STRATEGIA NAȚIONALĂ
PRIVIND REZILIENȚA ENTITĂȚILOR CRITICE

CUPRINS

LISTA DE ACRONIME ȘI ABREVIERI

ACS	Autoritățile Competente Sectoriale
AI	Inteligență Artificială
APT	Advanced Persistent Threat
CBRN	Chimic, Biologic, Radiologic și Nuclear
CNCPIC	Centrul Național de Coordonare a Protecției Infrastructurilor Critice
DDoS	Atac cibernetic, din surse multiple, prin care se urmărește indisponibilizarea, blocarea sau epuizarea resurselor unui sistem informatic, rețea sau componentă a acesteia
DNSC	Directoratul Național de Securitate Cibernetică
ECIED	Entități Critice de Importanță Europeană Deosebită
Furnizor de servicii DNS	Conform definiției de la art. 4 lit. i) din OUG nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, cu modificările și completările ulterioare
GLIREC	Grupul de lucru interinstituțional pentru reziliența entităților critice
GPS	Sistem de Poziționare Globală
GREC	Grupul de Reziliență a Entităților Critice
ICS	Sistem de Control Industrial
IoT	Internet of Things
IT	Tehnologia Informației
IXP	Internet Exchange Point
NATO	Organizația Tratatului Atlanticului de Nord
ODD	Obiectiv de Dezvoltare Durabilă
OS	Obiectiv specific
OT	Operational Technology/Tehnologie Operațională
PIN	Număr de Identificare Personal
Registru de nume TLD	Conform definiției de la art. 4 lit. bb) din OUG nr. 155/2024
SMS	Serviciul de mesaje scurte
UAS	Sistem aerian fără pilot
UE	Uniunea Europeană

LISTA DE FIGURI

CAPITOLUL I - INTRODUCERE

În deplin acord cu prevederile Constituţiei României şi Legii nr. 294/2024 privind reziliența entităților critice, precum şi pentru modificarea unor acte normative, Strategia naţională privind reziliența entităților critice, denumită în continuare Strategie, este instrumentul de planificare de nivel superior prin care se asigură, la nivel naţional, cadrul general pentru organizarea şi coordonarea unitară a activităţilor care privesc consolidarea rezilienței entităților critice.

Documentul are la bază prevederile Strategiei de securitate internă a Uniunii Europene, care promovează o abordare integrată a protejării infrastructurilor critice și a gestionării amenințărilor hibride, elementele cheie ale Rapoartelor de analiză prospectivă elaborate de divizia de cercetare a Comisiei UE, direcțiile Strategiei Naționale de Apărare a Țării 2025 – 2030 și este aliniat cu alte documente strategice relevante în domeniul securității și rezilienței.

Prin aplicarea acestor instrumente, România reafirmă angajamentul pentru consolidarea unui cadru coerent de guvernanță, prevenire, protecție, răspuns și redresare în domeniul rezilienței entităților critice.

Strategia are ca scop dezvoltarea unui sistem național integrat, care să consolideze reziliența entităților critice identificate și să asigure continuitatea serviciilor esențiale, în fața tuturor amenințărilor și/sau pericolelor, cu accent pe cele fizice, cibernetice, naturale și hibride.

Fundamentul Strategiei îl constituie legislația națională în domeniul rezilienței entităților critice, precum şi actele normative subsecvente care asigură cadrul pentru funcționarea în siguranță a obiectivelor care furnizează servicii esențiale pentru cetățeni și pentru buna funcționare a statului.

Strategia vizează un orizont de timp până în anul 2031, se actualizează la intervale de cel puțin o dată la fiecare 4 ani și are în vedere nivelul actual de dezvoltare a domeniului rezilienței entităților critice, proiectele și activitățile aflate în derulare sau planificate, experiența și standardele internaționale relevante, precum și obligațiile legale ce decurg din calitatea României de stat membru al Uniunii Europene.

Prezenta Strategie se aplică ACS și entităților critice care furnizează servicii esențiale în sectoarele: Energie, Transporturi, Bancar, Infrastructuri ale pieței financiare, Sănătate, Apă potabilă, Ape uzate, Infrastructura digitală, Administrație publică, Spațiu și Producția, prelucrarea și distribuția de alimente.

Termenii utilizați în prezenta Strategie sunt cei prevăzuți la art. 3 din Legea nr. 294/2024.

CAPITOLUL II - VIZIUNEA

Viziunea:

„Un nivel ridicat de reziliență a entităților critice, care să asigure predictibilitate în livrarea serviciilor esențiale, într-o Românie modernă, competitivă, adaptată la realitățile globale."

Strategia se axează pe următoarele principii directoare:

- *Stabilirea şi asumarea răspunderii pentru asigurarea rezilienței entităților critice*. Răspunderea principală pentru protecția elementelor de infrastructură critică, prin care entitățile critice prestează un serviciu esențial la nivel național, aparţine acestora, cu rol de suport din partea ACS.
- *Controlul activităţilor*. Cadrul legislativ şi de reglementare asigură controlul activităţilor ce se desfăşoară la nivelul entităților identificate ca fiind critice.
- *Management integrat*. Toate ACS și entitățile critice identificate trebuie să implementeze și să dezvolte sisteme de management prin care să se asigure că măsurile privind reziliența sunt implementate într-o manieră coerentă și coordonată.
- *Prioritatea asigurării rezilienței entităților critice*. Entitățile critice trebuie să aibă ca prioritate asigurarea resurselor financiare şi materiale necesare creşterii gradului de reziliență a acestora.

- *Optimizarea rezilienței.* Măsurile de asigurare a rezilienței entităților critice trebuie optimizate astfel încât să se asigure cel mai înalt nivel posibil, luând în considerare evoluțiile din mediul intern și internațional de securitate, dar și potențialul economic al statului.
- *Diminuarea riscurilor.* Măsurile tehnice, operaționale și securitate, adoptate în baza analizelor de risc, vor fi prioritizate pentru creșterea nivelului de reziliență a entităților critice.
- *Pregătirea pentru situații de criză.* Se va pune accent pe construirea unei culturi a pregătirii și răspunsului imediat la situații de criză, pentru diminuarea consecințelor acestora.

CAPITOLUL III - CADRUL DE GUVERNANȚĂ PENTRU REALIZAREA OBIECTIVELOR STRATEGICE, PRIORITĂȚILOR ȘI CADRUL LEGAL EXISTENT

Cadrul de guvernanță stabilit conform prevederilor Legii nr. 294/2024 definește structura, responsabilitățile și mecanismele de coordonare prin care statul român, împreună cu entitățile critice, urmărește realizarea obiectivelor strategice și a priorităților pentru creșterea rezilienței acestora.

Cadrul de guvernanță din domeniul rezilienței entităților critice este structurat pe trei niveluri: i.coordonare strategică (prim-ministru și Guvern), ii.coordonare tehnică și operațională (CNCPIC și ACS, cu sprijinul Grupului de lucru interinstituțional pentru reziliența entităților critice), respectiv iii.implementare (entități critice).

Prezenta Strategie constituie documentul central care stabilește obiectivele, prioritățile, responsabilitățile și mecanismele de cooperare interinstituțională. Implementarea acesteia este supravegheată de ACS, iar CNCPIC asigură punctul unic de contact cu Uniunea Europeană și coordonează procesele de evaluare/revizuire a riscurilor, monitorizare, raportare și adaptare periodică a politicilor de reziliență. Schema cadrului de guvernanță specifică domeniului rezilienței entităților critice este detaliată în figura nr. 1.

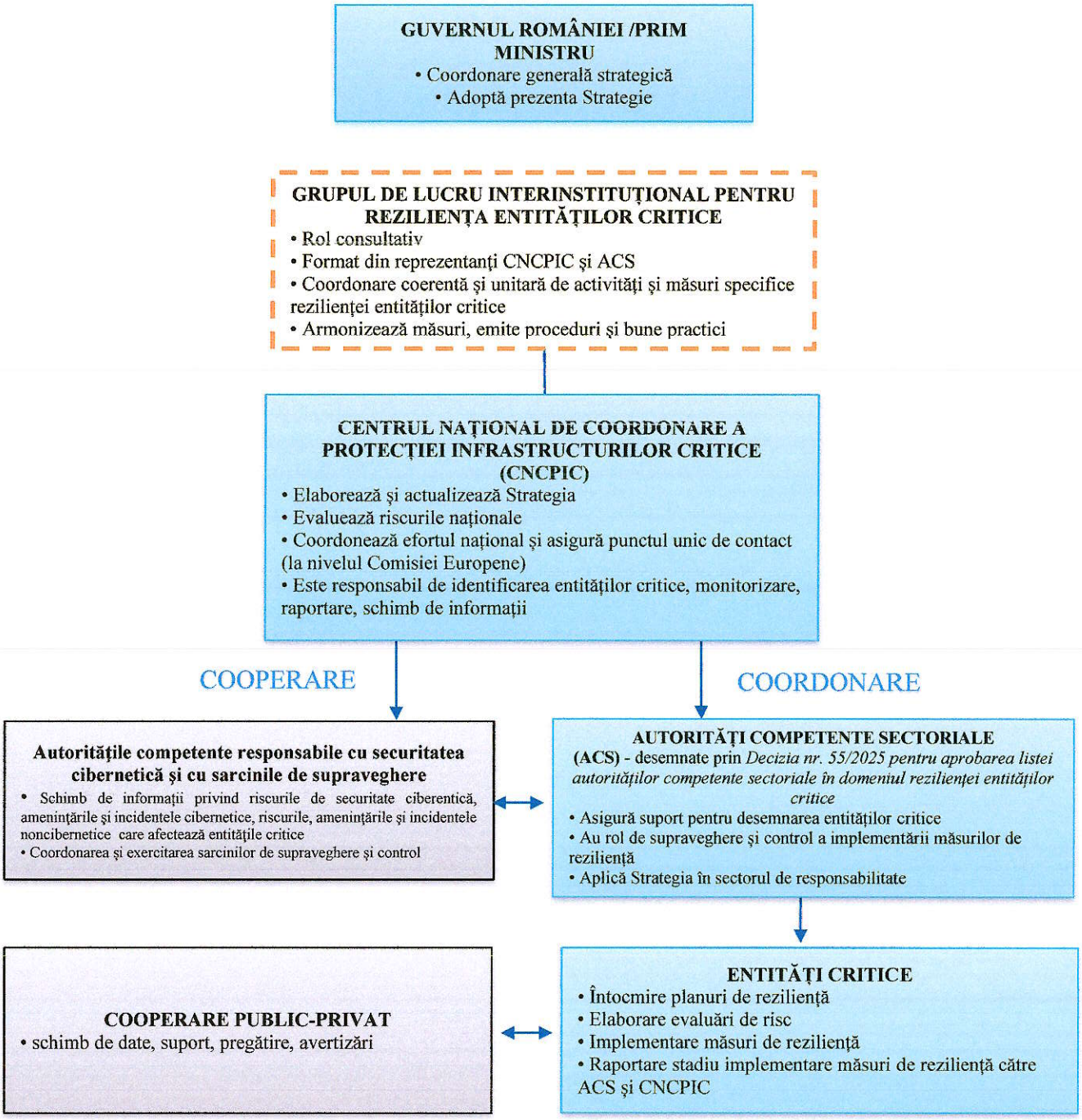

Figura nr. 1 - Schema cadrului de guvernanță specific domeniului rezilienței entităților critice

1. Cadrul legal existent

Acte normative europene

- Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului;
- Regulamentul delegat (UE) 2023/2450 al Comisiei din 25 iulie 2023 de completare a Directivei (UE) 2022/2557 a Parlamentului European și a Consiliului prin stabilirea unei liste de servicii esențiale.

