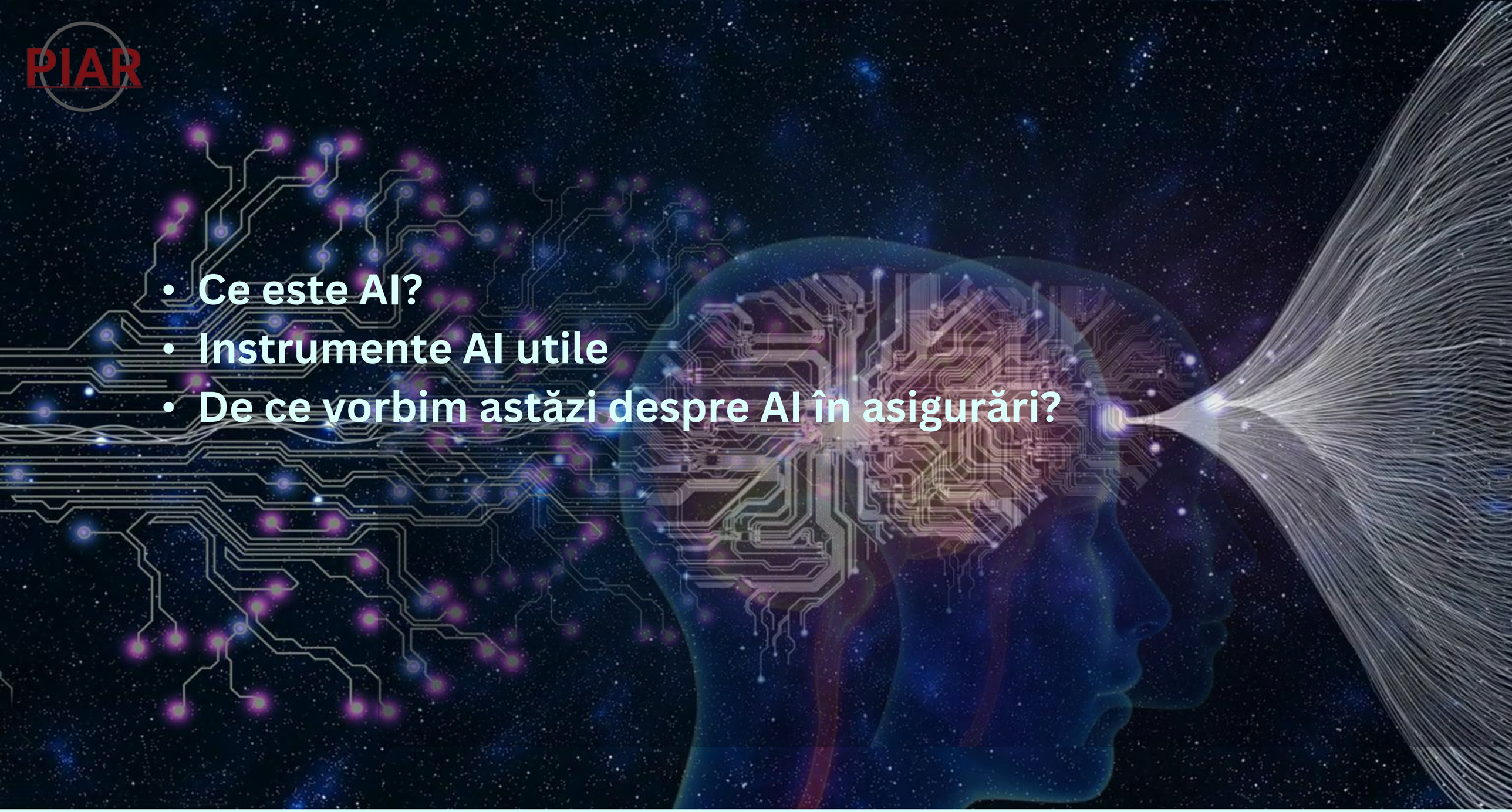
AI & Cybersecurity în Asigurări


PIAR
• Ce este AI?
• Instrumente AI utile
• De ce vorbim astăzi despre AI în asigurări?

