BIZBARCELONA
L'espai on fer créixer negocis i petites empreses
by Barcelona Activa

10 CLAUS PER A UNA EMPRESA CIBERSEGURA

CONTINGUTS

LA CIBERSEGURETAT ÉS URGENT

Sabies que un 75 % de les víctimes de *ransomware* (un ciberatac que bloqueja les dades dels ordinadors) són ara petites i mitjanes empreses?

Algunes dades impactants

Cada 10 segons es produeix un atac de ransomware a tot el món.
El 92 % d'empreses que van pagar el rescat després d'un ciberatac mai van recuperar les seves dades.
El 43 % de les pimes espanyoles encara no ha adoptat plans d'avaluació i mitigació de la ciberseguretat.

Els ciberatacs són una realitat que està a l'ordre del dia. La pandèmia i el teletreball van propiciar una escalada d'aquests intents maliciosos d'accedir de manera no autoritzada als equips informàtics d'individus i empreses per robar-ne les dades i exigir el pagament d'un rescat.

Sovint, els ciberatacs són aleatoris i massius, això significa que els hackers no només persegueixen grans corporacions, sinó que qualsevol empresa se'n pot veure afectada. Els especialistes temen una explosió d'amenaces el 2024 i 2025 a causa de la intel·ligència artificial, cada vegada més sofisticada i difícil de detectar.

QUÈ ÉS LA CIBERSEGURETAT

Aquest concepte engloba totes aquelles eines i estratègies que adoptis per protegir les dades de la teva empresa i garantir que pugui continuar funcionant amb normalitat. Ofereix seguretat real i directa, i disminueix l'exposició als ciberatacs, com fa un cartell d'alarma a la porta de casa.

En cas de patir un ciberatac, la ciberseguretat protegeix els sistemes amb defenses coordinades que bloquegen l'intrús i alerten de la seva presència. Podràs aprendre sobre el seu comportament per anar sempre un pas endavant i anticipar-te als seus atacs. I, a més a més, ajuda a reparar els possibles danys que produeixin aquests intents en la teva infraestructura tecnològica.

La tríada CIA és un model que recull els tres principis fonamentals per protegir la informació i que pots utilitzar per establir controls i polítiques eficaces:

- **CONFIDENCIALITAT**: són els esforços de la teva organització per protegir les dades sensibles i mantenir-les privades o secretes.
- **INTEGRITAT**: es tracta de mantenir la coherència, exactitud i fiabilitat de la teva informació i evitar que persones no autoritzades la manipulin.
- **DISPONIBILITAT**: cal garantir el funcionament dels sistemes i les dades perquè les persones autoritzades hi puguin accedir.

PRINCIPALS RISCOS PER A PIMES I PERSONES TREBALLADORES AUTÒNOMES

1. RANSOMWARE

També conegut com a segrest de dades, bloqueja l'accés a un equip informàtic per demanar-ne un rescat a canvi. Es recomana no pagar aquest rescat, ja que en la majoria de casos els ciberatacants no retornen les dades.

2. MALWARE

És un software maliciós, dissenyat per infectar i danyar els equips a través d'internet, el correu electrònic o la descàrrega d'arxius. Les conseqüències van des del robatori d'informació fins al bloqueig de l'accés al dispositiu o l'espionatge

3. ATACS D'ENGINYERIA SOCIAL

Aquest conjunt d'atacs inclou la suplantació d'identitat, la manipulació i l'estafa mitjançant canals com el correu electrònic (*phishing*), els SMS (*smishing*), els codis QR (*quishing*) o les ordres falses de transferències.

4. DDOS (*DISTRIBUTED DENIAL OF SERVICE*)

Mitjançant molts ordinadors zombis infectats amb *malware* i controlats des d'un sol dispositiu, els *hackers* es connecten a un servidor (un web) de manera massiva. El servidor és incapaç de gestionar el flux i s'acaba bloquejant.

5. ATAC DE FORÇA BRUTA

Consisteix a provar múltiples combinacions de contrasenyes fins a encertar la correcta. La intel·ligència artificial ha potenciat aquesta pràctica, ja que permet generar grans quantitats de contrasenyes possibles automàticament.

