GUIA

LA CIBERSEGURETAT ÉS CLAU PER DIGITALITZAR EL TEU NEGOCI

www.ciberseguretat.cat | #NegoCibersegur

Índex

Llegenda

Les propostes (bones pràctiques) que es fan en aquesta guia es valoren en funció de l'esforç o els recursos que poden representar per a l'empresa o negoci. S'indiquen amb unes claus angleses:

Pocs esforços o recursos a destinar.

Nivell mitjà d'esforços o recursos a destinar.

Requereix un alt esforç o recursos importants a destinar per posar en pràctica.

Presentació

El segle XXI és un segle de reptes tecnològics. En només vint anys, la tecnologia ha canviat la nostra manera de moure'ns, de relacionar-nos, de viure i de treballar. Però aquests canvis necessiten un temps de digestió per part de la societat. La tecnologia avança molt més ràpid que no pas sovint som capaços d'entomar.

Els grans canvis comporten també grans reptes associats. La ciutadania del segle XXI és una societat eminentment tecnològica: tothom, més o menys intensament, fa servir la tecnologia en el seu dia a dia.

L'ecosistema de negoci té uns fonaments tecnològics indiscutibles. Les relacions entre clients i proveïdors es produeixen un entorn TIC indiscutible: des dels petits autònoms fins a les grans corporacions, passant per la petita i la mitjana empresa.

L'Agència de Ciberseguretat de Catalunya engega la iniciativa NegoCibersegur per fer un pas més en la cultura de ciberseguretat al país. El teixit empresarial, autònoms, pimes i grans empreses, no poden tancar les portes a una demanda indiscutible: el repte d'empoderar-se des d'un punt de vista tecnològic, el repte de protegir els seus negocis i les seves àrees d'influència de les ciberamenaces.

La transformació digital experimentada en els darrers anys les ha exposat a unes realitats noves: la seguretat de la informació, el manteniment dels sistemes informàtics, el tractament de dades, els atacs de ciberdelinqüents... Perquè les ciberamenaces existeixen, i cada vegada més l'entorn de negoci és el preferit pels ciberdelinqüents.

L'Agència de Ciberseguretat de Catalunya, com a principal pilar d'un país digitalment avançat, vol estar al costat d'aquests empresaris, autònoms, emprenedors del país, vertader motor de la productivitat i de l'economia catalana. Com a impulsora de les TIC a Catalunya, l'Agència treballa en la protecció contra les noves amenaces i minimitza els danys causats per una ciberdelinqüència que ha fet del cibercrim un dels negocis més lucratius.

El teixit empresarial català, en tota la seva dimensió, ha d'estar preparat per a aquests reptes. Perquè la cibersegurat és clau per digitalitzar els negocis. Un negoci protegit és un negoci segur, productiu, competitiu, solvent. Un negoci del segle XXI.