Acte normative naționale

- Legea nr. 294/2024 privind reziliența entităților critice, precum și pentru modificarea unor acte normative;

- Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, cu modificările și completările ulterioare;
- Hotărârea Parlamentului nr. 48/2025 privind aprobarea Strategiei naționale de apărare a țării pentru perioada 2025-2030;
- Hotărârea de Guvern nr. 1115/2025 pentru aprobarea normelor, procedurilor și măsurilor prevăzute la art. 1 alin. (3) din Legea nr. 294/2024 privind reziliența entităților critice, precum și pentru modificarea unor acte normative;
- Decizia prim-ministrului nr. 55/2025 pentru aprobarea listei autorităților competente sectoriale în domeniul rezilienței entităților critice;
- Decizia prim-ministrului nr. 171/2025 pentru aprobarea componenței și a Regulamentului de organizare și funcționare ale Grupului de lucru interinstituțional pentru reziliența entităților critice.

2. Coordonare națională

Coordonarea la nivel național a activităților privind reziliența entităților critice se realizează de către Prim-ministru.

Responsabilitatea pentru organizarea și desfășurarea activităților necesare implementării legislației specifice domeniului rezilienței entităților critice, în temeiul prevederilor art. 9 alin. (2) din Legea nr.294/2024, revine CNCPIC din cadrul Ministerului Afacerilor Interne, în calitate de autoritate competentă la nivel național.

3. Instituții responsabile:

CNCPIC are atribuții privind:
- elaborarea și actualizarea Strategiei;
- coordonarea procesului de identificare a entităților critice;
- monitorizarea implementării măsurilor de reziliență;
- cooperarea cu autoritățile din statele membre ale Uniunii Europene și cu Comisia Europeană.

Autoritățile Competente Sectoriale - ACS
Sectoarele specifice domeniului rezilienței entităților critice sunt gestionate de autoritățile competente, responsabile pentru:
- suport pentru identificarea entităților critice din sector;
- evaluarea periodică a gradului de conformare al entităților critice cu măsurile de reziliență din planurile dedicate;
- evaluarea riscurilor sectoriale;
- colectarea și transmiterea rapoartelor periodice către CNCPIC;
- stabilirea, alături de CNCPIC și de comun acord cu autoritățile competente responsabile cu securitatea cibernetică, a mecanismelor și a căilor de comunicare în scopul schimbului de informații privind riscurile de securitate cibernetică, amenințările cibernetice și incidentele cibernetice și riscurile, amenințările și incidentele noncibernetice și al exercitării sarcinilor de supraveghere.

Grupul de lucru interinstituțional pentru reziliența entităților critice - GLIREC
- organism consultativ, format din reprezentanți ai CNCPIC și ACS;
- asigură sprijin operațional, schimbul de informații și armonizarea măsurilor pentru îmbunătățirea activității în domeniul rezilienței entităților critice;
- concentrează și aliniază eforturile pentru implementarea Strategiei și a politicilor de reziliență.

Entitățile critice sunt entitățile cu personalitate juridică de drept public sau privat care furnizează servicii esențiale în sectoarele și subsectoarele din anexa la Legea nr. 294/2024 și au rol de:
- aplicare a măsurilor concrete de reziliență;
- evaluare a riscurilor la care sunt expuse;
- întocmire și menținere a unui plan de reziliență;

- raportare a incidentelor și a stadiului implementării măsurilor.

Autoritățile competente responsabile cu securitatea cibernetică și cu sarcinile de supraveghere și asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică

- cooperează cu CNCPIC și ASC în scopul schimbului de informații privind riscurile de securitate cibernetică, amenințările și incidentele cibernetice, precum și riscurile, amenințările și incidentele noncibernetice/de altă natură decât cibernetică);
- cooperează în scopul coordonării și exercitării sarcinilor de supraveghere și control;
- colaborează cu CNCPIC și ACS în vederea optimizării proceselor de identificare, monitorizare și analiză a amenințărilor, vulnerabilităților și riscurilor cibernetice asupra entităților critice.

3. Cooperare internațională

România participă activ la mecanismele de cooperare prevăzute de Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului, inclusiv la Grupul de Reziliență a Entităților Critice (GREC) instituit la nivelul UE.

CAPITOLUL IV – ANALIZA CONTEXTULUI ȘI DEFINIREA PROBLEMELOR

Context internațional

Directiva (UE) 2022/2557, transpusă la nivel național prin Legea nr. 294/2024, stabilește cadrul comun pentru managementul rezilienței acestor entități și, totodată:

- **reafirmă necesitatea consolidării rezilienței fizice** a entităților critice, prin îmbunătățirea capacității acestora de a face față amenințărilor și de a implementa măsuri specifice menite să asigure furnizarea neîntreruptă, pe piața internă, a serviciilor esențiale pentru menținerea funcțiilor societale și a activităților economice vitale, în limita articolului 114 din Tratatul de Funcționare al UE;
- **confirmă responsabilitatea finală a statelor membre** în gestionarea măsurilor de reziliență aplicate entităților critice de pe teritoriul lor;
- **stabilește procedura de identificare** a entităților critice și a entităților critice de importanță europeană deosebită (ECIED), precum și modul de evaluare, prin misiuni de consiliere, a măsurilor implementate de acestea pentru îndeplinirea obligațiilor legale;
- **instituie obligativitatea elaborării planurilor de reziliență,** prin care entitățile trebuie să detalieze măsurile adoptate, la un nivel care să permită evaluarea eficacității și asumarea responsabilității, ținând cont de riscurile identificate.

Context național

România va implementa măsurile și acțiunile necesare pentru consolidarea rezilienței entităților critice identificate, având în vedere rolul esențial al acestora în asigurarea furnizării neîntrerupte, pe piața internă, a serviciilor indispensabile menținerii funcțiilor societale și activităților economice vitale.

Prin realizarea obiectivelor strategiei, nivelul de reziliență al entităților desemnate ca fiind critice va fi îmbunătățit, iar politicile comune din domeniu vor fi adoptate și puse în aplicare.

În acest context, la nivel național vor fi identificate entitățile critice, prin parcurgerea etapelor specifice stabilite în art. 6 din Legea nr. 294/2024, după cum urmează:

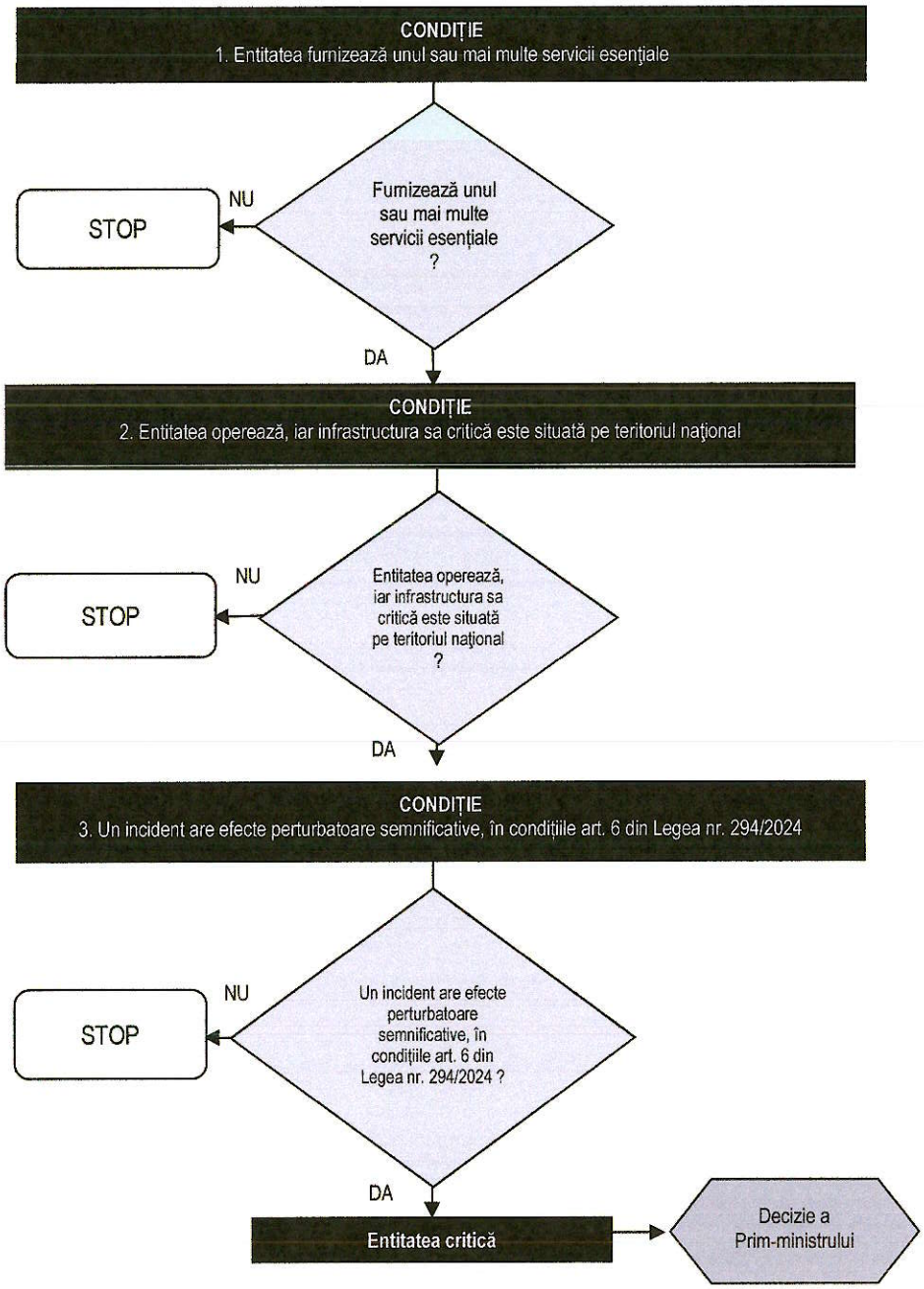

Figura nr. 2 - Schema procesului de identificare a entităților critice

Analiza contextului actual de securitate, a amenințărilor și vulnerabilităților

Contextul actual de securitate, atât la nivel internațional, cât și european, este marcat de o complexitate și o instabilitate accentuate, iar amenințările se manifestă pe multiple planuri (militar, cibernetic, hibrid sau economic), într-o manieră interconectată și cu potențial de creare a unor efecte în cascadă. În acest cadru, procesul de asigurare a rezilienței entităților critice trebuie să evolueze rapid, să fie unul adaptabil la și impulsionat de un mediu de risc tot mai divers, influențat de globalizare, demersurile unor actori ostili de contestare a ordinii de drept internaționale, libera circulație a persoanelor și bunurilor, schimbările climatice și hazardurile naturale, digitalizarea accelerată, precum și de recrudescența criminalității organizate și a terorismului la nivel internațional (atât ca factori perturbatori de sine stătători, dar mai ales în scenariul utilizării lor ca proxy de către actori statali ostili în cadrul unor campanii hibride).

