MINISTERUL DEZVOLTĂRII
ECONOMICE ȘI DIGITALIZĂRII

Agenția pentru Securitate Cibernetică

MINISTRY OF ECONOMIC
DEVELOPMENT AND DIGITALIZATION

Agency for Cyber Security

MD-2012, mun. Chișinău, str. A. Pușkin nr. 26, tel. (+373 69) 111115, e-mail: secretariat@asc.gov.md

ORDIN

Nr. 03 „5" februarie 2026

Cu privire la aprobarea Raportului privind realizarea Planului de acțiuni al Agenției pentru Securitate Cibernetică pentru anul 2025

În scopul asigurării transparenței activității Agenției pentru Securitate Cibernetică și în temeiul pct. 11 subpct. 12) Regulamentul cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică, aprobat prin Hotărârea Guvernului nr. 1028/2023

ORDON:

1. Se aprobă Raportul privind realizarea Planului de acțiuni al Agenției pentru Securitate Cibernetică pentru anul 2025 (în continuare – Raport de activitate), conform anexei.

2. Secția metodologie, standarde, cercetare și dezvoltare va asigura:

2.1. expedierea Raportului de activitate aprobat către Cancelaria de Stat și Ministerul Dezvoltării Economice și Digitalizării;

2.2. plasarea Raportului aprobat pe pagina web oficială a Agenției pentru Securitate Cibernetică.

3. Controlul asupra executării prezentului ordin se pune în sarcina Directorului adjunct.

Director **Mihai LUPAȘCU**

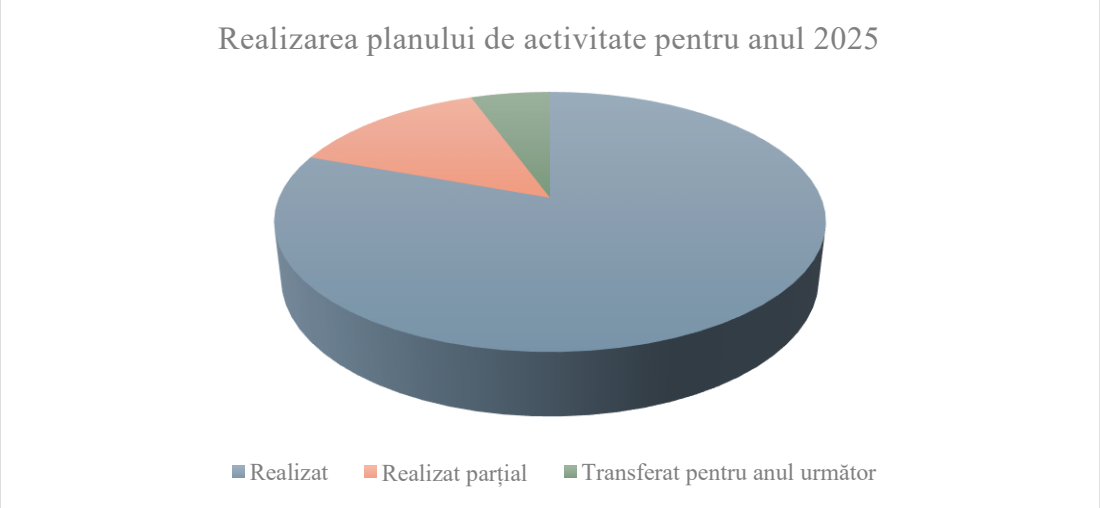
Anexă
la Ordinul nr. 03 din.05.02.2026

APROBAT
Director al Agenției pentru Securitate Cibernetică
Mihai Lupașcu

Raport privind realizarea Planului de acțiuni al Agenției pentru Securitate Cibernetică pentru anul 2025

Chișinău 2026

Planul de activitate al Agenției pentru Securitate Cibernetică a fost implementat, în mare parte, conform obiectivelor stabilite, cu progrese semnificative în consolidarea capacităților naționale de prevenire, monitorizare și răspuns la incidente cibernetice. În pofida faptului că Agenția se află într-o etapă relativ recentă de constituire, majoritatea acțiunilor planificate au fost realizate integral, iar unele parțial, fiind create premisele necesare pentru funcționarea durabilă a mecanismelor instituționale în domeniul securității cibernetice.



Pentru fortificarea Agenției, a fost pus accent pe operaționalizarea CSIRT-ului național, dezvoltarea infrastructurii IT, implementarea soluțiilor de monitorizare, detecție și răspuns la incidente (inclusiv SIEM, MISP, ticketing și protecție DDoS), precum și pe gestionarea incidentelor și vulnerabilităților la nivel național. Procesele de monitorizare continuă, notificare și asistență acordată furnizorilor de servicii au fost asigurate constant, iar la nivel normativ a fost aprobat Conceptul tehnic al registrului de stat al incidentelor cibernetice precum și a Regulamentului cu privire la modul de ținere a acestuia. Prin aceste acte normative a fost creat cadrul normativ privind dezvoltarea propriu-zisă a unui registru național.

În paralel, Agenția a realizat progrese importante în identificarea, evidența și interacțiunea cu furnizorii de servicii esențiali și importanți, în conformitate cu Legea nr. 48/2023. Au fost transmise notificări, și emise acte administrative individuale de desemnare în calitate de furnizor de servicii, contribuind la stabilirea listei furnizorilor de servicii și la responsabilizarea acestora prin obligativitatea normativă de a respecta prevederile Legii 48/2023 și a actelor de punere în aplicare a acesteia. Totodată, a fost elaborat și aprobat cadrul normativ pentru supravegherea și controlul de stat în domeniul securității cibernetice.

Cooperarea națională și internațională a reprezentat un pilon important al activității Agenției, concretizată prin parteneriate cu instituții europene și internaționale relevante, participarea la exerciții comune, activarea mecanismului Cyber Reserve și organizarea de evenimente de tip CTF și TTX. Aceste acțiuni au contribuit la consolidarea schimbului de informații, a interoperabilității și a capacității de reacție la amenințări cibernetice complexe.

În ceea ce privește resursele umane și partea financiară a Agenției, au fost depuse eforturi semnificative pentru recrutarea, instruirea și menținerea personalului, precum și pentru asigurarea disciplinei bugetar-fiscale și a raportării financiare.

Marea majoritatea acțiunilor au fost realizate integral, unele acțiuni au fost realizate parțial sau transferate pentru perioada următoare, în principal din cauza constrângerilor de resurse și a proceselor normative în derulare, acestea urmând a fi continuate în anul următor pentru atingerea deplină a obiectivelor stabilite.

OBIECTIVELE ASC

I

Obiectivul general I: Consolidarea echipei de răspuns la incidente cibernetice la nivel național;

Indicatori asociați obiectivelor:

1. PNA, Capitolul 31, pct. 8
2. PNA, Capitolul 10, pct. 1-5

Riscuri asociate realizării obiectivelor:

Riscuri interne

1. Crearea recentă a Agenției.

3. Resurse proprii limitate pentru achiziția echipamentelor hardware și software.

2. Recrutarea personalului necesar în contextul recentei organizării a Agenției.

Riscuri externe

1. Lipsa unei cooperări active a actorilor din sectorul securității cibernetice.
2. Lipsa resurselor umane suficiente.
3. Lipsa specialiștilor IT calificați pentru proiectare și implementare
4. Posibile întârzieri în livrarea echipamentelor și integrarea acestora
5. Probleme de compatibilitate între soluțiile existente și noile tehnologii

