SPECIFICAȚII TEHNICE (F4.1)

Numărul procedurii de achiziție: ***21030975/ ocds-b3wdp1-MD-1605704596871***
Denumirea procedurii de achiziție: ***Lotul 1 Servicii de suport tehnic şi consultanţa pentru platforma tehnologica (Hardware şi Software de sistem) pentru anul 2021 (începînd cu 01.01.2021 pînă la 31.12.2021, la solicitarea Benificiarului) (lista în Anexa nr 1)***

Cod CPV	Denumirea bunurilorşi/sau a serviciilor	Modelul articolului	Țara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7	8
	Bunuri/Servicii:						
	Lotul 1:						
79400000-8	**Servicii de analiză, consultanță continuă și evaluare a securității cibernetice a sistemelor IT (servicii de scanări de vulnerabilități lunare, consultanță, testare a securității cibernetice din cadrul CNAS)**				1.Specificațiile tehnice obiectului achiziției. • Scanări de vulnerabilităţi lunare conform standardelor internaționale cu instrumente speciale. Analiza vulnerabilităților sistemelor informaționale CNAS (inclusiv din Cloud) și identificarea celor adevărate din cele false. Raportarea lunară către CNAS a vulnerabilităților depistate și recomandările viabile de fixare. Consultanță la fixarea vulnerabilităților și a breșelor de securitate depistate precum și consultanță la aplicarea măsurilor compensatorii de protecție cibernetică. Prin acest serviciu se va asigura identificarea posibilelor vulnerabilităţi care apar zilnic la nivelul sistemelor de operare, bazelor de date și aplicațiilor software.	• Scanarea proactivă a infrastructurii TI cu instrumente speciale privind existenta configurări greșite, identificarea puncte vulnerabile, componente dăunătoare și înaintarea recomandărilor cu privire la modul de eliminare a riscurilor existente. Lucrări se realizează în conformitate cu următoarele proceduri:: 1. Verificarea existenței vulnerabilităților cu un scaner automatizat. 2. Identificarea vulnerabilităților prin analiza rezultatelor scanării și căutarea anomaliilor. 3. Verificarea posibilităților de realizare a vulnerabilităților și clasificarea acestora pe niveluri. 4. Elaborarea recomandărilor privind minimizarea impactul potențial al vulnerabilităților prin aplicarea măsurilor compensatorii de protecție cibernetică. 5. Monitorizarea rezultatelor remedierii vulnerabilităților prin procesului de retestare	Setul de standarde internaționale ISO/IEC 27000, recomandări asociației independente profesionale ISACA.

Cod CPV	Denumirea bunurilorşi/sau a serviciilor	Modelul articolului	Ţara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
						Mai multe detalii sunt descrise în file "DescriereaIndeplinirii Cerinţelor", 6 file, 29 KB	
					• Consultanţă în securizarea infrastructurii, a Cloud-urilor, a reţelelor WAN, LAN, a elementelor IT, prin analiza eficacităţii tehnologice a soluţiilor de protecţie automatizate, a ecranelor de protecţie precum şi consultanţă la aplicarea cerinţelor minime de securitate cibernetică pentru instituţiile de stat. Consultarea continuă conform standardelor internaţionale la identificarea anumitor soluţii şi a produselor necesare securizării sistemului informaţional al Autorităţii contractante.	• În procesul de diagnosticare complexă a setărilor pentru echipamente de reţea şi server, de evaluat conformitatea acestora cu recomandările producătorilor şi cele mai bune practice (CIS Benchmarks). Identificarea: 1. La nivelul echipamentului de reţea: a) disponibilităţii punctului de eşec (Single Point of Failure) unic în topologia reţelei fizice şi logice; b) prezenţa vulnerabilităţilor şi potenţialelor ameninţări în setările serviciilor de reţea utilizate; c) incoerenţa în sistemele failover; d) necesităţii optimizării infrastructurii reţelei; e) neconformităţii cu cerinţele privind securitatea informaţiei 2. La nivelul serverului: a) setărilor software cheie a serviciilor de bază: Windows Active Directory, serviciilor poştale, Virtualization hypervisor; etc.; b) necesitatea optimizării arhitecturii platformei pentru respectării cerinţelor minime obligatorii de securitate cibernetică conform HG nr. 201 din 28.03.17; c) inconsecvenţelor în setările curente ale software-ului cu recomandările producătorului şi cerinţele de securitate a informaţiei. ***Mai multe detalii sunt descrise în file "Descrierea Indeplinirii Cerinţelor", 6 file, 29 KB***	CIS Benchmarks, Cisco SAFE Reference Guide.
					• Servicii de teste de penetrare (Penetration testing) a infrastructurii autorităţii contractante	• Analiza complexă a securităţii sistemelor informatice ale Beneficiarului expuse în	Penetration testing