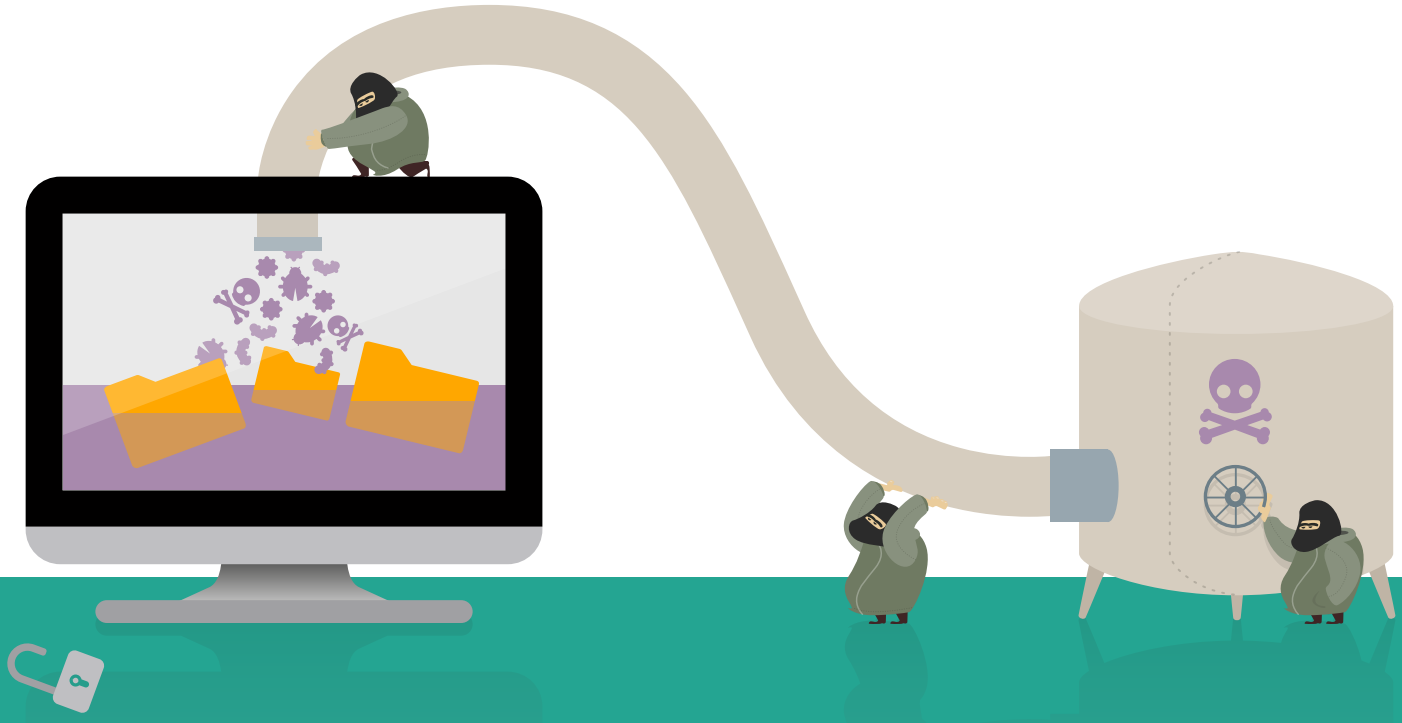
Sr. Oriol Torruella i Torres
Director de l'Agència de
Ciberseguretat de Catalunya

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

PROTEGEIX-TE DEL PROGRAMARI MALICIÓS

Evita el compromís dels actius del negoci i sigues conscient de la importància de protegir-los amb eines eficaces.



El programari maliciós està pensat per prendre el control d'un sistema informàtic, interferir en el seu funcionament, desestabilitzar-lo i malmetre'l. Cada vegada és més avançat, complex i multifuncional. La sensibilització i prevenció en l'entorn empresarial són essencials per lluitar contra els atacs de *malware*. Cal aplicar bones pràctiques en la gestió TI per minimitzar els riscos. També serà de gran ajuda disposar de proteccions i solucions que es trobin en el mercat que anul·lin l'acció dels incidents.

Protegeix-te del programari maliciós

Bones pràctiques

1. **Establir una política de contrasenyes que protegeixi les dades i els equips.** Les contrasenyes han de ser fortes i complexes, úniques i unipersonals, i cal fixar-ne una caducitat i un número de caràcters adequat.

2. **Actualitzar sistemes operatius i programes.** Els desenvolupadors informàtics treballen per millorar, a cada actualització, el rendiment i la seguretat de sistemes i programes. Cal fer actualitzacions periòdiques per tancar escletxes per on podria entrar programari maliciós.

3. **Verificar les procedències dels correus electrònics i revisar els enllaços abans de clicar-los.** Els missatges via correu electrònic són una de les portes d'entrada de programari maliciós. S'ha de verificar la procedència i tenir cura amb els enllaços externs que adjunten els correus, ja que poden portar a pàgines que continguin codi maliciós.

4. **Informar-se de les novetats en les variants de *ransomware* i altres tipus de programari maliciós.** La tipologia dels ciberatacs evoluciona constantment, i si bé no cal ser un expert en ciberseguretat, sí que és del tot recomanable estar al dia d'allò que succeeix en aquest àmbit.

5. **Gestionar correctament usuaris i permisos d'accés.** Les rotacions de personal que experimenten les empreses fan indispensable tenir un acurat control d'altes i baixes, i de modificacions dels usuaris que tenen accés a dades i arxius.

6. **Assegurar els dispositius i les xarxes de connexió.** Tots els dispositius relacionats amb l'empresa han de tenir instal·lat un antivirus. També cal controlar les xarxes a les quals es connecten els equips; es pot fer aplicant un nivell de seguretat a les xarxes sense fils i amb la implementació de sistemes de tallafocs.

Què podem fer immediatament?