Tendințe, provocări și mecanisme de răspuns actuale:

- Digitalizarea accelerată – extinderea tehnologiilor de tipul IoT, AI și a infrastructurilor bazate pe tehnologii inteligente generează beneficii, dar și riscuri noi, legate de interconectivitate, supra-dependență de acestea și vulnerabilități cibernetice;
- Interdependența sectoarelor critice – o perturbare într-un sector poate avea efecte în lanț asupra altor domenii; actorii ostili urmăresc ca, prin destabilizarea unui sector inițial, să genereze efecte asimetrice, a căror origine este dificil de atribuit, la nivelul cât mai multor domenii conectate, fie ele critice sau nu;
- Schimbările climatice accelerate și hazardurile naturale – creșterea frecvenței fenomenelor meteo extreme impune modernizarea infrastructurilor și adaptarea la condițiile climatice, totul bazat pe o cultură a pregătirii pentru criză, în vederea reacției rapide la evenimente preponderent imprevizibile ca frecvență și impact;
- Amenințările hibride și geopolitice – atacurile cibernetice, dezinformarea și sabotajul fac trecerea, prin efectele asimetrice, de la instrumente tactice la obiective strategice în conflictele moderne;
- Cooperarea public–privată – majoritatea infrastructurilor critice sunt gestionate/operate de entități private, ceea ce impune parteneriate solide și schimb de informații eficient între ACS și aceste entități identificate ca fiind critice;
- Cooperarea civil–militară – pe aceleași considerente, dar și pentru maximizarea impactului unor tehnologii, servicii sau bunuri cu uz dual în procesul de consolidare a rezilienței generale a statului, devine obligatorie o mai bună cooperare între cele două componente ale societății, bazată pe încredere, schimb de informații în timp util și focus pe utilitatea creată la nivelul partenerului în gestionarea unui eveniment, respectiv testarea în comun a mecanismelor de intervenție pentru gestionarea unor crize;
- Rol sporit în arhitectura de securitate europeană - România își propune să devină hub strategic pentru NATO și UE în Marea Neagră, contribuind la consolidarea rezilienței energetice a celor două blocuri, conectivitatea sporită și sigură și, prin sinergia dintre acestea, la securitatea generală a frontierei/flancului estice/estic.

Pentru a fi eficiente, toate acțiunile menite să asigure un nivel crescut de reziliență trebuie să se raporteze la complexitatea și dinamismul mediului internațional de securitate.

1. Principalele amenințări din mediul internațional

1.1. Amenințări cibernetice:

- Atacuri ransomware care pot paraliza rețele, obiective strategice, spitale, sisteme energetice sau financiare;
- Spionaj cibernetic realizat de actori statali sau grupări avansate (APT);
- Sabotaj digital asupra infrastructurii critice (rețele electrice, apă, transport);
- Furt de date sensibile, inclusiv informații personale, financiare sau tehnologii strategice;
- Atacuri asupra lanțului de aprovizionare IT (compromiterea furnizorilor de software /hardware).

1.2. Conflicte geopolitice și tensiuni internaționale:

- Războaie și conflicte regionale care destabilizează fluxurile energetice și comerciale;
- Sancțiuni economice ce pot afecta furnizori sau parteneri strategici;
- Militarizarea spațiului cibernetic și atacuri hibride între state;
- Instabilitate politică în zone-cheie pentru aprovizionarea cu energie, materii prime sau tehnologii.

1.3. Amenințări fizice și terorism:

- Atacuri teroriste asupra rețelelor de transport, centrale energetice, instituții publice;
- Sabotaj fizic asupra conductelor, rețelelor electrice sau telecomunicațiilor;

- Atacuri cu drone la instalațiile sensibile.

1.4. Amenințări de tip economic, financiar și de piață:
- Suprafața de contact dintre nevoia de competitivitate economică și cea de autonomie strategică a UE, complicată de volatilitatea economică asociată unor demersuri de repoziționare a polilor de putere globali;
- Crize economice internaționale, cu impact asupra finanțării și operaționalității;
- Volatilitate energetică (prețuri crescute, penurii, manipulare de piață);
- Dependență de furnizori unici pentru tehnologii sau resurse strategice;
- Atacuri asupra sistemului financiar global (fraude, destabilizare valutară).

1.5. Amenințări biologice și pandemii:
- Blocaje în lanțurile de aprovizionare globală cu medicamente, precursori sau echipamente de protecție;
- Presiune asupra infrastructurii medicale și sociale;
- Reducerea capacității de operare a entităților critice.

1.6. Schimbări climatice și dezastre naturale:
- Inundații, incendii, cutremure care pot distruge centre de date și/sau rețele fizice;
- Condiții meteo extreme, cu impact asupra energiei, transporturilor, agriculturii;
- Creșterea riscului de migrație și a conflictelor pentru resurse.

1.7. Campanii de dezinformare și influență:
- Manipulare informațională orchestrată de actori statali sau non-statali, utilizând tehnologii de amplificare bazate pe AI;
- Propagandă digitală vizând destabilizare politică sau economică;
- Atacuri asupra încrederii în entități ce prestează servicii esențiale (prin intermediul unor active critice).

1.8. Amenințări asupra lanțurilor de aprovizionare globale:
- Blocaje comerciale sau embargouri;
- Compromiterea furnizorilor critici (hardware, software, materiale rare);
- Instabilitate în regiunile producătoare de resurse strategice.

2. Principalele amenințări la adresa sectoarelor și subsectoarelor interne

2.1. Energie

a) Energie electrică:
- Atacuri cibernetice care vizează producerea, transportul, distribuția și furnizarea energiei electrice (inclusiv activitățile de dispecerizare și piața de energie), având potențial de întreruperi majore, avarii fizice și impact asupra securității naționale (inclusiv, dar nelimitându-se la atacuri asupra sistemelor OT, ransomware, atacuri APT, compromiterea lanțului de aprovizionare, exploatarea vulnerabilităților echipamentelor care nu beneficiază de suport, amenințări interne, scurgeri de date tehnice sensibile etc.);
- Sabotaj fizic asupra stațiilor de transformare, liniilor de transport, centrelor de dispecerizare;
- Defecțiuni tehnologice sau erori umane;
- Perturbări generate de fenomene meteo extreme (furtuni, caniculă, îngheț);
- Perturbări ale lanțului de aprovizionare (echipamente, software, piese de schimb);
- Suprasolicitarea rețelei/blackout accidental;
- Atacuri hibride cu scop de destabilizare politico-economică.

b) Sisteme de încălzire și răcire centralizată:
- Atacuri cibernetice asupra sistemelor informatice și de comunicații ale operatorilor de producție și transport al agentului termic, precum și a sistemelor automate de control;
- Defecțiuni ale rețelelor de distribuție (conducte, schimbătoare de căldură);
- Sabotaj fizic sau incendii;

- Întreruperea/sistare furnizării de combustibili (gaze, păcură);
- Vârfuri de consum neacoperite de producție.

c) Petrol:
- Atacuri cibernetice asupra platformelor de extracție și rafinării;
- Atacuri asupra conductelor (explozie, sabotaj, furt);
- Scăderi drastice ale fluxurilor de import/export;
- Poluări accidentale sau deteriorări ale instalațiilor;
- Instabilitate geopolitică.

d) Gaze:
- Sabotaj asupra conductelor de transport/depozite/platformelor/instalațiilor de forare;
- Atacuri cibernetice asupra infrastructurii de producție, transport, distribuție și înmagazinare;
- Explozii/defecțiuni tehnice din materialelor defecte, mentenanței insuficiente/tardive;
- Perturbări geopolitice privind aprovizionarea internațională.

e) Hidrogen:
- Risc crescut de incendii sau explozii;
- Atacuri cibernetice asupra sistemelor de producție și stocare;
- Vulnerabilități tehnologice specifice infrastructurii emergente;
- Sabotaj asupra capacităților de stocare și transport.

2.2. Transporturi

a) Transport aerian:
- Atacuri cibernetice asupra aeroporturilor, sistemelor de navigație și companiilor aeriene;
- Drone ostile/interferență GPS;
- Atacuri fizice asupra infrastructurii aeroportuare;
- Incidente tehnice, defecțiuni ale sistemelor radar;
- Evenimente meteorologice severe.

b) Transport feroviar:
- Atacuri cibernetice asupra semnalizării și centralizării;
- Sabotaj la nivelul șinelor, podurilor, macazurilor;
- Coliziuni sau deraieri cauzate de defecțiuni tehnice;
- Furturi de materiale (cabluri, echipamente).

c) Transport pe apă:
- Atacuri cibernetice la nivelul autorităților portuare sau navelor;
- Blocarea infrastructurii portuare prin incidente fizice;
- Drone ostile/interferență GPS;
- Piraterie informatică asupra sistemelor de navigație maritimă;
- Poluări accidentale.

d) Transport rutier:
- Atacuri cibernetice asupra sistemelor inteligente de trafic;
- Accidente majore, blocaje rutiere;
- Distrugerea infrastructurii (poduri, tuneluri, centre de control);
- Proteste, blocaje deliberate ale arterelor.

e) Transport public:
- Atacuri cibernetice asupra sistemelor de ticketing și dirijare;
- Incidente fizice sau vandalism;
- Defecțiuni tehnice ale vehiculelor sau rețelelor electrice;
- Supraaglomerare în situații de urgență.