Ce este Inteligența Artificială?

AI (Inteligența Artificială) este un tip de tehnologie care îi permite unui computer să „învețe” din date, să ia decizii și să rezolve probleme, la fel cum ar face un om – doar că mai repede și fără să obosească.

Instrumente AI

Grok, dezvoltat de compania lui Elon Musk, concurează cu ChatGPT

ChatGPT, asistent AI avansat creat de OpenAI

Gemini, model de AI de la Google DeepMind

ChatPlayground este o platformă care permite utilizatorilor să compare diverse modele de AI

Claude AI este un model lingvistic dezvoltat de Anthropic

Canva, instrument online pentru design grafic

Exemple de Prompturi AI

Scenariu: Crearea unei oferte personalizate

„Generează o propunere de poliță pentru un client de 45 de ani, fumător, care dorește asigurare de viață pe 20 de ani, cu acoperire pentru boli grave.”

- **ChatGPT** sau **Claude.ai** – pentru redactarea rapidă și clară a ofertelor
- **Tidio AI / Zendesk AI** – pentru răspuns automat în chatbot

Scenariu: Detectarea fraudelor

„Analizează aceste 500 de dosare de daună și semnalează orice anomalie legată de frecvența daunelor sau valori suspecte.”

- **Google Cloud AutoML**
- **Darktrace** – AI pentru securitate și analiză comportamentală

Scenariu: Rezumat al unei polițe pentru client

„Rezumă această poliță de 20 de pagini într-un text de maximum 5 fraze, pe înțelesul unui client fără experiență în asigurări.”

- **ChatGPT** - cu document upload
- **Claude.ai** - bun la procesarea textelor lungi

Exemple de Prompturi AI

Scenariu: Răspuns automat la întrebări frecvente

„Creează un răspuns automat pentru întrebarea ‘Ce acoperă asigurarea mea de locuință în caz de inundație?”

- **ChatGPT/Grok**
- **Tars AI, Drift AI** – pentru chatbot personalizat pe site-uri de asigurări

Scenariu: Securitate cibernetică în rețea

„Monitorizează și raportează orice comportament anormal în accesarea bazelor de date ale clienților în timp real.”

- **Darktrace, CrowdStrike Falcon** – soluții AI pentru detectare și răspuns la amenințări
- **Azure Sentinel** (Microsoft AI pentru securitate)

Scenariu: Training intern / simulări

„Creează un test cu 5 întrebări pentru noii angajați despre ce trebuie făcut la preluarea unei cereri de daună.”

- **ChatGPT/Grok**
- **Khanmigo, Tome.app** – pentru creare de lecții interactive cu AI

Unde se folosește deja AI în asigurări?

- **Evaluarea riscurilor automatizată**

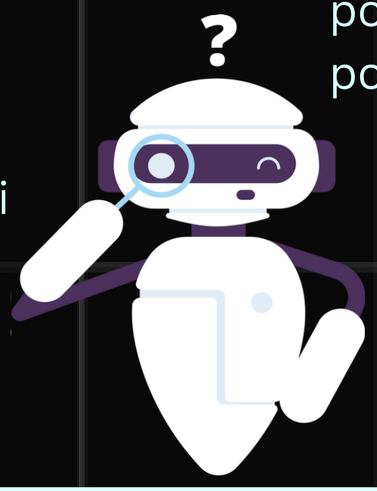
AI analizează rapid istoricul clientului, datele demografice, stilul de viață, chiar și comportamentul online (unde este permis), pentru a calcula nivelul de risc asociat.

- **Găsirea poliței potrivite pentru client**

Pe baza răspunsurilor și nevoilor clientului, AI recomandă pachetul cel mai potrivit.