Nr.	Acțiuni	Indicator de monitorizare	Termen de inițiere	Termen de realizare	Subdiviziune responsabilă	Responsabil	Comentarii
1	Coordonarea procesului de asigurare a securității cibernetice, de prevenire și de soluționare a incidentelor cibernetice	Realizarea analizei strategice privind incidentele de securitate cibernetică și coordonarea acțiunilor de răspuns la astfel de incidente, inclusiv prin organizarea unor cursuri specializate de către experți calificați. Interacțiunea strategică cu entități relevante. Desfășurarea unor exerciții și antrenamente comune de consolidare a capacităților de reacție la atacuri cibernetice, inclusiv de blocare a atacurilor cibernetice simulate	ianuarie 2025	decembrie 2025 iunie 2025	CSIRT SPA SCSI	Radu Vieru Andrițchi Nicoleta Boțan Valentina	**Realizat** Procesul de asigurare a securității cibernetice a fost asigurat prin angajarea personalului tehnic în cursuri de formare și vizite de studiu la instituții ce au livrat informații și experiențe proprii.
	1.1. Operaționalizarea centrului de date local 1.1.1 Dezvoltarea arhitecturii IT pentru infrastructura hibridă Definirea cerințelor tehnice Proiectarea rețelelor și componentelor critice 1.1.2 Identificarea și achiziționarea componentelor esențiale Elaborarea specificațiilor tehnice	1.1 Document de arhitectură IT finalizat Specificații tehnice finalizate și aprobate Achiziționarea echipamentelor conform specificațiilor Instalarea și testarea componentelor realizată cu succes	ianuarie 2025	decembrie 2025	CSIRT	Radu Vieru	**Realizat** Activitățile aferente dezvoltării arhitecturii IT pentru infrastructura hibridă au fost realizate conform planificării inițiale. Au fost definite cerințele tehnice, având în vedere nevoile de scalabilitate, disponibilitate și integrare cu mediile existente, iar pe baza acestora a fost proiectată arhitectura de rețea și au fost identificate componentele critice ale infrastructurii.

	Stabilirea cerințelor de securitate și performanță Lista componentelor: servere, soluții de networking, stocare scalabilă, rack & power management, securitate fizică						În etapa de identificare și achiziționare a componentelor esențiale, au fost elaborate specificațiile tehnice detaliate pentru fiecare categorie de echipamente, incluzând cerințele de securitate și performanță. Lista componentelor necesare a fost stabilită și validată, acoperind servere, soluții de networking, sisteme de stocare scalabilă, echipamente de rack și power management, precum și elemente de securitate fizică.
	1.2 Implementarea și configurarea echipamentelor hardware 1.2.1 Instalarea și configurarea rețelelor și securității IT Configurare switching, firewalling, VPN Implementarea soluțiilor de securitate 1.2.2 Instalarea si configurarea	1.2 Infrastructura de rețea configurată și testată cu succes Politicile de securitate aplicate și validate VPN funcțional și testat pentru acces securizat Firewall implementat și configurat conform cerințelor de securitate ESXi instalat și optimizat pentru performanță ridicată vCenter configurat și funcțional pentru administrare centralizată	ianuarie 2025	iunie 2025	CSIRT	Radu Vieru	**Realizat** Activitățile de implementare și configurare a echipamentelor hardware au fost realizate conform arhitecturii aprobate și cerințelor tehnice definite anterior, asigurând funcționarea corectă și securizată a infrastructurii IT. Instalarea și configurarea rețelelor și securității IT Au fost instalate și configurate echipamentele

	platformei de virtualizare Instalarea serverelor ESXi Instalarea serverului de administrare vCenter						de rețea, incluzând componentele de switching, cu definirea VLAN-urilor și a politicilor de trafic necesare pentru separarea și optimizarea fluxurilor de date. Configurarea soluțiilor de firewalling a fost realizată pentru a controla accesul la resursele interne și externe, iar conexiunile VPN au fost implementate pentru a permite acces securizat la infrastructură. Totodată, au fost implementate soluțiile de securitate IT, asigurând protecția infrastructurii împotriva accesului neautorizat și a amenințărilor cibernetice, în conformitate cu cerințele de securitate stabilite.
	1.3 Implementarea sistemelor de autentificare și identitate 1.3.1 Configurarea Active Directory și politicilor de Securitate	1.3 Active Directory configurat și operațional Politici de grup aplicate și testate conform cerințelor de securitate Validarea accesului securizat pentru utilizatori PKI implementat și testat Certificare digitală operațională pentru autentificare securizată	ianuarie 2025	decembrie 2025	CSIRT	Radu Vieru	**Realizat** Activitățile de implementare a sistemelor de autentificare și identitate au fost realizate conform cerințelor de securitate stabilite. A fost configurată infrastructura Active Directory și au fost

	1.3.2 implementarea infrastructurii PKI 1.3.3 Integrarea cu Microsoft 365 și Azure AD Configurare Single Sign-On (SSO) Activare MFA						aplicate politicile de securitate necesare. A fost implementată infrastructura PKI pentru gestionarea certificatelor digitale și securizarea comunicațiilor. De asemenea, a fost realizată integrarea cu Microsoft 365 și Azure AD, incluzând configurarea Single Sign-On (SSO) și activarea autentificării multifactor (MFA), asigurând un control unitar și securizat al accesului.
	1.4 Integrarea soluțiilor IT Microsoft 365 1.4.1 Configurarea Microsoft 365 pentru utilizatori Gestionare identități și politici de acces 1.4.2 Integrarea serviciilor OneDrive, SharePoint, Teams Politici de partajare și protecție DLP 1.4.3 Migrarea e-mailului la Exchange Online	1.4 Conturile utilizatorilor configurate și gestionate conform politicilor de acces Serviciile OneDrive, SharePoint și Teams integrate și funcționale Conturile de e-mail migrate cu succes la Exchange Online Tenant Azure integrat cu M365, arhitectura configurata si sisteme instalatea in Azure	ianuarie 2025	iunie 2025	CSIRT	Radu Vieru	**Realizat** Activitățile de integrare a soluțiilor Microsoft 365 au fost realizate. A fost configurat mediul Microsoft 365 pentru utilizatori, incluzând gestionarea identităților și aplicarea politicilor de acces. Au fost integrate serviciile OneDrive, SharePoint și Teams, cu definirea politicilor de partajare și protecție a datelor (DLP). Migrarea serviciului de e-mail către Exchange Online

	Configurare protecție anti-spam și criptare Interconectarea infrastructurii locale cu Azure pentru continuitatea serviciilor						a fost realizată cu succes, fiind configurate mecanismele de protecție anti-spam și criptare. Totodată, a fost realizată interconectarea infrastructurii locale cu Azure, asigurând continuitatea și disponibilitatea serviciilor IT.
2	Monitorizarea, analiza și, dacă e cazul, informarea despre amenințările cibernetice, vulnerabilitățile și incidentele cibernetice la nivel național	Monitorizarea și plasarea vulnerabilităților la nivel național pe pagina oficială a agenției	ianuarie 2025	Continuu	CSIRT SPA SCMM	Radu Vieru Mereneanu Mihaela	**Realizat** În scopul realizării Obiectivului nr2, echipa CSIRT monitorizează activ spațiul cibernetic național, notificând instituțiile vizate. Procesul continuu de monitorizare este realizat printr-un proces de scanare a vulnerabilităților. În cazul identificării unor vulnerabilități cibernetice cu potențial impact asupra publicului sau instituțiilor, s-a acționat prompt și transparent, prin transmiterea de mesaje și recomandări clare, accesibile, care indică măsurile de protecție și prevenire necesare.

3	Acordarea asistenței furnizorilor de servicii, la solicitarea acestora, în procesul de monitorizare și protecție de către aceștia a rețelelor și sistemelor informatice pe care le dețin	Acordarea asistenței solicitate de către furnizorii de servicii la fiecare solicitare	ianuarie 2025	Conform termenului indicat în solicitare, dar nu mai mult de 30 de zile	CSIRT	Radu Vieru	**Realizat** În scopul realizării Obiectivului nr3, echipa CSIRT a oferit asistență tuturor instituțiilor care au solicitat acest lucru. În plus au fost furnizate soluții de securitate anti DDoS.
4	Recepționarea notificărilor privind incidentele cibernetice	Înregistrarea notificărilor în Registrul notificărilor	ianuarie 2025	Continuu	CSIRT	Radu Vieru	**Realizat** Echipa CSIRT a înregistrat toate incidentele cibernetice în Registrul notificărilor, având până la 31.12.2025 - 40 incidente de securitate cibernetică.
5	Asigurarea răspunsului la incidentele cibernetice și acordarea asistenți furnizorilor de servicii	Răspuns la fiecare incident cibernetic Acordarea de asistență la fiecare solicitare Realizarea analizei strategice privind incidentele de securitate cibernetică și coordonarea acțiunilor de răspuns la astfel de incidente, inclusiv prin organizarea unor cursuri specializate de către experți calificați	ianuarie 2025	Conform termenului stabilit prin orientările metodologice	CSIRT	Radu Vieru	**Realizat** Echipa CSIRT răspuns prompt și remediat toate incidentele cibernetice raportate către ASC. Totodată a oferit suport tuturor instituțiilor ce au solicitat acest lucru. Suportul a fost oferit în urma incidentelor de securitate cibernetică, sau la identificarea unei vulnerabilități critice în infrastructura instituției vizate.

