Care este rolul SRI în implementarea programelor PNRR?

PNRR cuprinde o agendă ambițioasă de reforme și investiții care oferă oportunitatea statului de a-și moderniza economia, de a stimula dezvoltarea durabilă și de a face față provocărilor viitoare într-un mod eficient și adaptabil.

În implementarea acestui program național esențial pentru dezvoltarea țării, rolul principal al SRI rămâne cel stabilit de Legea nr. 51/1991 privind securitatea națională, republicată, cu modificările și completările ulterioare, respectiv de a contribui la asigurarea stării de legalitate, de echilibru şi de stabilitate socială, economică şi politică necesară existenței şi dezvoltării statului național român, menținerii ordinii de drept şi a climatului de exercitare neîngrădită a drepturilor, libertăților şi îndatoririlor fundamentale ale cetățenilor.

În egală măsură, Strategia Națională de Apărare a Țării pentru perioada 2020-2024, stabilește importanța vitală pentru securitatea națională a unor direcții de acțiune, printre care se regăsesc: realizarea infrastructurii necesare pentru implementarea procesului de digitalizare a României, în scopul eficientizării activității aparatului administrativ şi a creșterii calității serviciilor publice, precum și necesitatea dezvoltării unor sisteme de comunicare compatibile cu capabilitățile moderne de comunicații şi tehnologia informației, care să concretizeze transformarea digitală, sau asigurarea digitalizării instituțiilor din domeniul apărării țării şi securității naționale, a serviciilor publice şi a mecanismelor interinstituționale prin intermediul evoluțiilor tehnologice recente.

Realizarea obiectivelor Strategiei implică un efort conjugat al autorităților naționale cu responsabilități în domeniu şi al societății civile, o condiție complementară pentru operaționalizarea acestei strategii naționale de apărare a țării fiind și asigurarea unui cadru legislativ coerent şi aplicat, menit a contribui la consolidarea culturii de securitate.

Astfel, prin adoptarea Legii nr. 58 din 14 martie 2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative, SRI a fost desemnat ca autoritate competentă la nivel național în domeniul cyber intelligence, precum şi pentru cunoașterea, analizarea, prevenirea şi contracararea incidentelor şi atacurilor cibernetice care reprezintă amenințări, riscuri şi vulnerabilități la adresa securității naționale a României.

Securitatea cibernetică este un element vital al pilonului PNRR pentru Transformarea Digitală, deoarece contribuie la protejarea datelor și infrastructurilor digitale, la prevenirea atacurilor cibernetice și la asigurarea încrederii utilizatorilor și investitorilor în procesul de digitalizare a țării.

Cum poate fi folosită expertiza tehnică a SRI, garantând drepturile și libertățile individuale?

În ceea ce privește contribuția SRI, în ansamblul unităților din care este alcătuit, în proiectele de digitalizare a instituțiilor publice prin utilizarea fondurilor naționale sau europene, precizăm că aceasta vizează implicit și direcția de acțiune anterior prezentată cu relevanță în planul relaționării și colaborării interinstituţionale de tip integrat.

Garanțiile oferite societății civile, din perspectiva implicării Serviciului Român de Informații în proiecte strategice de digitalizare, referitoare la păstrarea echilibrului necesar protejării drepturilor și libertății cetățenilor, derivă din cadrul normativ ce reglementează organizarea și funcționarea instituției. Activitatea pentru realizarea securității naționale este organizată și coordonată de către Consiliul Suprem de Apărare a Țării și este supusă controlului democratic permanent prin intermediul Comisiei comune permanente a Camerei Deputaților și Senatului. Potrivit HP nr. 30/1993, Comisia veghează la îndeplinirea de către SRI a misiunilor ce îi revin în conformitate cu prevederile legale în vigoare şi efectuează un control concret şi permanent asupra activităților Serviciului Român de Informații. În realizarea atribuțiilor care îi revin, Comisia solicită SRI, prin intermediul directorului acestuia, rapoarte, informări, explicații, documente, date şi informații şi poate audia persoane în legătură cu problemele analizate. SRI este obligat să pună la dispoziția Comisiei, în termen de 7 zile lucrătoare, rapoartele, informările, explicațiile, documentele, datele şi informațiile solicitate şi să permită audierea personalului militar și civil indicat de comisie. Comisia se poate sesiza din oficiu cu privire la acele acțiuni care ar putea afecta activitatea SRI sau ar crea suspiciuni cu privire la legalitatea acesteia.

Totodată, există atât mecanisme interne de verificare, cât şi externe, instituite de lege, care vizează în permanență ca activitatea instituțională să se desfășoare strict în conformitate cu legile în vigoare, cu respectarea procedurilor şi competențelor specifice.

Care sunt atribuțiile SRI clar definite în realizarea Cloudului guvernamental?