- **Procesarea rapidă a daunelor**

AI poate analiza fotografii, formulare, și detalii trimise de client pentru a estima costurile și a accelera soluționarea.



- **Detectarea fraudelor**

AI „învață” din dosarele vechi și poate identifica tipare suspecte în cererile noi

- **Chatboți și asistenți virtuali pentru clienți**

Disponibili 24/7, acești „roboți de conversație” pot răspunde la întrebări frecvente, oferi statusul poliței, ajuta cu pașii unei daune etc.

Beneficii pentru angajați și clienți

- **Procesare mai rapidă a cererilor și daunelor**

AI poate analiza documente, imagini și formulare în câteva secunde – ceea ce înseamnă timpi de așteptare mai scurți pentru clienți și mai puțin stres pentru angajați.

- **Reducerea riscurilor și a erorilor umane**

AI lucrează cu precizie matematică și poate identifica greșeli sau incoerențe pe care un om grăbit le-ar putea rata.

- **Recomandări personalizate pentru clienți**

AI analizează nevoile fiecărui client și propune polițe potrivite, crescând satisfacția și șansele de conversie.

- **Detectarea mai eficientă a fraudelor**

Prin analizarea tiparelor și comportamentelor suspecte, AI poate semnala rapid cazurile de fraudă înainte ca ele să producă pierderi.

Beneficii pentru angajați și clienți

- **Telematică**

În asigurările auto, AI analizează datele de la vehiculele conectate pentru a evalua comportamentul de conducere, permițând modele de asigurare bazate pe utilizare care recompensează conducerea în siguranță.

- **Asigurare de sănătate**

AI ajută la analizarea datelor pacienților și la prezicerea costurilor de asistență medicală, ceea ce ajută asigurătorii să proiecteze planuri de sănătate mai bune și să gestioneze cererile mai eficient.

- **Economie de timp pentru angajați**

AI preia sarcinile repetitive și administrative, permițând angajaților să se concentreze pe consiliere, relaționare și decizii strategice.

Aceste tehnologii nu numai că eficientizează operațiunile, dar stimulează și inovația în ofertele de produse, ceea ce duce în cele din urmă la o industrie a asigurărilor mai centrată pe client.

Provocările asociate utilizarii etice și responsabile a AI

Utilizarea etică și responsabilă a AI este esențială, în special în sectoare sensibile precum asigurările, unde deciziile pot avea un impact semnificativ asupra vieții și bunăstării financiare a clienților. Iată câteva dintre provocările cheie asociate cu utilizarea etică și responsabilă a AI:

Erori și corectitudine

Date cu erori: Sistemele AI pot moșteni erori prezente în datele din mediu test, ceea ce duce la un tratament nedrept al anumitor grupuri. De exemplu, dacă datele istorice reflectă discriminarea sistemică, modelele AI pot perpetua aceste prejudecăți în subscriere sau procesarea cererilor.

Transparență algoritmică: Multe modele AI, în special algoritmii de învățare profundă, funcționează ca si "cutii negre", ceea ce face dificilă înțelegerea modului în care se iau deciziile. Această lipsă de transparență poate ascunde erori și poate împiedica responsabilitatea.

Confidențialitatea și securitatea datelor

Utilizarea datelor personale: AI se bazează adesea pe seturi mari de date, care pot include informații personale sensibile. Asigurarea faptului că datele sunt colectate, stocate și utilizate în conformitate cu reglementările de confidențialitate (cum ar fi GDPR) este o provocare semnificativă.

Încălcări ale datelor: Cu cât sunt colectate și procesate mai multe date, cu atât este mai mare riscul de încălcare a datelor, care pot expune informații sensibile și pot duce la furt de identitate sau fraudă.

