AZiTREND

Ghidul securității cibernetice a rețelelor și sistemelor informatice din spațiul cibernetic național civil

Aplicabilitate pentru soluții video integrate

Ghidul securității cibernetice a rețelelor și sistemelor informatice din spațiul cibernetic național civil - aplicabilitate pentru soluții video integrate

Tehnologia video joacă un rol esențial în securitatea organizațiilor și a infrastructurilor critice, iar **securitatea cibernetică a sistemelor video integrate** devine o prioritate.

Sistemele moderne de supraveghere video nu mai sunt simple camere care înregistrează imagini; ele sunt echipate cu **inteligență artificială (AI), analiză comportamentală, recunoaștere facială și monitorizare IoT**, devenind puncte vulnerabile în ecosistemul de securitate cibernetică.

Compania **AZITREND**, specializată în dezvoltarea de **soluții personalizate de video management, analiză video și integrare a securității video**, înțelege provocările generate de digitalizarea accelerată și de **noile riscuri cibernetice**.

În acest context, ghidul de față oferă un cadru clar și structurat pentru protejarea infrastructurilor video împotriva atacurilor cibernetice, aliniindu-se la cerințele **Ordonanței de Urgență nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil** și **Directivei NIS 2**.

Obiectivele ghidului:

- oferirea de **recomandări practice** pentru protejarea rețelelor video și a infrastructurilor de stocare și analiză video;
- explicarea **cerințelor legale** impuse de Directiva NIS 2 și legislația națională;
- sprijinirea entitățile esențiale și importante în **implementarea măsurilor de securitate cibernetică**;
- evidențierea **strategiilor eficiente de prevenire și reacție** în fața atacurilor cibernetice asupra sistemelor video.

Public-țintă:

- **operatori de infrastructuri critice** ce utilizează soluții de video management;
- **instituții publice și private** care implementează sisteme video avansate;
- **echipelor IT și specialiștilor în securitate** care administrează platforme de analiză video;
- **companiilor de securitate** care oferă servicii de video monitoring și integrare.

Prin aplicarea acestor măsuri, organizațiile își pot asigura **continuitatea operațională**, protejând **datele, rețelele și utilizatorii** împotriva amenințărilor cibernetice moderne.

Cadrul legislativ și instituțional

Reglementările europene și naționale stabilesc cerințe stricte pentru protejarea rețelelor și sistemelor informatice, inclusiv cele utilizate pentru **management video, analiză video și soluții video integrate de securitate**. Pentru a asigura un nivel ridicat de securitate, companiile care furnizează astfel de soluții trebuie să respecte un set clar de obligații impuse prin **Ordonanța de Urgență nr. 155/2024** și **Directiva NIS 2**.

Ordonanța de Urgență nr. 155/2024

Această reglementare națională creează **cadrul juridic și instituțional** necesar pentru protejarea rețelelor și sistemelor informatice din spațiul cibernetic național civil. Se aplică tuturor entităților esențiale și importante care gestionează date sensibile și oferă servicii critice, incluzând **furnizorii de soluții video integrate**. Printre obligațiile principale, impuse de OUG 155/2024 se numără:

- Implementarea măsurilor tehnice și organizatorice pentru **gestionarea riscurilor cibernetice**;
- Raportarea **incidentelor de securitate cibernetică** în termenii și condițiile stabilite de autorități;
- Efectuarea **auditului de securitate cibernetică** la intervale regulate.

Directiva NIS 2 și alinierea la standardele europene

Directiva NIS 2, adoptată de Uniunea Europeană, extinde cerințele de securitate cibernetică pentru toate **sectoarele esențiale**, inclusiv securitatea fizică și digitală bazată pe **sisteme video inteligente**. Directiva impune:

- **Obligații mai stricte de raportare** a incidentelor de securitate;
- Cerințe mai riguroase privind **evaluarea și gestionarea riscurilor**;
- Creșterea **cooperării transfrontaliere** între entitățile europene pentru combaterea amenințărilor cibernetice.

Autorități competente și responsabilități

În România, **Directoratul Național de Securitate Cibernetică (DNSC)** este principala autoritate responsabilă cu monitorizarea și aplicarea măsurilor de securitate impuse de OUG 155/2024 și NIS 2. DNSC colaborează cu **Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)** și alte autorități naționale și internaționale pentru:

- Stabilirea **standardelor și ghidurilor** de securitate cibernetică;
- Supravegherea **implementării măsurilor de protecție** de către entitățile esențiale și importante;
- Asigurarea unui cadru eficient de **răspuns la incidente** și schimb de informații între statele UE.