Cod CPV	Denumirea bunurilorşi/sau a serviciilor	Modelul articolului	Ţara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
					din exteriorul infrastructurii şi din interiorul acesteia. Ofertantul va prezenta în Planul de proiect, vectori de atac reali care ar putea fi aplicaţi de către persoane necunoscute în scopul sustragerii datelor din cadrul sistemelor informaţionale sau subminării securităţii informaţionale. Testele de penetrare reprezintă o modalitate de evaluare a securităţii unui sistem informatic prin simularea unui atac, prin exploatarea vulnerabilităţilor existente şi cunoscute intr-un mod asemănător încercărilor de exploatare realizate de către un atacator, cu diferenţa ca acestea vor fi efectuate intr-un mod etic, cu permisiunea Beneficiarului. Procesul implica o analiza activa a sistemelor informatice pentru orice vulnerabilităţi existente care ar putea rezulta din configuraţia inadecvata şi din breşe cunoscute sau necunoscute, hardware şi software. Scopul serviciilor prestate: • asigurarea unui climat funcţional şi protejat al sistemului informaţional, precum şi asigurarea cerinţelor minime obligatorii de securitate cibernetică pentru instituţiile de stat. • monitorizarea procesul de securizare continuu a sistemelor informatice de către experţi ai Prestatorului şi raportarea lunară existenţa/apariţia vulnerabilităţilor în contextul sistemului informaţional cu o dinamică avansată şi complexă. • creşterea vigilenţei la incidente de securitate cibernetică prin pregătire,. Îndeplinirea cerinţelor faţă de servicii din Anexa nr. 1 Ca urmare a serviciilor prestate, Prestatorul va oferi livrabilele conform Anexei nr.2	Internet şi din interiorul infrastructurii, testând eficacitatea măsurilor de securitate implementate prin simularea unor atacuri informatice de tip Black Box şi Grey Box, respectiv. Scopuri: - evaluarea securităţii infrastructurii din perspectiva vizitatorului încercând să obţină acces la contul utilizatorului de serviciu - evaluarea securităţii infrastructurii din perspectiva utilizatorului care cunoaşte unele informaţii ce ţin de topologia infrastructurii precum şi conturi de acces de utilizator (VPN) ***Mai multe detalii sunt descrise în file "Descrierea Indeplinirii Cerinţelor", 6 file, 29 KB***	Execution Standard technical Guide, NIST SP 800-42, NIST SP 800-115, Open Source Security Testing Methodology Manual v3.

Cod CPV	Denumirea bunurilorşi/sau a serviciilor	Modelul articolului	Ţara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
79400000-8	**Instruirea profesională a personalului CNAS în domeniul securităţii cibernetice pe parcursul anului 2021**				1. Domeniul instruirii de dezvoltare profesională -"Securitate cibernetică" 2.Tipul de instruire Internă 3. Obiectivele generale de dezvoltare profesională referitoare la cunoştinţele care trebuie să fie acumulate şi abilităţile care trebuie să fie dezvoltate de către funcţionarii publici în urma participării acestora la activităţile de instruire Îmbunătăţirea cunoştinţelor participanţilor la activitatea de instruire privind securitatatea cibernetică, riscurilor actuale de compromitere a informaţiilor din interior. Importanţa respectării normelor interne, naţionale şi internaţionale de securitate cibernetică, etc. 4. Subiectele/tematicile de instruire obligatorii de a fi examinate - Formarea culturii securităţii cibernetice; - Importanţa respectării normelor interne, naţionale şi internaţionale de securitate cibernetică; - Conştientizarea riscurilor actuale de compromitere a informaţiilor din interior (sustragere, copiere, distrugere, divulgare, scurgere) şi impactul acestora; - Modalităţi şi reguli de setare a parolelor, precum şi asimilarea tehnicilor de igienă cibernetică în procesul de activitate. 5. Durata acceptată pentru activităţile de instruire Minim 2 ore academice de instruire per grup pentru specialiştii CNAS (utilizatori de sisteme informaţionale); Minim 2 ore academice de instruire pentru conducerea CNAS;	Activităţilor de instruire vor fi realizate on-line. Conţinutul detaliat al cursului este prezentat în anexă Anexa A la file "DescriereaIndeplinirii Cerinţelor", 6 file, 29 KB. La necesitatea, programul de instruire va fi adoptat la necesităţile specifice ale Bebeficiarului Instruirea va fi interactivă şi prevede expedieri de 2 ori (cel puţin) a mesajelor de phishing către toţi utilizatorii Beneficiarului în caz de necesitate, în funcţie de nivelul de pregătire a utilizatorilor din acest domeniu, la decizia Prestatorului serviciilor. Cursul de instruire va fi disponibil în limba română şi rusă. ***Mai multe detalii sunt descrise în file "Descrierea Indeplinirii Cerinţelor", 6 file, 29 KB***	