Les quatre primeres pràctiques (contrasenyes, actualitzacions, precaució amb els missatges rebuts i informació) han de ser d'aplicació immediata en qualsevol negoci digitalitzat, i a més són senzilles i econòmiques de portar a terme.

Què és el més rendible?

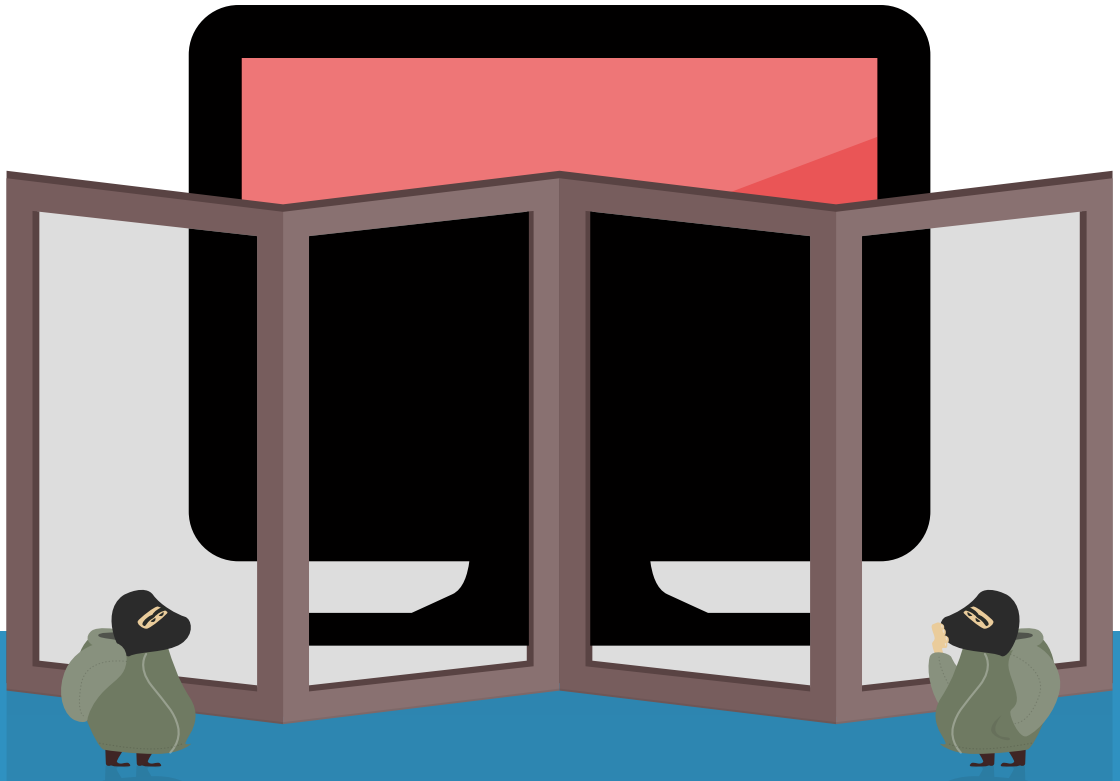
Abans de fer qualsevol pas en fals, cercar l'assessorament d'empreses especialistes en ciberseguretat.

Què és el més efectiu?

La combinació de totes les pràctiques descrites, i deixar-se assessorar per serveis professionals en cas que algun dels consells no sapiguem com portar-lo a terme.

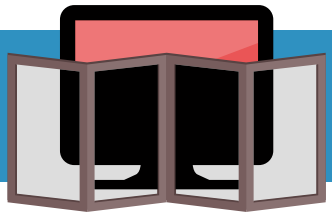
LA INFORMACIÓ A L'EMPRESA: UN TRESOR A PROTEGIR

Per garantir la confidencialitat
i la privadesa, cal seguir el que estableix
la legislació vigent.



Un dels actius del nostre negoci és la informació. I, evidentment, aquesta informació ha d'estar ben guardada, ben conservada i ben assegurada. Però, a més a més, la privacitat és un dret fonamental en la Unió Europea, i les dades que emmagatzema un negoci, per llei, han d'estar ben custodiades. Tota empresa que vulgui ser productiva i competitiva ha de tenir sempre present el compliment dels requisits legals i la seva reputació en el mercat on ofereix productes i serveis; aquelles que n'ofereixen en els canals digitals tenen responsabilitats en matèria de ciberseguretat que no es poden obviar.