Responsabilitate

Responsabilitatea luarii deciziilor: Când sistemele AI iau decizii, poate fi neclar cine este responsabil pentru acele decizii: fie că este vorba de dezvoltatori, asigurători sau AI în sine. Această ambiguitate complică responsabilitatea în cazul unor erori sau rezultate negative.

Conformitatea cu reglementările: Respectarea reglementărilor existente în timp ce navighează în peisajul în evoluție al guvernanței AI poate fi o provocare pentru organizații.

Transparență și explicabilitate

Lipsa explicabilității: Multe modele AI, în special cele complexe, nu sunt explicabile, ceea ce face dificilă înțelegerea modului în care se iau deciziile. Acest lucru poate eroda încrederea în rândul clienților și al autorităților de reglementare.

Nevoia de comunicare clară: Asigurătorii trebuie să comunice clienților modul în care AI este utilizată în procesele de luare a deciziilor, ceea ce poate fi o provocare dacă algoritmii de bază nu sunt ușor de interpretat.

Provocările asociate utilizarii etice și responsabile a AI

Utilizarea etică a IA

Manipulare și exploatare: Există riscul ca AI să fie folosită pentru a manipula clienții, cum ar fi prin marketing direcționat care exploatează vulnerabilități sau îndemnuri comportamentale care ar putea să nu fie în interesul consumatorului.

Consimțământ informat: Asigurarea faptului că clienții înțeleg modul în care vor fi utilizate datele lor, astfel ca obținerea consimțământului informat poate fi dificilă, mai ales atunci când sistemele AI sunt complexe.

Automatizarea locurilor de muncă și impactul asupra forței de muncă

Automatizarea locurilor de muncă: Implementarea AI poate duce la înlocuirea locurilor de muncă în anumite roluri, ridicând provocari etice cu privire la impactul asupra angajaților și la nevoia de recalificare.

Diversitatea forței de muncă: Asigurarea diversității în echipele de dezvoltare AI este crucială pentru a atenua prejudecățile și a promova considerentele etice, dar obținerea acestei diversități poate fi o provocare.

Provocare legală și de reglementare

Reglementări în evoluție: Peisajul de reglementare pentru AI este în dezvoltare, iar organizațiile trebuie să rămână informate cu privire la noile legi și linii directoare care guvernează utilizarea AI.

Standarde globale: Diferite țări au reglementări proprii cu privire la AI, ceea ce face dificilă respectarea tuturor legilor aplicabile pentru asigurătorii multinaționali.

Percepția și încrederea publică

Construirea încrederii: Câștigarea încrederii publicului în sistemele AI este esențială, în special în asigurări, unde deciziile pot avea consecințe semnificative. Percepțiile negative despre AI pot împiedica adoptarea și acceptarea.

Dezinformare: Răspândirea dezinformării despre capacitățile și riscurile AI poate duce la teamă și scepticismul publicului, complicând eforturile de implementare responsabilă a AI.

Abordarea acestor provocări necesită o abordare cu mai multe fațete, inclusiv dezvoltarea de orientări etice, cadre de guvernanță solide și dialog continuu între părțile interesate.

Asigurătorii și dezvoltatorii AI trebuie să acorde prioritate transparenței, corectitudinii și responsabilității pentru a se asigura că AI este utilizată în mod responsabil și etic, în cele din urmă beneficiind atât industria, cât și clienții săi.

Ce face AI în securitate cibernetică?

- **Monitorizează continuu** sistemele pentru activitate suspectă
- **Detectează și oprește atacuri** în timp real
- **Analizează modele de comportament** pentru a anticipa breșe de securitate
- **Prioritizează amenințările** în funcție de severitate și impact

De ce e important în asigurări?