Acest cadru legislativ și instituțional impune **cerințe clare** pentru furnizorii de soluții video integrate, consolidând **securitatea datelor** și protejând infrastructurile esențiale împotriva amenințărilor cibernetice.

Principii fundamentale ale securității cibernetice

Implementarea eficientă a măsurilor de securitate cibernetică în cadrul **soluțiilor video integrate** se bazează pe o serie de principii esențiale, menite să asigure protecția datelor, continuitatea operațională și conformitatea cu reglementările naționale și europene.

Aceste principii oferă un cadru general pentru proiectarea, implementarea și menținerea sistemelor sigure, atât pentru **furnizorii de soluții video**, cât și pentru organizațiile care le utilizează.

1. Principiul responsabilității și conștientizării

Companiile care furnizează **soluții video integrate**, precum AZITREND, trebuie să dezvolte o **cultură a securității cibernetice**, în care fiecare angajat, de la nivel operațional la management, să fie conștient de riscurile și măsurile necesare pentru prevenirea incidentelor. **Formarea continuă** și testarea procedurilor de răspuns la atacuri cibernetice sunt esențiale pentru reducerea vulnerabilităților.

2. Principiul proporționalității

Măsurile de securitate trebuie să fie **proporționale cu riscurile identificate** în infrastructurile de management video. De exemplu, un **sistem VMS bazat pe cloud** necesită **măsuri avansate de criptare și autentificare multifactor**, în timp ce un **sistem de supraveghere localizat** poate fi protejat prin **securizarea fizică a serverelor și a rețelei interne**.

3. Principiul cooperării și schimbului de informații

Amenințările cibernetice evoluează rapid, iar cooperarea dintre **furnizorii de soluții de securitate**, **clienți**, **autorități** și **organizații internaționale** este vitală. **Partajarea informațiilor despre atacuri cibernetice**, vulnerabilități și măsuri de protecție între entitățile din industrie contribuie la **creșterea rezilienței colective**.

4. Principiul minimizării efectelor

În cazul unui incident cibernetic, obiectivul principal trebuie să fie **limitarea impactului** asupra operațiunilor. Acest lucru presupune **implementarea unor planuri de răspuns la incidente**, utilizarea **backup-urilor securizate** și capacitatea de a **restabili rapid funcționalitatea sistemelor afectate**.

5. Principiul satisfacerii interesului public

Soluțiile video integrate sunt utilizate în **infrastructuri esențiale**, iar protecția acestora nu este doar un obiectiv comercial, ci și **o necesitate pentru siguranța publică**. Orice vulnerabilitate exploatată în astfel de sisteme poate avea **consecințe grave asupra securității naționale**, ceea ce impune adoptarea celor mai **înalte standarde de protecție**.

Prin aplicarea acestor principii fundamentale, furnizorii de **soluții video integrate** pot asigura **confidențialitatea, integritatea și disponibilitatea** datelor, contribuind la creșterea securității cibernetice la nivel național și internațional.

Entitățile vizate și obligațiile acestora

În conformitate cu **Ordonanța de Urgență nr. 155/2024** și **Directiva NIS 2**, securitatea cibernetică nu este doar o preocupare tehnică, ci și o **obligație legală** pentru entitățile care operează **sisteme de management video, analiză video și soluții video integrate de securitate**. Aceste entități sunt împărțite în **două categorii principale**, fiecare având responsabilități specifice pentru protecția infrastructurii digitale.

Entități esențiale - Această categorie include organizațiile care oferă servicii critice și a căror compromitere ar putea afecta securitatea națională sau infrastructurile esențiale. Printre acestea se numără:

- **Furnizorii de soluții video integrate** utilizate în infrastructuri critice (transport, energie, sănătate, apărare);
- **Operatorii de rețele video pentru supraveghere publică**, inclusiv autorități locale și forțe de ordine;
- **Furnizorii de servicii cloud** care găzduiesc date și analize video critice.