La informació a l'empresa: un tresor a protegir



Bones pràctiques

1. **Establir mesures de protecció específiques en funció del tipus de dades a protegir.** El personal només ha de poder accedir a aquells fitxers desats en dispositius mòbils que necessiti per a les seves rutines de feina. Tampoc han de tenir entrada als serveis d'emmagatzemament que continguin dades que no estiguin autoritzats a conèixer o a consultar.

2. **Establir una política clara de confidencialitat i comunicacions segures.** La privacitat s'empara en lleis i reglaments que els responsables del negoci han de conèixer i complir. També tota aquella legislació relacionada amb la ciberseguretat.

3. **Tenir polítiques internes de contractació de tercers.** En cas de facilitar dades a tercers, per exemple a una assessoria, s'ha de subscriure un contracte d'encàrrec de tractament.

4. **Aplicar polítiques de bloqueig de dispositius i de taules netes per evitar que la documentació confidencial estigui a l'abast de qualsevol.** Hi ha sistemes perquè es bloquegin els dispositius al cap d'un temps breu de no fer-los servir. Damunt de la taula de feina, és convenient no tenir-hi informació sensible.

5. **Informar els treballadors del compliment de la legislació.** Els empleats han d'estar al cas de les seves obligacions respecte del tractament de dades, especialment l'obligació relativa al deure de confidencialitat.

6. **Tenir un pla de resposta en cas de crisi de reputació digital**, saber com s'ha d'actuar, quins actors han d'intervenir-hi i quins passos cal seguir des del primer moment.

Què podem fer immediatament?

Totes les mesures descrites es poden dur a terme amb personal intern que tingui uns certs coneixements i capacitats tècniques en la matèria.

Què és el més rendible?

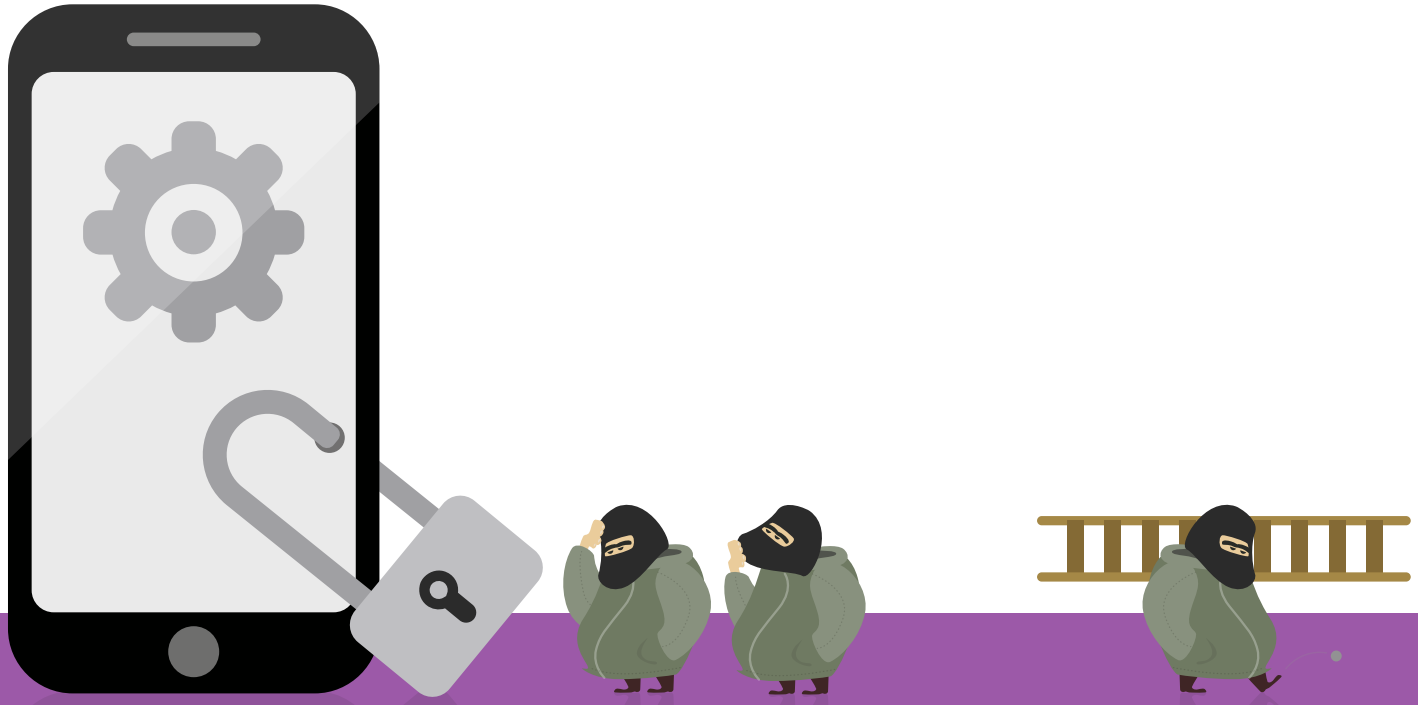
Cercar assessorament en professionals de la matèria per optimitzar els recursos i els esforços.

