



## DTI – DIAGNÒSTIC TÈCNIC INTERIOR

SERVEI INTEGRAL DE CIBERSEGURETAT PER PROTEGIR ELS RECURSOS INTERNS DE L'EMPRESA

Aquesta protecció s'aconsegueix avaluant la xarxa, els servidors i les polítiques de seguretat contra les vulnerabilitats internes.

Aquest servei ofereix una visió tècnica i actualitzada sobre la seguretat interna per mitjà de mètodes tant manuals com automatitzats per a simular i detectar atacs, i proporciona a les empreses les eines necessàries per fer front eficaçment a les amenaces modernes.

### QUÈ INCLOU?

#### 1. Anàlisi de la configuració de xarxa interna:

- Avaluació dels dispositius de xarxa per verificar que estiguin configurats de manera segura i conforme a les millors pràctiques de la indústria.
- Identificació de configuracions dèbils que puguin permetre un accés no autoritzat o fuga de dades.

#### 2. Avaluació de Seguretat de Servidors i Estacions de Treball:

- Inspecció de maquinari i programari per identificar fallades de seguretat, com ara programari no actualitzat o mal configurat.
- Comprovació de l'efectivitat de les mesures de seguretat implementades, inclosa la protecció contra el malware i la gestió de pegats.

#### 3. Simulació de tècniques actuals d'atac:

- Realització de proves tant manuals com automatitzades fent servir les tècniques més recents i avançades utilitzades per cibercriminals per detectar i explotar vulnerabilitats dins de la infraestructura de TI.
- Aquestes tècniques inclouen, però no es limiten a, proves de penetració interna que simulen atacs per identificar punts dèbils en la seguretat de la xarxa i els sistemes.

#### 4. Informe de Correccions i Recomanacions:

- Presentació d'un informe exhaustiu que destaca els riscos identificats i proporciona recomanacions detallades per a mitigar-los.
- Propostes de millora basades en les troballes de les simulacions i l'anàlisi, orientades a reforçar les defenses internes de l'empresa.

### COM AJUDA AIXÒ LA MEVA EMPRESA?

- **Defenses Millorades:** Reforç de la seguretat interna contra tècniques sofisticades i actuals usades pels atacants.
- **Prevenió d'Atacs:** Increment de la capacitat dels sistemes de l'empresa per detectar i mitigar intrusions internes de manera efectiva.
- **Protecció Proactiva:** Implementació de solucions de seguretat avançades que responen a les últimes tàctiques i tècniques d'atac, mantenint la infraestructura segura davant les amenaces emergents.

### A QUI VA ADREÇAT?

- Petites i mitjanes empreses que busquen una avaluació detallada de la seva seguretat interna amb un enfocament actualitzat en la detecció d'amenaces.
- Organitzacions que requereixen un servei tècnic avançat per protegir-se de les tècniques d'intrusió modernes i sofisticades.
- Negocis interessats a enfortir les seves defenses internes mitjançant un enfocament pràctic i actualitzat en seguretat cibernètica.

### Contacte

Departament de Tecnologia i Innovació

Imma Navarra

inavarra@pimec.org | Tel. 93 496 45 00

Clica [aquí](#) per  
accedir al servei