Obligațiile entităților esențiale:

- ✓ Implementarea unui **cadru strict de securitate cibernetică** pentru prevenirea atacurilor și gestionarea riscurilor;
- ✓ **Monitorizarea continuă** a rețelelor video și detectarea amenințărilor cibernetice;
- ✓ **Raportarea incidentelor majore** către autoritățile competente în termen de 24-72 de ore;
- ✓ **Realizarea de audituri de securitate** și evaluări periodice ale vulnerabilităților.

Entități importante - Această categorie cuprinde organizații care nu sunt esențiale, dar care pot avea un impact semnificativ asupra securității cibernetice la nivel național. Acestea includ:

- **Companiile care furnizează sisteme VMS (video management systems)** pentru sectorul privat;
- **Integratorii de soluții video** care colaborează cu instituții publice și private;
- **Companiile de securitate** care gestionează sisteme de monitorizare video.

Obligațiile entităților importante:

- ✓ Aplicarea **măsurilor de protecție proporționale cu riscurile identificate**;
- ✓ Raportarea incidentelor care pot afecta infrastructura sau utilizatorii finali;
- ✓ Colaborarea cu autoritățile și furnizorii de securitate cibernetică pentru **îmbunătățirea protecției sistemelor video**.

Prin respectarea acestor obligații, entitățile care gestionează **soluții video integrate** contribuie la creșterea **rezilienței cibernetice** și la protejarea datelor sensibile împotriva amenințărilor emergente.

Măsuri de gestionare a riscurilor de securitate cibernetică

Gestionarea riscurilor cibernetice în cadrul **soluțiilor video integrate** presupune identificarea, evaluarea și aplicarea măsurilor necesare pentru **prevenirea, detectarea și atenuarea amenințărilor** care pot afecta securitatea rețelelor și a sistemelor informatice. **Directiva NIS 2** și **Ordonanța de Urgență nr. 155/2024** impun **cerințe stricte** privind măsurile tehnice, operaționale și organizatorice pe care entitățile esențiale și importante trebuie să le implementeze.

Identificarea și evaluarea riscurilor - **Prima etapă** în gestionarea securității cibernetice este **evaluarea riscurilor** asociate sistemelor video integrate. **Aceasta presupune:**

- Analiza **vulnerabilităților hardware și software** din infrastructura video;
- Identificarea **amenințărilor specifice** (atacuri de tip DDoS, malware, acces neautorizat);
- Evaluarea impactului unui posibil atac asupra **continuității operaționale și a confidențialității datelor**.

Măsuri tehnice de protecție - Pentru a preveni atacurile cibernetice asupra sistemelor de **management video (VMS) și analiză video**, este esențial să fie implementate măsuri tehnice eficiente, printre care:

- **Criptarea datelor** transmise și stocate pentru a preveni interceptarea fluxurilor video;
- **Autentificarea multifactor (MFA)** pentru accesul la sistemele de supraveghere;
- **Patch-uri și actualizări regulate** pentru software-ul și firmware-ul echipamentelor;
- **Segmentarea rețelelor** pentru a izola sistemele video de rețelele IT critice.

Securitatea lanțului de aprovizionare - Având în vedere că multe soluții video sunt furnizate de terți, este esențial să fie implementate **măsuri de securitate pentru lanțul de aprovizionare**, inclusiv:

- **Verificarea și auditarea** furnizorilor de echipamente și software;
- Impunerea de **cerințe minime de securitate** în contractele cu furnizorii;
- Monitorizarea accesului la infrastructura video de către partenerii externi.

Politici și proceduri operaționale - Entitățile care gestionează soluții video integrate trebuie să aibă **politici clare de securitate**, inclusiv:

- **Reguli stricte de acces** la sistemele video și de gestionare a utilizatorilor;
- **Planuri de răspuns la incidente**, care includ protocoale de detecție și remediere a atacurilor;
- **Testări periodice** pentru identificarea vulnerabilităților înainte ca acestea să fie exploatate.

Prin aplicarea acestor măsuri, furnizorii și utilizatorii de **soluții video integrate** pot reduce **riscurile cibernetice**, protejând infrastructurile critice și asigurând **conformitatea cu cerințele legislative**.

Conformitatea și auditul în domeniul securității cibernetice

Respectarea reglementărilor în domeniul securității cibernetice este esențială pentru **furnizorii de soluții video integrate** și pentru organizațiile care le utilizează. **Ordonanța de Urgență nr. 155/2024** și **Directiva NIS 2** impun cerințe stricte de **conformitate**, audit periodic și raportare, menite să asigure securitatea rețelelor și a sistemelor informatice împotriva amenințărilor cibernetice.