Què és el més efectiu?

Contractar una empresa dedicada a la privacitat i a la ciberseguretat que implementi aquestes mesures si no ho podem fer amb recursos interns del nostre negoci.

DISPOSITIUS DE FEINA, A PUNT!

Evita ensurts i gestiona correctament i amb seguretat els dispositius de feina que es mouen amb tu.



Els dispositius mòbils s'han convertit en una eina imprescindible en gran part dels sectors empresarials. Tenir-los al dia i ciberprotegits ens permet sortir més empoderats digitalment, ja que seran menys vulnerables als incidents. És vital establir controls molt clars pel que fa a les aplicacions que s'utilitzen, els clients de correu, els sistemes d'accés als arxius que l'empresa ha de gestionar… La pèrdua de dades, ja sigui per pèrdua física del dispositiu o per una fuita provocada per negligència o per un tercer, pot tenir conseqüències molt negatives des del punt de vista productiu i de reputació.

Dispositius de feina, a punt!

Bones pràctiques

1. **Fer servir una contrasenya o patró de desbloqueig.** Aquesta acció és del tot imprescindible perquè terceres persones no puguin tenir accés al dispositiu i no sigui usat amb finalitats poc ètiques.

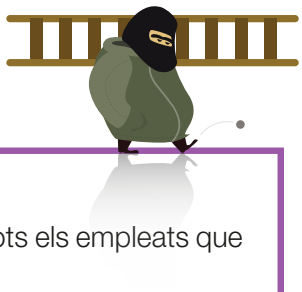
2. **Descarregar aplicacions només des de botigues oficials**. Fer-ho des d'altres llocs és una pràctica potencialment perillosa. Apple, Google i Microsoft fan un esforç per monitoritzar tot allò que ofereixen a les seves plataformes, tot i que sempre cal estar alerta perquè els cibercriminals se les empesquen i se'n surten a l'hora d'introduir codi maliciós en algunes aplicacions.

3. **Tenir cura de dades personals o sensibles, accessibles des del mòbil.** És necessari que els arxius, a dins dels dispositius, estiguin xifrats. Els que són especialment sensibles o de caràcter personal no s'hi haurien d'emmagatzemar.

4. **Fer còpies de seguretat amb freqüència.** Als dispositius mòbils s'hi emmagatzema molta informació essencial, i la prevenció és un factor clau. Les còpies de seguretat ens permetran tenir la capacitat de reacció necessària perquè els nostres sistemes i/o els nostres clients no es vegin afectats.

5. **Instal·lar antivirus també als dispositius mòbils.** No fer-ho implica ser més vulnerables als embats de qualsevol tipus de programari maliciós. Cal triar l'antivirus que millor s'adapti a les nostres necessitats i actualitzar-lo periòdicament.

6. **Implantar sistemes d'eliminació remota de dades.** Hi ha aplicacions per fer aquesta operació, i així en cas de pèrdua o robatori del dispositiu la persona que el trobi o l'hagi robat no tindrà accés al seu contingut; per tant, el negoci o empresa no es veurà compromès.



