A·D·Q·A

CAMPANYA VNG EMPRESES CIBERSEGURES

Si vols mantenir el negoci obert
TANCA LA PORTA

ens Esquema Nacional de Seguridad

LA PRIMERA EMPRESA DEL GARRAF ACREDITADA PER L'ESQUEMA NACIONAL DE SEGURIDAD

bsi. ISO 9001 Quality Management

Un minut per presentar-nos

- ADQA s'ha consolidat com el proveïdor de solucions globals en les TIC. Un únic proveïdor per a totes les necessitats,
- ADQA té més de 25 anys d'experiència en cadascuna de les àrees de negoci.
- Amb certificat de qualitat ISO 9001:2015, com a garantia del millor servei
- **Primera empresa del Garraf amb la certificació ENS, en categoria ALTA**

Espanya és el tercer país del món en nombre de ciberatacs

I afecten a tot tipus d'empreses i institucions

Un risc afegit: la RGPD

Multes molt quantioses per robatori de dades

Quines són les situacions més habituals?

I què posen en risc a les empreses?

Correus electrònics enganyosos:

Coneguts com *phishing*, suplanten la identitat d'una companyia per a robar dades compromeses com contrasenyes o dades de targetes de crèdit.

Poden semblar menys perillosos, però poden portar a situacions molt compromeses.

Quines són les situacions més habituals?

I què posen en risc a les empreses?

Ransomware:

Un programa maliciós que segresta l'ordinador de l'usuari, encripta les dades, i el deixa inoperatiu.

Se sol demanar un rescat important a canvi de la contrasenya que el desbloqueja.

Quines són les situacions més habituals?

I què posen en risc a les empreses?

Atacs contra la web:

Del tipus DDOS o hackejat de la web. No només poden fer caure el servei web sinó que sovint l'infecten per a allotjar-hi programes maliciosos, cosa que, a ulls de Google compromet molt la seva reputació.

Addicionalment, si es dona el cas del robatori de dades personals, les conseqüències a nivell legal poden ser severes.

Per què són atacades les empreses?

I sobretot: per què tenen èxit els ciberatacs?

Poca consciència sobre ciberseguretat:

Tret de sectors especialment sensibles com el financer, moltes empreses no han assumit que hi ha un risc real de ser atacats.

Manca d'inversió en ciberseguretat:

Relacionat amb la falta de consciència, les empreses petites i no tan petites no destinen un pressupost de tecnologia a protegir-se contra els atacs.

Poca formació en ciberseguretat:

En moltes ocasions el factor humà és una porta d'entrada per als ciberatacs. Formar l'equip i protegir-se contra descuits és imprescindible.

La ciberseguretat explicada a tothom

El símil amb la seguretat d'una casa

En una casa la seguretat es basa en acumular diferents sistemes

Protegir-se davant dels atacs

Què hem de fer per a protegir-nos?

1. Auditar els riscos de la vostra infraestructura
2. Aplicar mesures de seguretat
3. Ciberseguretat en continuitat
4. Sensibilitzar i formar l'equip

1- Auditar els riscos de la vostra infraestructura

Un control exhaustiu, físic, lògic i de polítiques

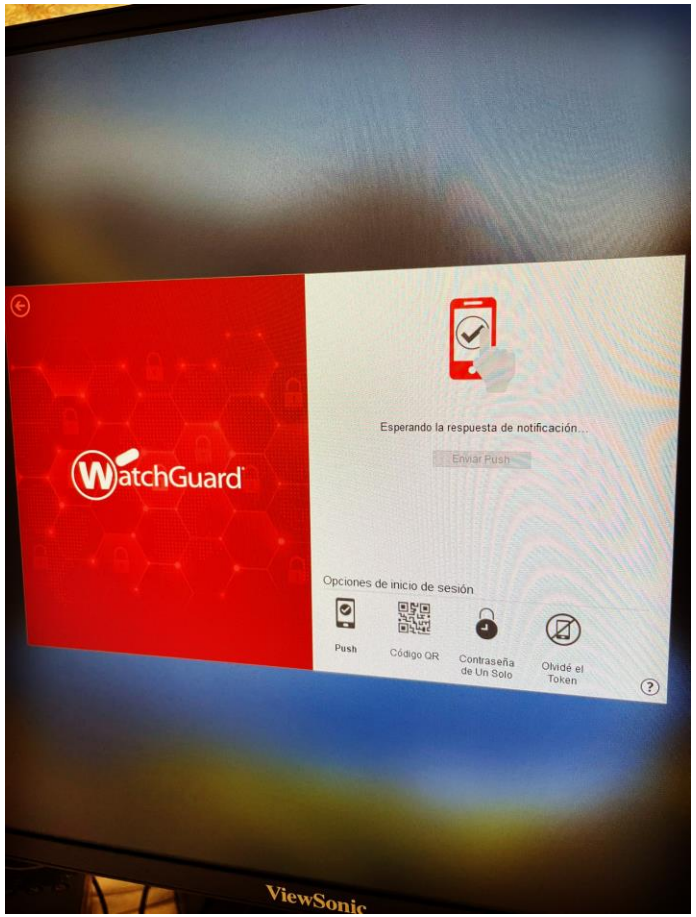
- Arquitectura de la seguretat
- Control d'accés
- Polítiques de drets
- Inventariat d'actius
- Sistemes de detecció d'intrusions
- Firewall
- Política de contrasenyes
- Nivell de conscienciació del personal
- Protecció d'equips portàtils
- Segregació de xarxes
- Seguretat Endpoint
- Còpies de seguretat

