerable amb permisos d'accés remots.

***Hack* a codi**
Alterar un programari, servei web o llibreria subministrat per un proveïdor.

***Hack* a les relacions comercials**
Comprometre el correu electrònic d'un client/proveïdor per suplantar-lo i aconseguir desviar la facturació.

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

www.ciberseguretat.cat

#NegoCibersegur

El contingut d'aquesta guia 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:

Generalitat de Catalunya
Autoria: Agència de Ciberseguretat de Catalunya