



CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ – CERT-RO

DECIZIE nr. 88 din 30 aprilie 2020

privind aprobarea Listei standardelor și specificațiilor europene și internaționale

EMITENT

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ - CERT-RO

Publicat în MONITORUL OFICIAL nr. 465 din 2 iunie 2020

În temeiul art. 32 alin. (4) și (8) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare, denumită în continuare *Legea NIS*, pentru implementarea cerințelor minime de securitate în rețelele și sistemele informatice care asigură furnizarea serviciilor esențiale ori furnizează serviciile digitale identificate în temeiul Legii NIS,

în vederea asigurării desfășurării activității de audit de securitate a rețelelor și sistemelor informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale,

în calitate de autoritate competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice care asigură furnizarea serviciilor esențiale ori furnizează serviciile digitale,

în temeiul prevederilor art. 12 alin. (5) și (8) din Hotărârea Guvernului nr. 494/2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO,

directorul general al Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO emite prezenta decizie.

Articolul 1

Se aprobă **Lista standardelor și specificațiilor europene și internaționale**, denumită în continuare *LSSEINIS*, prevăzută în anexa care face parte integrantă din prezenta decizie.

Articolul 2

(1) *LSSEINIS* este aplicabilă atât operatorilor de servicii esențiale și furnizorilor de servicii digitale, cât și auditorilor de securitate a rețelelor și sistemelor informatice.

(2) Standardele și/sau specificațiile europene și internaționale se aplică individual sau grupate în funcție de domeniile, subdomeniile, măsurile și cerințele de securitate, după caz, stabilite în conformitate cu normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice.

Articolul 3

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

Directorul general al Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO,

Cătălin-Petrică ARAMĂ

București, 30 aprilie 2020

Nr. 88

LISTA
standardelor și specificațiilor europene și internaționale

Nr. crt.	Standarde & Specificații europene și internaționale	Emitent	Domenii de securitate aplicabile			
			Governanță	Protecție	Apărare	Reziliență
1.	ISO/IEC 27001:2013. Tehnologia informației – Tehnici de securitate – Sisteme de gestionare a securității informațiilor – Cerințe.	Organizația Internațională de Standardizare (ISO)	X	X	X	X
2.	ISO/IEC 27002:2013. Tehnologia informației – Tehnici de securitate – Cod de practică pentru controale de securitate a informațiilor.	ISO	X	X	X	X
3.	ISO/IEC 27003:2017. Tehnologia informației – Tehnici de securitate – Sisteme de gestionare a securității informațiilor – Ghid.	ISO		X	X	
4.	ISO/IEC 27004:2016. Tehnologia informației – Tehnici de securitate – Managementul securității informației - Monitorizare, măsurare, analiză și evaluare.	ISO		X	X	
5.	ISO/IEC 27005:2018. Tehnologia informației – Tehnici de securitate – Managementul riscului pentru securitatea informațiilor.	ISO	X			X
6.	ISO/IEC 27010:2015. Tehnologia informației – Tehnici de securitate – Managementul securității informațiilor pentru comunicații intersectoriale și inter-organizaționale.	ISO	X			
7.	ISO/IEC 27013:2015. Tehnologia informației – Tehnici de securitate – Ghid privind implementarea integrată a ISO / IEC 27001 și ISO / IEC 20000-1.	ISO	X	X	X	X
8.	ISO/IEC 27014:2013. Tehnologia informației – Tehnici de securitate - Guvernarea securității informațiilor.	ISO	X			
9.	ISO/IEC 20000-1:2018. Tehnologia informației – Managementul serviciilor – Partea 1: Cerințe de sistem de gestionare a serviciilor.	ISO	X	X	X	X
10.	ISO/IEC 21827:2008. Tehnologia informației – Tehnici de securitate – Ingineria securității sistemelor – Modelul maturității capabilității® (SSE-CMM®).	ISO			X	
11.	ISO/IEC/IEEE 12207:2017. ISO / IEC / IEEE 12207: 2017. Ingineria sistemelor și a software-ului – Procese ale ciclului de viață software.	ISO	X	X		
12.	ISO/IEC 10181-2:1996. ISO / IEC 10181-2: 1996. Tehnologia informației - Interconectare sisteme deschise - Cadre de securitate pentru sisteme deschise: Cadru de autentificare.	ISO		X		
13.	ISO/IEC 10181-3:1996. ISO / IEC 10181-3: 1996. Tehnologia informației – Interconectare sisteme deschise – Cadre de securitate pentru sisteme deschise: Cadru de control al accesului.	ISO		X		
14.	ISO/IEC 19790:2012. ISO / IEC 19790: 2012 Tehnologia informației – Tehnici de securitate – Cerințe de securitate pentru module criptografice.	ISO		X		
15.	ISO/IEC 11770-1:2010. ISO / IEC 11770-1: 2010. Tehnologia informației – Tehnici de securitate – Management cheie- Partea 1: Cadru.	ISO		X		
16.	ISO/IEC 11770-5:2011. SO / IEC 11770-5: 2011. Tehnologia informației – Tehnici de securitate – Management cheie – Partea 5: Managementul cheie de grup.	ISO		X		
17.	ISO/IEC 27032:2012. ISO / IEC 27032: 2012. Tehnologia informației – Tehnici de securitate – Linii directe pentru securitatea cibernetică.	ISO		X	X	X
18.	ISO/IEC 27033-1:2015. SO / IEC 27033-1: 2015. Tehnologia informației – Tehnici de securitate – Securitatea rețelei – Partea 1: Prezentare generală și concepte.	ISO	X	X		
19.	ISO/IEC 27033-2:2012. ISO / IEC 27033-2: 2012. Tehnologia informației – Tehnici de securitate – Securitatea rețelei – Partea 2: Linii directe pentru proiectarea și implementarea securității rețelei.	ISO		X		
20.	ISO/IEC 27033-3:2010. ISO / IEC 27033-3: 2010. Tehnologia informației – Tehnici de securitate – Securitatea rețelei – Partea 3: Scenarii rețea de referință – Amenințări, tehnici de proiectare și probleme de control.	ISO			X	
21.	ISO/IEC 27033-4:2014. ISO / IEC 27033-4: 2014. Tehnologia informației - Tehnici de securitate – Securitate rețea – Partea 4:	ISO		X	X	

Nr. crt.	Standarde & Specificații europene și internaționale	Emitent	Domenii de securitate aplicabile			
			Guvernanță	Protecție	Apărare	Reziliență
	Securizarea comunicațiilor între rețele folosind gateway-uri de securitate.					
22.	ISO/IEC 27033-5:2013. ISO / IEC 27033-5: 2013. Tehnologia informației — Tehnici de securitate – Securitate rețea – Partea 5: Securizarea comunicațiilor prin rețele folosind rețele virtuale private (RVP).	ISO		X	X	
23.	ISO / IEC 27033-6: 2016. Tehnologia informației – Tehnici de securitate – Securitate rețea – Partea 6: Securizarea accesului la rețeaua IP wireless.	ISO		X	X	
24.	ISO/IEC 27034-1:2011. Tehnologia informației - Tehnici de securitate - Securitatea aplicațiilor - Partea 1: Prezentare generală și concepte.	ISO		X	X	
25.	ISO/IEC 27034-5:2017. Tehnologia informației - Tehnici de securitate - Securitatea aplicațiilor - Partea 5: Structura datelor de protocoale și securitatea aplicațiilor.	ISO		X		
26.	TR 103 305-1 V3.1.1 (2018-09). CYBER; Controale critice de securitate pentru o apărare cibernetică eficientă; Partea 1: Controalele critice de securitate.	Institutul European de Standardizare în Telecomunicații (ETSI)	X	X	X	X
27.	TR 103 305-2 V2.1.1 (2018-09). CYBER; Controale critice de securitate pentru o apărare cibernetică eficientă; Partea 2: Măsurare și audit.	ETSI			X	
28.	TR 103 305-3 V2.1.1 (2018-09). CYBER; Controale critice de securitate pentru o apărare cibernetică eficientă; Partea 3: Implementarea sectorului de servicii	ETSI	X	X		
29.	TR 103 305-4 V2.1.1 (2018-09). CYBER; Controale critice de securitate pentru o apărare cibernetică eficientă; Partea 4: Mecanisme de facilitare.	ETSI	X			
30.	TR 103 305-5 V1.1.1 (2018-09). CYBER; Controale critice de securitate pentru o apărare cibernetică eficientă; Partea 5: Îmbunătățirea confidențialității.	ETSI	X		X	
31.	TR 103 304 V1.1.1 (2016-07). CYBER; Protecția informațiilor personale (PII) în serviciile mobile și cloud.	ETSI		X		
32.	TS 103 307 V1.3.1 (2018-04). CYBER; Aspecte de securitate pentru interfețele LI și RD.	ETSI		X		
33.	TR 103 331 V1.2.1 (2019-09). CYBER; Schimb de informații amenințate structurate.	ETSI		X	X	
34.	TR 103 369 V1.1.1 (2016-07). CYBER; Proiectare cerințe de ecosistem.	ETSI	X			
35.	TR 103 370 V1.1.1 (2019-01). Ghid practic introductiv la standardele tehnice pentru confidențialitate.	ETSI	X	X	X	X
36.	TR 103 303 V1.1.1 (2016-04). CYBER; Măsuri de protecție pentru ICT(Tehnologia informației și comunicațiilor) în contextul infrastructurii critice.	ETSI		X		X
37.	TS 103 458 V1.1.1 (2018-06). CYBER; Aplicarea criptării bazată pe atribute (ABE) pentru protecția PII și a datelor cu caracter personal pe dispozitive IoT, WLAN, cloud și servicii mobile – Cerințe la nivel înalt.	ETSI		X		
38.	TS 103 487 V1.1.1 (2016-04). CYBER; Cerințe de securitate de bază privind funcțiile sensibile pentru NFV(Virtualizarea funcției de rețea)și platformele conexe.	ETSI		X	X	X
39.	TR 103 308 V1.1.1 (2016-01). CYBER; Linie de bază de securitate privind interceptarea legală (LI) și datele păstrate (RD) pentru Virtualizarea funcției de rețea (NFV) și platformele conexe.	ETSI		X		X
40.	TR 103 306 V1.4.1 (2020-03). CYBER; Ecosistemul securității cibernetică globale.	ETSI	X			
41.	TR 103 309 V1.1.1 (2015-08). CYBER; Protecție implicită – tehnologie de securitate a platformei.	ETSI	X	X	X	X
42.	TR 103 305 V1.1.1 (2015-05). CYBER; Controale critice de securitate pentru o apărare cibernetică eficientă.	ETSI			X	X
43.	GS ISI 007 V1.1.1 (2018-12). Indicatori de securitate a informațiilor (ISI); Linii directe pentru construirea și exploatarea unui centru securizat de operațiuni de securitate (SOC).	ETSI		X	X	X
44.	GS ISI 008 V1.1.1 (2018-06). Indicatori de securitate a informațiilor (ISI); Descrierea unei abordări generale de	ETSI			X	

Nr. crt.	Standarde & Specificații europene și internaționale	Emitent	Domenii de securitate aplicabile			
			Guvernanță	Protecție	Apărare	Reziliență
	gestionare a informațiilor de securitate și evenimente (SIEM) la nivelul întregii organizații.					
45.	EG 203 310 V1.1.1 (2016-06). CYBER; Impactul informaticii cuantice asupra securității sistemelor de Tehnologia informațiilor și comunicațiilor (ICT); Recomandări privind continuitatea activității și selectarea algoritmului.	ETSI				X
46.	ANSI/ISA 18.2:2016 Managementul sistemelor de alarmă pentru procesul industrial.	Societatea Internațională de Automatizare (ISA)	X	X		
47.	ISA 62443-1-1:2007 Securitate pentru sisteme de automatizare și control industrial. Partea 1-1: Terminologie, concepte și modele.	ISA	X	X	X	X
48.	ISA 62443-2-1:2009. Securitate pentru sisteme de automatizare și control industrial. Partea 2: Stabilirea unui program de securitate a sistemelor de automatizare industrială și control.	ISA		X		
49.	ANSI/ISA 62443-3-3:2013 Securitate pentru sisteme de automatizare și control industrial. Partea 3-3: Cerințe de securitate a sistemului și niveluri de securitate.	ISA		X	X	
50.	FIPS PUB 140-2 Cerințe de securitate pentru modulele criptografice.	Institutul National de Standarde și Tehnologie (NIST)		X		
51.	FIPS PUB 200 Cerințe minime de securitate pentru informații federale și sisteme de informații.	NIST	X	X	X	X
52.	SP 800-30 Ghid managementul riscului pentru sistemele de tehnologie a informației.	NIST	X	X		X
53.	SP 800-53, Revizia 4, Controale de securitate și confidențialitate pentru sisteme informaționale federale și organizații.	NIST	X	X		
54.	SP 800-150 Ghid pentru schimbul de informații despre amenințarea cibernetică.	NIST	X		X	
55.	SP 800-181 Inițiativa națională pentru educația în domeniul securității cibernetice (NICE). Cadrul forței de muncă pentru securitate cibernetică.	NIST	X	X		
56.	SP 1800-14 Protejarea integrității rutării pe Internet: validarea originii rutelor Protocolului BGP.	NIST		X		
57.	SP 1800-12 Certificate de verificare PIV derivate.	NIST		X		
58.	SP 1800-5 Managementul activelor IT.	NIST	X			X
59.	SP 1800-4 Securitatea dispozitivelor mobile: platforme cloud și hibrid.	NIST		X		
60.	Cadru pentru îmbunătățirea securității cibernetice a infrastructurii critice, versiunea 1.1	NIST	X	X	X	X
61.	IEC 62443-4-2:2019, Securitate pentru sisteme de automatizare și control industrial - Partea 4-2: Cerințe tehnice de securitate pentru componentele IACS.	Comisia Electrotehnică Internațională (IEC)		X		
62.	IEC 62443-4-1:2018, Securitate pentru sisteme de automatizare și control industrial - Partea 4-1: Cerințe de securitate pentru dezvoltarea vieții produsului.	IEC		X		X
63.	IEC 62443-2-1:2010, Rețele de comunicații industriale - Securitatea rețelelor și a sistemului - Partea 2-1: Stabilirea unui program de securitate a sistemului de automatizare și control industrial.	IEC	X	X		
64.	IEC TS 62443-1-1:2009, Rețele de comunicații industriale - Securitatea rețelei și a sistemului - Partea 1-1: Terminologie, concepte și modele.	IEC	X	X	X	X
65.	IEC 62443-2-1:2010, Rețele de comunicații industriale - Securitatea rețelei și a sistemului - Partea 2-1: Stabilirea unui program de securitate a sistemului de automatizare și control industrial.	IEC	X	X		
66.	API STD 1164 Securitatea controlorului și supravegherea achiziției de date (SCADA) în domeniul conductelor .	Institutul American al Petrolului (API)		X	X	
67.	COBIT® 2019 Cadru: Introducere și metodologie.	Asociația de Audit și Control a Sistemelor Informaționale (ISACA)	X	X	X	X
68.	COBIT 5 pentru securitatea informațiilor.	ISACA	X	X	X	X
69.	Modelul de afaceri pentru securitatea informațiilor (BMIS).	ISACA				X
70.	CRAMM Versiunea 5.1 Ghid de utilizare.	CESG/ GOV.UK	X	X	X	X
71.	Model de maturitate al managementului securității informațiilor (O-ISM3).	Open Group			X	X