Obligațiile privind conformitatea - Pentru a se alinia cerințelor legale, entitățile esențiale și importante din domeniul securității video trebuie să implementeze și să demonstreze respectarea unui set de măsuri de securitate:

- **Adoptarea unui cadru de gestionare a riscurilor** conform standardelor internaționale (ISO 27001, NIST CSF, IEC 62443);
- **Documentarea și actualizarea politicilor de securitate cibernetică**;
- **Implementarea unor măsuri tehnice și organizatorice eficiente** pentru protecția rețelelor video;
- **Raportarea periodică** a stării de securitate către autoritățile competente.

Auditul de securitate cibernetică - Auditul de securitate este un proces esențial pentru verificarea eficienței măsurilor de protecție și identificarea vulnerabilităților. Conform Directivei NIS 2, auditul trebuie să fie efectuat periodic și să includă:

- **Testarea infrastructurilor IT și video** pentru a detecta punctele slabe;
- **Evaluarea conformității cu cerințele legale** și standardele de securitate;
- **Analiza capacității organizației** de a răspunde eficient la incidente de securitate;
- **Propunerea de măsuri corective** și implementarea acestora într-un plan de acțiune.

Autoevaluarea și planurile de măsuri corective - Pe lângă auditurile externe, entitățile care gestionează soluții video integrate trebuie să realizeze autoevaluări periodice, monitorizând:

- Respectarea **protocolului de securitate** și nivelul de conștientizare al angajaților;
- Modul în care sunt gestionate **actualizările și vulnerabilitățile** identificate;
- Rezultatele testelor de penetrare și **exercițiile de simulare a atacurilor**.

Prin adoptarea unei **culturi a conformității** și implementarea auditului ca practică continuă, organizațiile pot asigura un **nivel ridicat de protecție** și se pot adapta rapid la **noile amenințări cibernetice**.

Monitorizarea și raportarea incidentelor de securitate cibernetică

Într-un mediu digital interconectat, **monitorizarea și raportarea incidentelor de securitate cibernetică** reprezintă un pilon esențial al protecției infrastructurilor IT, inclusiv al sistemelor de **management video (VMS) și analiză video**utilizate pentru securitate. **Ordonanța de Urgență nr. 155/2024** și **Directiva NIS 2** impun obligații clare pentru **entitățile esențiale și importante**, menite să asigure **detecția rapidă a atacurilor, atenuarea impactului acestora și coordonarea eficientă a răspunsului**.

Monitorizarea activă a sistemelor video integrate - Pentru a preveni și detecta amenințările cibernetice, organizațiile trebuie să implementeze mecanisme de monitorizare continuă a infrastructurii IT și a rețelelor video. Acestea includ:

- **Sisteme de detecție a intruziunilor (IDS) și prevenire a atacurilor (IPS)**, capabile să identifice activități anormale;
- **Logarea și analiza traficului de rețea**, inclusiv înregistrarea accesului la sistemele video;
- **Instrumente de analiză a comportamentului utilizatorilor (UEBA)** pentru identificarea activităților suspecte;
- **Alertare automată și notificare în timp real** atunci când sunt detectate amenințări.

Clasificarea și raportarea incidentelor de securitate - Conform Directivei NIS 2, incidentele trebuie clasificate în funcție de impactul asupra infrastructurii și serviciilor esențiale. Categoriile principale includ:

- **Incidente minore**, care nu afectează funcționarea serviciilor, dar necesită analiză;
- **Incidente semnificative**, care pot compromite datele sau afecta funcționalitatea sistemelor;
- **Incidente critice**, care cauzează întreruperi severe sau pierderi majore de date.

  Raportarea incidentelor trebuie să respecte **termene clare**:
  - ✓ **În termen de 24 de ore** – notificare preliminară către autoritățile competente;
  - ✓ **În termen de 72 de ore** – raport detaliat, inclusiv măsurile adoptate pentru atenuarea impactului.