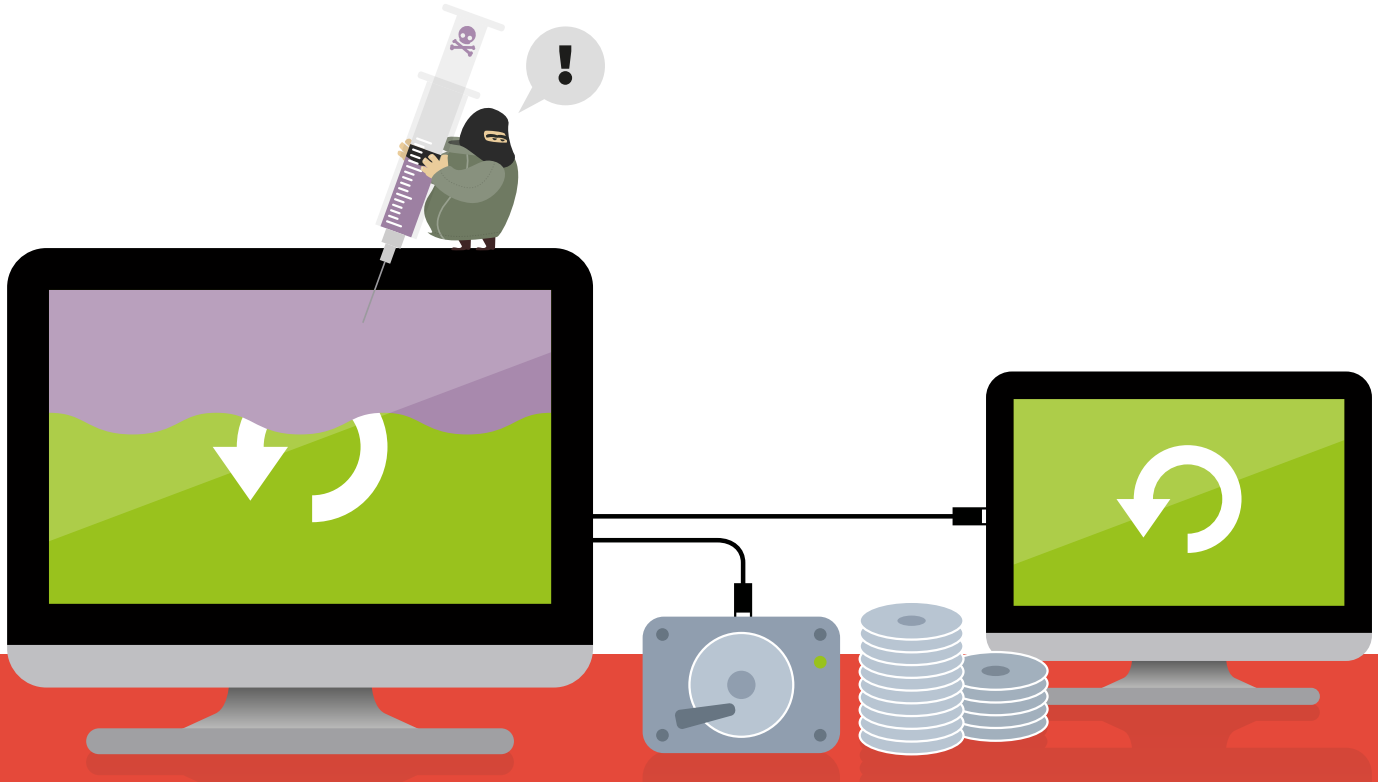
Què podem fer immediatament?
Aplicar totes les mesures i elaborar un document amb el reglament establert. Tots els empleats que utilitzin els dispositius d'empresa haurien de signar el document.

Què és el més rendible?
Assignar un responsable per portar a terme aquestes mesures i supervisar-les. Pot ser una persona de l'empresa o comptar amb una assessoria legal externa.

Què és el més efectiu?
Contractar una empresa que s'encarregui d'implantar totes les directrius necessàries per gestionar els dispositius mòbils de manera segura.

LES CÒPIES DE SEGURETAT, EL PLA A

Si no vols perdre informació,
desa còpies de seguretat regularment
i tingues a mà plans d'emergència que
funcionin per si falla alguna cosa.



La pèrdua de dades als negocis es pot produir per errors humans o per factors tecnològics. En ambdós casos, la continuïtat del negoci ha d'estar assegurada, i en aquest sentit les còpies de seguretat hi juguen un paper clau. Qualsevol incident tècnic pot deixar tocat el nostre negoci si no tenim les eines i els plans necessaris per evitar experimentar interrupcions llargues. Amb un pla d'emergència i de contingència, el temps sense servei serà petit i el nostre negoci (i la nostra reputació) no es veuran afectats. Els plans s'han d'haver testejat i saber aplicar-los quan sigui l'hora.

Les còpies de seguretat, el pla A

Bones pràctiques

1. **Fer còpies de seguretat de tots els arxius del negoci de manera freqüent.** Existeixen al mercat eines que permeten fer-ne de manera sistemàtica i còmoda.