10 CLAUS PER TENIR UNA EMPRESA CIBERSEGURA

1. FORMA'T PER REDUIR L'EXPOSICIÓ A AMENACES

Tant tu com cada membre del teu equip representeu una bretxa de seguretat, si no teniu els coneixements d'actuació necessaris. És essencial formar-te i formar la teva plantilla en ciberseguretat i garantir que coneixeu les solucions de protecció que apliqueu, de manera que no perdin la seva efectivitat per desconeixement. Organitza cursos de sensibilització i prova de fer exercicis de simulació (per exemple, de *phishing*) per veure com reacciona el teu equip i què cal fer diferent.

Si no saps per on començar, l'Institut Nacional de Ciberseguretat (INCIBE) ofereix cursos gratuïts online per a microempreses i autònoms al seu web.

2. CONTROLA LA TEVA INFRAESTRUCTURA INFORMÀTICA

Les auditories de ciberseguretat són una eina fonamental. Permeten detectar possibles vulnerabilitats a la teva empresa, avaluar la robustesa dels teus sistemes de seguretat i identificar bretxes potencials, amb l'objectiu de prendre mesures preventives a temps. Això no només significa instal·lar un antivirus, sinó crear tota una estratègia de ciberprotecció a mida que respongui a les teves necessitats.

Compta amb el suport d'una persona experta per realitzar una auditoria minuciosa.

3. ALLOTJA LES DADES MANERA SEGURA

Coneixes el concepte ***sobirania de dades***? Es refereix a què les dades estan subjectes a les lleis i la governança del país on es recullen, processen i emmagatzemen.

Tot i això, la majoria d'empreses allotgen les seves dades en grans empreses amb seus a països com els Estats Units o la Xina, dels quals desconeixen la regulació. És una bona idea allotjar les dades a un servei europeu per tenir una garantia legislativa davant de qualsevol problema.

Diverses empreses ofereixen centres de dades instal·lats a Espanya que et permeten allotjar les teves dades al núvol, compleixen amb la normativa europea i que, a més, ofereixen serveis de suport i assessorament, com l'empresa NuuBB, Arsys o Acens.

4. LA IMPORTÀNCIA DE LES CÒPIES DE SEGURETAT

Les còpies de seguretat externes s'han convertit en una estratègia empresarial essencial, ja que permeten guardar i protegir les dades importants d'una pèrdua permanent en cas de patir un atac greu.

La desaparició d'aquesta informació podria portar la teva empresa a fer fallida o, en cas contrari, podries tardar anys a reconstruir-la.

És una pràctica preventiva contra sorpreses desagradables que has de fer amb regularitat i automatitzar.

Pots emmagatzemar la teva còpia en format físic, a un disc dur o un USB, i/o en format digital, al núvol (en un servidor extern). Hi ha opcions tant gratuïtes com de pagament, però al contractar-les cal tenir en compte quant espai necessites, el nivell de seguretat que ofereixen i la facilitat d'ús.

Els professionals recomanen automatitzar la còpia i fer backups amb freqüència, decidir de quina informació cal tenir còpia, xifrar el contingut i tenir una còpia fora de les teves oficines.

5. ESTIGUES AL DIA DE LES ACTUALITZACIONS

Els dispositius digitals i el *software* que utilitzem cada dia estan exposats a vulnerabilitats de seguretat. És per això que els editors i fabricants de software ofereixen actualitzacions periòdiques per corregir aquestes fallades.

Identifica tots els dispositius i programes que utilitzes i actualitza'ls sense retards, informa't regularment de les actualitzacions i descarrega-les només dels llocs web oficials, i recorda provar les actualitzacions sempre que sigui possible.

6. INSTAL·LA ANTIVIRUS I TALLAFOCS

Aquests programes de seguretat són imprescindibles per bloquejar els atacs maliciosos.

L'antivirus escaneja, detecta i elimina el *malware* que pugui posar en perill el funcionament dels equips, mentre que el tallafocs filtra el tràfic que passa per la teva xarxa per evitar els accessos no autoritzats.

S'ha d'intentar evitar programes gratuïts, ja que sovint no resulten prou eficients, caduquen i són senyal d'un ordinador poc protegit, fet que atrau els atacants.

Busca un antivirus que sigui compatible amb el teu ordinador, que compti amb les funcions que t'interessen (tallafocs, antiphishing...), que sigui fàcil d'utilitzar, que no requereixi grans coneixements per part de l'usuari, que t'ofereixi una solució integral i que s'adeqüi al teu pressupost.

L'OCU ofereix un **comparador** que et pot ajudar a triar.