Cooperarea cu autoritățile și echipele de răspuns - Entitățile care gestionează soluții video integrate trebuie să colaboreze activ cu Directoratul Național de Securitate Cibernetică (DNSC) și echipele CERT (Computer Emergency Response Team), asigurând:

- **Raportarea corectă și detaliată** a incidentelor conform cerințelor legale;
- **Schimbul de informații** cu alte entități afectate pentru prevenirea atacurilor viitoare;
- **Participarea la exerciții de răspuns la incidente**, pentru îmbunătățirea capacității de reacție.

Prin implementarea unor **procese robuste de monitorizare și raportare**, organizațiile pot crește **reziliența cibernetică** și pot limita impactul atacurilor asupra **sistemelor de securitate video** și a datelor gestionate.

Managementul crizelor și continuitatea operațională

Gestionarea eficientă a crizelor cibernetice este esențială pentru **furnizorii de soluții video integrate** și organizațiile care utilizează astfel de sisteme în infrastructuri critice.
În cazul unui atac cibernetic major, întreruperea funcționării sistemelor de **management video (VMS)** sau analiza video poate avea un impact semnificativ asupra **securității fizice și a protecției datelor**. **Ordonanța de Urgență nr. 155/2024** și **Directiva NIS 2** impun măsuri pentru **asigurarea continuității operaționale**, inclusiv **strategii de prevenire, răspuns și recuperare**.

Planificarea continuității operaționale - Un Plan de Continuitate a Activității (PCA) trebuie să includă măsuri pentru detectarea timpurie a atacurilor, protejarea infrastructurii esențiale și recuperarea rapidă a sistemelor. Acesta trebuie să cuprindă:

- **Identificarea și clasificarea activelor critice**, inclusiv a componentelor software și hardware esențiale pentru funcționarea sistemelor video integrate;
- **Definirea scenariilor de criză**, de la atacuri ransomware la întreruperi de rețea și compromiterea datelor;
- **Stabilirea responsabilităților în cazul unui incident**, asigurând o reacție rapidă și coordonată.

Răspunsul la incidente majore și gestionarea crizelor - Un răspuns eficient la incidente presupune o abordare organizată, bazată pe:

- **Activarea unui plan de răspuns la incidente** imediat după detectarea unei amenințări;
- **Crearea unei echipe de gestionare a crizelor (Cyber Incident Response Team – CIRT)**, formată din specialiști IT, responsabili de securitate și factori de decizie operațională;
- **Menținerea comunicației interne și externe**, pentru a evita dezinformarea și panica în rândul utilizatorilor și clienților.

Recuperarea și învățarea din incidente - Pentru a reduce efectele unui atac cibernetic și a preveni incidente viitoare, organizațiile trebuie să implementeze:

- **Proceduri de backup și restaurare**, cu date critice replicate în medii sigure și testate periodic;
- **Analiza post-incident**, pentru identificarea punctelor slabe și îmbunătățirea măsurilor de securitate;
- **Simulări și exerciții de răspuns**, pentru a testa eficiența planurilor de continuitate și pregătirea echipelor responsabile.

Prin aplicarea acestor strategii, **furnizorii și utilizatorii de soluții video integrate** pot asigura **reziliența operațională**, menținând **siguranța și funcționalitatea sistemelor video** în fața amenințărilor cibernetice emergente.

Formare și conștientizare în securitatea cibernetică

Pentru a asigura **protecția eficientă a sistemelor video integrate**, nu este suficientă doar implementarea unor soluții tehnice avansate.
Factorul uman rămâne unul dintre cei mai vulnerabili puncte într-o infrastructură IT, iar atacatorii exploatează frecvent **erori umane, lipsa de conștientizare și practici de securitate deficitare**. De aceea, **formarea continuă și conștientizarea** reprezintă elemente fundamentale ale unei **strategii eficiente de securitate cibernetică**.

Programe de training pentru personalul tehnic și non-tehnic - În funcție de nivelul de acces și responsabilitate, fiecare categorie de angajați trebuie să beneficieze de instruire specifică:

- **Personal IT și administratorii sistemelor video** – trebuie să participe la cursuri avansate privind **securitatea rețelelor, protecția datelor, răspunsul la incidente și bunele practici de administrare a sistemelor video**;
- **Operatorii de sisteme video și agenții de securitate** – trebuie instruiți în **recunoașterea atacurilor cibernetice, gestionarea accesului securizat și manipularea corectă a echipamentelor de supraveghere**;
- **Angajații și utilizatorii finali** – trebuie educați cu privire la **igiena cibernetică**, metodele de recunoaștere a atacurilor de tip phishing și protecția datelor personale.