Conform legislaţiei în vigoare (HG nr. 112/2023[1], Art. 1, Alin. (2)), **Cloudul privat guvernamental (CPG)** reprezintă o **infrastructură informatică şi de comunicaţii de interes naţional** în sensul Legii nr. 163/2021 *privind adoptarea unor măsuri referitoare la infrastructuri informatice şi de comunicaţii de interes naţional şi condiţiile implementării reţelelor 5G*, fapt ce reclamă necesitatea adoptării unor mecanisme de securitate cibernetică adecvate.

Compromiterea CPG prin intermediul atacurilor cibernetice ar putea avea un **impact major asupra securității naționale a României**, sens în care componenta de **securitate cibernetică** este esențială în operaționalizarea acestuia. Conform legii nr. 14/1992, cu modificările și completările ulterioare, Serviciul Român de Informații este entitatea responsabilă în domeniul informațiilor privitoare la **securitate națională**.

În acest context, **Serviciul Român de Informații** (SRI) -autoritate națională în domeniul *cyber intelligence* - se numără printre instituțiile implicate în proiectul de Cloud Guvernamental, **Ministerul Cercetării, Inovării și Digitalizării** (MCID), **Autoritatea pentru Digitalizarea României** (ADR) și **Serviciul de Telecomunicații Speciale** (STS).

Conform prevederilor OUG nr. 89/2022[2], principalele **responsabilități** ce revin **instituției noastre sunt**:

---

[1] Privind aprobarea Ghidului de guvernanţă a platformei de cloud guvernamental.

[2] Privind înființarea, administrarea şi dezvoltarea infrastructurilor şi serviciilor informatice de tip cloud utilizate de autoritățile şi instituțiile publice, cu modificările și completările ulterioare.

(1) asigurarea **securității cibernetice a serviciilor de cloud de tip SaaS[3]** furnizate entităților găzduite din **cloudul intern** prin cunoașterea, prevenirea și contracararea atacurilor, amenințărilor, riscurilor și vulnerabilităților cibernetice, inclusiv a celor complexe, de tip Advanced Persistent Threat;

(2) cunoașterea, prevenirea și contracararea atacurilor cibernetice complexe, de tip **APT**, îndreptate împotriva **serviciilor IaaS[4] și PaaS[5]** furnizate din **cloudul intern**, prin schimbul nemijlocit și automat al informațiilor referitoare la incidentele de securitate, fără a transfera date de conținut, în cooperare cu STS, conform competențelor fiecărei instituții;

(3) asigurarea implementării, administrării tehnice și operaționale, mentenanța, precum și dezvoltarea ulterioară a serviciilor de securitate cibernetică din cloudul intern, de tip SaaS, și **sprijinirea ADR**, la cerere, în realizarea **securității cibernetice** a **cloudului dedicat** din CPG.

Cine coordonează proiectul?

În cadrul proiectului, coordonarea proceselor se află în apanajul ADR, în mod similar cu modelul altor state membre UE, unde coordonarea instituțiilor cu atribuții pe linia de digitalizare se regăsesc în sfera civilă, în sectorul guvernamental.

Care este utilitatea acestuia?

CPG reprezintă o **infrastructură digitală ce integrează aplicații și sisteme informatice** aferente administrației publice din România, menită să ofere servicii de înaltă calitate cetățenilor României, fiind o prioritate asumată de către Guvernul României în **Programul de Guvernare** și prin **Planul Național de Redresare și Reziliență (PNRR)** (*Componenta 7 - Transformare digitală*).

Materializarea demersului de creare și implementare a CPG implică o serie de **avantaje funcționale** în procesul de guvernare digitală, precum diminuarea procesului birocratic aferent relaționării cetățean-instituții, reducerea activităților și costurilor de administrare, dar și creșterea gradului de securitate cibernetică a instituțiilor implicate.

Cine se va ocupa de administrarea datelor?

Conform art. 38, alin. (14) din H.G. nr. 112/2023 **privind aprobarea Ghidului de guvernanţă a platformei de cloud guvernamental,** utilizatorul de servicii de cloud (USC -autoritate și instituție publică din România care utilizează servicii de cloud furnizate în cadrul Platformei) are calitate de proprietar/**administrator**, fiind **responsabil de prelucrarea datelor** și **stabilește drepturi și criteriile de acces la datele prelucrate**, pentru personalul propriu, în vederea îndeplinirii îndatoririlor de serviciu și pentru autorități și instituții terțe, în vederea îndeplinirii obligațiilor legale.

Cine se va ocupa de mentenanță și investiții operaționale după realizarea proiectului prin PNRR?

Aceste aspecte sunt detaliate de legiuitor în CAPITOLUL II al H.G. nr. 112/2023, care reglementează politica, strategia, criteriile tehnice și operaționale privind implementarea,

---

[3] *Software ca serviciu.*
[4] *Infrastructura ca serviciu.*
[5] *Platforma ca serviciu.*

operarea, mentenanța și dezvoltarea ulterioară a Platformei și CPG, regulile privind stabilirea nivelului agreat de servicii, precum și cele privind migrarea și interconectarea sistemelor informatice.