Nr. crt.	Standarde & Specificații europene și internaționale	Emitent	Domenii de securitate aplicabile			
			Guvernanță	Protecție	Apărare	Reziliență
72.	Controale CIS, Versiunea 7.1.	Centrul pentru Securitatea Internetului	X	X	X	X
73.	Manualul de examinare al FFIEC .	Consiliul Federal de Examinare a Instituțiilor Financiare (FFIEC)	X	X	X	X
74.	Managementul serviciilor IT (ITIL) v3	Set de practici în managementul serviciilor IT (ITIL)	X	X	X	X
75.	Cadru de evaluare a amenințărilor, a activelor și a vulnerabilității critice din punct de vedere operațional (OCTAVE)	Universitatea Carnegie Mellon	X	X		
76.	CIP Versiunea 5	Corporația Nord Americană de Încredere Electrică (NERC)	X	X	X	X
77.	Securitatea informațiilor general acceptate.	Asociația de Securitate a Sistemelor Informaționale	X	X	X	X
78.	Cele zece cele mai mari riscuri de securitate pentru aplicații web.	The Open Web Application Security Project	X	X	X	X
79.	Norme tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale.	CERT-RO/ GOV.RO	X	X	X	X
80.	Norme tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile furnizorilor de servicii digitale.	CERT-RO/ GOV.RO	X	X	X	X