	5.1 Dezvoltarea arhitecturii și capacităților CSIRT 5.1.1 Implementarea sistemului de ticketing	Raport de testare și analiză comparativă finalizat, selectarea soluției optime Sistemul de ticketing implementat și funcțional, Fluxuri operaționale stabilite și validate, Rapoarte automate de incident generate cu succes Descrierea rolurilor si responsabilităților pentru membrii echipei CSIRT	ianuarie 2025	iunie 2025	CSIRT SPA	Radu Vieru	**Realizat** A fost implementat sistemul de ticketing, permițând documentarea și stocarea vulnerabilităților identificate și incidentelor de securitate cibernetică raportate.
	5.2 Implementarea soluțiilor de detecție și răspuns 5.2.1 Identificarea și implementarea unei soluții SIEM 5.2.2 Configurarea regulilor de corelare și monitorizare a log-urilor 5.2.3 Crearea sistemului de gestionare a Indicatorilor de Compromitere (IoC) Integrarea platformelor de monitorizare și răspuns	Soluția SIEM instalată și funcțională, Evenimentele de securitate centralizate și monitorizate Rapoarte de alertare generate în timp real Sistemul de gestionare IoC implementat și testat	ianuarie 2025	iunie 2025	CSIRT SPA	Radu Vieru	**Realizat** Soluția SIEM a fost instalată și este în proces de configurare. Urmează a fi implementat sistemul de gestionare IoC.
	5.3 Integrarea cu platforme de Threat Intelligence	MISP implementat și operațional Număr de parteneri conectați la platformă: minim 2	ianuarie 2025	iunie 2025	CSIRT SPA	Radu Vieru	**Realizat** Platforma de schimb de informații (MISP) este

	5.3.1Implementarea și configurarea MISP Conectarea la surse externe și parteneri						operațională, având loc schimbul de date tehnice, fluxurile de incidente partajate și indicatori de compromitere (IoC).
	5.3.2 Implementarea unei soluții de comunicare securizată 5.3.1 Implementarea platformei comunicare si schimb de informații cu alte echipe de răspuns la incidente	Mattermost implementat și operaționalizat Instituții conectate: minim 2	ianuarie 2025	decembrie 2025	CSIRT SPA	Radu Vieru	**Transferat pentru anul viitor** Instituirea și implementarea platformei pentru comunicare și schimb de informații este planificată pentru anul 2026.
6	Cooperarea, la nivel național și internațional, cu echipele de răspuns la incidente cibernetice, inclusiv în cadrul unei platforme de management al incidentelor cibernetice și pentru schimbul de informații	Înregistrarea echipei de răspuns la incidente cibernetice pe platformele de schimb de informații (MISP) Asigurarea funcționalității platformei de management al incidentelor cibernetice și schimb de informații	ianuarie 2025	decembrie 2025	SCSI CSIRT SPA	Boțan Valentina Radu Vieru Andrițchi Nicoleta	**Realizat** Platforma de schimb de informații (MISP) este operațională, având loc schimbul de date tehnice, fluxurile de incidente partajate și indicatori de compromitere (IoC).
7	Gestionarea crizelor în domeniul securității cibernetice la nivel național în conformitate cu planul de răspuns la incidente și crize cibernetice la nivel național	Întocmirea planului de răspuns la incidentele cibernetice Organizarea împreună cu partenerii străini, a cursurilor de instruire tematică în domeniul securității cibernetice pentru angajații instituțiilor publice	ianuarie 2025	iunie 2025	CSIRT SPA	Radu Vieru	**Realizat parțial** În scopul întocmirii planului operațional de răspuns la incidente au fost organizate cursuri tematice pentru angajații echipei CSIRT, dar și a angajaților instituțiilor publice.

8	8.1 Stabilirea cadrului operațional 8.1.1 Selecția soluțiilor tehnologice 8.1.2 Implementarea procedurilor de prevenire a incidentelor	Document de definire a serviciilor cheie finalizat și aprobat Soluțiile tehnologice selectate și implementate	ianuarie 2025	iunie 2025	CSIRT SPA	Radu Vieru	**Realizat parțial** Documentația a fost aprobată parțial. Soluțiile tehnologice au fost selectate și implementate în proporție de 50%.
	8.2 Formalizarea Serviciilor si activităților CSIRT 8.2.1 Monitorizare și Detectare Integrare cu SIEM, analiză log-uri, detectare anomalii 8.2.2 Răspuns la Incidente Investigație, documentare, atenuare, raportare 8.2.3 Threat Intelligence Analiza IoC, distribuire, partajare alerte 8.2.4 Managementul Vulnerabilităților Scanare activă și pasivă, testare de penetrare	Definirea și descrierea generală fiecărui serviciu Definirea procedurilor operaționale și soluțiilor tehnologice aferente	ianuarie 2025	iunie 2025	CSIRT SPA	Radu Vieru	**Realizat** S-au realizat următoarele activități: Răspuns la incidente precum și investigarea, documentarea, atenuarea și raportarea; Threat Intelligence și analiza IoC, distribuirea și partajarea alertelor; Managementul Vulnerabilităților Scanare activă și pasivă, testarea de penetrare; Implementarea soluției de protecție împotriva atacurilor DDoS

	8.2.5 Protecție împotriva atacurilor DDoS Implementarea soluțiilor de protecție împotriva atacurilor distribuite de tip Denial-of-Service Integrarea soluțiilor de filtrare a traficului pentru prevenirea supraîncărcării infrastructurii Monitorizarea și răspunsul automatizat la atacurile volumetrice și aplicaționale						
	8.3 Elaborarea procedurilor 8.3.1 Detectare, investigare, izolare a incidentelor 8.3.2 Răspuns structurat pentru fiecare tip de incident: ransomware, phishing, DDoS, malware Procedura de detectare și investigare	Elaborarea ghidurilor specifice pentru fiecare categorie de incident	ianuarie 2025	iunie 2025	CSIRT SPA	Radu Vieru	**Realizat parțial** Au fost clasificate tipurile de incidente și au fost realizate playbookuri pentru anumite tipuri de incidente în proporție de 70%.

9	Înregistrarea incidentelor cibernetice care au fost notificate în Registrul de stat al incidentelor cibernetice	Crearea Registrului de stat al incidentelor cibernetice;	ianuarie 2025	decembrie 2025	SCSI CSIRT SPA 08 09	Radu Vieru Radu Scripnic	**Realizat parțial** A fost aprobată Hotărârea Guvernului nr. 822/2025 privind aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor cibernetice” și a Regulamentului cu privire la modul de ţinere a Registrului de stat al incidentelor cibernetice. Caietul de sarcini în vederea implementării registrului este în proces de elaborare.
10	Monitorizarea numelui de domenii din spațiul de adrese în Internet al Republicii Moldova și pe cele legate de domeniul de nivel superior. md, analiza riscurilor, precum și impactul potențial al acestora asupra statului, societății și securității rețelelor și sistemelor informatice	Asigurarea funcției continue al adreselor menționate în acțiune și finalizarea analizei la zi a riscurilor legate de acestea	ianuarie 2025	decembrie 2025	SPA 03	Radu Vieru	**Realizat** Numele de domenii din spațiul de adrese în Internet al Republicii Moldova au fost scanate și monitorizate continuu, asigurând funcționarea stabilă și sigură a acestora. Activitățile desfășurate au vizat identificarea domeniilor și evaluarea nivelului de risc asociat fiecăruia.
11	Asigurarea protecției informațiilor atribuite la secretul de stat, a	Desemnarea persoanei responsabile din cadrul instituției	ianuarie 2025	decembrie 2025	CSIRT SJRU		**Realizat parțial.** Procesele interne sunt în desfășurare; având în vedere