În ce alte proiecte de digitalizare a altor instituții publice prin fonduri naționale sau europene este implicat SRI, Institutul pentru Tehnologii Avansate, Cyberint sau Rasirom (regie aflată în coordonarea SRI)?

I. **ȚIȚEICA 3** - *„Asigurarea protecției cibernetice atât pentru infrastructurile TIC publice, cât și pentru cele private cu valențe critice pentru securitatea națională, prin utilizarea tehnologiilor inteligente”* este un **proiect propus de SRI** în cadrul Planului Național de Redresare și Reziliență al României (PNRR), Componenta C7 - Transformarea digitală. Prin intermediul acestuia se vizează asigurarea unui **nivel ridicat de securitate cibernetică pentru entități publice și private**, prin utilizarea unor soluții bazate pe Inteligența Artificială, în conformitate cu standardele de la nivelul UE, beneficiind de un buget în valoare de 100 milioane euro, bani proveniți din Investiția I12.

Proiectul **ȚIȚEICA 3** reprezintă o continuare a **ȚIȚEICA 1** și a **ȚIȚEICA 2** în contextul evoluțiilor continue din spațiul cibernetic, care generează **riscuri și amenințări la adresa infrastructurilor IT&C** cu valențe critice pentru securitatea națională. În acest sens, proiectul vizează **adoptarea unor soluții tehnice, care să poată preveni materializarea unor atacuri cibernetice la adresa instituțiilor** a căror activitate este esențială pentru buna funcționare a statului român.

II. În ceea ce privește activitatea **RA RASIROM** pe acest segment, menționăm că HG 60/1995 stabilește controlul asupra Regiei din partea Parlamentului, respectiv coordonarea de către SRI şi atribuţiile exprese ale acesteia în domeniul securităţii naţionale;

RA RASIROM, este persoană juridică română care administrează bunuri proprietate privată a statului în temeiul prevederilor Legii nr. 15/1990 privind reorganizarea unităţilor economice de stat ca regii autonome şi societăţi comerciale, cu modificările ulterioare, ale Regulamentului de organizare şi funcţionare prevăzut în anexa nr. 1 la hotărâre şi ale celorlalte acte normative care reglementează activitatea regiilor autonome. Atribuțiile ministerului de resort, prevăzute de Legea nr. 15/1990, se îndeplinesc de către Serviciul Român de Informații;

Regia Autonomă "Rasirom" este integrator de soluţii de securitate fizică şi informatică. Aceasta implementează proiecte de tehnologie în domeniul securităţii naționale, protejează infrastructuri critice ale statului, asigură funcționarea continuă și sigură a sistemelor tehnologice pentru instituțiile din Sistemul Naţional de Apărare, Ordine Publică şi Siguranţă Naţională și alți beneficiari.

Principalele obiective ale RA RASIROM sunt:

- realizarea de produse software și prelucrarea informatică a datelor;
- securizarea cibernetică şi fizică a infrastructurilor critice naționale şi europene;
- asigurarea obiectivelor naționale de interes strategice.

RA RASIROM furnizează produse de înaltă calitate, testate și verificate din perspectiva activității specifice instituției din sistemul național de apărare în cadrul căreia

funcționează, conform legii (art. 43 din Legea nr. 14/1992), esențiale pentru gestionarea în parametri optimi a unor infrastructuri critice diverse, existente sau în curs de implementare în cadrul instituțiilor fundamentale ale statului român, în deplină concordanță cu obiectivele asumate la nivel de stat pentru apărarea ordinii şi valorilor constituționale.

În ceea ce privește implicarea RA RASIROM, în proiectele de digitalizare a instituțiilor publice prin utilizarea fondurilor naționale sau europene, precizăm că în baza OUG nr. 109/2023, RA RASIROM i-a fost atribuit rolul de contractor-integrator în ceea ce privește elementele Hub-ului Financiar cu componentă de securitate națională.

Care sunt garanțiile oferite societății românești pentru beneficiile implicării SRI și STS în proiectele de digitalizare care, în sine, înseamnă transparentizarea și democratizarea informațiilor publice?

Din perspectiva SRI, considerăm că răspunsul la această întrebare este inclus în cele comunicate în cadrul întrebărilor anterioare.

În contextul războiului din Ucraina provocat de agresiunea Rusiei, dar și al provocărilor interne (alegeri, extremism, corupție) cum păstrează SRI echilibrul între drepturile și libertățile cetățenilor și protejarea acestora?

Din perspectiva SRI, considerăm că răspunsul la această întrebare este inclus în cele comunicate în cadrul întrebărilor anterioare.