- Lucrăm cu **date personale sensibile** (CNP, venituri, starea de sănătate)
- Orice breșă de securitate poate duce la **pierderi de încredere, amenzi și daune reputaționale**
- AI ajută la **protejarea clienților și respectarea reglementărilor (ex: GDPR)**

Cybersecurity în asigurări

Securitatea cibernetică este o preocupare critică pentru industria asigurărilor, deoarece se confruntă cu provocări și riscuri unice asociate cu dependența tot mai mare de tehnologiile digitale și cantitățile mari de date sensibile pe care le gestionează. Iată câteva aspecte cheie ale securității cibernetice în sectorul asigurărilor:

Peisajul amenințărilor

Atacuri cibernetice: Industria asigurărilor este o țintă principală pentru infractorii cibernetici datorită datelor valoroase pe care le deține. Amenințările comune includ atacuri ransomware, scheme de phishing și breșe de date.

Amenințări interne: Angajații sau contractorii cu acces la informații sensibile pot reprezenta un risc, fie prin intenții rău intenționate, fie prin acțiuni neintenționate.

Confidențialitatea și securitatea datelor

Informații sensibile: Companiile de asigurări colectează și stochează o mulțime de informații personale și financiare, inclusiv numere de securitate socială, dosare medicale și detalii de plată. Protejarea acestor date împotriva breșelor este esențială.

Conformitatea cu reglementările: Asigurătorii trebuie să respecte diverse reglementări privind protecția datelor, cum ar fi Regulamentul general privind protecția datelor (GDPR) în Europa și Legea privind portabilitatea și responsabilitatea asigurărilor de sănătate (HIPAA) din SUA, care impun cerințe stricte privind gestionarea datelor și confidențialitatea.

Evaluarea si managementul riscurilor

Evaluări de vulnerabilitate: Asigurătorii trebuie să-și evalueze în mod regulat sistemele pentru vulnerabilități și să implementeze măsuri de atenuare a riscurilor.

Riscul terților: Mulți asigurători se bazează pe furnizori terți pentru diverse servicii, ceea ce poate introduce riscuri suplimentare de securitate cibernetică. Managementul eficient al furnizorilor și due diligence sunt esențiale.

Răspuns la incidente și recuperare

Planuri de răspuns la incidente: Dezvoltarea și menținerea unui plan robust de răspuns la incidente este crucială pentru minimizarea impactului unui incident cibernetic. Aceasta include identificarea personalului cheie, strategiile de comunicare și procedurile de recuperare.

Continuitatea afacerii: Asigurătorii trebuie să se asigure că au planuri de continuitate a afacerii pentru a menține operațiunile în timpul și după un incident cibernetic.

Cybersecurity în asigurări

Instruirea și conștientizarea angajaților

Instruire în domeniul securității cibernetice: Instruirea periodica a angajaților cu privire la cele mai bune practici de securitate cibernetică, cum ar fi recunoașterea tentativelor de phishing și securizarea datelor sensibile, este esențială pentru reducerea erorilor umane.

Cultura securității: Promovarea unei culturi de conștientizare a securității cibernetice în cadrul organizației poate ajuta angajații să-și înțeleagă rolul în protejarea informațiilor sensibile.

Tehnologie si instrumente

Soluții avansate de securitate: Asigurătorii adoptă din ce în ce mai mult tehnologii avansate de securitate cibernetică, cum ar fi inteligența artificială (AI) și învățarea automată, pentru a detecta și a răspunde amenințărilor în timp real.

Criptare și control al accesului: Implementarea protocoalelor puternice de criptare și a controalelor de acces poate ajuta la protejarea datelor sensibile împotriva accesului neautorizat.

Reglementari si conformitate

Cerințe de conformitate: Asigurătorii trebuie să navigheze într-un peisaj complex de reglementări legate de securitatea cibernetică, inclusiv legi specifice statului din SUA (de exemplu, Regulamentul de securitate cibernetică din New York) și standarde internaționale.

Răspundere și asigurare: Pe măsură ce riscurile cibernetice cresc, asigurătorii dezvoltă, de asemenea, produse de asigurare cibernetică pentru a acoperi companiile împotriva pierderilor cauzate de incidentele cibernetice. Acest lucru creează un rol dublu pentru asigurători atât ca protectori, cât și ca subscriitori ai riscului cibernetic.

