TECNOideas2.0 és una empresa que **presta serveis de ciberseguretat ofensiva**, que inclou test d'intrusió —físics, sistemes o webs—, auditoria de seguretat en indústria 4.0, anàlisi forense juntament amb perícia judicial, consultoria legal en tecnologies de la informació i també ofereix formació, tant a nivell de seguretat per a empleats i directius d'empreses en general, com una formació específica més tècnica per a personal de tecnologies de la informació.

TECNOideas2.0 neix **a l'any 2009** oferint serveis informàtics generals, com venda i manteniment de xarxes i equips, gestió de projectes, etc. A tota mena de clients i en sectors molt diversos.

En el 2018 decidim especialitzar-nos en ciberseguretat, per l'augment de la demanda en aquests serveis per part dels nostres clients i per l'experiència del **nostre personal** en aquests temes.

Comptem amb personal amb una dilatada experiència en **l'àmbit tecnològic, informàtic, industrial i empresarial, tots ells** especialistes en ciberseguretat.

Tenint també en les nostres files **docents requerits en universitats com la de Castella-La Manxa i conferenciants dels millors esdeveniments d'Espanya.**

Els nostres mètodes no inclouen l'ús de grans plataformes de programari o les típiques llistes de ISOS o departaments de tecnologia d'algun ens o govern, encara que també les podem seguir sota petició.

Creixem i ens nodrim de les fallades i el coneixement compartit del hacking ètic. Investiguem i delimitem les nostres recerques prèvies, per a després buscar forats en els sistemes.

Fem *pentesting* (test de penetració) i qualsevol acció dins del **hacking ètic** per a provar els seus sistemes. I repetim totes les auditories, quan se suposen solucionades les fallades, per a la seva total seguretat i confiança.

Ètica. SOM ÈTICS: hem enfocat la nostra visió empresarial en aquesta paraula. No venem al millor postor els serveis que puguem oferir de tercers, sinó que solen ser empreses que també ens presten aquests serveis o que consumim nosaltres, ja que l'exemple és la millor demostració de qualitat.

Per què? Creiem que no és ètic indicar als clients els problemes que tenen, solucionar-los i després certificar que ho hem solucionat.

No obstant això, no deixem als clients, sinó que l'ajudem a buscar

als millors professionals i les millors solucions. Ens comprometem a fer un seguiment i anar de la mà amb ells durant tot el procés.

Abans de res, **claredat de conceptes.** Ens agrada que els clients ens entenguin, per això volem definir tres paraules que es repeteixen constantment en aquest sector:

Hacker: últimament s'ha desfigurat aquesta definició i se la fa sinònim de delinqüents informàtics.
Un *hacker* és algú que busca coneixement, provar-se dia a dia, compatir-ho i demostrar on ha arribat. Per exemple mostrant-li a una empresa on té vulnerabilitats en els seus sistemes perquè li posin solució.

Si ho fa per a benefici propi, segrestant dades, fent que una empresa no pugui treballar o, en definitiva buscant un lucre econòmic és un **ciberdelinqüent.**
Si el que fa és vulnerar un programari o maquinari per copiar-ho pel seu compte, és un ***cracker.***

Pentesting o test de penetració: accions tècniques concretes per a poder entrar en un sistema informàtic sense les claus adequades.

Hacking ètic: **anàlisi dels sistemes i programari informàtic, per a trobar possibles vulnerabilitats i, com no, les seves solucions a través de l'especialització tècnica, del coneixement compartit.**

Informació prèvia sobre l'obligatorietat que determinades empreses tinguin un responsable de ciberseguretat

MARC NORMATIU

Reial decret 43/2021, de 26 de gener pel qual es desenvolupa el Reial decret llei 12/2018, de 7 de setembre, **de seguretat de les xarxes i sistemes d'informació.**

Publicat en el BOE del 28 de gener de 2021, pàgines 8187 a 8214.

CONTINGUT

Estableix que els operadors de serveis essencials ***hauran de nomenar una persona o òrgan col·legiat responsable de la seguretat de la informació*** que exercirà les funcions de punt de contacte i coordinació tècnica amb l'autoritat competent i els Equips de Resposta a Incidents de Ciberseguretat (CSIRT) de referència. **Aquest servei pot ser externalitzat.**

L'objecte de la Llei és:

- Crear un marc estratègic institucional de seguretat de les xarxes i sistemes d'informació.

- La supervisió del compliment de les obligacions de seguretat dels operadors de serveis essencials.

- La gestió d'incidents de seguretat.

Per tot això, la llei s'aplicarà:

- Als serveis essencials dependents de les xarxes i sistemes d'informació de diversos sectors estratègics.

- Als serveis digitals que siguin mercats en línia, motors de cerca en línia i serveis de computació en núvol.