	datelor cu caracter personal în conformitate cu prevederile actelor normative din domeniile respective, precum și a secretului comercial și a intereselor de afaceri ale furnizorului de servicii în procesul de exercitare a competenței sale legale	și organizarea instruirii personalului					numărul redus de candidați pentru funcția respectivă, acestea sunt organizate și adaptate în mod corespunzător.
12	Informarea Serviciul de Informații și Securitate cu privire la incidentele cibernetice cu impact semnificativ, prevenite, în curs de realizare sau soluționate, care au vizat obiectivele infrastructurii critice	Determinarea cazurilor cu impact semnificativ conform metodologiei Informarea Serviciului de Informații și Securitate în toate cazurile care au un impact semnificativ care au vizat obiectivele infrastructurii critice	ianuarie 2025	Conform orientării metodologice	SCSI CSIRT SPA SJRU		**Realizat** Serviciul de Informații și Securitate a fost informat despre incidentele cu impact semnificativ asupra infrastructurii critice, prin expedierea rapoartelor.
13	Emiterea avertizărilor timpurii, alertelor, anunțurilor și diseminarea informațiilor privind amenințările cibernetice,	Plasarea conținutului pe pagina oficială a agenției Organizarea unor campanii de sensibilizare și informare privind pericolele din spațiul cibernetic și măsurile de protecție ce pot fi luate de către persoanele fizice și juridice;	ianuarie 2025	Continuu	SPA SCSI SMSCD	Valentina Boțan Mihaela Mereneanu	**Realizat** Au fost emise 52 de alerte timpurii. Toate informațiile relevante au fost plasate pe pagina oficială a Agenției, asigurând astfel accesul rapid și transparent al

	vulnerabilitățile și incidentele cibernetice						publicului la date actualizate despre riscurile cibernetice. În paralel, pentru a ajunge la un public cât mai larg și diversificat, au fost publicate postări de tip awareness pe paginile de socializare ale Agenției, menite să informeze, să previnăși să ofere recomandări practice privind protecția în mediul digital. Mesajele au fost concepute pentru a fi ușor de înțeles și aplicat, astfel încât fiecare utilizator să poată adopta comportamente sigure în mediul online.
14	Colectarea și analiza datelor criminalistice, furnizarea analizelor dinamice privind riscurile, incidentele cibernetice și conștientizarea situației în materie de securitate cibernetică	Instruirea personalului Colectarea și analiza datelor pentru fiecare incident cibernetic	ianuarie 2025	decembrie 2025	CSIRT SPA	Radu Vieru	**Realizat parțial** S-a efectuat angajarea personalului echipei tehnice în cursuri și sesiuni de formare în scopul dobândirii abilităților de colectare și analiză a datelor pentru contracaraea unui incident ciberntic. Acțiunea a fost realizată în proporție de 50%.
15	Scanarea proactivă a rețelelor și a sistemelor informatice ale solicitantului	Efectuarea acțiunilor menționate la fiecare cerere a unui furnizor de servicii	ianuarie 2025	Continuu	CSIRT SPA	Radu Vieru	**Realizat** Echipa CSIRT a răspuns pozitiv la solicitările și cererile unor furnizori de

	pentru a detecta vulnerabilitățile cu un impact potențial semnificativ, în conformitate cu legislația						scanare proactive a rețelelor și a sistemelor informatice. Astfel au fost realizate scanări proactive la fiecare cerere a unui furnizor de servicii.
16	Implementarea, în procesul schimbului de informații cu furnizorii de servicii și cu alte persoane relevante, a instrumentelor și soluțiilor tehnice securizate și asigurarea, în conformitate cu prevederile legislației, a protecției informațiilor de care ia cunoștință în exercitarea atribuțiilor	Implementarea soluției tehnice securizate pentru realizarea schimbului de informații	ianuarie 2025	decembrie 2025	SCSI CSIRT SPA	Radu Vieru Boțan Valentina Andrițchi Nicoleta Lapteanu Gheorghe	**Realizat** Soluția de criptare pentru schimbul de informații a fost implementată.
17	Exercitarea atribuțiilor de coordonator al procesului de divulgare coordonată a vulnerabilităților	Elaborarea metodologiei privind procesul de divulgare coordonată a vulnerabilităților Identificarea persoanelor fizice sau juridice implicate Negocierea calendarului de divulgare	ianuarie 2025	decembrie 2025	CSIRT SMSCD SJRU	Radu Vieru Scripnic Radu Arseni Ștefan	**Realizat** Cadrul normativ privind procesul de divulgare coordonată a vulnerabilităților a fost aprobat prin Hotărârea Guvernului nr. 824/2025pentru aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în

							domeniul securității cibernetice

II

Obiectivul general II: Supravegherea și controlul de stat al respectării de către furnizorii de servicii a cadrului normativ în domeniul securității cibernetice;

Indicatori asociați obiectivelor:

1. PNA, Capitolul 31, pct. 8
2. PNA, Capitolul 10, pct. 1-5

Riscuri asociate realizării obiectivelor:

Riscuri interne

1. Crearea recentă a Agenției.

2. Recrutarea personalului necesar în contextul recentei organizării a Agenției.

Riscuri externe

1. Lipsa unei cooperări active a actorilor din sectorul securității cibernetice.

2. Lipsa resurselor umane suficiente.

Nr.	Acțiuni	Indicator de monitorizare	Termen de inițiere	Termen de realizare	Subdiviziune responsabilă	Responsabil	Comentarii
1	Emiterea de acte cu caracter obligatoriu, recomandări și îndrumări metodologice pentru furnizorii de servicii, în vederea conformării acestora cu prevederile legislației și a remedierii deficiențelor constatate, și stabilirea termenului în care aceștia trebuie să se conformeze	Emiterea cel puțin a unei recomandări	ianuarie 2025	decembrie 2025	DSC	Scripnic Radu	**Transferat pentru anul viitor** A fost aprobată Hotărârea de Guvern nr. 825/2025 pentru aprobarea Regulamentului cu privire la supravegherea și controlul de stat asupra respectării cadrului normative în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice.
2	Examinarea sesizărilor cu privire la neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor de către furnizorii de servicii	Examinarea tuturor sesizărilor	De la momentul depunerii sesizării	maxim 30 de zile de la depunerea sesizării	DSC		**Transferat pentru anul viitor** A fost aprobată Hotărârea de Guvern nr. 825/2025 pentru aprobarea Regulamentului cu privire la supravegherea și controlul de stat asupra respectării cadrului normative în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice.
3	Restricționarea utilizării ori accesul la o rețea sau un sistem informatic când sunt îndeplinite condițiile	Întocmirea metodologiei pentru acțiunea menționată Restricționarea accesului în toate cazurile prevăzute de lege	ianuarie 2025	continuu	DSC		**Transferat pentru anul viitor** A fost aprobată Hotărârea de Guvern nr. 825/2025 pentru aprobarea Regulamentului cu privire la supravegherea și

	stabilite de legislația în domeniul securității cibernetice						controlul de stat asupra respectării cadrului normative în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice.
4	Notificarea utilizatorilor serviciilor și autorităților publice care realizează politica de stat în domeniul respectiv și, în cazul în care există, autoritatea cu funcții regulatorii pe piața din domeniul în care se prestează serviciul respectiv, despre restricționarea utilizării sau a accesului la o rețea sau sistem informatic	Notificarea în toate cazurile	ianuarie 2025	Continuu	DSC		**Realizat parțial.** Au fost operate notificări, însă din lipsa personalului și a cadrului normativ complet, această funcție a fost parțial realizată.

III

Obiectivul general III: Cooperarea la nivel național și internațional și schimbul de informații în materie de securitate cibernetică

Indicatori asociați obiectivelor:

1. PNA, Capitolul 31, pct. 8
2. PNA, Capitolul 10, pct. 1-5

Riscuri asociate realizării obiectivelor:

Riscuri interne

1. Crearea recentă a Agenției.
2. Recrutarea personalului necesar în contextul recentei organizării a Agenției.
3. Lipsa resurselor financiare suficiente.