Tehnologii emergente si provocari

Securitatea cloud: Pe măsură ce tot mai mulți asigurători trec la soluții bazate pe cloud, asigurarea securității mediilor cloud devine esențială. Aceasta include înțelegerea modelelor de responsabilitate partajată și punerea în aplicare a măsurilor de securitate adecvate.

IoT și dispozitive conectate: Creșterea Internetului lucrurilor (IoT) introduce noi vulnerabilități, deoarece dispozitivele conectate pot fi puncte de intrare pentru atacuri cibernetice. Asigurătorii trebuie să evalueze riscurile asociate cu aceste tehnologii.

Securitatea cibernetică este un aspect vital al industriei asigurărilor, necesitând atenție și investiții continue.
Pe măsură ce amenințările cibernetice continuă să evolueze, asigurătorii trebuie să adopte o abordare proactivă a securității cibernetice, concentrându-se pe managementul riscurilor, instruirea angajaților și implementarea tehnologiilor avansate de securitate.
Prin prioritizarea securității cibernetice, asigurătorii își pot proteja datele sensibile, pot menține încrederea clienților și pot asigura conformitatea cu cerințele de reglementare.

Automatizarea procesului de underwriting și evaluare a riscurilor

Underwriting-ul este procesul prin care o companie de asigurări evaluează riscul pe care și-l asumă atunci când oferă o poliță. Aceasta implică analiza datelor personale, istoricului medical, financiar, comportamental sau de business al clientului, în funcție de tipul de asigurare (viață, auto, property, sănătate, business etc.).

Procesul tradițional este adesea:

- Manual și consumator de timp;
- Subiectiv, în funcție de experiența evaluatorului;
- Limitat la un număr restrâns de variabile;
- Vulnerabil la erori umane sau documente incomplete.

Cum intervine AI în automatizarea procesului de underwriting?

- AI poate procesa volume mari de date structurale și nestructurate (rapoarte medicale, documente PDF, imagini, fișiere audio etc.).
- Modelele de machine learning analizează istoricul clienților și comportamentul acestora pentru a estima riscul în timp real.
- Scorurile sunt recalibrate continuu pe baza datelor noi (self-learning models).
- Automatizarea permite emiterea rapidă a polițelor (minute, nu zile), eliminând blocajele administrative.

Provocări și riscuri de cybersecurity asociate

Automatizarea bazată pe AI aduce și riscuri semnificative de securitate cibernetică, mai ales într-un domeniu sensibil ca asigurările:

a. *Protecția datelor personale*

- Modelele AI prelucrează informații sensibile (CNP, date medicale, scoruri de credit etc.).
- Atacurile cibernetice pot compromite aceste date, afectând reputația și conformitatea legală (GDPR).

b. *Manipularea modelelor de AI*

- Modelele pot fi manipulate prin "data poisoning" – introducerea intenționată a unor date false pentru a influența scorul de risc.
- Se impune validarea și auditarea continuă a algoritmilor.

c. *Accesul neautorizat și lipsa trasabilității*

- Automatizarea completă, fără controale umane, poate duce la decizii inexplicabile (black-box models).
- Este esențială implementarea unor soluții de AI Explainability și Zero Trust Architecture.

Ce este NIS2 și de ce contează pentru companiile de asigurări?

Directiva NIS2 (Network and Information Systems Directive 2), adoptată la nivelul UE și obligatorie din octombrie 2024, impune **standardele minime de securitate cibernetică** pentru entitățile esențiale și importante, inclusiv companiile de asigurări.

Companiile de asigurări sunt vizate explicit, deoarece sunt considerate **operatori critici de servicii financiare** – iar compromiterea infrastructurii lor ar putea afecta stabilitatea economică și încrederea publicului.