QUAN

En menys de tres mesos a partir de la data de publicació en el BOE. És a dir, les empreses implicades han de tenir el seu Responsable de seguretat de la informació (CISO) o un servei extern que cobreixi aquest lloc abans del 28 d'abril de 2021.

QUÈ HAN DE FER LES EMPRESES AFECTADES?

És molt important assenyalar que la llei especifica que **les empreses**, a més de tenir a aquest responsable en nòmina (tret que el servei estigui externalitzat) **han de facilitar els mitjans i posar tota l'obstinació a fer les seves tasques.**

Entre les moltes tasques que ha de complir i efectuar destaquem les següents:

- Anàlisi i gestió de riscos.
- Gestió de riscos de tercers o proveïdors.
- Catàleg de mesures de seguretat, organitzatives, tecnològiques i físiques.
- Gestió del personal i professionalitat.
- Adquisició de productes o serveis de seguretat.
- Detecció i gestió d'incidents.
- Plans de recuperació i assegurament de la continuïtat de les operacions.
- Millora contínua.
- Registre de l'activitat dels usuaris.

QUÈ ÉS I QUÈ FA EL RESPONSABLE DE LA SEGURETAT DE LA INFORMACIÓ O CISO?

Les funcions del CISO són molt variades i essencials per a complir amb tots els protocols que marca la llei. Destaquem:

a) Elaborar i proposar per a l'aprovació de l'organització, les polítiques de seguretat, que inclouran les mesures tècniques i organitzatives, adequades i proporcionades, per a gestionar els riscos que es plantegin per a la seguretat de les xarxes i sistemes d'informació utilitzats.

També per a prevenir i reduir al mínim els efectes dels ciberincidents que afectin l'organització i els serveis.

(Article 6.2 d'aquest reial decret).

b) Supervisar i desenvolupar l'aplicació de les polítiques de seguretat, normatives i procediments derivats de l'organització, supervisar la seva efectivitat i dur a terme controls periòdics de seguretat.
c) Elaborar el document ***Declaració d'Aplicabilitat de mesures de seguretat.***

(Article 6.3 paràgraf 2n d'aquest reial decret.)

d) Actuar com a capacitador de bones pràctiques en seguretat de les xarxes i sistemes d'informació, tant en aspectes físics com lògics.
e) Remetre a l'autoritat competent, a través del CSIRT (Equip de Resposta a Incidents de Ciberseguretat) de referència i sense dilació indeguda, les notificacions d'incidents que tinguin efectes pertorbadors en la prestació dels serveis als quals es refereix l'article 19.1 del Reial decret llei 12/2018, de 7 de setembre.
f) Rebre, interpretar i supervisar l'aplicació de les instruccions i guies emanades de l'autoritat competent, tant per a l'operativa habitual com per a l'esmena de les deficiències observades.
g) Recopilar, preparar i subministrar informació o documentació a l'autoritat competent o al CSIRT de referència, a la seva sol·licitud o per pròpia iniciativa.

UN CISO EXTER LA MILLOR SOLUCIÓ

QUÈ US PODEM OFERIR?

Avantatges

- Estalvi significatiu, per la diferència entre el cost del nostre servei i el sou que pot arribar a tenir un CISO professional.

- Confiança i competitivitat, ja que la nostra empresa compta amb professionals qualificats per a prestar tots els nostres serveis amb la major eficiència.

- Contacte únic, ja que qualsevol necessitat en seguretat us la podem proporcionar nosaltres directament o a través dels nostres partners, que són els que utilitzem per a nosaltres.

PER QUÈ TECNOideas?

Perquè oferim serveis informàtics des de l'any 2009.

Perquè som especialistes en ciberseguretat des de l'any 2018.

Perquè **som ètics**.

Perquè tenim un equip d'experts perfectament formats.

Perquè valorem no sols la tècnica, sinó el tracte humà. Amb TECNOideas podreu parlar amb un tècnic expert: no sols utilitzem màquines per a fer el treball.

Perquè sabem escoltar i comprendre les **necessitats reals** d'una empresa, sigui gran o pime.

Perquè podem ajustar les tarifes als requeriments reals d'una empresa.

Perquè TECNOideas està qualificat per a complir tots els requisits que marca la llei.

ALGUNES DE LES TITULACIONS DEL NOSTRE EQUIP

- Enginyeria Electrònica Industrial
- Enginyeria Tècnica Informàtica de Sistemes
- Màster en direcció d'equips directius
- Màster en Indústria 4.0
- ICS Security Architect
- Pèrit informàtic col·legiat

Formem part des del 2019 del Catàleg del Incibe, el [Instituto de Ciberseguridad de España.]

Posseïm la màxima certificació professional (nivell Negre) del **[Centro de Ciberseguridad Industrial.]**

I a més posseïm aquestes **certificacions internacionals**: