
ROMANIA
SRI
Patria a priori
SERVICIUL ROMAN DE INFORMATII
BULETIN
CLOUD

DEFINIȚII

CLOUD COMPUTING – un ansamblu distribuit de servicii de calcul, aplicații, acces la informații și stocare de date. Acesta funcționează fără a fi necesar ca utilizatorul să cunoască întreaga configurație a rețelei și amplasarea fizică a acesteia, fiind, totodată, caracterizat de un nivel de accesibilitate facil pentru beneficiarii sistemului. Mai mult, un astfel de sistem prezintă un grad ridicat de reziliență, ceea ce contribuie la eficientizarea stocării și accesării datelor.

CLOUD GUVERNAMENTAL – infrastructură de tip cloud, constând într-un ansamblu de resurse și servicii de tehnologia informației, comunicații și securitate cibernetică, utilizat în comun de autorități și instituții publice din România, precum și de către structurile aflate în coordonarea și subordonarea acestora.

TIPURI DE CLOUD

În funcție de cele mai comune metode de implementare a soluțiilor de cloud computing, pot fi întâlnite următoarele tipuri de cloud:

CLOUD PUBLIC – reprezintă un tip de resursă pusă la dispoziție (de obicei de către un terț) pentru un număr ridicat de utilizatori, fără a fi necesar ca aceștia să facă parte dintr-o organizație/ instituție/ entitate comună. Practic, cloud-ul public presupune un mod de lucru bazat pe utilizarea comună a resurselor oferite de furnizor, acestea fiind asigurate cu ajutorul unor componente fizice partajate și accesate prin intermediul unei rețele publice. De asemenea, datele stocate într-un cloud public se află pe echipamentele fizice ale furnizorului terț. Suplimentar, acest tip de cloud este caracterizat de faptul că mentenanța și accesibilitatea acestui tip de cloud sunt asigurate de către furnizor, iar clientul poate utiliza serviciile respective, indiferent de locație sau dispozitiv, dacă deține permisiunile necesare.

CLOUD PRIVAT – reprezintă o categorie de resurse care, spre deosebire de cloud-ul public, sunt asigurate de furnizor doar pentru un client specific, accesul la aceste resurse fiind posibil doar prin intermediul unei rețele private. De asemenea, în ceea ce privește cloud-ul privat, există opțiunea de a stoca totalitatea componentelor fizice în centrul de date al

INFO BOX

Cloud-ul hibrid creează atât o resursă care asigură caracteristicile cloud-ului public pentru cea mai mare parte dintre activitățile zilnice din cadrul unei rețele cât și o resursă gestionată la nivelul organizației, cu caracteristici specifice cloud-ului privat.

clientului, atât pentru creșterea nivelului de securitate cibernetică, cât și pentru asigurarea mentenanței și accesibilității doar de către personalul specializat din cadrul organizației.

Comparativ cu cloud-ul public, cel privat este caracterizat de un nivel de scalabilitate și flexibilitate mai scăzut (acesta fiind bazat pe un număr redus de utilizatori). Cu toate acestea, este important de menționat faptul că nivelul de scalabilitate și flexibilitate este considerabil mai înalt în comparație cu o rețea fizică internă.

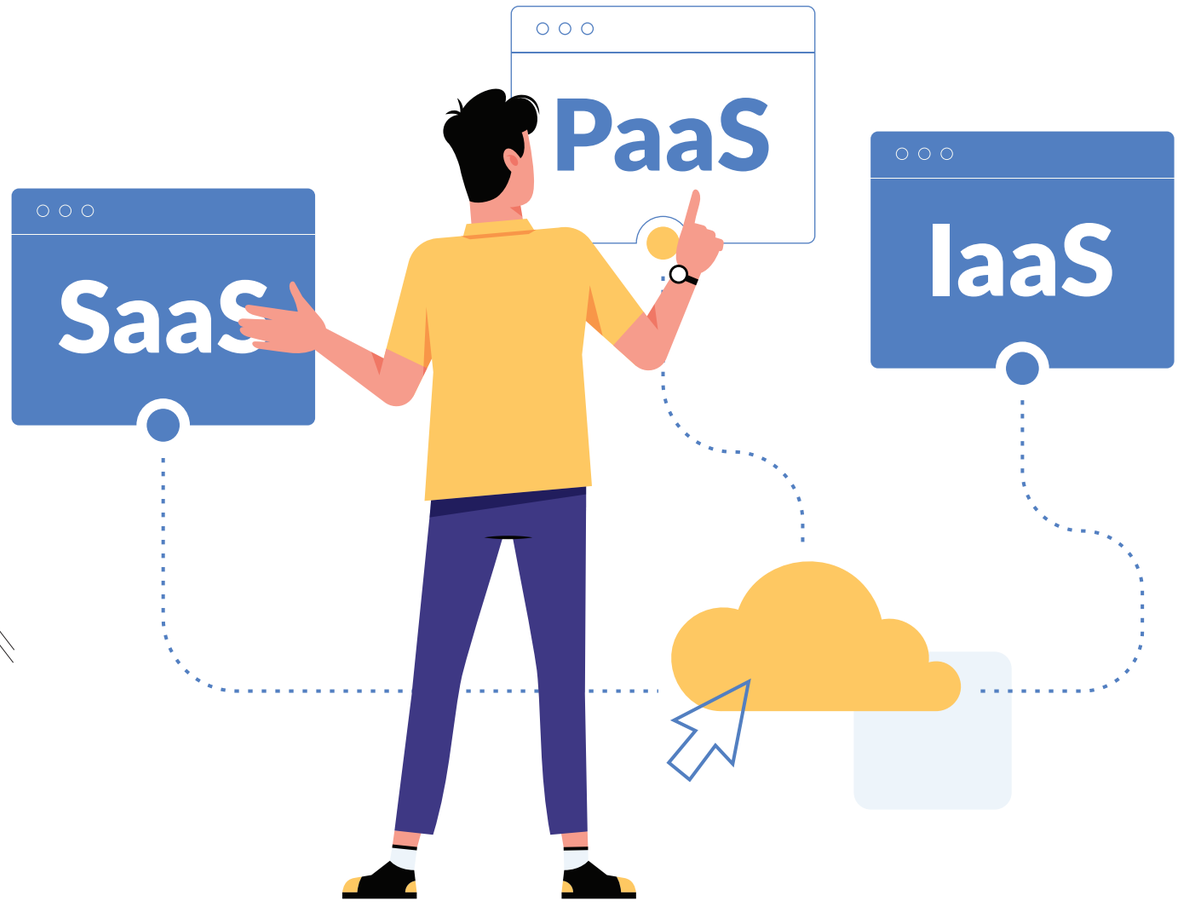
CLOUD HIBRID – presupune un model de resursă care combină o parte dintre caracteristicile cloud-ului privat cu cele ale cloud-ului public, în vederea asigurării unui echilibru între măsurile de securitate cibernetică și necesitățile de flexibilitate, scalabilitate sau accesibilitate. Practic, premisa de la care pornește sistemul de cloud hibrid este aceea că, în cadrul unei organizații, există 2 tipuri de activități:

- cele uzuale (care necesită cea mai mare cantitate de resurse și pentru care trebuie asigurată scalabilitatea);
- cele cu nivel ridicat de sensibilitate (care necesită măsuri accentuate de securitate cibernetică).

Astfel, cloud-ul hibrid creează atât o resursă care asigură caracteristicile cloud-ului public pentru cea mai mare parte dintre activitățile zilnice din cadrul unei rețele și o resursă gestionată la nivelul organizației, cu caracteristici specifice cloud-ului privat.

CLOUD DE COMUNITATE - resursele computaționale sunt puse în comun de către două sau mai multe organizații cu scopul de a atinge anumite obiective de business sau cerințe specifice.

Echipamentele IT sunt localizate fie într-un centru de date intern, sau unul extern, sub atenta supraveghere a partenerilor asociați. Cloud-ul de comunitate prezintă avantajele reducerii costurilor de mentenanță și operaționale și reușește să limiteze potențiale riscuri de securitate.



MODELE DE LIVRARE A **SERVICIILOR DE CLOUD**

Pentru ca infrastructura de cloud, inclusiv cea de tip guvernamental, să își atingă obiectivele de utilitate publică și instituțională, aceasta trebuie să asigure următoarele servicii, în baza modelelor:

IAAS – INFRASTRUCTURE AS A SERVICE (infrastructura oferită ca serviciu)

La acest nivel se pot oferi servicii de infrastructură virtuală ce asigură puterea de calcul, transparența și independența necesare portării sistemelor informatice actuale insularizate la nivelul instituțiilor proprietare, indiferent de tehnologiile în care au fost implementate.