Riscuri externe

1. Lipsa unei cooperări active a actorilor din sectorul securității cibernetice.
2. Lipsa resurselor umane suficiente.
3. Practica europeană recentă cu adoptarea Directivei NIS 2, instituții omolog nou create în baza directivei menționate

Nr.	Acțiuni	Indicator de monitorizare	Termen de inițiere	Termen de realizare	Subdiviziune responsabilă	Responsabil	Comentarii
1	Asigurarea interacțiunii strategice la nivel internațional și schimbul de experiență cu alte state, organizații internaționale sau entități create de acestea privind aspectele legate de securitatea cibernetică	Interacțiunea strategică cu următoarele autorități: CCB- Belgia, ENISA- EU,DNSC, ECSO Desfășurarea unor exerciții și antrenamente comune de consolidare a capacităților de reacție la atacuri cibernetice, inclusiv de blocare a atacurilor cibernetice simulate	ianuarie 2025	decembrie 2025		Radu Vieru Boțan Valentina Andrițchi Nicoleta	**Realizat** ASC interacționează și menține relații de cooperare cu instituții internaționale relevante, inclusiv cu (ENISA), cu care a fost încheiat un Acord care a permis accesul și activarea mecanismului Cyber Reserve. Activarea mecanismului Cyber Reserve s-a desfășurat cu succes, demonstrând capacitatea instituțională a ASC de a utiliza instrumente europene avansate pentru gestionarea incidentelor de securitate cibernetică și consolidarea răspunsului național la amenințări. La data de 25 iunie, ASC a devenit membru al Organizației Europene pentru Securitate Cibernetică (ECSO), consolidând astfel cooperarea instituțională la nivel european și participarea activă în inițiativele relevante din domeniul securității cibernetice. Au fost organizate CTF și TTX în comun cu DNSC, precum și cu instituții similare din Ucraina. În ianuarie 2025 secția de cooperare a organizat o vizită de studiu a 6 colegi la instituția omoloagă din Belgia,

							CCB în cadrul căreia am primit informații referitoare la modul de organizare și funcționarea a CERT-ului național din Belgia.
2	Asigurarea interacțiunii în domeniul securității cibernetice cu autoritățile și instituțiile publice și cu furnizorii de servicii	Interacțiunea strategică cu furnizorii de servicii și entitățile relevante	ianuarie 2025	Continuu		Boțan Valentina Andrițchi Nicoleta Lapteanu Gheorghe	**Realizat** ASC a facilitat și asigurat interacțiunea cu autoritățile și instituțiile publice, precum și cu furnizorii de servicii, prin organizarea și coordonarea mai multor exerciții și evenimente de profil: Exerciții CTF: Cel mai amplu exercițiu a avut loc la data de 30-31 octombrie, servind atât drept activitate de testare a competențelor tehnice, cât și ca platformă de cooperare și networking între sectorul public și cel privat. Moldova Cyber Security Forum: Eveniment de două zile, desfășurat în aprilie, care a reunit reprezentanți ai sectorului public, ai sectorului privat și instituții partenere naționale și internaționale. În cadrul forumului, ASC a organizat un CTF, contribuind la crearea unei platforme de colaborare și schimb de experiență între participanți.
3	Intermedierea schimbului de informații între furnizorii de servicii și	Crearea platformelor Semnarea acordurilor de schimb de informații cu entintăți relevante	ianuarie 2025	decembrie 2025		Boțan Valentina Andrițchi Nicoleta	**Realizat** ASC aplică schimbul de informații criptat și securizat. În cadrul activării Cyber Reserve în perioada electorală,

	alte persoane juridice prin crearea și gestionarea unor platforme, inclusiv tehnico-tehnologice, și a comunităților de încredere, facilitând în acest sens semnarea acordurilor de schimb de informații între participanții la astfel de platforme și comunități						a demonstrat capacitatea instituțională a ASC de a gestiona schimbul de informații sensibile în condiții de siguranță și eficiență, consolidând cooperarea cu partenerii internaționali.
4	Înregistrarea și ținerea evidenței acordurilor privind schimbul de informații în materie de securitate cibernetică, semnate de către furnizorii de servicii	Crearea registrului intern privind acordurile semnate	ianuarie 2025	Continuu		Boțan Valentina Andrițchi Nicoleta	**Realizat** A fost creat registrul intern, în care toate acordurile au fost digitizate și înregistrate, iar registrul este accesibil angajaților ASC.

IV

Obiectivul general IV: Asigurarea punctului național unic de contact

Indicatori asociați obiectivelor:

1. PNA, Capitolul 10, pct. 1-5
2. PNA, Capitolul 31, pct. 8

Riscuri asociate realizării obiectivelor:

Riscuri interne

1. Crearea recentă a Agenției.

2. Recrutarea personalului necesar în contextul recentei organizării a Agenției.

Riscuri externe

1. Lipsa unei cooperări active a actorilor din sectorul securității cibernetice.

2. Lipsa resurselor umane suficiente.

Nr.	Acțiuni	Indicator de monitorizare	Termen de inițiere	Termen de realizare	Subdiviziune responsabilă	Responsabil	Comentarii
1	Asigurarea interacțiunii autorităților și instituțiilor publice naționale cu autoritățile similare din alte state și/sau cu organizațiile internaționale ori entitățile instituite de acestea;	Interacțiunea strategică cu următoarele autorități: CCB- Belgia, ENISA- EU,DNSC,	ianuarie 2025	decembrie 2025	SCSI	Boțan Valentina Andrițchi Nicoleta	**Realizat** ASC cooperează cu Ministerul Apărării în contextul parcursului de aderare a Republicii Moldova la proiectele PESCO și alte inițiative de securitate europeană. La nivel internațional: în acest an, ASC a semnat un Memorandum de Înțelegere cu ECCC, obținând acces la cursuri specializate și suport tehnic, echipa tehnică devenind membru FIRST. ASC colaborează activ cu EUPM, facilitând cooperarea cu experți desemnați din țări precum Olanda, Danemarca, Finlanda și Suedia, ceea ce a contribuit la consolidarea relațiilor bilaterale în domeniul securității cibernetice. Cooperarea cu Lituania vizează atât participarea la proiectele PESCO, Lituania fiind stat pilon, cât și parteneriate tehnice, inclusiv în domeniul DNS firewall. Cu ANSSI – Franța, ASC desfășoară schimb de informații privind sistemul de network sensor. Cooperarea cu Regatul Unit se realizează prin intermediul Ambasadei UK și MAE, facilitând schimbul de informații, transferul de expertiză și suportul tehnic al BAE Systems pentru dezvoltarea și operaționalizarea CSIRT-ului național.

							ASC interacționează cu instituțiile de securitate cibernetică din Ucraina, echipa ucraineană a participat la TTX co-organizat de ASC în iulie. Cooperarea cu NATO s-a concretizat prin desfășurarea de cursuri și programe de instruire cu suportul organizației, precum cursul din 12-23 mai în Macedonia de Nord la care am luat parte. Prin programul e-GA, ASC colaborează cu Estonia, beneficiind de suport în dezvoltare și operaționalizare, financiar, evenimente și traininguri specializate. Cooperarea cu OSCE a contribuit la operaționalizarea ASC prin furnizarea de echipamente tehnice. ASC beneficiază din partea OSCE de workshopuri privind măsuri diplomatice în cadrul setului de instrumente pentru diplomația cibernetică al UE. Drept exemplu, workshopul din 16-17 octombrie. Colaborarea cu DCAF a adus programe de training, desfășurat în 21 mai în domeniul politicilor de securitate și a domeniului legal al securității cibernetice.
2	Transmiterea, la cererea autorităților și instituțiilor publice sau a echipelor de răspuns la incidentele cibernetice,	Răspuns întocmit pentru fiecare solicitare	ianuarie 2025	Conform termenului indicat în solicitare	SCSI	Boțan Valentina Andrițchi Nicoleta	**Realizat** Procedura de transmitere a notificărilor și solicitărilor privind incidentele cibernetice către punctele unice de contact din alte state este implementată și funcțională; până în prezent, nu au fost primite solicitări de transmitere.

	punctelor unice de contact din alte state notificări și solicitări privind incidentele cibernetice;						
3	Transmiterea autorităților și instituțiilor publice naționale, conform competenței acestora, notificări și cereri în materie de securitate cibernetică primite din alte state sau de la organizații internaționale ori de la entitățile instituite de acestea;	Examinarea notificărilor și expedierea acestora în adresa entității	ianuarie 2025	Maxim în 3 zile de la momentul recepționării notificării	SCSI	Boțan Valentina Andrițchi Nicoleta	**Realizat** Procedura de transmitere către autoritățile și instituțiile publice naționale a notificărilor și cererilor în materie de securitate cibernetică primite din alte state sau de la organizații internaționale este implementată și funcțională; până în prezent nu au fost înregistrate astfel de notificări sau cereri.