2.3. Sectorul bancar

- Atacuri cibernetice: ransomware, DDoS, fraude avansate, atacurile avansate APT, emergente (utilizarea tehnologiilor AI);
- Breșe de date și compromiterea sistemelor de plăți;
- Fraudă internă sau erori operaționale;
- Instabilitate financiară sau volatilitate globală;

- Atacuri hibride orientate pe destabilizarea încrederii publice.

2.4. Infrastructuri ale pieței financiare

- Atacuri cibernetice asupra burselor de valori și contrapărților centrale;
- Breșe de date și compromiterea sistemelor de plăți;
- Blocarea sistemelor de compensare și decontare;
- Atacuri asupra integrității datelor financiare;
- Suprasolicitări sau congestii în momente critice.

2.5. Sectorul sănătății

- Atacuri cibernetice asupra spitalelor și sistemelor utilizate pentru gestionarea serviciilor medicale, echipamentelor critice și a datelor pacienților, cu potențial de perturbare a continuității activităților, risc direct asupra vieții pacienților și impact asupra confidențialității datelor;
- Probleme logistice legate de medicamente și echipamente;
- Defecțiuni ale sistemelor critice (oxigen, IT medical, energie);
- Pandemii, epidemii, crize de personal;
- Sabotaj sau furt de materiale medicale critice.

2.6. Apă potabilă

- Atacuri cibernetice asupra stațiilor de pompare și tratare;
- Contaminare accidentală sau deliberată a surselor de apă;
- Degradarea infrastructurii (conducte vechi, avarii);
- Secetă severă/scăderea debitelor surselor naturale.

2.7. Ape uzate

- Atacuri cibernetice asupra stațiilor de epurare;
- Deversări necontrolate cauzate de avarii;
- Poluări industriale accidentale;
- Probleme de capacitate în perioade de precipitații abundente.

2.8. Infrastructură digitală

- Atacuri cibernetice avansate asupra furnizorilor de IXP (internet exchange point), furnizorilor de servicii DNS, registrelor de nume TLD, furnizorilor de cloud computing, furnizorilor de centre de date, furnizorilor de servicii de încredere, furnizorilor de rețele de furnizare de conținut, furnizorilor de rețele publice de comunicații electronice, furnizorilor de servicii de comunicații electronice destinate publicului;
- Sabotaj fizic asupra cablurilor de fibră, nodurilor de comunicații;
- Suprasolicitări în situații de criză (colaps al rețelelor);
- Erori de configurare și vulnerabilități software;
- Campanii de dezinformare și atacuri hibride.

2.9. Administrație publică

- Atacuri cibernetice asupra sistemelor informatice guvernamentale;
- Compromiterea bazelor de date cu informații sensibile;
- Sabotaj administrativ (blocarea serviciilor publice);
- Dependență ridicată de sisteme informatice depășite;
- Atacuri hibride în perioade electorale.

2.10. Spațiu

- Atacuri cibernetice asupra sateliților și stațiilor de sol;
- Interferențe radio, spoofing și jamming;
- Coliziuni orbitale sau deșeuri spațiale;
- Sabotaj asupra infrastructurii terestre de control.

2.11. Producția, prelucrarea și distribuția de alimente

- Atacuri cibernetice asupra lanțurilor de aprovizionare/logistică;
- Contaminare accidentală sau deliberată;
- Crize agricole (secetă, boli la plante/animale);
- Perturbări ale transportului și depozitării;
- Creșteri bruște ale prețurilor/instabilitate economică.

3. Principalele vulnerabilități ale entităților critice

3.1. Vulnerabilități tehnologice și infrastructurale

3.1.1. Dependență puternică de importuri pentru tehnică de vârf, precum și de servicii digitale avansate furnizate de entități străine;
3.1.2. Implementarea unor tehnologii care nu respectă cerințele de securitate;
3.1.3. Uzura fizică și morală a echipamentelor vitale, coroborată cu neasigurarea în termenele legale sau la standarde de calitate a lucrărilor de mentenanță;
3.1.4. Nerespectarea măsurilor de protecție a sistemelor informatice și de comunicații;
3.1.5. Deficiențe în infrastructura de comunicații și energie pentru situații de urgență;
3.1.6. Vulnerabilități în lanțul de aprovizionare, inclusiv la nivelul subcontractorilor;
3.1.7. Vulnerabilități în relație cu entități terțe, interconectate;
3.1.8. Expunerea la riscuri naturale sau catastrofale (inundații, cutremure, incendii), fără măsuri adecvate de protecție.

3.2. Vulnerabilități umane și de resurse

3.2.1. Lipsa de conștientizare și instruire periodică a personalului;
3.2.2. Acces neautorizat sau abuz de privilegii din perspectiva accesului la date sau componente de infrastructură;
3.2.3. Lipsa instrumentelor de monitorizare și detecție, precum și deficiențe în planurile de răspuns la incidente, continuitate, recuperare și gestionarea situațiilor de crize;
3.2.4. Deficit de personal calificat în domeniile cibernetic, ingineresc și operativ, generat inclusiv din perspectiva guvernanței organizațiilor precum și a cheltuielilor alocate pentru atragerea și menținerea acestuia;
3.2.5. Fluctuații frecvente și imprevizibile de personal;
3.2.6. Lipsa culturii organizaționale privind securitatea fizică și cibernetică la toate nivelurile.
3.2.7. Insuficiența resurselor financiare pentru modernizare și retehnologizare;

3.3. Vulnerabilități organizaționale și manageriale

3.3.1. Managementul defectuos al resurselor de toate tipurile;
3.3.2. Lipsa planurilor eficiente de continuitate a activității și de recuperare în caz de criză;
3.3.3. Deficiențe în cooperarea și schimbul de informații între entități critice sau cu ACS;
3.3.4. Procese interne insuficient securizate sau neuniform reglementate;
3.3.5. Expunerea la presiuni politice, economice sau sociale care pot afecta deciziile strategice ale entității;
3.3.6. Grad crescut de interdependență între entități critice.

3.4. Vulnerabilități de securitate și cibernetice

3.4.1. Suprafață de contact cyber în continuă extindere;
3.4.2. Evaluarea entităților critice ca ținte soft de către actorii statali ostili;
3.4.3. Deficiențe în activitatea de asigurare a protecției fizice;
3.4.4. Dependența excesivă de un număr limitat de furnizori sau tehnologii critice;
3.4.5. Expunerea la riscuri emergente în domeniul securității cibernetice.

CAPITOLUL V - OBIECTIVE STRATEGICE ŞI PRIORITĂŢI DEDICATE CONSOLIDĂRII REZILIENŢEI ENTITĂŢILOR CRITICE

Strategia naţională privind reziliența entităţilor critice este un instrument de planificare de nivel superior, care propune măsuri menite să contribuie la creşterea nivelului de reziliență a entităţilor critice prin consolidarea capabilităţilor ACS de a coordona eficient răspunsul la provocările ce se manifestă în mediul intern şi internaţional de securitate.

1. Obiectiv strategic

Obiectiv strategic: Creşterea nivelului de reziliență a macro-sistemului prin care sunt livrate servicii esenţiale cetăţenilor, operatorilor privaţi şi autorităţilor statului, ca efect cumulativ al unui nivel suficient de reziliență a entităţilor critice, pentru prevenirea sau limitarea efectelor generate de perturbarea funcţionalităţii sau distrugerea elementelor de infrastructură critică prin intermediul cărora sunt furnizate serviciile esenţiale.

2. Obiective specifice şi direcţii de acţiune

OS 1. Consolidarea capacităţii instituţionale şi a guvernanţei naţionale pentru asigurarea rezilienţei entităţilor critice

Direcţia de acţiune 1.1. Evaluarea şi actualizarea periodică a cadrului de reglementare la evoluţiile strategice internaţionale şi la cele mai avansate standarde şi practici în domeniul rezilienţei entităţilor critice.

Direcţia de acţiune 1.2. Implementarea unui proces strategic de evaluare continuă a entităţilor critice, pentru consolidarea capacităţii de răspuns la ameninţări complexe.

Direcţia de acţiune 1.3. Promovarea unei culturi naţionale robuste de securitate, prin consolidarea programelor de formare şi dezvoltare profesională la nivelul ACS şi al entităţilor critice.

Direcţia de acţiune 1.4. Crearea unui cadru eficient de schimb de informaţii şi bune practici pentru toate entităţile critice, în vederea creşterii nivelului de cunoaştere situaţională şi a capacităţii de reacţie.

Direcţia de acţiune 1.5. Dezvoltarea unui cadru strategic integrat pentru decizii bazate pe evaluări complexe ale riscurilor de la nivelul entităţilor critice, care să fie integrate în evaluarea de risc naţională.

OS 2. Consolidarea cooperării internaţionale şi asigurarea armonizării permanente cu politicile şi standardele Uniunii Europene în domeniul rezilienţei entităţilor critice

Direcţia de acţiune 2.1. Dezvoltarea, extinderea şi consolidarea cadrului de cooperare internaţională, prin intensificarea parteneriatelor (bi)multilaterale şi prin participarea activă la iniţiative comune în domeniul securităţii şi rezilienţei.

Direcţia de acţiune 2.2. Creşterea nivelului de implicare în fundamentarea programelor de finanţare ale Uniunii Europene, concomitent cu identificarea oportunităţilor disponibile şi maximizarea absorbţiei fondurilor.

Direcţia de acţiune 2.3. Asigurarea conformităţii continue cu standardele, politicile şi mecanismele europene, inclusiv prin respectarea şi operarea corespunzătoare a fluxurilor de raportare către Comisia Europeană şi către alte organisme relevante.

Direcţia de acţiune 2.4. Participarea activă la schimburi de bune practici în cadrul GREC, în vederea îmbunătăţirii proceselor naţionale şi alinierii la tendinţele europene privind reziliența.

Direcţia de acţiune 2.5. Reprezentarea şi implicarea României în cadrul forumurilor decizionale internaţionale, care elaborează politici, reglementări şi standarde cu impact asupra domeniului rezilienţei entităţilor critice, pentru a contribui la formarea cadrului strategic şi normativ global.

OS 3. Întărirea capacităților de prevenire, reacție și asigurare a continuității în furnizarea serviciilor esențiale ale entităților critice în fața incidentelor majore

Direcția de acțiune 3.1. Dezvoltarea și implementarea planurilor de reziliență, însoțite de testarea periodică a acestora prin exerciții interne derivate din rezultatele evaluărilor de risc, pentru asigurarea unui nivel adecvat de pregătire și adaptabilitate.

Direcția de acțiune 3.2. Elaborarea unor ghiduri privind răspunsul la incidente majore, atât fizice, cât și cibernetice, cu sprijinul DNSC, pentru diseminarea bunelor practici la nivel național.