PAAS – PLATFORM AS A SERVICE (platforma software oferită ca serviciu)

Model prin care se pun la dispoziție o serie de servicii care asigură medii de execuție pentru aplicații web, sisteme de gestiune a bazelor de date, servere de aplicații și servere web, sisteme de operare, instrumente de dezvoltare a aplicațiilor, etc. Este un model cu un grad de independență mai scăzut față de IaaS, deoarece poate oferi un număr limitat de servicii de tipul celor enumerate anterior.

SAAS – SOFTWARE AS A SERVICE (aplicații oferite ca servicii)

Oferă servicii de furnizare a unor soluții software – poștă electronică, desktop virtualizat, comunicare și colaborare, managementul electronic al documentelor (EDM), gestionarea resurselor întreprinderii (ERP), managementul conținutului (CM), etc. în care furnizorul gestionează toate componentele hardware și software, inclusiv mentenanța și actualizările. Cu alte cuvinte, este un model de licențiere și livrare a aplicațiilor software pe baza unui abonament.

XAAS – EVERYTHING AS A SERVICE (orice ca serviciu)

Reprezintă un model de punere la dispoziția

INFO BOX

În implementările tradiționale de cloud, utilizatorii trebuie să inițieze o instanță computațională și să încarce cod în cadrul acesteia. Apoi, utilizatorul decide cât timp trebuie să ruleze această instanță și plătește pentru instanța respectivă. Prin intermediul serverless computing, dezvoltatorii creează codul, iar furnizorul de cloud îl încarcă în sistem și execută acea unitate de cod ca răspuns la solicitările venite.

utilizatorilor, la cererea acestora, pe baza unor drepturi de acces și în limita capacităților disponibile în cloud, a unui număr extins de produse, instrumente și tehnologii sub formă de servicii, cele mai importante fiind infrastructura ca serviciu (IaaS), platforma ca serviciu (PaaS) și software ca serviciu (SaaS);

În ultimii ani s-a dezvoltat și recunoscut de către specialiștii IT un nou tip de serviciu în Cloud, numit Serverless Computing.

Serverless Computing asigură funcționalitatea aplicației, fără ca dezvoltatorul aplicației software să fie implicat în gestionarea resurselor de infrastructură sau în gestionarea puterii de calcul. Arhitectura Serverless este extrem de scalabilă și receptivă la evenimente, încât aceasta utilizează resurse de calcul numai în cazul în care o anumită funcție este îndeplinită, sau un trigger este lansat din aplicație.

De exemplu, serverless, sau Cloud Computing bazat pe evenimente, este un serviciu Cloud care execută funcții specializate, cum ar fi procesare de imagini sau actualizări în bazele de date relaționale.

În implementările tradiționale de cloud, utilizatorii trebuie să inițieze o instanță computațională și să încarce cod în cadrul acesteia. Apoi, utilizatorul decide cât timp trebuie să ruleze această instanță și plătește pentru instanța respectivă. Prin intermediul serverless computing, dezvoltatorii creează codul, iar furnizorul de cloud îl încarcă în sistem și execută acea unitate de cod ca răspuns la solicitările venite. Nu este necesar ca utilizatorii să se preocupe de aspectele legate de server sau de instanța de cloud. Utilizatorii trebuie doar să plătească în funcție de numărul de execuții pe care codul programat l-a realizat.

BENEFICII ȘI AVANTAJE ALE **CLOUD-ULUI GUVERNAMENTAL**

Implementarea conceptului de cloud guvernamental în România va avea ca efect eficientizarea activităților și fluxurilor instituționale, cu impact în planul diminuării birocrației și ameliorării interacțiunii cu cetățenii.

BENEFICII

➲ adaptarea cadrului legislativ la evoluția și dinamica înregistrate în ultimii ani în domeniul IT&C;

Actul normativ de implementare a cloud-ului guvernamental va reglementa, în termeni clari, realizarea acestui proiect major de informatizare a statului și va cuprinde o serie de valențe de orientare strategică în domeniul IT&C.