Cod CPV	Denumirea bunurilorşi/sau a serviciilor	Modelul articolului	Ţara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
					Minim 8 ore academice de instruire per grup pentru specialiştii din domeniul tehnologii informaţionale. 6. Informaţia succintă privind grupul-ţintă pentru care se organizează instruirea a) Categoria de participanţi - Specialiştii CNAS (utilizatori de sisteme informaţionale). - Conducerea CNAS. - Specialişti din domeniul tehnologii informaţionale. b) Domeniul de competenţă al participanţilor Administrarea şi gestionarea eficientă a sistemului public de asigurări sociale. c) Numărul de participanţi 1. 1235 participanţi - utilizatori de sisteme informaţionale (62 grupe). 2. 4 participanţi – conducerea CNAS (1 grup). 3. 57 participanţi – specialişti din domeniul tehnologii informaţionale (3 grupe). d) Informaţia privind preferinţele din punctul de vedere al realizării programelor de instruire - Realizarea activităţilor de instruire online, după caz, în contextul situaţiei epidemiologice din Republica Moldova; - Testarea practică a angajaţilor prin diverse tehnici de manipulare la disponibilitatea de a oferi date tehnice interne persoanelor terţe – inginerie socială, cu întocmirea unui Raport a testării angajaţilor. - Elaborarea şi furnizarea materialelor de suport participanţilor la curs; - Adaptarea programului de instruire elaborat iniţial la necesităţile specifice ale angajaţilor/CNAS, îl prezintă conducerii CNAS spre aprobare şi îl realizează în strictă conformitate cu contractul încheiat; - Evaluarea cursului de instruire şi întocmirea Raportului privind activitatea de instruire.		

Cod CPV	Denumirea bunurilorşi/sau a serviciilor	Modelul articolului	Ţara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
					- Folosirea stilului interactiv de instruire, evitând sesiunile teoretice de lungă durată. Cursul de instruire se va desfăşura în limba română. Profilul prestatorului de servicii Serviciile de instruire urmează a fi oferite de către specialişti în domeniul protecţiei datelor cu caracter personal, experţi în securitatea cibernetică. Criterii minime de calificare: •Diplomă/certificate de studii a formatorului/formatorilor în domenii relevante serviciilor prestate; •Experienţă în prestarea serviciilor de dezvoltare profesională în domeniul în care se organizează activitatea de dezvoltare profesională menţionată. Procedura de aplicare: În vederea demonstrării conformităţii cu cerinţele solicitate, aplicantul va prezenta: • Programul de instruire în corespundere cu cerinţele expuse de CNAS •Scrisoarea de intenţie a formatorului care să cuprindă informaţii cu privire la rezultatele activităţii anterioare în domeniul prestării serviciilor de dezvoltare profesională de domeniu (descrierea succintă a celor mai relevante activităţi de instruire realizate); •Curriculum vitae a formatorului care va cuprinde informaţii cu privire la experienţa în prestarea serviciilor de dezvoltare profesională în domeniul în care se organizează activitatea de dezvoltare profesională menţionată. •Copie a diplomei/certificatelor de studii a formatorului; •Copie a actelor de identitate ale formatorului; •Oferta financiară (în lei MDL) privind onorariul solicitat pentru îndeplinirea sarcinilor care revin.		