2. **Fer procediments d'emmagatzematge al núvol o en físic.** Els serveis d'emmagatzematge al núvol són estructures robustes, amb alta disponibilitat, fiabilitat i, cada cop més, dotades de serveis de seguretat com ara registres d'accés, però sovint mancats de traçabilitat interna. En suport físic tenim més control de proximitat, però el cost és més elevat i també més probable l'entrada de ciberatacs.

3. **Documentar tots els sistemes i guardar les còpies originals dels programes.** En cas d'una fallada generalitzada, només si comptem amb un pla d'emergència que funcioni i tenim tots els sistemes i els seus elements i documents (amb les còpies originals), estarem capacitats per reprendre l'activitat de manera ràpida i amb el mínim impacte.

4. **Controlar els accessos a la informació a fi i efecte d'evitar la fuita de dades.** En l'entorn empresarial, la monitorització, és a dir, el control de tota l'activitat de caire tecnològic, constitueix un dels pilars del bon funcionament de tota l'estructura. Aquesta vigilància és útil per establir de manera acurada qui té accés a què i detectar qualsevol tipus d'activitat sospitosa de convertir-se en un possible incident.

5. **Disposar d'un pla d'emergència i restauració en cas de pèrdua de dades.** Hem de tenir un protocol que garanteixi que tots els engranatges poden tornar a funcionar en cas d'incident, sigui quin sigui l'origen.

6. **Establir una política d'ús de programes de compartició de dades.** La utilització de serveis d'emmagatzematge extern s'ha d'establir amb normes precises si no volem veure informació classificada del negoci per les xarxes socials o a l'abast de qualsevol competidor.

Què podem fer immediatament?

Totes aquestes mesures són imprescindibles i necessiten d'un seguiment i certs coneixements. Estudiar la possibilitat d'assignar algú de l'estructura de personal que tingui coneixements bàsics de ciberseguretat.

Què és el més rendible?

Formar personal intern i assignar-los la responsabilitat d'aquesta tasca, així com documentar tots els processos.

Què és el més efectiu?

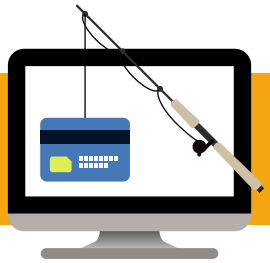
Contractar una empresa especialista en plans de continuïtat que implementi les mesures.

CIBERSEGURETAT: SINÒNIM DE CONFIANÇA

La creació d'un ecosistema de confiança en el negoci entre empresa, clients i proveïdors és imprescindible per a la qualitat i la continuïtat del servei.

La ciberseguretat és una palanca generadora de la confiança necessària per promoure l'ús de les noves tecnologies i la transformació digital, imprescindibles per al bon funcionament de l'activitat econòmica. Un servei de qualitat és necessari, però també donar garanties als clients i als proveïdors, mostrar amb fets que les seves dades estaran segures i que no podran ser alterades, robades ni usades per fer quelcom que el client no ha consentit. La confiança s'assoleix si es compleixen tots els requisits necessaris per fomentar-la. Confiança és fidelització. I la tecnologia és un element necessaria per assolir aquesta confiança i fidelització.

Ciberseguretat: sinònim de confiança



Bones pràctiques

1 **Formar la plantilla per detectar casos d'enginyeria social i notificar incidents que puguin amenaçar el negoci.** Cal que els treballadors sàpiguen reconèixer quines són les principals tècniques d'enginyeria social. El correu electrònic, les aplicacions de missatgeria instantània, les xarxes socials o, fins i tot, el telèfon són canals a través dels quals es produeixen.

2 **Instal·lar certificats SSL amb una autoritat de certificació per a les passarel·les de pagament i en webs de comerç electrònic.** L'experiència de pagament a través de la xarxa ha de transmetre confiança. El client ha de tenir la certesa que els seus diners i les seves dades estan ben protegits.

3 **Conèixer i aplicar solucions tecnològiques que enforteixin la cadena de subministrament i donin transparència als clients.** Implementar el xifrat de la web que resolgui la privacitat de l'usuari, aplicar passarel·les de pagament segures, o blocar la navegació a llocs web que no disposin de certificats vàlids, en són algunes.

4 **Utilitzar sistemes de monitorització del trànsit de dades de la xarxa i activar protocols pel canvi de credencials en cas d'indicis d'atacs.** Les xarxes de l'empresa abasten cada cop més entorns, amb l'ús de serveis mòbils/remots i serveis al núvol. Cal pensar on s'emmagatzemen i processen les dades del negoci i quin tipus d'atacs podrien interferir-hi.