➲ crearea unei infrastructuri IT&C sigure și scalabile, comună tuturor instituțiilor din sectorul public și aplicarea modelului PCU (Punct de Contact Unic) în relaționarea cu cetățeanul;

Acest beneficiu este esențial în condițiile în care, în prezent, la nivelul autorităților statului nu există un cadru general unitar privind dezvoltarea sistemelor informatice, iar costurile de interconectare generate sunt foarte ridicate.

➲ diminuarea deficiențelor manageriale în domeniul IT&C de la nivelul instituțiilor publice;

Vor putea fi diminuate efectele negative generate de numărul și nivelul de expertiză scăzute ale angajaților cu atribuții în administrarea/implementarea sistemelor informatice din cadrul instituțiilor publice.

Totodată, abordarea integrată a procesului

de informatizare național va avea ca efect și eliminarea tratării în mod sectorial/teritorial a sistemelor informatice, dar și a carențelor de comunicare intra și inter-instituționale la nivelul acestor sisteme.

- promovarea liberei concurențe pe piață și descurajarea practicilor anticoncurențiale;

Având în vedere diversitatea tehnologică pe care o poate oferi o astfel de infrastructură, implementarea cloud-ului guvernamental se poate constitui într-un impuls pentru piața IT&C autohtonă, prin promovarea concurenței, creșterea productivității, precum și a locurilor de muncă în domeniu.

AVANTAJE

Pe lângă beneficiile cuantificabile prin efectele produse de implementarea unei infrastructuri de cloud guvernamental, materializarea acestui demers va aduce o serie de avantaje de ordin funcțional, cu impact asupra eficientizării activităților instituționale și a relaționării cu cetățeanul:

- creșterea numărului de servicii electronice aferente evenimentelor de viață ale cetățeanului, în concordanță cu prevederile Strategiei Naționale România Digitală - conceptul e-Guvernare 2.0;
- eficientizarea relaționării dintre cetățean și instituțiile statului;
- asigurarea în timp real a schimbului inter-instituțional de date în mediul online;
- creșterea nivelului de securitate a datelor, precum și structurarea, organizarea și standardizarea mai bună a acestora;
- asigurarea unor măsuri unitare de securitate cibernetică la nivelul infrastructurilor componente ale cloud-ului guvernamental;
- optimizarea costurilor de licențiere și mentenanță software, precum și a costurilor aferente achizițiilor hardware și mentenanței specifice;
- posibilitatea de administrare facilă și diminuare a costurilor de menținere în parametri de funcționare optimi a sistemelor informatice;
- reducerea activităților de administrare la nivelul instituțiilor implicate, cu posibilitatea relocării parțiale a personalului către alte zone de activitate;
- alocarea dinamică a resurselor, în funcție de perioadele de vârf ale activității instituțiilor ale căror sisteme sunt integrate;

- asigurarea scalabilității sistemului în funcție de nevoile instituțiilor pe termen mediu și lung;
- acces facil la aplicații software și posibilitatea recuperării rapide a datelor în cazul apariției unor situații critice;
- diminuarea costurilor aferente cu personalul în condițiile creșterii gradului de automatizare a operațiunilor și administrării centralizate;
- creșterea nivelului de cooperare, precum și posibilitatea realizării de parteneriate și schimburi de date cu alte instituții;
- posibilitatea implementării facile a unor politici de tipul Bring Your Own Device (BYOD), care vor determina scăderea suplimentară a costurilor de achiziție cu licențe și dispozitive hardware de acces, precum și creșterea mobilității utilizatorilor.

LIMITĂRI/DEZAVANTAJE ALE SOLUȚIILOR DE CLOUD

Este necesar ca organizațiile să conștientizeze că, dincolo de beneficiile și avantajele tehnologiei de cloud, există și o serie de limitări/dezavantaje ale tehnologiei cloud computing, între care menționăm:

Dependența de serviciile de suport oferite de către furnizor

În situația în care un sistem de tip cloud este adoptat la nivelul unei organizații, așa cum a fost precizat anterior, o parte din managementul rețelelor este transferată către furnizorul de servicii de cloud. În acest sens, în eventualitatea apariției unor probleme de funcționalitate a rețelelor, organizația devine dependentă de Serviciul Clienți al furnizorului în vederea soluționării acestor aspecte. Mai mult, Serviciul Clienți poate fi indisponibil la momentul apariției problemelor tehnice, aspect ce generează întârzieri până în punctul restabilirii funcționalității rețelelor.

