HUB

Cambra Digital Vic

Ciberseguretat 2.0: la IA i els nous riscos de les pimes.

cambra Digital

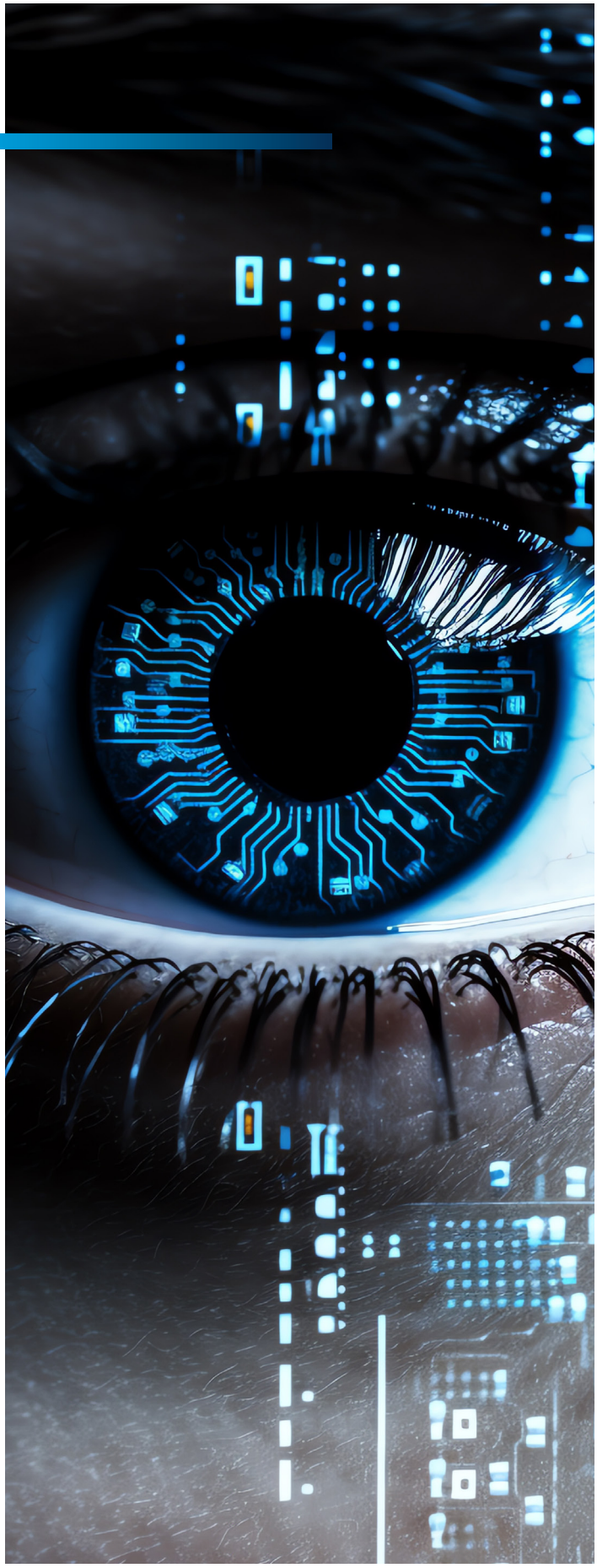
Cofinanciado por la Unión Europea
Cofinançat per la Unió Europea
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Fondos Europeos
Fons Europeus
cámaras Fundación INCYDE
Cambra de Comerç de Barcelona

El **HUB cambraDigital VIC** és un espai obert a tot el teixit empresarial del territori.

Ofereix solucions d'espais de treball flexible així com sales de reunions i una zona per cocrear o connectar amb altres empresaris i empresàries. El HUB és un projecte polivalent que vol promoure les TIC, la innovació i la internacionalització en els plans de negoci de les pimes i start-ups del territori.

ÍNDEX

1. Introducció



La intel·ligència artificial (IA) és una eina extraordinàriament útil per a accelerar determinats processos productius, dur a terme tasques repetitives i monòtones i incrementar la productivitat. També és un dels eixos imprescindibles que defineixen la ciberseguretat 2.0.

En comparació amb la ciberseguretat tradicional, basada en la protecció de la informació de manera reactiva, sorgeix aquest concepte que ens obliga a ser proactius. Ha estat una evolució, els primers passos de la qual es van donar amb la tríada formada per la confidencialitat, la integritat i la disponibilitat. Després, es va incorporar la seguretat OT o de la tecnologia de les operacions, que en va prioritzar el control.

2. La IA i la seguretat

La simbiosi entre totes dues és clara i inequívoca. El motiu és la capacitat de la IA per a gestionar volums de dades molt grans i l'eficiència que té per dur a terme tasques complexes, ja que disposa d'algorismes que processen amb rapidesa. A més, identifica patrons que podrien detectar amenaces. Els sistemes d'informació actuals i les xarxes generen quantitats ingents de dades molt complicades de gestionar amb els mètodes tradicionals.

D'altra banda, té la capacitat d'aprendre de manera contínua gràcies a l'aprenentatge automàtic. En conseqüència, s'adapta més bé als nous contextos i ciberdelictes. De fet, es pot entrenar perquè detecti activitats sospitoses en temps real. Identifica ràpidament qualsevol anomalia mitjançant l'anàlisi de patrons de trànsit en la xarxa, de transaccions dels usuaris i de comportaments del sistema.

Una altra de les aplicacions que té es relaciona amb la seva resposta en cas de possibles incidents de seguretat. En aquest sentit, ofereix un servei enorme a les pimes i organitzacions, que poden actuar i recuperar-se amb més celeritat i eficàcia. D'altra banda, pot donar una informació molt valuosa sobre l'amenaça, el seu origen i la naturalesa que té, així com de les solucions.

2.1 Els sistemes autònoms d'IA

Són sistemes que operen sense necessitat d'intervenció humana. Són independents i estan capacitats per a prendre decisions sobre seguretat i respondre per si mateixos a les amenaces que detectin. Fan servir tècniques d'aprenentatge profund i incorporen les seves pròpies experiències.

2.2 Algunes eines d'IA per a pimes

Teniu a la vostra disposició diverses eines d'IA que podeu aplicar a diferents àrees de les pimes. Us n'esmentem algunes de les més populars:

1 ChatGPT

És la que lidera, a hores d'ara, el desenvolupament d'aquesta tecnologia. És molt útil per a analitzar les dades del vostre negoci, crear anuncis o polir l'estratègia de màrqueting.

2 Salesforce Einstein

Us ofereix recomanacions avançades i prediccions amb les dades.

3 Analytics Intelligence

Amb aquesta eina podreu descobrir tendències i noves oportunitats.

4 Kuki

Està especialitzada en botigues virtuals i us ajuda a guiar els clients durant el procés de compra.

3. Els riscos de la IA per a les pimes

Sens dubte, la IA té avantatges notables i gens exagerats. No obstant això, heu de parar atenció als possibles riscos que comporta. El primer indicador es va descobrir el mes de maig, quan el científic britànic Geoffrey Hinton, un dels creadors, va renunciar al seu lloc a Google. Entre les seves explicacions, va al·legar que haurien d'haver esperat abans de llançar-la.

El mateix van deixar per escrit 1.300 experts en una carta, en què suggerien la necessitat de frenar el llançament de la IA, almenys, durant sis mesos. El motiu és que l'evolució d'aquesta tecnologia és infinitament més ràpida que el ritme que segueixen els legisladors per a regular-la. Us expliquem alguns dels perills que comporta aquesta asincronia.

3.1 Responsabilitat objectiva indeterminada

Imagineu que una màquina autònoma guiada per IA provoca un accident. Partim de la base que, encara que és una tecnologia increïble, també falla. De fet, pot ser objecte de demandes de responsabilitat civil pels danys que causi. Amb el buit legal actual, seria impossible determinar si qui ha de pagar és l'empresa que feia servia la IA o el proveïdor d'aquesta tecnologia.

La Unió Europea ha estat el primer territori que s'ha adonat d'aquest problema. A l'octubre del 2022, la Comissió va presentar una proposta de revisió i una altra d'una directiva específica per a aquesta tecnologia, totes dues vinculades a la responsabilitat. Tanmateix, encara estan en el procés d'al·legacions i no s'han aprovat.

3.2 Informació falsa

La IA és capaç d'imitar la veu de qualsevol persona, de crear imatges falses i, fins i tot, de proporcionar informació completament errònia. No és difícil imaginar el que això pot suposar per al sistema polític d'un país en mans inadequades, per a l'honor d'una persona o per a la vostra imatge com a marca. Amb les eines correctes, qualsevol persona pot iniciar una campanya de descrèdit sense que us pugui protegir res ni ningú.

3.3 La doble cara de la IA pel que fa a la ciberseguretat

Efectivament, la intel·ligència artificial és una arma de doble tall pel que fa a la ciberseguretat. Ja hem vist com us pot ajudar. Així i tot, també és fonamental que en tingueu presents els efectes menys controlables. Les aplicacions que fan servir IA manegen moltes dades,

però no queda molt clar on s'emmagatzemen ni a quina mena de tractaments estan sotmeses. Això, lògicament, és un gran atractiu per als ciberdelinqüents, i les pimes miren amb preocupació aquest fet.

D'altra banda, la intel·ligència artificial està igualment disponible per als ciberdelinqüents. Tot i que, de moment, encara no han generat cap programa maliciós o malware, hi ha tres àrees clau en què els models lingüístics són atractius:

1- Suplantació d'identitat molt més eficaç.

2- Els ciberdelinqüents que fan servir el programaria de segrest o ransomware poden automatitzar els rescats i estalviar temps per a dedicar-se a delinquir més.

3- Millora les estafes telefòniques.

3.4 Plantilles desmotivades i sense formació a les pimes

S'ha parlat tant dels llocs de treball que es poden substituir pels sistemes d'IA que, inevitablement, s'ha introduït en les plantilles una certa temença. Segons la Fundación Aquae, la IA ocuparà un 16% dels llocs de treball la dècada vinent. De fet, el Parlament Europeu ha quantificat en un 14% les feines automatizables als països de l'OCDE, i el 32% dels llocs de treball es veuran afectats d'una manera o una altra.

Per tant, és cert que aquesta tecnologia podrà fer moltes feines, però també ho és que se'n crearan altres de noves. El motiu és que aquestes solucions avançades necessiten humans per a gestionar-se i mantenir-se.

Un sistema educatiu enfocat en la nova realitat i la formació dels treballadors jugarà un rol essencial amb un objectiu doble. D'una banda, evitarà la desocupació a llarg termini i, de l'altra, garantirà que hi hagi mà d'obra qualificada per a aquest context nou.

3.5 Risc de biaixos i minva dels drets fonamentals

Els biaixos, intencionals o involuntaris, són una realitat perquè depenen de les dades que gestioni el sistema o del disseny que tingui. En conseqüència, els seus resultats podrien reflectir o replicar discriminacions o desigualtats racials i ètniques, sexistes, per edat o de qualsevol altra naturalesa. Per agreujar aquest problema, l'ús de dades numèriques per a descriure una realitat social complexa hi proporciona una pàtina d'objectivitat que és completament falsa. És el fenomen conegut com a mathwashing. Ja us podeu imaginar el que suposaria una presa de decisions basada en un sistema constituït així, per exemple, a l'hora de demanar un prés-

tec. Igualment, provocaria discriminacions en el vostre àmbit a l'hora de decidir qui s'ha de contractar o acomiadar, si hi ha biaixos d'edat, racials, religiosos o sexistes.

3.6 Amenaça a les democràcies

Molts experts temen que pugui estimular la inestabilitat política i, per extensió, l'econòmica i social. El motiu és que és una eina amb què es pot manipular qualsevol procés democràtic. D'aquesta manera, ens pot portar a una situació de desconfiança generalitzada. Per començar, implica un determinat perill en el tractament de la informació del procés democràtic. Si ja heu vist l'esfera mediàtica en què s'han convertit les xarxes socials, imagineu el que suposaria alimentar-les amb informació no verificada i que barreja opinions i coneixements.

Seria un gran difusor de notícies falses. Algunes persones ho podrien fer servir amb finalitats de desinformació i per tal de distorsionar l'opinió pública. Així mateix, podria tenir un gran impacte en el sentit del vot, en una direcció o l'altra. La ciutadania es quedaria sense capacitat per a prendre decisions informades i autònomes. En definitiva, tots estaríem en mans dels propietaris d'empreses privades amb finalitats comercials que ens proveeixen d'intel·ligència artificial.

4. Quins perills ens esperen en el futur immediat?

L'Agència de la Unió Europea per a la Ciberseguretat (ENISA) ha elaborat una llista amb les principals amenaces que preveu que hi haurà en el futur immediat, concretament, el 2030.

Segons els seus càlculs, els perills estaran diversificats i seran molt semblants als actuals, però amb matisos més complexos per les tecnologies utilitzades. Hi destaquen:

1 Campanyes de desinformació avançada. Ja les hem pogut veure en nombroses campanyes electorals arreu del món.

2 Un augment de comportaments autoritaris en els poders públics i de la vigilància digital i, en conseqüència, una pèrdua de privacitat.

3 Errors humans, la majoria dels quals pel que fa als sistemes ciberfísics actuals.

4 Atacs per mitjà de dispositius intel·ligents.

5 Increment d'amenaces híbrides.

6 Manca d'habilitats.

7 Sobreutilització de la intel·ligència artificial.

En resum, la ciberseguretat 2.0 és extremadament important i convé que us hi familiaritzeu. Tot i que hi ha parts que no estan exemptes de polèmica, constituirà un pas de gegant en la manera d'abordar la seguretat a les pimes amb l'ajuda inestimable de la IA. Per tant, és vital una formació de qualitat i us convidem a participar en els nostres cursos i seminaris. "Consulteu la nostra agenda i apunteu les dates que us interessin!"

HUB

CambraDigital Vic

cambra Digital

Cofinanciado por la Unión Europea
Cofinançat per la Unió Europea
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA
Fondos Europeos
Fons Europeus
cámaras Fundación INCYDE
Cambra de Comerç de Barcelona