OS 4. Dezvoltarea competențelor și culturii de securitate

Direcția de acțiune 4.1. Formarea profesională pentru personalul specializat de la nivelul entităților critice.

Direcția de acțiune 4.2. Organizarea de cursuri și workshop-uri periodice pe teme de securitate pentru entități critice.

OS 5. Creșterea nivelului de reziliență a entităților critice

Direcția de acțiune 5.1. Adaptarea priorităților strategice în vederea asigurării unui nivel ridicat de reziliență a entităților critice.

Direcția de acțiune 5.2. Identificarea celor mai bune soluții pentru creșterea capacităților de adaptare și de restaurare a funcționalității infrastructurilor critice prin intermediul cărora entitățile critice furnizează servicii esențiale.

Direcția de acțiune 5.3. Încheierea de acorduri și parteneriate public-private, respectiv civil-militare.

Direcția de acțiune 5.4. Evaluarea permanentă a rezilienței elementelor de infrastructură critică.

CAPITOLUL VI - MĂSURI NECESARE PENTRU A CONSOLIDA REZILIENȚA GENERALĂ A ENTITĂȚILOR CRITICE

Implementarea Directivei (UE) 2022/2557 se realizează în contextul unui peisaj complex și în continuă evoluție a amenințărilor la care este expusă infrastructura critică din Uniunea Europeană, marcat recent de agresiunea rusă împotriva Ucrainei și caracterizat de interacțiunea și interesele de multe ori aliniate dintre actorii ostili statali, proxy-urile acestora, respectiv un spectru larg de teroriști, extremiști sau chiar persoane din interior. Numărul actelor, tentativelor și activităților de pregătire a sabotajului infrastructurii critice a crescut din 2022 și a înregistrat o creștere accelerată în 2024, afectând un număr semnificativ de state membre.

Mai mult, Europa este continentul cu cel mai rapid nivel de încălzire din cauza schimbărilor climatice. Inundațiile, secetele și incendiile forestiere devin mai frecvente, iar fenomenele meteorologice extreme au, de asemenea, un impact și asupra infrastructurii critice, respectiv serviciilor esențiale.

Directiva (UE) 2022/2557 pune în sarcina Comisiei Europene adoptarea de orientări neobligatorii pentru a specifica în detaliu măsurile tehnice, de securitate și de reziliență organizațională care pot fi luate de entitățile critice.

Conform cadrului legislativ național, măsurile menite să asigure un nivel ridicat al rezilienței entităților critice se stabilesc în conformitate cu prevederile art. 13 din Legea nr. 294/2024, în urma unui proces complex, ținând cont de specificul entității și de serviciul esențial furnizat, pe baza informațiilor relevante rezultate din evaluarea riscurilor efectuată de CNCPIC conform art. 5 din legea menționată, precum și a rezultatelor evaluării riscurilor realizate de aceste entități.

Măsurile menite să asigure un nivel ridicat al rezilienței entităților critice pot fi tehnice, de securitate și organizatorice și sunt adoptate în mod adecvat și proporțional cu evaluările de risc menționate.

Întreprinderilor mici şi mijlocii, în înţelesul Legii nr. 346/2004 privind stimularea înfiinţării şi dezvoltării întreprinderilor mici şi mijlocii, cu modificările şi completările ulterioare, identificate drept entităţi critice, le revin obligaţii în temeiul cap. III din Legea nr. 294/2024, iar acestea pot adopta măsuri specifice de reziliență stabilite în actele normative incidente domeniului propriu de responsabilitate, cu luarea în considerare a cerinţelor de la art. 13 din Legea nr. 294/2024.

Aşadar, **accesul la consultanță și finanțări dedicate întreprinderilor mici și mijlocii** — folosind măsurile prevăzute de Legea nr. 346/2004 (consultanță, dezvoltare tehnologică, sprijin pentru inovare, digitalizare), pentru a moderniza infrastructura și procesele — astfel încât să fie pregătite să răspundă cerinţelor Legii nr. 294/2024, **planurile de continuitate și management al riscului** — elaborarea de planuri de continuitate, backup, securitate fizică/cibernetică, asigurări etc., pentru a reduce vulnerabilitatea, **dialogul cu ACS / CNCPIC — pentru clarificări, interpretări și sprijin**, precum și **cooperarea proactivă** sunt unele din instrumentele care pot facilita adaptarea la noul cadru legislativ și pot transforma obligațiile în unele gestionabile, proporționale, evitând suprapunerile sau golurile de responsabilități.

În marja activităților desfășurate la nivel european pentru implementarea prevederilor Directivei (UE) 2022/2557, CNCPIC a inițiat un amplu proces de consultare a celor mai relevante asociații profesionale interne cu responsabilități în sectoarele de activitate prevăzute de directiva în cauză, cu scopul de a utiliza cunoașterea acumulată pentru consolidarea unui document de ghidaj comprehensiv în ceea ce privește stabilirea unui set de măsuri.

Imaginea de ansamblu cu privire la un set consolidat de propuneri de măsuri necesare consolidării rezilienței este următoarea:

1. Măsuri tehnice

1.1 Redundanță pentru sistemele critice: copii de rezervă și servere alternative:
- Acces securizat la rețea și comunicații radio;
- Copiere de rezervă zilnică pentru toate bazele de date operaționale;
- Generatoare de rezervă activate și testate periodic;
- Sisteme redundante pentru aer condiționat, electricitate etc.;
- Contracte pentru furnizare/ intervenții/ reparații rapide de la terți la rețelele de electricitate, apă, ventilație.

1.2 Monitorizare și mentenanță predictivă, pentru prevenirea defecțiunilor:
- Identificarea timpurie a riscurilor hidrologice și structurale care afectează entitățile;
- Implementarea unei rețele integrate de senzori de înaltă precizie în infrastructura critică;
- Monitorizarea continuă a performanței infrastructurii;
- Utilizarea tehnologiilor de mentenanță predictivă pentru prevenirea defecțiunilor.

2. Măsuri de securitate

2.1 Întreținerea prioritară a echipamentelor de securitate

2.2 Contracararea sistemelor fără pilot, inclusiv a UAS

2.3 Protecția spațiilor și a infrastructurii critice:
- Instalarea de garduri anti-escaladare și bariere fizice rezistente la impact;
- Sisteme de detectare a intruziunilor la nivelul perimetrului (senzori de mișcare, camere termice, radar);
- Patrule fizice regulate și monitorizarea personalului de securitate 24/7;
- Sisteme electronice de control al accesului bazate pe carduri de identificare, coduri PIN sau date biometrice;
- Zone bine definite: publice, controlate, restricționate;
- Audituri periodice ale permiselor de acces și verificări ale comportamentului angajaților;
- Acoperire video completă în zonele sensibile: porți de acces, perimetru, piste, zone de marfă;
- Analiză video automată pentru detectarea comportamentelor suspecte sau a activităților neobișnuite;
- Copiere de rezervă securizată a înregistrărilor pentru perioadele impuse de lege.

3. Măsuri organizatorice

3.1 Planificarea continuității afacerii: dezvoltarea și actualizarea periodică a unui plan de continuitate pentru scenarii critice (pandemie, incendiu, dezastru natural, atac terorist, defecțiune IT majoră, o combinație a unora /tuturor celor de mai sus);

3.2 Managementul crizelor și răspunsul la situații de urgență: stabilirea unei structuri de comandă și control pentru incidentele majore;

3.3 Securitatea, instruirea și conștientizarea angajaților: programe de instruire continuă pentru recunoașterea și răspunsul la amenințările de securitate:

- Menținerea unui stoc de echipamente individuale de protecție pentru scenarii legate de sănătate/CBRN;
- Programe periodice de instruire pentru toți angajații privind recunoașterea comportamentelor suspecte;
- Exerciții comune pentru simularea atacurilor sau a incidentelor de securitate;
- Instruirea angajaților pentru un răspuns rapid la amenințări;
- Dezvoltarea unei metodologii pentru un răspuns constant, temeinic și adaptabil al personalului tehnic, operațional și managerial;
- Instruirea personalului privind riscurile, identificarea semnelor unui atac sau vulnerabilitate și furnizarea de răspunsuri adecvate;
- Verificare/Indicatori/Practici pentru prevenirea sabotajului intern;
- Elaborarea de îndrumări privind utilizarea tehnologiilor compatibile în diferite sectoare și state membre.

3.4 Măsuri privind resursele umane:

- Plan de rotație a personalului pentru a asigura odihna și înlocuirea în caz de indisponibilitate;
- Lista personalului de rezervă certificat pentru funcții cheie;
- Instruire continuă pentru răspunsul la situații de urgență.

3.5 Parteneriate și colaborare între părțile interesate: implicarea partenerilor publici și privați pentru un răspuns eficient la incidente

3.6 Cultura rezilienței organizaționale: promovarea unei culturi a rezilienței prin leadership, comunicare deschisă și exerciții/instruire:

- Plan de comunicare internă cu personalul – notificări rapide prin SMS/e-mail;
- Protocol de comunicare externă cu autoritățile publice relevante și mass-media;
- Simulări de întrerupere a serviciilor pentru a testa răspunsul sistemului și al personalului.

3.7 Adaptarea la schimbările climatice:

- Abordare unificată a pregătirii pentru apărare și a adaptării la schimbările climatice;
- Planuri-cadru de continuitate pentru apărare și restaurarea infrastructurii în caz de evenimente extreme, atacuri cibernetice.

CAPITOLUL VII - CADRUL GENERAL DE COOPERARE ÎNTRE CNCPIC, ACS ȘI AUTORITĂȚILE COMPETENTE RESPONSABILE CU SECURITATEA CIBERNETICĂ ȘI CU SARCINILE DE SUPRAVEGHERE ȘI ASIGURARE A RESPECTĂRII MĂSURILOR PENTRU UN NIVEL COMUN RIDICAT DE SECURITATE CIBERNETICĂ

Cadrul general de cooperare între CNCPIC, ACS și autoritățile competente responsabile cu securitatea cibernetică și cu sarcinile de supraveghere și asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică se realizează în condițiile stabilite în anexa nr. 3 la hotărârea de Guvern nr. 1115/2025 pentru aprobarea normelor, procedurilor și măsurilor prevăzute la art. 1 alin. (3) din Legea nr. 294/2024 privind reziliența entităților critice, precum și pentru modificarea unor acte normative.
Diagrama de flux în ceea ce privește cooperarea între CNCPIC, ACS și DNSC, ca autoritate competentă responsabilă cu securitatea cibernetică și cu sarcinile de supraveghere și asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică este prezentată în schema din figura nr. 3.

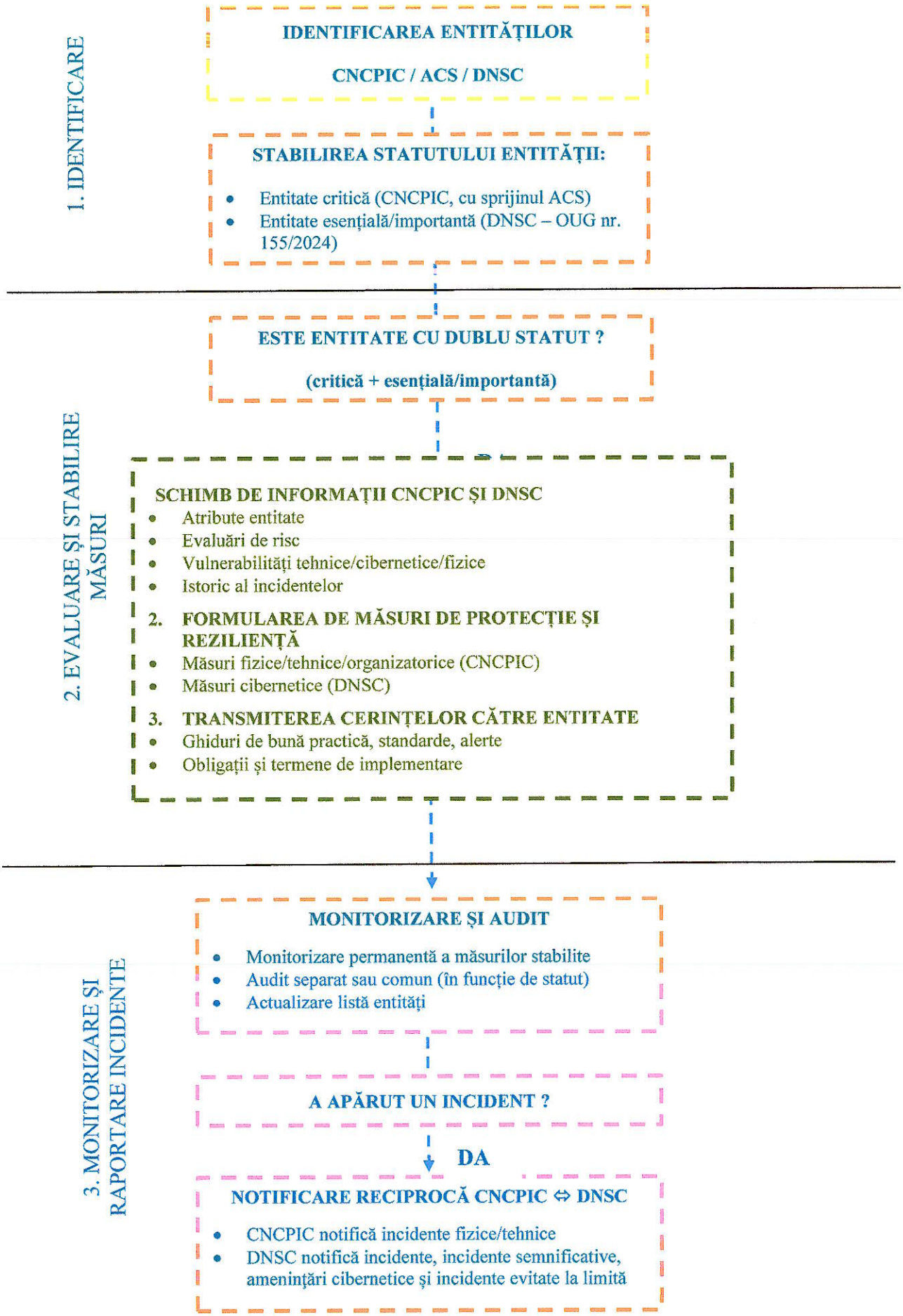

Figura nr. 3. Schema cadrului de cooperare între CNCPIC, ACS ȘI DNSC

CAPITOLUL VIII - CONSOLIDAREA COOPERĂRII ÎNTRE SECTORUL PUBLIC ŞI SECTORUL PRIVAT ÎN DOMENIUL REZILIENȚEI ENTITĂȚILOR CRITICE

Domeniul rezilienței entităților critice creează în ansamblu un cadru preventiv - proactiv, dar completat de partea reactivă, prin planurile de măsuri asociate, pentru operaționalizarea căruia implicarea sectorului privat este esențială, deoarece o mare parte dintre serviciile esențiale sunt prestate de către companii private sau mixte.

Protecția informațiilor clasificate/sensibile este un element delicat, context în care trebuie echilibrate măsurile ce se impun cu nevoia de a relaționa rapid, nebirocratic, respectiv de a nu crea în sarcina viitoarelor entități obligații disproporționate, care afectează concurența loială sau care le pot pune în imposibilitatea de a le îndeplini.

Abordarea acestui domeniu implică eforturi bidirecționale susținute pentru creșterea nivelului de încredere reciprocă, dar și conștientizarea importanței pentru securitatea națională pe care o reprezintă imaginea integrată privind reziliența sistemului prin care sunt livrate serviciile esențiale.

Cooperarea transfrontalieră este un alt factor de referință pentru creionarea unei imagini situaționale integrate la nivel european, dar și pentru adresarea holistică a unor probleme de reziliență ce transcend granițele fizice dintre state, mixul public-privat și interdependențele în creștere dintre infrastructurile critice moderne reflectând realități curente.

Grupul de lucru interinstituțional este un alt mecanism-cheie, deoarece facilitează coordonarea practică între CNCPIC, ACS și entitățile critice identificate, dar reprezintă și platforma de relaționare a acestora cu mediul privat relevant pentru domeniul de referință, respectiv cu cel academic și non-guvernamental, actori ce pot îmbogăți discuțiile din marja efortului de asigurare a rezilienței entităților critice.

CAPITOLUL IX – REZULTATE AȘTEPTATE ȘI INDICATORI

Rezultatele așteptate în urma implementării Strategiei sunt:
a) Un cadru legislativ și de reglementare modernizat, armonizat cu cerințele și standardele europene și internaționale, care să ofere premisele necesare pentru gestionarea coerentă a rezilienței entităților critice.
b) Creșterea nivelului de protecție și reziliență a entităților critice, prin reducerea vulnerabilităților, consolidarea capacităților de prevenire și răspuns și îmbunătățirea continuității operaționale.
c) Definirea și operaționalizarea clară a rolurilor, responsabilităților, competențelor și mecanismelor de răspundere, astfel încât toate instituțiile implicate să contribuie coerent și eficient la asigurarea rezilienței entităților critice.
d) Dezvoltarea unui cadru solid și funcțional de cooperare între entitățile critice interdependente, care să faciliteze coordonarea, schimbul de informații și acțiunea comună în situații de risc sau incident.
Indicatorii pe baza cărora se va măsura evoluția implementării Strategiei sunt prezentați în anexă, iar cei care pot fi corelați cu referire la indicatorii naționali de dezvoltare durabilă sunt următorii:

OS 1 – Consolidarea capacității instituționale și a guvernanței naționale pentru asigurarea rezilienței entităților critice

Indicatori:
- Gradul de acoperire a nevoilor identificate, cuantificat inclusiv prin numărul de proiecte de acte normative elaborate;
- Gradul de acoperire a nevoilor identificate, cuantificat inclusiv prin număr de ghiduri/metodologii elaborate și diseminate;
- Număr entități critice identificate;
- Număr avertizări/număr informări;
- Număr de programe dezvoltate/număr de participanți instruiți;
- Număr de activități derulate;
- Număr de exerciții desfășurate/raport de lecții învățate elaborat;
- Proceduri aprobate/număr acorduri semnate.

***Corelare cu indicatori naționali de dezvoltare durabilă*:** ODD 16 – Pace, justiție și instituții eficiente.

OS 2 – Consolidarea cooperării internaționale și asigurarea armonizării permanente cu politicile și standardele Uniunii Europene în domeniul rezilienței entităților critice

Indicatori:
- Număr de parteneri identificați;
- Număr evenimente de promovare/număr bune practici documentate;
- Număr parteneriate dezvoltate /număr proiecte comune depuse;
- Număr de întâlniri la care s-a participat/număr de bune practici identificate.

***Corelare cu indicatori naționali de dezvoltare durabilă*:** ODD 17 – Parteneriate pentru realizarea obiectivelor.

OS 3 – Întărirea capacităților de prevenire, reacție și asigurare a continuității în furnizarea serviciilor esențiale ale entităților critice în fața incidentelor majore

Indicatori:
- Număr planuri finalizate și aprobate;
- Număr exerciții desfășurate;
- Număr de ghiduri distribuite/ număr participanți la sesiuni de instruire.

***Corelare cu indicatori naționali de dezvoltare durabilă*:** ODD 9 – Industrie, inovare și infrastructură.

OS 4 – Dezvoltarea competențelor și culturii de securitate

Indicatori:
- Număr module de formare dezvoltate;
- Platformă e-learning funcțională /Număr de cursuri online disponibile;
- Număr de participanți instruiți;
- Număr de workshop-uri realizate.

***Corelare cu indicatori naționali de dezvoltare durabilă*:** ODD 4 – Educație de calitate și ODD 16 – Instituții eficiente.

OS 5 – Creșterea nivelului de reziliență a entităților critice

Indicatori:
- Număr de politici/strategii corelate;
- Număr de infrastructuri critice evaluate;
- Număr de revizuiri post-incident/ exercițiu;
- Număr de informări/ rapoarte transmise.

***Corelare cu indicatori naționali de dezvoltare durabilă*:** ODD 9 – Industrie, inovare și infrastructură și ODD 12 – Consum și producție responsabile.

CAPITOLUL X - PROCEDURI DE MONITORIZARE ȘI EVALUARE

CNCPIC și ACS în domeniul rezilienței entităților critice vor acționa pentru:
- Monitorizarea planului de acțiune aferent implementării prezentei Strategii;
- Asumarea de către fiecare ACS a obligațiilor specifice pentru implementarea Strategiei[1];
- Analiza utilizării resurselor umane, materiale și financiare disponibile pentru asigurarea implementării obiectivelor Strategiei.

[1] În marja unor reevaluări ulterioare ale mediului de securitate, care impun recalibrarea obiectivelor din Strategie și, implicit, a direcțiilor de acțiune prin care acestea sunt implementate.

Monitorizarea Strategiei va fi efectuată prin colectarea regulată şi sistematică de date şi informaţii cu privire la activităţile prevăzute în Planul de acţiune al acesteia, conform anexei la prezenta Strategie.