Campanii de conștientizare și bune practici - Pe lângă trainingul formal, organizațiile trebuie să implementeze campanii periodice de conștientizare, care să includă:

- **Simulări de atacuri cibernetice** pentru testarea reacțiilor personalului la incidente reale;
- **Exerciții de social engineering**, pentru identificarea vulnerabilităților umane;
- **Materiale educative și sesiuni de informare**, care să acopere cele mai noi amenințări și metode de protecție.

Crearea unei culturi a securității cibernetice - Un mediu de lucru sigur necesită mai mult decât reguli și proceduri. Organizațiile trebuie să promoveze o cultură a securității cibernetice, prin:

- **Stimularea raportării prompte a incidentelor**, fără teamă de repercusiuni;
- **Integrarea securității cibernetice în toate procesele operaționale**;
- **Încurajarea colaborării** între echipele IT, administratorii de securitate fizică și utilizatorii finali.

Prin aplicarea acestor măsuri, organizațiile care gestionează **soluții video integrate** pot reduce semnificativ **riscurile umane** și pot crea un mediu **sigur, educat și pregătit** pentru a face față provocărilor cibernetice.

Viitorul securității cibernetice în industria soluțiilor video integrate

Odată cu avansul tehnologic rapid și creșterea interconectivității, industria **soluțiilor video integrate** se află într-o continuă transformare.

Sistemele de **video management (VMS), analiza video avansată și supravegherea bazată pe inteligență artificială** devin din ce în ce mai complexe, iar **amenințările cibernetice evoluează simultan**, punând presiune pe furnizori și utilizatori pentru a adopta măsuri de securitate din ce în ce mai avansate.

Tendințe emergente în securitatea cibernetică pentru soluțiile video - Pe măsură ce tehnologia avansează, următoarele tendințe vor influența viitorul securității în industria soluțiilor video:

- **Integrarea inteligenței artificiale (AI) și machine learning (ML)** – Algoritmii avansați permit **detectarea anomaliilor** și identificarea comportamentelor suspecte în timp real, însă utilizarea AI deschide și noi vectori de atac asupra datelor și modelelor predictive.
- **Extinderea utilizării IoT în infrastructurile video** – Camerele și dispozitivele IoT conectate la rețea oferă beneficii operaționale semnificative, dar sunt și vulnerabile la atacuri dacă nu sunt securizate corespunzător.
- **Adoptarea tehnologiilor cloud și edge computing** – Migrarea analizelor video în cloud și procesarea datelor la marginea rețelei (edge computing) vor reduce latența și costurile, dar vor necesita **măsuri avansate de criptare și autentificare**.
- **Implementarea blockchain pentru securitate și integritate** – Blockchain-ul poate fi utilizat pentru **validarea înregistrărilor video**, prevenind modificările neautorizate și falsificarea dovezilor.

Impactul reglementărilor europene și standardizarea securității - Adoptarea **Directivei NIS 2**, combinată cu reglementările privind **protecția datelor (GDPR) și securitatea infrastructurilor critice**, va impune:

- **Cerințe mai stricte de conformitate și audit** pentru furnizorii de soluții video;
- **Creșterea transparenței** în raportarea incidentelor de securitate;
- **Standardizarea protocoalelor de securitate** pentru sistemele video utilizate în infrastructuri critice.

Reziliență cibernetică și viitorul protecției sistemelor video - Pentru a face față provocărilor emergente, furnizorii și utilizatorii de **soluții video integrate** trebuie să adopte:

- **O abordare proactivă** în identificarea și gestionarea riscurilor;
- **Colaborarea extinsă** între sectorul privat, autoritățile de reglementare și instituțiile de securitate cibernetică;
- **Investiții continue în tehnologii de protecție**, precum criptarea avansată, inteligența artificială defensivă și autentificarea biometrică.

Industria **soluțiilor video integrate** trebuie să evolueze continuu pentru a rămâne **rezilientă** în fața amenințărilor digitale și pentru a asigura un **mediu securizat și conform cu cerințele viitorului digital**.

AZiTREND

Strada Biharia, nr. 67-77, Corp F Sector 1 Bucharest, RO
0755 111 200 / office@azitrend.ro
https://azitrend.ro