2- Aplicar mesures de seguretat

Polítiques de seguretat

Definició i implantació de les polítiques de seguretat

Normes per a usuaris i processos



2- Aplicar mesures de seguretat

Correu electrònic segur

Google Workspace, Office 365

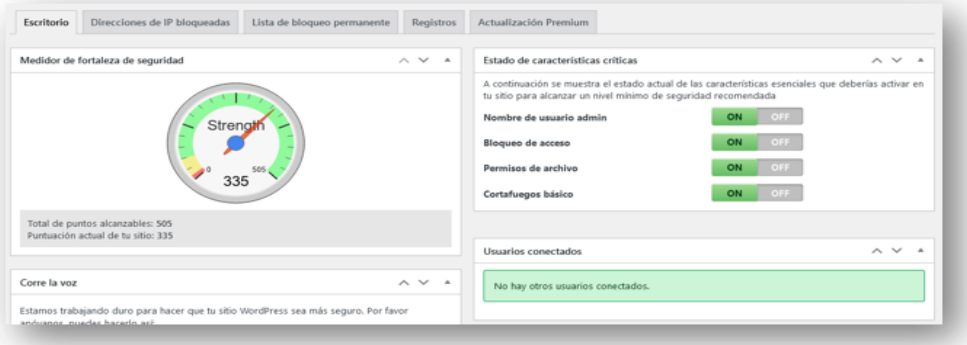
La millor manera de lluitar contra el phising

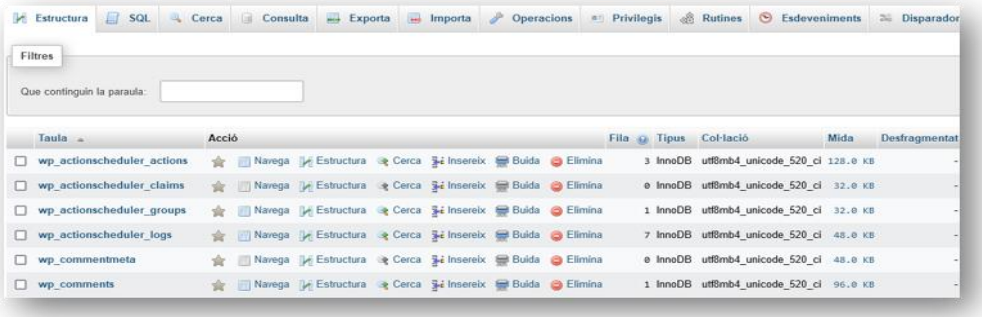
2- Aplicar mesures de seguretat

Seguretat en entorn web

Allotjament web segur

Actualitzacions, WAF, DDOS ...





2- Aplicar mesures de seguretat

Seguretat en les telecomunicacions

Xarxes privades virtuals segures

Comunicació entre seus amb màxima protecció

2- Aplicar mesures de seguretat

Firewall

Tallafocs de nova generació

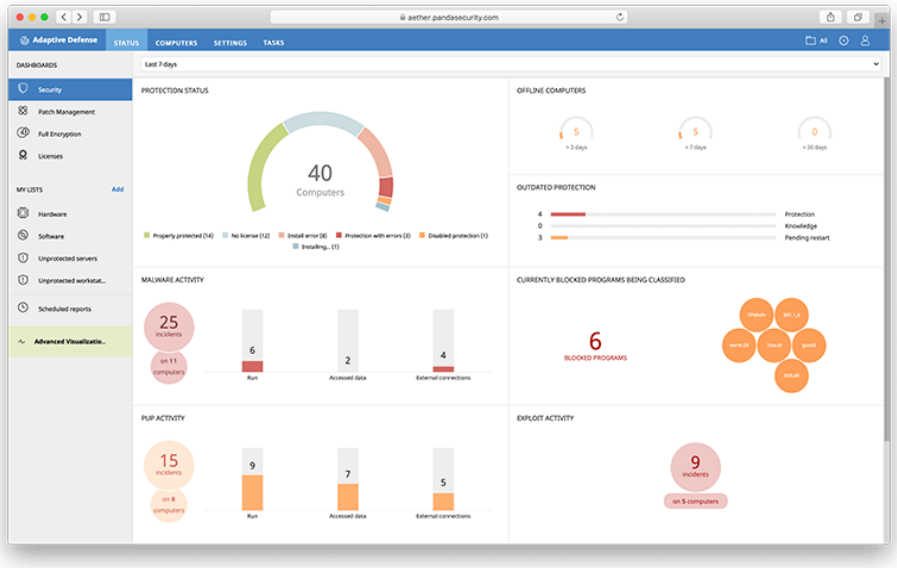
Networking amb seguretat

2- Aplicar mesures de seguretat

EndPoint Security

Protecció dels equips de treball

Unint EPP (Protecció) i EDR (Detecció i Resposta)



3- Seguretat en continuitat

La figura del responsable de seguretat

Monitoratge i adaptació continuada

Un ull permanentment posat sobre la seguretat de l'empresa

4- Sensibilitzar i formar l'equip

Donar al personal eines per a identificar atacs

Formació bàsica en seguretat i protocols d'actuació per a prevenir i respondre als ciberatacs

Un ull permanentment posat sobre la seguretat de l'empresa

En síntesi

Penseu en les conseqüències

Valoreu què passaria si patiu un atac com el del clínic, un frau per e-mail, o un atac a la web.

Confiança zero

No us penseu que no us poden atacar. Valoreu avui mateix quin és el vostre nivell de protecció.

Poseu-vos-hi avui mateix

Valoreu quin és el vostre nivell de protecció. Entreu a www.seguretat.info, feu el test d'autoavaluació de la campanya **VNG Empreses Cibersegures** i poseu-vos en mans expertes per a emprendre les mesures adequades.

Gràcies per la vostra atenció

Estem oberts a les vostres preguntes