7. GESTIÓ D'ACCESSOS I CONTRASENYES

Implementa una política d'accessos i contrasenyes, que inclogui canviar-les sovint i un nivell de complexitat alt.

Pots utilitzar gestors de contrasenyes per assegurar millor l'accés: són aplicacions que serveixen de caixa forta per guardar totes les contrasenyes, crear-ne de robustes i compartir-les de manera segura amb altres usuaris de l'empresa.

Com a extra, pots aplicar l'autentificació en dos passos, que també demana als usuaris introduir un codi secret enviat per correu o SMS.

Hi ha administradors de contrasenyes gratuïts, com Google Password Manager o el clauer d'iCloud, que només les guarden i sincronitzen.
Els gestors de contrasenyes, en canvi, ofereixen moltes més funcions de seguretat.
La solució que contractis t'ha de generar contrasenyes segures, permetre't compartir-les sense perill i comptar amb alerta en cas de filtració.

8. UTILITZA MISSATGERIA PROFESSIONAL SEGURA

El correu electrònic i els sistemes de missatgeria són algunes de les principals vies d'entrada dels ciberatacs.

El més recomanable és comunicar-se a través de sistemes de missatgeria segurs, allotjats directament per un proveïdor de serveis conegut, utilitzar sempre protecció *antispam* i comptar amb la recuperació de missatges en cas de pèrdua, ciberatac o desastre.

Els serveis més populars com Microsoft Outlook o Gmail ofereixen protecció avançada contra *phishing, spam i malware*, però actualment hi ha moltes alternatives amb més opcions de seguretat i privacitat. Valora que tingui xifrat d'extrem a extrem, que s'adapti a tots els dispositius i que sigui fàcil d'utilitzar.

9. PROTEGEIX ELS TEUS DISPOSITIUS MÒBILS

Els dispositius mòbils també guarden informació confidencial i tenen accés a la xarxa corporativa, però moltes vegades es passen per alt quan es planifica una estratègia de ciberseguretat.

Si utilitzeu mòbils d'empresa, cal protegir-los amb contrasenya, controlar les aplicacions descarregades i els webs visitats, instal·lar-hi un antivirus i xifrar-ne les dades per evitar que persones no autoritzades hi accedeixin, per exemple, si et connectes des d'una xarxa pública.

La gestió dels dispositius mòbils rep el nom de *Mobile Device Management* (MDM). Són solucions que t'ajuden a administrar i protegir els mòbils d'empresa i les dades que emmagatzemen.

10. ANTICIPA'T A L'ATAC

Tenint en compte que les ciberamenaces estan cada dia més presents, ja no es tracta de preguntar-te si algun dia hauràs d'afrontar un ciberatac, sinó quan passarà.

Això significa que has d'implementar una estratègia de ciberseguretat fins i tot abans de tenir cap ensurt.

Totes aquestes eines treballaran per protegir-te anticipadament i defensar-te amb èxit si pateixes un atac, a més d'ajudar-te a seguir funcionant amb normalitat al més aviat possible si l'atac atura la teva activitat.

COM COMENÇAR A INVERTIR EN CIBERSEGURETAT

Actualment, existeixen ajudes econòmiques que et permetran afrontar el cost d'engegar una estratègia de ciberseguretat.

És el cas del Kit Digital, una ajuda del Govern d'Espanya dirigida a pimes i persones treballadores autònomes, que subvenciona la implantació de solucions digitals. Es pot utilitzar per millorar qualsevol aspecte de la teva digitalització, cosa que és molt útil per començar a invertir en ciberseguretat.

Sol·licita el teu bo digital a través del web AceleraPyme.es, i selecciona la solució o solucions que t'interessi aplicar a la teva empresa. Concedida l'ajuda, podràs escollir entre diversos Agents Digitalitzadors perquè et proporcionin el servei.

Confia en una persona experta

"Invertir en ciberseguretat garanteix que la resta d'inversions destinades a les altres àrees del negoci tinguin més fiabilitat i efectivitat. La inversió en ciberseguretat avala els projectes en què hagis invertit temps i recursos perquè es puguin dur a terme amb tota seguretat i no hagin estat en va", afirma Nicolás Blasyk, CEO de NuuBB.

BIZBARCELONA
L espai on fer créixer negocis i petites empreses
by Barcelona Activa

ww.bizbarcelona.com

Contingut elaborat perBizbarcelona,
amb la col·laboració de NUUBB

WWW.NUUBB.COM