Limitări în ceea ce privește controlul asupra managementului datelor

O limitare generată de implementarea unui model de tip cloud în cadrul unei organizații este cea referitoare la diminuarea controlului pe care aceasta îl va avea asupra propriilor date. Practic, implicarea unui terț în managementul bazelor de date poate deveni un dezavantaj, având în vedere faptul că o parte dintre responsabilitățile de administrare a acestora vor fi transferate către furnizorul de servicii. Mai mult, în situația în care furnizorul de servicii cloud nu dispune de un centru de date pe teritoriul statului in care este localizată organizația, datele vor fi stocate și gestionate într-un centru aflat în afara granițelor.

Elemente de acces la nivelul rețelelor de cloud ce le expun la atacuri cibernetice

Unul dintre elementele centrale ale unui atac cibernetic este cel de compromitere a unui utilizator din cadrul unei rețele, în vederea escaladării privilegiilor și obținerii de drepturi extinse. De asemenea, pentru atacatori este important ca utilizatorul compromis să dețină un nivel de acces la rețea care să-i permită mișcarea laterală în cadrul rețelei respective. În ceea ce privește sistemele de tip cloud, resursele alocate pentru toți utilizatorii și nivelul de acces al acestora în cadrul rețelei sunt similare, în cele mai multe cazuri, fiecare dintre utilizatori fiind conectat la o rețea comună de internet. Astfel, există posibilitatea ca, din perspectiva unui atacator cibernetic, rețelele de tip cloud să reprezinte o oportunitate în vederea facilitării escaladării de privilegii și mișcări laterale în cadrul acestora.

INFO BOX

Există posibilitatea ca, din perspectiva unui atacator cibernetic, rețelele de tip cloud să reprezinte o oportunitate în vederea facilitării escaladării de privilegii și mișcări laterale în cadrul acestora.

Costuri necesare pentru pregătirea personalului

Administrarea unor sisteme de tip cloud generează cheltuieli suplimentare pentru pregătirea personalului cu privire la modalitățile de funcționare a acestor servicii și la elementele de securitate cibernetică necesar a fi implementate. Mai mult, având în vedere faptul că tehnologiile de tip cloud se află într-un proces continuu de dezvoltare, iar abilitățile tehnice necesare gestionării acestora includ un nivel înalt de pregătire în domeniu, educarea personalului reprezintă o preocupare și o investiție constantă.

Dificultăți generate de schimbarea sau transferul către un alt furnizor de servicii cloud

Ulterior implementării serviciilor de tip cloud la nivelul unei organizații, toate datele acesteia vor fi stocate în cadrul soluțiilor oferite de furnizor. În eventualitatea în care organizația decide să schimbe toate soluțiile oferite de același furnizor, urmare a apariției unor neînțelegeri între părțile care au semnat acordul pentru servicii, este dificil pentru organizație să recurgă la acest demers, având în vedere că acțiunea necesită transferul tuturor datelor stocate către serverele puse la dispoziție de vechiul furnizor.

SECURITATEA CIBERNETICĂ

Componenta de securitate cibernetică este esențială în planul sistemelor de cloud computing, aceasta presupunând asigurarea confidențialității și integrității datelor utilizate la nivelul infrastructurii de bază, a aplicațiilor, precum și a platformelor utilizate.

Componentele de bază ale securității cibernetice în cloud trebuie să aibă în vedere:

- Securitatea datelor vehiculate la nivelul cloud;
- Identitatea și managementul accesului în cloud;
- Politici de securitate, detecție și mitigare a atacurilor cibernetice și incidentelor de securitate cibernetică în infrastructura de cloud;
- Retenția datelor (GDPR) și planul de continuitate al afacerii (BC) în cazul firmelor.

Securizarea sistemelor de cloud implică eforturi atât din partea furnizorilor de servicii de cloud, cât și a clienților care utilizează aceste servicii, indiferent dacă este vorba de persoane fizice sau juridice, cu scopul de a proteja următoarele elemente:

- Părți/ componente ale rețelelor și infrastructurii (routere, alimentare electrică, cabluri, aparatură de climatizare);
- Echipamente de stocare de date (ex. HDD);
- Servere de date (echipamente și software al rețelei principale/core);
- End user hardware (computere, echipamente mobile);
- Echipamente de virtualizare (echipamente

INFO BOX

Configurarea infrastructurii reprezintă o altă practică eficientă, având în vedere că cele mai multe breșe de securitate/ vulnerabilități de securitate cibernetică sunt rezultatul unor erori de configurare. Prin prevenirea unor astfel de vulnerabilități se reduc semnificativ riscurile de securitate în cloud.