Cod CPV	Denumirea bunurilorşi/sau a serviciilor	Modelul articolului	Ţara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
					Declaraţie de confidenţialitate Toate datele şi informaţiile primite de la personalul Casei Naţionale de Asigurări Sociale pentru realizarea obiectivului acestei sarcini trebuie tratate confidenţial şi pot fi utilizate doar în legătură cu executarea activităţilor descrise în prezentul Caiet de sarcini		

Semnat:_____

Numele, Prenumele: Ghincu Sergiu

În calitate de: Director General

Ofertantul: DAAC System Integrator S.R.L.

Adresa: mun.Chisinau str.Calea Ieşilor 10

Descrierea îndeplinirii cerințelor

Serviciul solicitat	Ariile ce urmează a fi evaluate (Descrierea succinta)	Livrabile
1.1 Servicii de analiză, consultanță continuă și evaluare a securității cibernetice a sistemelor IT		
Scanări de vulnerabilități lunare conform standardelor internaționale cu instrumente speciale. Analiza vulnerabilităților sistemelor informaționale CNAS (inclusiv din Cloud) și celor adevărate din cele false. Raportarea lunară către CNAS a vulnerabilităților depistate și recomandările viabile de fixare. Consultanță la fixarea vulnerabilităților și a breșelor de securitate depistate precum și consultanță la aplicarea măsurilor compensatorii de protecție cibernetică.	Scanarea proactivă a infrastructurii TI cu instrumente speciale privind existenta configurări greșite, identificarea puncte vulnerabile, componente dăunătoare și înaintarea recomandărilor cu privire la modul de eliminare a riscurilor existente. Lucrări se realizează în conformitate cu următoarele proceduri:: 1. Verificarea existenței vulnerabilităților cu un scaner automatizat. 2. Identificarea vulnerabilităților prin analiza rezultatelor scanării și căutarea anomaliilor. 3. Verificarea posibilităților de realizare a vulnerabilităților și clasificarea acestora pe niveluri. 4. Elaborarea recomandărilor privind minimizarea impactul potențial al vulnerabilităților prin aplicarea măsurilor compensatorii de protecție cibernetică. 5. Monitorizarea rezultatelor remedierii vulnerabilităților prin procesului de retestare	Raport lunar de vulnerabilități prezentat și explicat în detalii conducerii Autorității contractante (partea executivă) și specialiștii TI (partea tehnică) după fiecare scanare. Rapoartele de scanări de vulnerabilități vor include vulnerabilitățile detectate, catalogate in funcție de gravitatea lor. Raportul va include: - Descrierea vulnerabilităților; - Analiza vulnerabilităților și atribuirea gradelor de pericol; - Recomandări și modalități de remediere; - Consultanță de fixare a breșelor și vulnerabilităților. Rapoarte de analiză, va conține analiza rezultatelor testelor efectuate prin care se vor identifica și vor fi incluse recomandări de remediere conținând cele mai bune acțiuni/măsuri/metode ce trebuie întreprinse pentru eliminarea sau micșorarea riscului generat de vulnerabilitățile detectate
Consultanță în securizarea infrastructurii, a Cloud-urilor, a rețelelor WAN, LAN, a elementelor IT, prin analiza eficacității tehnologice a soluțiilor de protecție automatizate, a ecranelor de protecție precum și consultanță la aplicarea cerințelor minime de securitate cibernetică	În procesul de diagnosticare complexă a setărilor pentru echipamente de rețea și server, de evaluat conformitatea acestora cu recomandările producătorilor și cele mai bune practice (CIS Benchmarks). Identificarea: 1. La nivelul echipamentului de rețea: a) disponibilității punctului de eșec (Single Point of Failure) unic în topologia rețelei fizice și logice;	Raport de analiză a experților Prestatorului către conducerii Autorității contractante (partea executivă) și specialiștii TI (partea tehnică) privind implementării corecte și setării suficiente a ecranelor de protecție gen firewall la nivel de stații, servere, echipamente de rețea, etc. Elaborarea consultații în securizarea infrastructurii, a Cloud-urilor, a rețelelor WAN,