Obligațiile cheie din NIS2 pentru companiile de asigurări

a. Măsuri stricte de management al riscului cibernetic

- Politici clare de securitate;
- Protecție împotriva atacurilor;
- Securizarea lanțului de aprovizionare digitală (third-party vendors, furnizori de soluții AI etc.).

b. Raportarea incidentelor

- Obligația de notificare a incidentelor majore în termen de 24 de ore;
- Necesitatea unor proceduri documentate de răspuns la incidente.

c. Evaluări și audituri periodice

- Companiile trebuie să demonstreze conformitatea continuă, nu doar punctuală.

Implicarea DPO-ului (Responsabilul cu Protecția Datelor)

a. Evaluarea legalității datelor folosite de AI

- Verifică dacă datele prelucrate (inclusiv cele din surse externe) au consimțământ valid sau alt temei legal.
- Asigură că datele sunt minimizate, exacte și stocate în siguranță.

b. Coordonarea evaluărilor de impact (DPIA)

- În cazul folosirii AI pentru profilare automată sau luarea de decizii cu efecte juridice (ex: refuzul unei polițe), se impune o evaluare de impact GDPR.

c. Transparență față de clienți

- DPO-ul trebuie să se asigure că modelele AI nu devin „cutii negre” pentru clienți și că există o formă de explicație privind deciziile luate.

Implicarea CISO-ului (Chief Information Security Officer)

a. Securitatea algoritmilor AI și a infrastructurii

- Asigură protecția datelor de antrenare și a modelelor AI împotriva accesului neautorizat;
- Implementează controale privind integritatea modelelor și ale rezultatelor generate.

b. Gestionarea riscurilor din lanțul de aprovizionare

- Modelele AI cumpărate de la terți trebuie verificate pentru vulnerabilități;
- Soluțiile cloud sau API-urile externe trebuie evaluate înainte de integrare.

c. Colaborare cu departamentul de AI/Data Science

- CISO-ul trebuie să participe la definirea procedurilor de auditare a modelelor AI;
- Asigurarea implementării unor mecanisme de logare, back-up și rollback în cazul unui atac sau erori AI.

Colaborarea DPO–CISO–AI/IT pentru conformare NIS2

Un cadru eficient de conformare presupune o echipă transfuncțională:

ROL	Responsabilități în contextul AI & NIS2
DPO	Legalitate, protecția datelor, transparență și drepturile persoanei vizate
CISO	Securitate IT, continuitate operațională, control asupra vulnerabilităților AI
AI/IT	Dezvoltarea, testarea și operarea sigură a modelelor AI

Mituri și adevăruri despre AI

AI va înlocui complet oamenii

AI preia sarcinile repetitive sau voluminoase, dar oamenii rămân esențiali pentru empatie, creativitate, relaționare și luarea deciziilor complexe.
AI poate tria sute de cereri de ofertă, dar tu ești cel care înțelege nevoile reale ale clientului.

AI este perfect și obiectiv

AI poate reflecta părtiniri existente în datele pe care le-a învățat. De aceea este important ca oamenii să-l supervizeze și să-l corecteze.
Dacă un sistem AI a fost „hrănit” doar cu date de la un anumit tip de clienți, poate discrimina fără să își dea seama.

AI ia decizii singur și nu greșește

AI funcționează pe baza datelor primite. Dacă datele sunt greșite sau incomplete, și AI-ul va da rezultate greșite. Are nevoie de oameni să îl supravegheze.
Dacă cineva introduce greșit vârsta unui client, AI-ul poate recomanda o poliță nepotrivită.

AI înseamnă roboți cu formă umană

AI înseamnă, de cele mai multe ori, algoritmi invizibili care rulează în spate – nu roboți care merg sau vorbesc.
Sistemele care calculează riscuri, procesează daune sau recomandă polițe – toate sunt AI, dar nu arată ca în filme.