Mecanismul de monitorizare va consta în:

- Raportare periodică: instituțiile/entitățile reponsabile vor transmite anual către CNCPIC, până la 31 ianuarie al fiecărui an, pentru anul anterior, stadiul progresului înregistrat pentru fiecare rezultat aşteptat din sectorul de responsabilitate.
- Colectarea de date: CNCPIC, prin intermediul instrumentelor specifice, va realiza o analiză a stadiului de îndeplinire a rezultatelor aşteptate, în termen de o lună de la primirea datelor menționate la punctul de mai sus.
- Evaluarea periodică: cel puțin odată la fiecare 4 ani, CNCPIC va evalua și, eventual, actualiza cadrul strategic în baza unei analize a stadiului de îndeplinire a rezultatelor aşteptate și prin raportare la contextul internațional existent.

CAPITOLUL XI – IMPLICAȚII BUGETARE ȘI SURSE DE FINANȚARE

Identificarea și dezvoltarea resurselor financiare, inclusiv a componentelor legislative pentru punerea în aplicare a acestora, vor contribui la consolidarea rolului ACS implicate în implementarea Strategiei și creşterea capacității acestora de a menține și îmbunătăți reziliența entităților critice.

Fondurile necesare implementării activităților cuprinse în Planul de acțiune se asigură de către fiecare instituție/entitate cu responsabilități în realizarea obiectivelor, în raport cu prioritățile, resursele disponibile și etapele de realizare a acestora, cu încadrarea în bugetele anuale aprobate, precum și din alte surse legal constituite, potrivit legii.

Finanțarea implementării obiectivelor Strategiei se fundamentează pe:

a) identificarea şi dezvoltarea mecanismelor financiare, inclusiv a componentelor legislative pentru punerea în aplicare a măsurilor de reziliență;
b) alocarea prioritară/echilibrată de resurse bugetare la nivelul tuturor instituţiilor angrenate, în vederea susţinerii financiare a acţiunilor rezultate din Strategie;
c) atragerea şi valorificarea optimă a fondurilor externe nerambursabile.,

CAPITOLUL XII – IMPLICAȚII ASUPRA CADRULUI JURIDIC

Strategia nu are un impact asupra actelor normative în vigoare, aceasta fiind elaborată în temeiul prevederilor Legii nr. 294/2024, care asigură transpunerea la nivel național a Directivei (UE) 2022/2557.

PLAN DE ACȚIUNE
pentru implementarea, monitorizarea și evaluarea Strategiei naționale privind reziliența entităților critice

Obiectiv strategic: Creșterea nivelului de reziliență a macro-sistemului prin care sunt livrate servicii esențiale cetățenilor, operatorilor privați și autorităților statului, ca efect cumulativ al unui nivel suficient de reziliență a entităților critice, pentru prevenirea sau limitarea efectelor generate de perturbarea funcționalității sau distrugerea elementelor de infrastructură critică prin intermediul cărora sunt furnizate serviciile esențiale.

OS 1 – Consolidarea capacității instituționale și a guvernanței naționale pentru asigurarea rezilienței entităților critice

Direcții de acțiune	Acțiuni	Rezultate așteptate	Indicatori	Perioade de implementare	Instituții responsabile	Etapele evaluării
1.1. Evaluarea și actualizarea periodică a cadrului de reglementare la evoluțiile strategice internaționale și la cele mai avansate standarde și practici în domeniul rezilienței entităților critice	1.1.1. Elaborarea propunerilor de modificare și completare a cadrului normativ național	Proiecte de acte normative aliniate la standardele internaționale	Gradul de acoperire a nevoilor identificate, cuantificat inclusiv prin numărul de proiecte de acte normative elaborate	Permanent	GLIREC, CNCPIC, ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	1.1.2. Elaborarea de ghiduri și metodologii de implementare pentru entitățile critice	Facilitarea aplicării unitare a noilor reglementări	Gradul de acoperire a nevoilor identificate, cuantificat inclusiv prin număr de ghiduri/ metodologii elaborate și diseminate	Permanent	GLIREC, CNCPIC, ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
1.2. Implementarea unui proces strategic de evaluare continuă a entităților critice, pentru consolidarea capacității de răspuns la amenințări complexe	1.2.1. Identificarea și inventarierea entităților critice la nivel sectorial	Listă actualizată a entităților critice	Număr entități critice identificate	2026	CNCPIC, ACS, entități critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	1.2.2. Implementarea unui mecanism periodic de colectare și analiză a datelor relevante	Flux operațional funcțional pentru evaluarea riscurilor	Frecvența rapoartelor de evaluare	Permanent	CNCPIC, ACS, entități critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	1.2.3. Dezvoltarea unui mecanism specific de comunicare și avertizare timpurie pentru riscurile	Creșterea capacității de identificare anticipată a amenințărilor	- Număr avertizări; - Număr informări	Permanent	CNCPIC, ACS, entități critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate

Direcții de acțiune	Acțiuni	Rezultate așteptate	Indicatori	Perioade de implementare	Instituții responsabile	Etapele evaluării
	identificate și amenințări emergente					
1.3. Promovarea unei culturi naționale robuste de securitate, prin consolidarea programelor de formare și dezvoltare profesională la nivelul ACS și al entităților critice	1.3.1. Dezvoltarea și implementarea de programe de formare profesională pentru personalul ACS	Creșterea nivelului de competență profesională a personalului	- Număr de programe dezvoltate; - Număr de participanți instruiți	Trim. I 2027	GLIREC, CNCPIC, ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	1.3.2. Derularea unor activități de conștientizare privind cultura de securitate la nivelul entităților critice	Creșterea gradului de conștientizare și responsabilizare	- Număr de activități derulate; - Grad de participare	Anual	CNCPIC, ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	1.3.3. Organizarea de exerciții, simulări și aplicații comune (table-top și exerciții practice)	Îmbunătățirea cooperării interinstituționale și a capacității de reacție	- Număr de exerciții desfășurate; - Raport de lecții învățate elaborat	Anual	CNCPIC, ACS, entități critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
1.4. Crearea unui cadru eficient de schimb de informații și bune practici pentru toate entitățile critice, în vederea creșterii nivelului de cunoaștere situațională și a capacității de reacție	1.4.1. Elaborarea și aprobarea unui cadru procedural pentru schimbul de informații	Proceduri standardizate și acorduri pentru schimbul de informații	- Proceduri aprobate; - Număr acorduri semnate	2027	GLIREC, CNCPIC, ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	1.4.2. Organizarea de sesiuni periodice de schimb de bune practici	Creșterea nivelului de cunoaștere și aliniere interinstituțională	- Număr sesiuni organizate; - Număr participanți	Anual, începând cu 2027	CNCPIC	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
1.5. Dezvoltarea unui cadru strategic integrat pentru decizii bazate pe evaluări complexe ale riscurilor de la nivelul entităților critice, care să fie integrate în evaluarea de risc națională	1.5.1. Stabilirea mecanismelor de colectare, schimb și agregare a datelor privind riscurile de la nivelul entităților critice	Flux informațional coerent între entitățile critice, ACS și CNCPIC	Sistem operațional	2027	CNCPIC, ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	1.5.2. Implementarea unui mecanism de raportare a incidentelor de la nivelul entităților critice	Reducerea timpului de reacție la incidente	Număr incidente raportate	2027-2028	CNCPIC, ACS și entitățile critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	1.5.3. Integrarea rezultatelor evaluărilor de risc ale entităților critice în procesul de evaluare a riscurilor la nivel național	Creșterea acurateței și relevanței evaluării de risc naționale	Referințe explicite în evaluarea națională de risc	Anual	CNCPIC	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate

Direcții de acțiune	Acțiuni	Rezultate așteptate	Indicatori	Perioade de implementare	Instituții responsabile	Etapele evaluării
	1.5.4. Dezvoltarea capacității instituționale prin instruirea personalului implicat în evaluarea riscurilor	Personal instruit și capabil să aplice cadrul strategic integrat	-Număr de sesiuni de instruire; -Număr de persoane instruite	Permanent / anual	CNCPIC, ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate

OS 2 – Consolidarea cooperării internaționale și asigurarea armonizării permanente cu politicile și standardele Uniunii Europene în domeniul rezilienței entităților critice

Direcții de acțiune	Acțiuni	Rezultate așteptate	Indicatori	Perioade de implementare	Instituții responsabile	Etapele evaluării
2.1. Dezvoltarea, extinderea și consolidarea cadrului de cooperare internațională, prin intensificarea parteneriatelor (bi)multilaterale și prin participarea activă la inițiative comune în domeniul securității și rezilienței.	2.1.1. Identificarea și prioritizarea partenerilor strategici internaționali	Listă clară de parteneri relevanți pentru cooperare în domeniul securității și rezilienței	Număr de parteneri identificați	2027	GLIREC, CNCPIC, ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	2.1.2. Participarea la inițiative și exerciții comune internaționale în domeniul securității	Îmbunătățirea interoperabilității și schimbului de bune practici	Număr de inițiative/exerciții la care s-a participat	Anual	CNCPIC, ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	2.1.3. Organizarea de workshop-uri și conferințe naționale/internaționale tematice în parteneriat	Creșterea vizibilității și expertizei instituției în domeniul securității și rezilienței	- Număr de evenimente organizate; - Număr de participanți	Anual	GLIREC, CNCPIC, ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
2.2. Creșterea nivelului de implicare în fundamentarea programelor de finanțare ale Uniunii Europene, concomitent cu identificarea oportunităților disponibile și maximizarea absorbției fondurilor.	2.2.1. Analiza și identificarea oportunităților de finanțare disponibile în programele UE	Listă actualizată cu programe și apeluri de proiecte relevante	Număr programe/ apeluri identificate	Anual	CNCPIC, ACS și entități critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	2.2.2. Promovarea rezultatelor obținute din proiecte și schimbul de bune practici	Consolidarea vizibilității instituției și creșterea șanselor de succes în viitoare proiecte	- Număr evenimente de promovare; - Număr bune practici documentate	Permanent	CNCPIC, ACS și entitățile critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	2.2.3. Dezvoltarea parteneriatelor cu alte instituții/organizații pentru proiecte comune	Acces la resurse și experiență suplimentară	- Număr parteneriate dezvoltate; - Număr proiecte comune depuse	Permanent	CNCPIC, ACS și entitățile critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate

Direcții de acțiune	Acțiuni	Rezultate așteptate	Indicatori	Perioade de implementare	Instituții responsabile	Etapele evaluării
2.3. Asigurarea conformității continue cu standardele, politicile și mecanismele europene, inclusiv prin respectarea și operarea corespunzătoare a fluxurilor de raportare către Comisia Europeană și către alte organisme relevante	2.3.1. Revizuirea și actualizarea periodică a standardelor interne pentru alinierea cu legislația și reglementările europene	Standardele interne actualizate și conforme cu cerințele europene	Raport de conformitate actualizat	Permanent	CNCPIC	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	2.3.2. Elaborarea și operarea fluxurilor de raportare către Comisia Europeană	Rapoarte corecte, complete și transmise la timp	Procent rapoarte transmise la timp și fără observații	Conform termenelor prevăzute de legislație	CNCPIC	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
2.4. Participarea activă la schimburi de bune practici în cadrul GREC, în vederea îmbunătățirii proceselor naționale și alinierii la tendințele europene privind reziliența	2.4.1. Participarea la întâlnirile grupului GREC	Obținerea de bune practici și experiențe aplicabile la nivel național	- Număr de întâlniri la care s-a participat; - Număr de bune practici identificate	Anual	GLIREC, CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	2.4.2. Analiza și raportarea informațiilor colectate în cadrul GREC	Elaborarea de rapoarte de rezultat privind bunele practici și recomandări pentru îmbunătățirea proceselor naționale	- Număr de rapoarte redactate; - Număr de recomandări integrate în planurile naționale	Anual	GLIREC, CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	2.4.3. Organizarea de sesiuni interne de diseminare a bunelor practici	Creșterea gradului de cunoaștere și implementare a soluțiilor identificate	- Număr de sesiuni interne organizate; - Număr de participanți	Permanent	CNCPIC	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
2.5. Reprezentarea și implicarea României în cadrul forumurilor decizionale internaționale, care elaborează politici, reglementări și standarde cu impact asupra domeniului rezilienței entităților critice, pentru a contribui la formarea cadrului strategic și normativ global	2.5.1. Identificarea și prioritizarea forumurilor internaționale relevante (UE, ONU, NATO, OCDE, ISO, alte organisme de standardizare și cooperare)	Listă clară și actualizată a forumurilor prioritare pentru domeniul rezilienței entităților critice	- Listă aprobată de forumuri prioritare; - Număr de forumuri identificate și analizate	2027 (actualizare anuală)	CNCPIC	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	2.5.2. Participarea activă la reuniuni, grupuri de lucru și consultări internaționale	Creșterea vizibilității și influenței României în procesele decizionale	- Număr de reuniuni la care România participă	2031	CNCPIC	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	2.5.3. Elaborarea și promovarea de poziții naționale și contribuții tehnice pe teme de reziliență a entităților critice	Integrarea intereselor și bunelor practici naționale în documente strategice internaționale	- Număr de poziții naționale elaborate și utilizate	2031	CNCPIC	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate

Direcții de acțiune	Acțiuni	Rezultate așteptate	Indicatori	Perioade de implementare	Instituții responsabile	Etapele evaluării
	2.5.4. Coordonarea interinstituțională națională pentru armonizarea pozițiilor promovate la nivel internațional	Coerență și unitate a poziției României în forumurile internaționale	- Număr de reuniuni de coordonare; - Documente de poziție comune elaborate	Începând cu 2026	CNCPIC, ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate

OS 3 – Întărirea capacităților de prevenire, reacție și asigurare a continuității în furnizarea serviciilor esențiale ale entităților critice în fața incidentelor majore

Direcții de acțiune	Acțiuni	Rezultate așteptate	Indicatori	Perioade de implementare	Instituții responsabile	Etapele evaluării
3.1. Dezvoltarea și implementarea planurilor de reziliență, însoțite de testarea periodică a acestora prin exerciții interne derivate din rezultatele evaluărilor de risc, pentru asigurarea unui nivel adecvat de pregătire și adaptabilitate	3.1.1. Elaborarea planurilor de reziliență pentru entitățile critice	Planuri documentate și aprobate pentru fiecare entitate critică	Număr planuri finalizate și aprobate	2027	Entități critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	3.1.2. Organizarea exercițiilor interne pentru testarea planurilor	Testarea funcționalității planurilor și identificarea lacunelor	Număr exerciții desfășurate	Anual	Entități critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	3.1.3. Analiza rezultatelor exercițiilor și ajustarea planurilor	Planuri revizuite pe baza lecțiilor învățate	Număr modificări implementate; % recomandări aplicate	La 1 lună după fiecare exercițiu	ACS și entități critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
3.2. Elaborarea unor ghiduri privind răspunsul la incidente majore, atât fizice, cât și cibernetice, cu sprijinul DNSC, pentru diseminarea bunelor practici la nivel național	3.2.1. Analiza bunelor practici internaționale și naționale privind răspunsul la incidente majore (fizice și cibernetice)	Raport de analiză comparativă și recomandări pentru adaptarea ghidurilor	Raport elaborat și aprobat de echipa de proiect	Permanent	CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	3.2.2. Elaborarea ghidurilor și aprobarea oficială	Ghiduri aprobate pentru diseminare națională	Ghiduri aprobate oficial	Permanent	CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	3.2.3. Diseminarea ghidurilor și organizarea de sesiuni de instruire / workshop-uri	Creșterea gradului de conștientizare și capacitate de răspuns la incidente	Număr de ghiduri distribuite; Număr participanți la sesiuni de instruire	Permanent	CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate

OS 4 – Dezvoltarea competențelor și culturii de securitate

Direcții de acțiune	Acțiuni	Rezultate așteptate	Indicatori	Perioade de implementare	Instituții responsabile	Etapele evaluării
4.1. Formare profesională pentru personalul specializat de la nivelul entităților critice	4.1.1. Analiza nevoilor de formare profesională ale personalului din entitățile critice	Identificarea competențelor deficitare și a domeniilor prioritare de formare	- Raport de analiză elaborat; - Număr entități analizate	Anual	ACS și entități critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	4.1.2. Elaborarea programelor de formare profesională (curricula, suporturi de curs)	Programe de formare adaptate specificului entităților critice	- Număr programe elaborate; - Număr module de formare dezvoltate	Anual	ACS și entități critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	4.1.3. Implementarea mecanismelor de formare continuă (training periodic, e-learning)	Asigurarea actualizării permanente a competențelor	- Platformă e-learning funcțională; - Număr cursuri online disponibile	Anual	CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
4.2. Organizarea de cursuri și workshop-uri periodice pe teme de securitate pentru entități critice	4.2.1. Identificarea nevoilor de formare în domeniul securității pentru entitățile critice	Nevoi de instruire clar definite și prioritizate	- Număr de entități analizate; - Raport de evaluare realizat	2026	GLIREC, CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	4.2.2. Organizarea cursurilor de formare de bază pentru personalul entităților critice	Creșterea nivelului de competență și conștientizare în domeniul securității	- Număr de cursuri organizate; - Număr de participanți instruiți	Permanent, începând cu Trim. II 2026	CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	4.2.3. Organizarea workshop-urilor tematice și aplicațiilor practice (studii de caz, simulări de incidente)	Dezvoltarea capacității de reacție și gestionare a incidentelor	- Număr de workshop-uri realizate; - Feedback pozitiv (>80%)	Permanent	CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate

OS 5 – Creșterea nivelului de reziliență a entităților critice

Direcții de acțiune	Acțiuni	Rezultate așteptate	Indicatori	Perioade de implementare	Instituții responsabile	Etapele evaluării
5.1. Adaptarea priorităților strategice în vederea asigurării unui nivel ridicat de reziliență a entităților critice	5.1.1. Elaborarea unui plan de măsuri pentru creșterea rezilienței entităților critice	Cadru operațional clar pentru implementarea priorităților	Plan de măsuri aprobat	2026	CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	5.1.2. Corelarea priorităților strategice cu politicile și strategiile naționale și europene relevante	Aliniere strategică consolidată	Număr de politici/strategii corelate	Permanent	CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
5.2. Identificarea celor mai bune soluții pentru creșterea capacităților	5.2.1. Analiza stării actuale a infrastructurilor critice și a	Raport de evaluare a vulnerabilităților și	- Raport elaborat și aprobat;	2027	CNCPIC, ACS și entități critice	Anual, pe baza situației stadiului cu privire la

Direcții de acțiune	Acțiuni	Rezultate așteptate	Indicatori	Perioade de implementare	Instituții responsabile	Etapele evaluării
de adaptare și de restaurare a funcționalității infrastructurilor critice prin intermediul cărora entitățile critice furnizează servicii esențiale	nivelului de reziliență operațională	capacităților de adaptare și restaurare	- Număr de infrastructuri critice evaluate			gradul de îndeplinire a rezultatelor așteptate
	5.2.2. Analiza bunelor practici și a soluțiilor aplicabile la nivel național și european	Document de sinteză privind soluțiile optime de adaptare și restaurare	- Studiu comparativ realizat; - Număr de bune practici identificate	2026	CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
5.3. Încheierea de acorduri și parteneriate public-private, respectiv civil-militare.	5.3.1. Identificarea și cartografierea potențialilor parteneri din sectorul privat	Listă actualizată de parteneri relevanți	Număr parteneri identificați	Permanent	CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	5.3.2. Organizarea de consultări și grupuri de lucru cu actorii publici și privați	Aliniere așteptări și consolidarea încrederii între părți	- Număr întâlniri organizate; - Număr participanți	2027	CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
5.4. Evaluarea permanentă a rezilienței elementelor de infrastructură critică	5.4.1. Colectarea periodică de date privind starea infrastructurilor critice	Bază de date actualizată cu informații relevante	Grad de completare a datelor (%); nr. de rapoarte colectate	Semestrial	CNCPIC și ACS	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	5.4.2. Elaborarea rapoartelor de evaluare și a recomandărilor	Rapoarte de evaluare și planuri de măsuri propuse	- Număr de rapoarte finalizate; - Număr de recomandări formulate	Permanent	CNCPIC, ACS și entitățile critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	5.4.3. Revizuirea periodică a nivelului de reziliență în urma incidentelor sau exercițiilor	Ajustarea evaluărilor și îmbunătățirea continuă a procesului	Număr de revizuiri post-incident/ exercițiu	După fiecare incident/ exercițiu	ACS și entitățile critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate
	5.4.4. Raportarea către factorii decizionali	Fundamentarea deciziilor strategice	Număr de informări/ rapoarte transmise	Anual	CNCPIC, ACS și entitățile critice	Anual, pe baza situației stadiului cu privire la gradul de îndeplinire a rezultatelor așteptate

Notă:

Fondurile necesare implementării activităților cuprinse în prezentul Plan de acțiune se asigură de către fiecare instituție/entitate cu responsabilități în realizarea obiectivelor, în raport cu prioritățile, resursele disponibile și etapele de realizare a acestora, cu încadrarea în bugetele anuale aprobate, precum și din alte surse legal constituite, potrivit legii.