pentru instituțiile de stat. Consultarea continuă conform standardelor internaționale la identificarea anumitor soluții și a produselor necesare securizării sistemului informațional al Autorității contractante.	b) prezența vulnerabilităților și potențialelor amenințări în setările serviciilor de rețea utilizate; c) incoerența în sistemele failover; d) necesității optimizării infrastructurii rețelei; e) neconformității cu cerințele privind securitatea informației 2. La nivelul serverului: a) setărilor software cheie a serviciilor de bază: Windows Active Directory, serviciilor poștale, Virtualization hypervisor; etc.; b) necesitatea optimizării arhitecturii platformei pentru respectării cerințelor minime obligatorii de securitate cibernetică conform HG nr. 201 din 28.03.17; c) inconsecvențelor în setările curente ale software-ului cu recomandările producătorului și cerințele de securitate a informației.	LAN, a elementelor IT și recomandărilor de remediere conținând cele mai bune acțiuni/măsuri/metode ce trebuie întreprinse pentru eliminarea sau micșorarea riscului generat în domeniu.
Servicii de teste de penetrare a infrastructurii autorității contractante din exteriorul infrastructurii și din interiorul acesteia. Ofertantul va prezenta în Planul de proiect, vectori de atac reali care ar putea fi aplicați de către persoane necunoscute în scopul sustragerii datelor din cadrul sistemelor informaționale sau subminării securității informaționale. Testele de penetrare reprezintă o modalitate de evaluare a securității unui sistem informatic prin simularea unui atac, prin exploatarea vulnerabilităților existente și cunoscute intr-un mod asemănător încercărilor de exploatare realizate de către un	Analiza complexă a securităţii sistemelor informatice ale Beneficiarului expuse în Internet și din interiorul infrastructurii, testând eficacitatea măsurilor de securitate implementate prin simularea unor atacuri informatice de tip Black Box și Grey Box, respectiv. Scopuri: - evaluarea securității infrastructurii din perspectiva vizitatorului încercând să obțină acces la contul utilizatorului de serviciu - evaluarea securității infrastructurii din perspectiva utilizatorului care cunoaște unele informații ce țin de topologia infrastructurii precum și conturi de acces de utilizator (VPN)	Raport de analiză către conducerii Autorității contractante (partea executivă) și specialiștii TI (partea tehnică) a rezultatelor testelor efectuate în care se vor identifica vectori de atac reali care ar putea fi aplicați de către persoane necunoscute în scopul sustragerii datelor din cadrul sistemelor informaționale sau subminării securității informației și vor fi incluse cele mai bune măsuri și metode de remediere a problemelor și vulnerabilităților descoperite, în funcție de severitate și impact.

atacator, cu diferența ca acestea vor fi efectuate intr-un mod etic, cu permisiunea Beneficiarului. Procesul implica o analiza activa a sistemelor informatice pentru orice vulnerabilități existente care ar putea rezulta din configurația inadecvata și din breșe cunoscute sau necunoscute, hardware și software		
1.2 Instruirea profesională a personalului CNAS în domeniul securității cibernetice pe parcursul anului 2021		
Subiectele/tematicile de instruire obligatorii de a fi examinate: - Formarea culturii securităţii cibernetice; - Importanţa respectării normelor interne, naţionale şi internaţionale de securitate cibernetică; - Conştientizarea riscurilor actuale de compromitere a informaţiilor din interior (sustragere, copiere, distrugere, divulgare, scurgere) şi impactul acestora; - Modalităţi şi reguli de setare a parolelor, precum şi asimilarea tehnicilor de igienă cibernetică în procesul de activitate	Activităţilor de instruire vor fi realizate on-line. Conținutul detaliat al cursului este prezentat în anexă Anexa A. La necesitatea, programul de instruire va fi adoptat la necesităţile specifice ale Bebeficiarului Instruirea va fi interactivă și prevede expedieri de 2 ori (cel puțin) a mesajelor de phishing către toți utilizatorii Beneficiarului în caz de necesitate, în funcție de nivelul de pregătire a utilizatorilor din acest domeniu, la decizia Prestatorului serviciilor. Cursul de instruire va fi disponibil în limba română și rusă.	1. Programul de instruire și conștientizare a securității informațiilor pentru angajați va perfecționa: - crearea și menținerea unei atmosfere a securității informației corporative sigure, - dezvoltarea abilităților de răspuns adecvat la incidente cibernetice; - reducerea vulnerabilităților la atacurile cibernetice. 2. Materiale de suport pentru specialiștii CNAS și personal TI (în formă electronică):: - reguli de igienă digitală: - reguli contracarării phishingului; - Check List pentru personalul IT cu privire la metodele de organizare a lucrărilor la distanță în condiții de siguranță și ieșirea din acest mod; - Regulile de prevenire a atacurilor Ransomeware 3. Rezultate analitice ale procesării e-mailurilor de phishing (în cazul desfășurării).