INFO BOX

În utilizarea serviciilor de cloud un rol important îl ocupă drepturile și accesul pe care utilizatorii îl au la nivelul cloud, în sensul drepturilor/ privilegiilor pe care le au privind stocarea și partajarea de date.

de hosting, software pentru mașini virtuale);
- Sisteme de operare – SO (totalitatea soluțiilor SO);
- Middleware (managementul interfeței de programare a aplicațiilor – API).

Măsurile de securitate în cloud trebuie să aibă în vedere:

- Capacitatea de recuperare a datelor în situația în care se produce pierderea acestora;
- Protejarea datelor stocate și a rețelelor împotriva tentativelor de furt;
- Derularea unor activități de awareness menite să prevină erorile generate de lipsa de pregătire a resursei umane;
- Reducerea impactului generat de compromiterea unor date sau sisteme.

Modalități de securizare în cloud:

Criptarea datelor – constituie una din cele mai eficiente metode disponibile prin care se poate asigura securizarea datelor în cloud. O astfel de modalitate poate fi aplicată pe 3 paliere: criptarea în totalitate a comunicațiilor la nivelul cloud; criptarea anumitor date considerate a fi sensibile (ex. credențiale de acces); criptarea end-to-end a tuturor datelor încărcate în cloud.

Configurarea infrastructurii – reprezintă o altă practică eficientă, având în vedere că cele mai multe breșe de securitate/ vulnerabilități de securitate cibernetică sunt rezultatul unor erori de configurare. Prin prevenirea unor astfel de vulnerabilități se reduc semnificativ riscurile de securitate în cloud.

Stocarea si partajarea – în utilizarea serviciilor de cloud un rol important îl ocupă drepturile și accesul pe care utilizatorii îl au la nivelul cloud, în sensul drepturilor/ privilegiilor pe care le au privind stocarea și partajarea de date. Aceste drepturi pot fi restrânse sau lărgite în funcție de privilegiile fiecărui tip de utilizatori în parte, putând fi gestionate, în mod eficient, situații în care parte din utilizatori din cloud nu au aceleași drepturi de acces și partajare (ex. date cu acces restricționat).

EVALUARE ȘI CONCLUZII

O infrastructură de cloud guvernamental poate atrage beneficii și avantaje menite să eficientizeze costurile și activitatea statului. O implementare și gestionare conformă cu standardele de securitate în materie este de natură să reducă la minimum riscurile și vulnerabilitățile de securitate cibernetică, crescând, astfel, plus valoarea adusă de oportunitățile unui cloud guvernamental.

În aceste condiții, realizarea unei infrastructuri de acest tip, care să țină cont de toate recomandările, reglementările, bunele practici și standarde internaționale în materie, va reprezenta un catalizator al asigurării securității cibernetice, prin rezolvarea problemelor de disponibilitate a serviciilor și de reziliență la atacuri cibernetice, de asigurare a activităților de business continuity și de disaster recovery.

Implementarea unei infrastructuri de cloud guvernamental va fi de natură să amelioreze situația existentă, în prezent, la nivel național, în privința asigurării securității fizice a centrelor de date. Astfel, securitatea va fi abordată complet și unitar, începând cu nivelul rețelelor informatice, continuând cu centrul de date, sistemele informatice și terminând cu datele gestionate la nivelul acestora.

Aceste demersuri vor avea efecte în planul consolidării unei mai bune poziționări a României la nivelul Indicelui Economiei și Societății Digitale (DESI), dar și în planul realizării obiectivelor stipulate și asumate de statul român în Strategia Națională de Apărare a Țării, în Strategia Națională privind Agenda Digitală pentru România, precum și în proiectul Strategiei de Securitate Cibernetică a României.


ROMANIA
SRI
Patria a priori
SERVICIUL ROMAN DE INFORMATII
SIGURANȚĂ
PENTRU ROMÂNIA
WWW.SRI.RO/CYBERINT