5 **Fer auditories tècniques de seguretat per descobrir vulnerabilitats a la xarxa interna de l'empresa i al web.** La revisió dels controls, definits per la metodologia OWASP (*Open Web Application Security Project*), permet als auditors garantir el bon funcionament de plataformes web o apps, des del punt de vista de la ciberseguretat, amb la garantia que tots els vectors d'atac han estat revisats i que els errors de seguretat estan identificats.

Què podem fer immediatament?

Les mesures exposades requereixen coneixements especialitzats d'un cert nivell. Però també és necessari que la plantilla tingui certa preparació, i per tant és imprescindible la formació a dins de l'empresa i les xerrades de conscienciació.

Què és el més rendible?

Contractar serveis professionals especialitzats en privacitat i ciberseguretat.

Què és el més efectiu?

Una empresa o personal especialitzat que faci una supervisió de les solucions aportades.

Com pots adaptar la guia a la teva empresa?

Si has arribat fins aquí, et preguntaràs com pots adaptar tots els recursos de la campanya a la teva empresa. Et donem algunes idees inicials:

Primerament, establir un **calendari** on hauràs d'incloure com a principals accions: realitzar un autodiagnosi general amb l'ajut de l'eina **Avalua't**, realitzar una campanya interna de sensibilització amb el **material** aportat per la campanya, establir unes dates per a la realització d'un taller al teu equip segons el nivell tècnic, i realitzar revisions contínues dels teus equips de treball.

Si escau, recomanem escollir una persona perquè sigui la **responsable** d'aquesta difusió i de la cultura de la ciberseguretat a dins de l'organització.

Un cop establerts aquests elements, podràs començar a fer les diverses accions preestablertes. Per una banda, el teu equip haurà d'accedir a l'apartat **Avalua't** de la web **https://internetsegura.cat/empresa/** i descobrir quins coneixements té cada professional sobre la ciberseguretat. Paral·lelament, pots engegar una campanya interna de difusió i sensibilització a la teva empresa amb els materials disponibles com són els pòsters, *flyers*, bàners... que trobaràs sempre disponibles al web, a l'apartat **Recursos**.

En grups reduïts de 6 o 7 persones, et podràs apuntar al webinar amb el qual t'introduiràs al món de la ciberseguretat.

Després serà molt important fer una **reunió** per revisar el nivell de coneixement existent i quins **dubtes** més representatius tens sobre l'àmbit. Quan tinguis una llista de totes les qüestions exposades, podràs distribuir les guies de campanya als equips, segons les seves **necessitats** i inquietuds.

Pels que no facin **activitats professionals** relacionades directament amb la ciberseguretat, podràs indicar-los que consultin els materials que formen part de cada un dels cinc àmbits de **#NegoCibersegur.**

En canvi, pels que estan més familiaritzats amb qüestions tècniques més pròximes a la ciberseguretat (com ara l'ús de les tecnologies de la informació), podràs recomanar-los la consulta dels cursos tècnics, la guia ampliada, les **notícies** del web, etc.

Si tens més inquietuds, pots contactar amb nosaltres a través del correu electrònic **internetsegura@cesicat.cat**

Informa't de les novetats que es vagin publicant en aquesta guia i a l'apartat de **notícies** del web per si hi trobes altres propostes.

I recorda, per crear una **cultura en ciberseguratat**, planteja't accions durant l'any que ajudin a actualitzar aquests coneixements i aplicar-los a les activitats de negoci quotidianes. Una manera eficaç de fer memòria pot ser penjant el **pòster** de **#NegoCibersegur** a l'oficina.

DIGITALITZA EL TEU NEGOCI. FES-LO CIBERSEGUR!

Saps que a Catalunya hi ha moltes empreses dedicades a la ciberseguretat?

La ciberseguretat a Catalunya el 2019

356 EMPRESES

6.100 TREBALLADORS

APLICACIONS PRINCIPALS

Indústria
Mobilitat
Serveis financers
Comerç electrònic
Educació i formació
Salut
Govern
Smart City

809 M€ FACTURACIÓ

81% PIMES

52% TENEN MENYS DE 10 ANYS

Coneix-les!

DIGITALITZA EL TEU NEGOCI
FES-LO CIBERSEGUR

www.ciberseguretat.cat | #NegoCibersegur | |

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya