

GUVERNUL ROMÂNIEI
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

DECIZIE

pentru aprobarea tematicilor pentru formarea auditorilor de securitate cibernetică, a membrilor echipelor CSIRT și a responsabililor cu securitatea rețelelor și sistemelor informatice

În baza prevederilor art. 32 alin. (2) lit. e) și art. 33 alin. (2) lit. e) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare,

având în vedere dispozițiile art. 4 lit. f) din Ordonanța de urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată cu modificări și completări prin Legea nr. 11/2022,

pentru aplicarea Normelor privind autorizarea și verificarea furnizorilor de servicii de formare pentru securitate cibernetică, aprobate prin Ordinul directorului Directoratului Național de Securitate Cibernetică nr. 106/2022,

în temeiul art. 7 alin. (3) din Ordonanța de urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată cu modificări și completări prin Legea nr. 11/2022,

directorul Directoratului Național de Securitate Cibernetică emite prezenta decizie.

Art. 1. – (1) Se aprobă **Tematica pentru formarea auditorilor de securitate cibernetică**, prevăzută în anexa nr. 1.

(2) Se aprobă **Tematica pentru formarea membrilor echipelor CSIRT**, prevăzută în anexa nr. 2.

(3) Se aprobă **Tematica pentru formarea responsabililor cu securitatea rețelelor și sistemelor informatice**, prevăzută în anexa nr. 3.

Art. 2. – Anexele 1 – 3 fac parte integrantă din prezenta decizie.

Art. 3. – Prezenta decizie se publică în Monitorul Oficial al României, Partea I.

Directorul Directoratului Național de Securitate Cibernetică

Petre-Dan CÎMPEAN

București, 03 noiembrie 2022
Nr. 107

TEMATICA
pentru formarea auditorilor de securitate cibernetică

Formarea profesională	Tema		Instruire	
			Teoretic ă	Practică
Formarea auditorilor de securitate cibernetică	FA1	Termeni și noțiuni privind securitatea cibernetică aplicată la nivelul operatorilor de servicii esențiale și furnizorilor de servicii digitale în conformitate cu legislația în vigoare în domeniu securității cibernetică de la nivelul României și UE.	x	
	FA2	Identificarea operatorilor de servicii digitale: (1) Norme metodologice de identificare a operatorilor de servicii esențiale și furnizorilor de servicii digitale, conform Ordinului MCSI nr. 599/2019. (2) Stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale, conform Ordinului MCSI nr. 601/2019. (3) Auditul de securitate pentru stabilirea calității de operator de servicii esențiale, conform Legii nr. 362/2018.	x	x
	FA3	Standarde și specificații europene și internaționale aplicabile operatorilor de servicii esențiale, furnizorilor de servicii digitale și auditorilor de securitate cibernetică.	x	
	FA4	Evaluarea implementării cerințelor minime de asigurare a securității rețelelor și sistemelor informatice.	x	x
	FA5	Condiții și cerințe pentru auditorii de securitate cibernetică (1) Norme privind activitatea auditorilor. (2) Cerințe pentru auditorii de securitate cibernetică. (3) Codul etic al auditorului de securitate cibernetică.	x	x
	FA6	Auditul de securitate. (1) Desfășurarea auditului de securitate. (2) Documente de audit de securitate. (3) Cerințe referitoare la desfășurarea unui audit de securitate.	x	x
	FA7	Cerințe și recomandări privind întocmirea raportului de audit de securitate. Elaborare și completare raport de audit de securitate.	x	x
	FA8	Formulare/rapoarte utilizate în activitatea de audit de securitate. Modele și moduri de completare.		x
	FA9	Verificarea activității auditorilor de securitate cibernetică.	x	
	FA10	Roluri și responsabilități în baza Legii nr. 362/2018: (1) Coordonare strategică; (2) Autorități competente și responsabilități; Autoritatea competentă la nivel național	x	
		10 teme / nivel teoretic și practic	30 ore (15 ≥ IP ≥ 10)	

TEMATICA

pentru formarea membrilor echipelor CSIRT

Formarea profesională	Tema		Instruire	
			Teoretic ă	Practică
Formarea membrilor echipelor CSIRT	FE1	Alerte și avertizări. Modul de acțiune în cadrul alertelor și avertizărilor.	x	x
	FE2	Gestionarea, analiza și răspunsul în cazul vulnerabilităților identificate.	x	x
	FE3	Coordonarea răspunsului la vulnerabilitatea identificată.	x	x
	FE4	Analiza incidentelor de securitate cibernetică.	x	x
	FE5	Implementarea și evaluarea cerințelor minime de asigurare a securității rețelelor și sistemelor informatice	x	x
	FE6	Modalități și soluții de detectare a intruziunilor.	x	x
	FE7	Gestionarea artefactelor. Analiza, răspunsul și coordonarea răspunsului la artefacte.	x	x
	FE8	Continuitatea funcționării sistemelor și rețelelor informatice și recuperarea datelor în urma atacurilor cibernetice reușite.	x	x
	FE9	Exploatarea unei Platforme MISP și comunicarea cu echipa CSIRT națională.	x	x
	FE10	Stabilirea impactului unui incident de securitate cibernetică.	x	
	FE11	Analiza dinamică de risc de securitate cibernetică la nivelul operatorului esențial	x	
	FE12	Procesul de identificare a alertelor de securitate cibernetică, pregătirea documentelor de notificare și fluxul de notificare	x	x
	FE13	Analiza riscurilor de securitate la nivelul operatorului economic, conform standardelor și specificațiilor europene și internaționale stabilite prin Decizia directorului general CERT-RO nr. 88/2020.	x	
		13 teme / nivel teoretic și practic	30 ore (15 ≥ IP ≥ 10)	

TEMATICA
pentru formarea responsabililor cu securitatea rețelelor și sistemelor informatice

Formarea profesională	Tema		Instruire	
			Teoretic ă	Practică
Formarea responsabililor NIS	FI1	Termeni și noțiuni privind securitatea cibernetică aplicată la nivelul operatorilor de servicii esențiale și furnizorilor de servicii digitale în conformitate cu legislația în vigoare în domeniu securității cibernetică de la nivelul României și UE.	x	
	FI2	Mijloace și moduri de comunicare cu autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice stabilite în baza: (1) Legii nr. 362/2018; (2) a actelor normative subsecvente de nivel secundar și terțiar în aplicarea Legii nr. 362/2018; (3) OUG nr. 104/2021.	x	x
	FI3	Roluri și responsabilități în baza Legii nr. 362/2018: (3) Coordonare strategică; (4) Autorități competente și responsabilități; Autoritatea competentă la nivel național; Echipele de intervenție în caz de incidente de securitate informatică.	x	
	FI4	Normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale: (1) Implementarea cerințelor minime; (2) Monitorizarea aplicării; (3) Elaborarea raportului de conformitate.	x	x
	FI5	Analiza riscurilor de securitate la nivelul operatorului economic, conform standardelor și specificațiilor europene și internaționale stabilite prin Decizia directorului general CERT-RO nr. 88/2020.		x
	FI6	Procesul de identificare a alertelor de securitate cibernetică, pregătirea documentelor de notificare și fluxul de notificare.	x	x
	FI7	Procesul de identificare și stabilire a calității de operator de servicii esențiale: (1) Încadrarea operatorului economic ca furnizor de servicii esențiale. (2) Stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale. (3) Elaborarea și transmiterea documentație către autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice.		x
	FI8	Normele de aplicare a dispozițiilor privind verificarea și controlul îndeplinirii obligațiilor de securitate cibernetică pentru spațiul cibernetic național civil: (1) Monitorizare, supraveghere, control și sancționare.	x	
		8 teme / nivel teoretic și practic	30 ore (15 ≥ IP ≥ 10)	