

## ASSEGURANCES I CIBERSEGURETAT NOUS RISCS, NOVES NECESSITATS

La pandèmia ocasionada pel COVID-19, **amb l'augment del teletreball** i de la importància de les noves tecnologies en el desenvolupament dels negocis i empreses, ha mostrat la necessitat de la **ciberseguretat per a protegir-nos de possibles atacs informàtics**.

Accions tan quotidianes com connectar un disc de memòria a l'ordinador o fer un clic en un correu electrònic, poden donar lloc a un atac informàtic que tingui efectes negatius vers la nostra empresa o negoci.

Amb l'aplicació de les noves tecnologies hem millorat la forma de treballar, però tots els moviments d'informació que realitzem (transferències bancàries, dades dels nostres clients, contractes confidencials, contrasenyes, etc...) poden estar exposats a què ciberdelinqüents accedeixin als nostres sistemes informàtics, ens puguin infectar amb virus, ens impedeixin continuar treballant, ens extorsionin, robin o eliminin informació important de la nostra empresa.

### Principals exemples de riscos informàtics:

**Fuga d'informació:** un ciberdelinqüent penetra al sistema informàtic de l'empresa ocasionant la filtració i el descobert de dades essencials de la cartera de clients o del negoci, amb la conseqüent pèrdua econòmica i de reputació que això suposa.


**Malware:** un empleat rep un suposat e-mail d'una empresa de missatgeria i fa un clic a l'enllaç previst per a comunicar-li el lloc de lliurament del paquet. En realitat descarrega, sense que ell ho sàpiga, un programa d'encriptació de dades (ransomware). En aquest moment s'encripten i queden totalment inservibles les dades de l'empresa. Per tal de recuperar la informació s'ha d'abonar un rescat.

**Phising:** el director financer rep un e-mail fals presumptament enviat per l'entitat bancària de l'empresa en què indica que s'han d'actualitzar les seves dades bancàries per a evitar que els comptes de l'empresa es bloquegin. En realitat estarà facilitant les dades d'accés dels comptes bancaris de l'empresa als hackers informàtics.

**Suplantació o modificació web:** un ciberdelinqüent es fa amb el control de la web de l'empresa i decideix publicar notícies falses que comprometen la imatge i la reputació de l'empresa.

**La nostra Corredoria d'Assegurances ha negociat amb les asseguradores un producte exclusiu per a donar resposta a les noves necessitats de protecció.**

Restem a la seva disposició per ampliar-li aquesta informació i/o en breu ens posarem en contacte amb la seva empresa per a analitzar les necessitats d'assegurament i oferir-los la millor solució.

  
**Santiago Atienza Calderón**  
Tècnic Superior d'Assegurances  
Director Àrea d'Assegurances

Balaguer, juny 2020

Av. Prat de la Riba, 44-48  
25008 **LLEIDA**   
Tel. 873 401 000

Passeig de l'Estació, 19-23  
25600 **BALAGUER**  
Tel. 973 443 800

C. Sant Pelegrí, 13  
25300 **TÀRREGA**  
Tel. 973 500 710

Av. Font de Valldans, 5  
25740 **PONTS**  
Tel. 973 462 072

[www.teixido.net](http://www.teixido.net)

JURÍDIC

LABORAL

FISCAL

COMPTABLE

MERCANTIL

GESTORIA

PREVENCIÓ DE RISCOS

**CORREDORIA D'ASSEGURANCES**

N. Reg. D.G.S. J-2671 · Assegurança R. C. Llei 03/2020