V

Obiectivul general V: Identificarea și evidența furnizorilor de servicii

Indicatori asociați obiectivelor:

1. PNA, Capitolul 10, pct. 1-5
2. PNA, Capitolul 31, pct. 8

Riscuri asociate realizării obiectivelor:

Riscuri interne

1. Crearea recentă a Agenției.

2. Recrutarea personalului necesar în contextul recentei organizării a Agenției.

Riscuri externe

1. Lipsa unei cooperări active a actorilor din sectorul securității cibernetice.
2. Lipsa resurselor umane suficiente.
3. La pct. 4 lista furnizorilor nu există o opinie unică între autorități cu privire la tipul secret sau public al listei

Nr.	Acțiuni	Indicator de monitorizare	Termen de inițiere	Termen de realizare	Subdiviziune responsabilă	Responsabil	Comentarii
1	Identificarea persoanelor juridice de drept public și pe cele de drept privat în calitate de furnizori de servicii în sectoarele și subsectoarele critice în conformitate cu Legea 48/2023 privind securitatea cibernetică și Hotărârea Guvernului 860 privind identificarea furnizorilor de servicii 1.1. Solicitarea de la autoritățile publice și instituțiile de reglementare a informațiilor necesare pentru identificarea furnizorilor de servicii 1.2.Analiza și procesarea seturilor de date furnizate de autorități și instituții	Identificarea numărului total de persoane juridice conform acțiunii	ianuarie 2025	decembrie 2025	SIEFS	Lapteanu Gheorghe	**Realizat** În baza informațiilor solicitate, recepționate și analizate de la autoritățile publice și instituțiile de reglementare, au fost identificate persoanele juridice de drept privat și peroanele juridice de drept public, pentru a fi desemnate în calitate de furnizori de servicii esențiali/importanți.
2	Întocmirea Listei furnizorilor de servicii și menținerea evidenței furnizorilor de servicii 2.1. Notificarea prealabilă a furnizorilor de servicii identificați privind intenția de desemnare în calitate de furnizori esențiali sau furnizori importanți de servicii; 2.2 Recepționarea, evaluarea și analiza răspunsurilor și	Notificarea tuturor persoanelor juridice identificate Numărul de furnizori notificați Numărul furnizorilor	ianuarie 2025	decembrie 2025	SIEFS	Lapteanu Gheorghe	**Realizat parțial** Au fost transmise 307 notificări prealabile, recepționate și analizate informațiile privind corespunderea cu calitatea de furnizor și au fost emise 265 acte administrative individuale privind desemnarea în calitate de furnizor de servicii.

	informațiilor privind corespunderea sau necorespunderea cu calitatea de furnizor esențial/important de servici; 2.3. Emiterea actelor administrative de desemnare în calitate de furnizori esențiali/importanți de servicii și introducerea în lista furnizorilor de servicii.	introduși în listă					
3	Examinarea contestațiilor furnizorilor de servicii privind decizia de includere a acestora în lista furnizorilor de servicii	Examinarea tuturor contestațiilor persoanelor juridice sau reprezentanții acestora	ianuarie 2025	maxim 30 de zile de la depunerea contestației	SIEFS SJRU	Lapteanu Gheorghe Scripnic Radu	**Realizat** Au fost examinate 2 contestații și emise decizii în acest sens.
4	Ținerea evidenței furnizorilor de servicii identificați și, întocmirea, menținerea și actualizarea Listei furnizorilor de servicii 4.1.Colaborarea cu furnizorii de servicii identificați 4.1.1. Solicitarea datelor necesare pentru completarea listei 4.1.2. Procesarea și introducerea datelor recepționate	Întocmirea Listei furnizorilor de servicii Număr de furnizori a căror date au fost actualizate	ianuarie 2025	iunie 2025	SIEFS	Lapteanu Gheorghe	**Realizat** Au fost solicitate, recepționate și procesate informațiile și datele de la toți furnizorii de servicii notificați.

	4.2.Actualizarea listei furnizorilor de servicii critice 4.2.1 Revizuirea periodică a sectoarelor critice 4.2.3 Actualizarea informațiilor referitoare la furnizorii existenți	Întocmirea Listei furnizorilor de servicii Număr de furnizori a căror date au fost actualizate			SIEFS	Lapteanu Gheorghe	**Realizat** Au fost actualizate și ajustate toate datele prezentate de către furnizorii de servicii.
5	Interacționarea cu autoritățile publice responsabile de realizarea politicii de stat în sectoarele sau subsectoarele critice, stabilite de către Guvern, cu instituțiile publice responsabile de gestionarea unor domenii și subdomenii conexe sectoarelor și subsectoarelor respective, precum și cu autoritățile publice de reglementare a activității în aceste sectoare sau subsectoare	Interacțiunea cu toate autoritățile implicate Desfășurarea unor exerciții și antrenamente comune de consolidare a capacităților de reacție la atacuri cibernetice, inclusiv de blocare a atacurilor cibernetice simulate	ianuarie 2025	iunie 2025	SIEFS	Lapteanu Gheorghe	**Realizat** Au fost desfășurate ședințe de lucru cu autoritățile de reglementare și alte instituții de reglementare pentru clarificarea informațiilor care necesită a fi prezentate. Au fost organizate și desfășurate Exerciții de simulare a incidentelor cibernetice atât la nivel strategic și operațional cât și tehnic.

VI

Obiectivul general VI: Asigurarea orientării metodologice și reglementării domeniului securității cibernetice;

Indicatori asociați obiectivelor:

1. PNA, Capitolul 10, pct. 1-5
2. PNA, Capitolul 31, pct. 8

Riscuri asociate realizării obiectivelor:

Riscuri interne

1. Crearea recentă a Agenției.

2. Recrutarea personalului necesar în contextul recentei organizării a Agenției.

Riscuri externe

1. Lipsa unei cooperări active a actorilor din sectorul securității cibernetice.

2. Lipsa resurselor umane suficiente.

Nr.	Acțiuni	Indicator de monitorizare	Termen de inițiere	Termen de realizare	Subdiviziune responsabilă	Responsabil	Document de referință	Comentarii
1	Participarea la elaborarea actelor normative și a documentelor de politici în domeniul securității cibernetice	Avizarea actelor normative și a documentelor de politici, participarea la ședințele de lucru	ianuarie 2025	decembrie 2025	SJRU	Scripnic Radu	Legea 48/2023 privind securitatea cibernetică	**Realizat** Toate actele remise spre avizare au fost examinate și remis un răspuns în acest sens către autoritățile competente.
2	Furnizarea autorităților publice analize, informații statistice și generalizări ale practicii aplicării prevederilor legislației în procesul de elaborare de către acestea a actelor normative și a documentelor de politici în acest domeniu	Furnizarea informației în fiecare caz	ianuarie 2025	Continuu	SJRU	Scripnic Radu	Legea 48/2023 privind securitatea cibernetică	**Realizat** La solicitarea autorităților publice, analizele, informațiile statistice și generalizările privind aplicarea legislației în domeniul securității cibernetice au fost furnizate conform cererii.
	Participarea, inclusiv prin furnizarea informațiilor relevante, la elaborarea standardelor naționale în domeniul securității informației	Avizarea actelor normative și a documentelor de politici, participarea la ședințele de lucru	ianuarie 2025	Continuu	SJRU	Scripnic Radu	Legea 48/2023 privind securitatea cibernetică	**Realizat** A fost furnizată informația cu privire la lista standardelor necesare care urmează să fie adoptate în vederea consolidării protecției rețelelor și sistemelor informatice la nivel național.

	și securității cibernetice							
	Elaborarea și asigurarea promovarea celor mai bune practici și îndrumarea furnizorilor de servicii în gestionarea riscurilor, inclusiv pentru îndeplinirea cerințelor specifice de securitate privind rețelele și sistemele informatice	Elaborarea a 2 ghiduri și îndrumare practice Organizarea a 2 campanii de sensibilizare și informare privind pericolele din spațiul cibernetic și măsurile de protecție ce pot fi luate de către persoanele fizice și juridice Organizarea și desfășurarea a 2 de ateliere de lucru în domeniul securității cibernetice pentru personalul din sectorul public și privat deținători de elemente de	ianuarie 2025	Decembrie 2025	SJRU	Scripnic Radu	Legea 48/2023 privind securitatea cibernetică	**Realizat parțial** Au fost elaborate și distribuite broșuri care oferă recomandări privind politicile de securitate și principiile de reziliență cibernetică. Ghidul metodologic privind implementarea măsurilor de securitate cibernetică, destinat furnizorilor de servicii din sectoarele critice, este în proces de elaborare. ASC în colaborare cu experții EUPM a desfășurat **TTX** (table-top exercises) care simulează scenarii de amenințări hibride complexe. TTX-ul organizat în 8-9 iulie 2025 dedicat cadrului legal operațional, a reunit sectorul privat și cel public. Acest TTX a reprezentat și o masă rotunda pentru parteneriatul trilateral România-Moldova-Ucraina, țări care au luat parte la acest exercițiu.

		infrastructură critică						
	Elaborarea și aprobarea planului - național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice	Elaborarea planului național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice	ianuarie 2025	Decembrie 2025	DRICC SCSI	Radu Vieru Boțan Valentina Andrițchi Nicoleta	Legea 48/2023 privind securitatea cibernetică	**Realizat parțial** A fost aprobată Hotărârea de Guvern nr. 8232025 pentru aprobarea Regulamentului cu privire la elaborarea, actualizarea și implementarea Planului național de răspuns la incidente cibernetice și crize în domeniul securității cibernetice.

VII

Obiectivul general VII: Cercetare și dezvoltare

Indicatori asociați obiectivelor:

1. PNA, Capitolul 10, pct. 1-5
2. PNA, Capitolul 31, pct. 8

Riscuri asociate realizării obiectivelor:

Riscuri interne

1. Crearea recentă a Agenției.

2. Recrutarea personalului necesar în contextul recentei organizării a Agenției.

Riscuri externe

1. Lipsa unei cooperări active a actorilor din sectorul securității cibernetice.

2. Lipsa resurselor umane suficiente.

Nr.	Acțiuni	Indicator de monitorizare	Termen de inițiere	Termen de realizare	Subdiviziune responsabilă	Responsabil	Document de referință	Comentarii
1	Organizarea și coordonarea activităților de cercetare și dezvoltare în domeniul securității cibernetice	Participarea la instruiri de comun cu laboratoarele de securitate cibernetică din cadrul instituțiilor de învățământ superior (UTM-CYBERCOR)	ianuarie 2025	iunie 2025	SMSCD		Legea 48/2023 privind securitatea cibernetică	**Realizat** Echipa CSIRT a participat la evenimente și exerciții organizate în cadrul instituțiilor de învățământ superior (UTM-CYBERCOR)
2	Cooperarea cu instituții de cercetare din țară și de peste hotare în domeniul securității cibernetice	Interacțiunea strategică cu următoarele autorități: CCSC-RM STISC-RM, CCB- Belgia, ENISA- EU, și alte entități relevante. Asigurarea prin intermediul organismului național de standardizare, a aprobării standardelor naționale în domeniul	ianuarie 2025	Continuu	SCSI	Boțan Valentina	Art. 11 alin. (4) Legea 48/2023 privind securitatea cibernetică	**Realizat** ASC interacționează și menține relații de cooperare cu instituții internaționale relevante, inclusiv cu ENISA, cu care a fost încheiat un Acord de colaborare. ASC a devenit membru al Organizației Europene pentru Securitate Cibernetică (ECSO), consolidând astfel cooperarea instituțională la nivel european și participarea activă în inițiativele relevante din domeniul securității cibernetice. A fost semnat un Memorandum de Înțelegere cu ECCC prin care s-au pus bazele unei colaborări în ceea privește dezvoltarea

		securității informației și al securității cibernetice în baza standardelor și a specificațiilor tehnice europene și celor internaționale relevante pentru securitatea rețelelor și a sistemelor informatice						competențelor în materie de securitate ciberntică prin participarea la diverse proiecte europene, conferințe și evenimente tematice.

IX

Obiectivul general IX: Asigurarea resurselor umane

Indicatori asociați obiectivelor:

1. PNA, Capitolul 10, pct. 1-5
2. PNA, Capitolul 31, pct. 8

Riscuri asociate realizării obiectivelor:

Riscuri interne

1. Lipsa dosarelor pentru funcțiile publice vacante.

2. Neconfirmarea în funcție a funcționarilor publici debutanți.

3. Fluctuația personalului.

Riscuri externe

1. Interesul scăzut al funcționarilor publici de participare la activitățile de instruire.
2. Nerespectarea termenelor de prezentare a fișelor de evaluare.
3. Resurse financiare insuficiente planificate și alocate pentru dezvoltarea profesională a angajaților.
4. Nedepunerea în termenele stabilite a declarațiilor

Nr.	Acțiuni	Indicator de monitorizare	Termen de inițiere	Termen de realizare	Subdiviziune responsabilă	Responsabil	Comentarii
1	Formarea și menținerea unui efectiv de angajați profesioniști 1.1.1. Asigurarea necesarului de personal 1.1.2. Dezvoltarea profesională a personalului 1.1.3. Motivarea și menținerea personalului 1.1.4 Coordonarea și monitorizarea implementării procedurii de evaluare a performanțelor profesionale individuale	1. Nr. de concursuri organizate 2. Nr. de funcții publice scoase la concurs 3. Nr. de persoane angajate prin concurs 4. Planurile individuale de integrare aprobate și realizate 5. Nr. de funcționari publici debutanți confirmați în funcție 1. Elaborarea planului de instruire 2. Nr. de instruiri realizate 3. Nr. de personal instruit Organizarea evenimentelor necesare pentru menținerea personalului (chestionare periodice, cursuri de formare profesională)	ianuarie 2025	Decembrie 2025 Semestrial	SJRU	Scripnic Radu Donici Valentina	**Realizat** 58 de concursuri organizate; 16 funcții publice scoase la concurs; 12 persoane angajate prin concurs; 2 persoane angajate pin transfer; 8 Planuri de integrare aprobate; 4 funcționari publici debutanți confirmați în funcție; Planul de instruire elaborat/aprobat de conducere; 3 instruiri interne realizate; 45 de instruiri externe realizate; 35 de deplasări cu privire la dezvoltarea profesională; În cadrul ASC au fost organizate 2 evenimente privind Cyber Security; 2 module de limba engleză cu peste 90 de ore academice organizate în cadrul ASC; Nota informativă privind rezultatele evaluării elaborată/aprobată conducerea ASC.

		Nota informativă privind rezultatele evaluării					
2	2.1. Monitorizarea și asigurarea măsurilor privind respectarea regimului declarării averilor și intereselor personale Verificarea periodică a portalului ani.md pentru monitorizarea respectării procedurii 2.2. Monitorizarea și asigurarea respectării regimului juridic al cadourilor Întocmirea Registrul de evidență al cadourilor	2.1.1. 100% subiecți ai declarării asigurați cu semnătura electronică 2.1.2 100% declarații depuse anual, la angajare/ eliberare 2.1.3 100% subiecți ai declarării incluși în Registrul electronic al subiecților declarării 2.2.1. 100 % cadouri declarate și înregistrate în Registrul de evidență al cadourilor.	ianuarie 2025	Continuu	SJRU	Scripnic Radu Donici Valentina	**Realizat** 100% subiecți ai declarării asigurați cu semnătura electronică 100% declarații depuse anual, la angajare/ eliberare 100% subiecți ai declarării incluși în Registrul electronic al subiecților declarării

XI

Obiectivul general XI: Asigurarea responsabilității bugetar-fiscale a agenției

Indicatori asociați obiectivelor:

1. PNA, Capitolul 10, pct. 1-5
2. PNA, Capitolul 31, pct. 8

Riscuri asociate realizării obiectivelor:

Riscuri interne

1. Lipsa dosarelor pentru funcțiile publice vacante.
2. Neconfirmarea în funcție a funcționarilor publici debutanți.
3. Fluctuația personalului.

Riscuri externe

5. Interesul scăzut al funcționarilor publici de participare la activitățile de instruire.
6. Nerespectarea termenelor de prezentare a fișelor de evaluare.
7. Resurse financiare insuficiente planificate și alocate pentru dezvoltarea profesională a angajaților.
8. Nedepunerea în termenele stabilite a declarațiilor

Nr.	Acțiuni	Indicator de monitorizare	Termen de inițiere	Termen de realizare	Subdiviziune responsabilă	Responsabil	Comentarii
1	1.1. Elaborarea Proiectelor/Rapoartelor privind realizarea Strategiilor sectoriale de cheltuieli (SSC) cu privire la implementarea procesului CBTM pentru anii 2025-2027 1.1.1. Elaborarea Proiectului privind realizarea Strategiilor sectoriale de cheltuieli (SSC) 1.1.2. Elaborarea Raportului privind realizarea Strategiilor sectoriale de cheltuieli (SSC)	1 Proiect – realizat 100% 1 Raport – realizat 100%	ianuarie 2025	Martie 2025 Februarie 2025	SFA	Vîlcu Maria	**Realizat** Activitățile privind elaborarea Proiectelor/Rapoartelor de realizare a Strategiilor sectoriale de cheltuieli (SSC) pentru anii 2025–2027, în contextul implementării procesului CBTM, au fost realizate conform cerințelor metodologice. A fost elaborat Proiectul privind realizarea Strategiilor sectoriale de cheltuieli (SSC), care a fundamentat planificarea bugetară pe termen mediu, iar ulterior a fost întocmit Raportul privind realizarea Strategiilor sectoriale de cheltuieli (SSC), reflectând gradul de implementare a obiectivelor și utilizarea resurselor alocate.
	1.2. Raportarea sistemului de control intern managerial și emiterea declarației de răspundere managerială 1.2.1. Elaborarea Raportului anual privind controlul intern managerial	1 Raport – realizat 100% 1 Declarație – realizat 100%	ianuarie 2025	Martie 2025	SFA	Vîlcu Maria	**Realizat** Activitățile aferente raportării sistemului de control intern managerial și emiterii declarației de răspundere managerială au fost realizate conform cadrului normativ aplicabil. A fost elaborat Raportul anual privind controlul intern managerial, iar Declarația de răspundere managerială a fost emisă și publicată în termenul stabilit.

	1.2.2.Declarația de răspundere managerială emisă și publicată						
	1.3. Întocmirea Rapoartelor financiare ale Agenției 1.3.1 Rapoarte financiare întocmite și prezentate pentru verificare, aprobare și consolidare către organul ierarhic superior	3 Rapoarte realizate 100%	ianuarie 2025	Februarie 2025 Iulie 2025 Octombrie 2025	SFA	Vîlcu Maria	**Realizat** Activitățile privind întocmirea rapoartelor financiare ale Agenției au fost realizate conform cerințelor legale. Rapoartele financiare au fost întocmite și prezentate spre verificare, aprobare și consolidare către organul ierarhic superior, în termenele stabilite.
	1.4. Întocmirea Raportului privind performanța pe programe/subprograme la situația din 31 decembrie 2024 și 30 iunie 2025 1.4.1. Rapoarte privind performanța pe programe/subprograme prezentate către organul ierarhic superior	2 Rapoarte realizate 100%	ianuarie 2025	Februarie 2025 Iulie 2025	SFA	Vîlcu Maria	**Realizat** Activitățile privind întocmirea Raportului privind performanța pe programe/subprograme au fost realizate conform cerințelor instituționale. Rapoartele privind performanța pe programe/subprograme, la situația din 31 decembrie 2024 și 30 iunie 2025, au fost întocmite și prezentate către organul ierarhic superior.
	1.5. Întocmirea și prezentarea Dărilor de seamă și Rapoartelor Statistice 1.5.1 Dări de seamă fiscale lunare și anuale	12 Rapoarte lunare realizate 100 % (IPC21) 1 Raport anual realizat 100%	ianuarie 2025	Februarie 2025 Decembrie 2025	SFA	Vîlcu Maria	**Realizat** Activitățile privind întocmirea și prezentarea dărilor de seamă și rapoartelor statistice au fost realizate conform cerințelor legale. Dările de seamă fiscale lunare și anuale au fost elaborate și prezentate către Serviciul Fiscal, iar rapoartele

	elaborate și prezentate către Serviciul fiscal 1.5.2. Rapoarte Statistice elaborate și prezentate către Biroul Național de Statistică	(IALS 21) -Rapoarte IRM 19 (după necesitate) 11 Rapoarte trimestriale și anuale realizate 100%					statistice au fost întocmite și transmise către Biroul Național de Statistică.
2	2.1. Asigurarea procesului de finanțare a Agenției 2.1.1. Întocmirea informației privind necesitățile de finanțare ale Agenției conform metodologiei stabilite 2.1.2. Prezentarea proiectului de buget pentru anul 2026 și estimările pe anii 2027-2028 spre examinare și aprobare 2.1.3. Repartizarea resurselor financiare conform metodologiei stabilite	Numărul de informații întocmite 100% Proiect de budget prezentat spre aprobare -Alocații repartizate 100%	ianuarie 2025	Conform termenului stabilit de Ministerul Finanțelor	SFA	Vîlcu Maria	**Realizat** Activitățile privind asigurarea procesului de finanțare a Agenției au fost realizate conform metodologiei aplicabile. Informația privind necesitățile de finanțare ale Agenției a fost întocmită, proiectul de buget pentru anul 2026 și estimările pe anii 2027-2028 au fost prezentate spre examinare și aprobare, iar resursele financiare au fost repartizate conform metodologiei stabilite.
	2.2. Gestionarea bugetului Agenției 2.2.1. Organizarea și desfășurarea procedurilor de	Procese verbale, Dări de seamă, Contracte realizate 100%	ianuarie 2025	Conform termenului stabilit de Ministerul Finanțelor	SFA	Vîlcu Maria	**Realizat** Au fost realizate procese verbale, dări de seamă, Contracte realizate în proporție de 100% Numărul ordinelor de plată , notelor de transfer întocmite 100%

	Achiziții de mică valoare, COP, Licitații deschise 2.2.2. Monitorizarea executării cheltuielilor bugetare, transferurilor și datoriilor	Numărul ordinelor de plată , notelor de transfer întocmite 100%					
	2.3. Organizarea și ținerea evidenței contabile 2.3.1. Ținerea evidenței contabile a veniturilor și cheltuielilor	Cartea mare întocmită, notele contabile perfectate lunar, rapoarte întocmite și prezentate în termenul stabilit 100%	ianuarie 2025	Decembrie 2025	SFA	Vîlcu Maria	**Realizat** Cartea mare a fost întocmită, notele contabile perfectate lunar, rapoarte întocmite și prezentate în termenul stabilit 100%
	2.3.2. Asigurarea integrității valorilor materiale. Inventarierea bunurilor aflate în gestiunea Agenției	Rapoarte elaborate, documente primare de intrare/ieșire, listele de inventariere elaborate, procese verbale de primire-predare, contracte de răspundere materială, calcularea	ianuarie 2025	Decembrie 2025	SFA	Vîlcu Maria	**Realizat** Rapoartele au fost elaborate, documentele primare de intrare/ieșire întocmite și listele de inventariere completate conform cerințelor și termenelor stabilite.

		uzurii și amortizării a mijloacelor fixe și bunurile materiale, casarea.					

Abrevieri

ASC - Agenția pentru Securitate Cibernetică

DSC - Direcția supraveghere și control

SPA - Secția prevenire și analiză

SIEFS - Secția identificare și evidență furnizori de servicii

SCSI - Secția cooperare și schimb de informații

SMSCD - Secția metodologie, standarde, cercetare și dezvoltare

SJRU - Serviciul juridic și resurse umane

SFA - Serviciul financiar-administrativ

STI - Serviciul tehnologii informaționale și comunicații

SCMM - Serviciul comunicare și mass-media

SMD - Serviciul managementul documentelor