ANEXA A

Program de instruire în domeniul securității informațiilor

(pot fi adaptată la necesităţile specifice ale CNAS)

Durată (ore academice)	**Categoria de participanţi**		
	Specialiştii CNAS	**Specialiştii TI**	**Conducerea CNAS**
n/a	Mesaj (e-mail) de phishing nr.1	Mesaj (e-mail) de phishing nr.2	Mesaj (e-mail) de phishing nr.3
	Notă: va fi desfăşurat în caz de necesitate, în funcție de nivelul de pregătire a utilizatorilor din acest domeniu, la decizia Prestatorului serviciilor		
2	Subiect: Asimilarea tehnicilor de igienă cibernetică în procesul de activitate, modalităţi şi reguli de setare a parolelor Conținutul cursului: • Tendințe în atacurile cibernetice. Tehnologii, instrumente, ținte ale escrocilor; • Reguli pentru protejarea dispozitivelor digitale personale și corporative de scurgeri de informații și infecții malware: - securitatea dispozitivelor mobile; - securitatea PC; - securitatea sistemelor Cloud. • Protejarea conturilor împotriva compromitere: - securitatea parolelor; - contracararea metodelor de phishing; - contracararea malware, Ransomeware, etc. • Regulile de bază ale igienei digitale pe Internet		
1			Subiect: Formarea culturii securităţii cibernetice. Conținutul cursului: • Imaginea unui atacator modern; • Dezvoltarea instrumentelor de criminalitate informatică; • Specificul atacurilor cibernetice asupra diverselor obiecte: persoane fizice, instituții de stat, etc.; • Infrastructura și interacțiunea criminalilor cibernetici
1			Subiect: Importanţa respectării normelor interne, naţionale şi internaţionale de securitate cibernetică Conținutul cursului: • Standardul ISO 27001;

			• HG nr.201 din 28.03.17 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică; • HG nr.1123 din 14.12.10 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora; • Comunicări externe cu partenerii și mass-media înainte, în timpul și după incident.
2		Subiect: Conştientizarea riscurilor actuale de compromitere a informaţiilor - Investigarea incidentelor de securitate a informațiilor Conținutul cursului: • Scopurile și tehnicile atacurilor cibernetice; • Bazele răspunsului inițial la incidentele de securitate a informațiilor: - utilizarea modelelor de amenințare pentru a înțelege TTP atacanților; - Cyber Kill Chain; • Proces de răspuns: identificare, localizare, formarea indicatorilor, căutarea de noi noduri infectate; • Colectarea dovezilor digitale; • Răspuns simulat la incident.	
4		Subiect: Conştientizarea riscurilor actuale de compromitere a informaţiilor - Curs avansat de răspuns la incidente Conținutul cursului: • Roluri, echipe, procese; • Recomandări practice ale specialiștilor privind organizarea procesului de răspuns la incidente.	
n/a	Mesaj (e-mail) de phishing nr.4	Mesaj (e-mail) de phishing nr.5	Mesaj (e-mail) de phishing nr.6
	Notă: va fi desfășurat în caz de necesitate, în funcție de nivelul de pregătire a utilizatorilor din acest domeniu, la decizia Prestatorului serviciilor		

1		Subiect: Şedinţă comună pentru Conducerea CNAS şi management IT privind analiza rezultatelor e-mailurilor de phishing: • Discutarea rezultatelor testării de phishing, • Recomandări • Intrebari si raspunsuri Notă: va fi desfăşurat în cazul expedierii a e-mail-urilor de phishing