Ghid Complet

Conformitatea cu OUG nr. 155/2024

NIS2@RO - Securitate Cibernetică

Parcursul documentelor și termenelor pentru entități

nis2consult.ro

Prezentare Generală

Ce este OUG nr. 155/2024?

Ordonanța de Urgență nr. 155/2024 transpune Directiva NIS2 în legislația română, stabilind un cadru cuprinzător pentru securitatea cibernetică la nivel național.

Entități Vizate

Entitățile din sectoarele din Anexele 1 și 2 care își desfășoară activitatea în România și îndeplinesc criteriile de dimensiune specificate.

Termen limită pentru notificare: 30 de zile de la intrarea în vigoare

Domenii Cheie de Conformitate

Notificare și înregistrare, evaluarea riscurilor, autoevaluarea maturității, auditurile de securitate și raportarea incidentelor.

1

Notificarea Inițială și Înregistrarea

Termen: 30 de zile de la intrarea în vigoare a OUG nr. 155/2024

Informații Necesare

- Date de identificare ale entității (denumire, CUI, adresă)
- Activitatea desfășurată (coduri CAEN)
- Dimensiunea entității (salariați, cifra de afaceri)
- Persoana responsabilă cu securitatea cibernetică

Modalități de Transmitere

Principal: Platforma NIS2@RO

Alternativ: E-mail la evidenta@dnsc.ro sau depunere fizică

Platforma NIS2@RO

Instrumentul principal de notificare

2

Evaluarea Nivelului de Risc

Termen: 60 de zile de la comunicarea deciziei de înregistrare

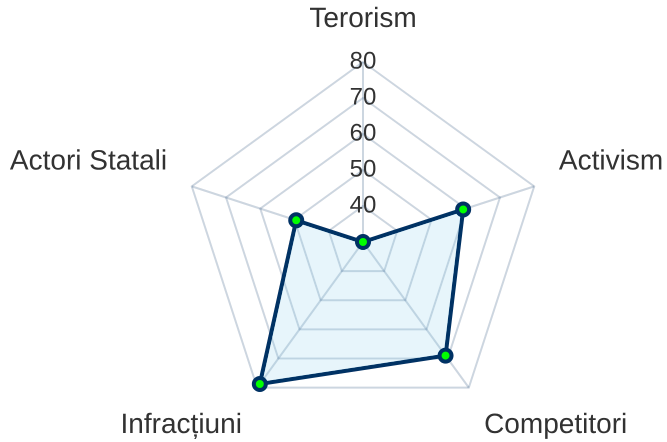
Metodologia de Evaluare

Entitățile utilizează Instrumentul ENIRE@RO sau Platforma NIS2@RO pentru calculul nivelului de risc, considerând dimensiunea entității, natura atacului, impactul și probabilitatea de materializare.

Categorii de Cerințe de Securitate

- **Basic** - **0-99 puncte**
- **Important** - **100-199 puncte**
- **Esențial** - **200-1500 puncte**
- **Excepții:** Sectorul bancar, TIC B2B

Tipologii de Actori și Atacuri



3

Autoevaluarea Nivelului de Maturitate

Termen: Anual + Prima evaluare în 60 de zile de la evaluarea riscului

Procesul de Autoevaluare

1. Evaluarea măsurilor de gestionare a riscurilor
2. Identificarea nivelului de maturitate
3. Elaborarea raportului de autoevaluare
4. Asumarea raportului de către management

Documentul Rezultat

Raportul trebuie să reflecte starea reală a măsurilor implementate și să identifice ariile care necesită îmbunătățiri.

> *Notă: Entitățile esențiale trebuie să întocmească și un plan de măsuri pentru remedierea deficiențelor în termen de 30 de zile.*

Evaluare Continuă

Îmbunătățire Permanentă

4

Planul de Măsuri pentru Remedierea Deficiențelor

Termen: 30 de zile de la realizarea autoevaluării

Aplicabilitate

Obligatoriu doar pentru Entitățile Esențiale conform clasificării din OUG nr. 155/2024.

Procesul de Remediere

1. **Identificarea Deficiențelor**
   În urma autoevaluării
2. **Elaborarea Planului**
   Asumat de management
3. **Transmiterea către DNSC**
   În termen de 30 de zile
4. **Implementarea Măsurilor**
   Conform termenelor asumate

Plan de Măsuri

Remediere Deficiențe

5

Auditul de Securitate Cibernetică

Când se realizează auditul?

- Periodic: Conform ordinului Directorului DNSC
- Ad-hoc: La solicitarea motivată a DNSC
- După un incident semnificativ sau schimbări majore

Cine realizează auditul?

Auditorii de securitate cibernetică atestați de DNSC.
Costurile sunt suportate de entitatea auditată.

Procesul post-audit

- Transmiterea rezultatelor către DNSC în termen de 5 zile
- Întocmirea planului de măsuri în 15 zile lucrătoare
- Notificarea implementării măsurilor în 5 zile de la termen

6

Raportarea Incidentelor de Securitate

Entitățile esențiale și importante trebuie să raporteze orice incident cu impact semnificativ.

Termene de Raportare

24 ore	Avertizare timpurie
72 ore	Raportare inițială
30 zile	Raport final
La cerere	Raport intermediar

Platforma de Raportare

Raportarea se face prin Platforma Națională pentru Raportarea Incidentelor de Securitate Cibernetică (PNRISC).

Conținutul Raportului Final

Descriere detaliată, tipul amenințării, măsurile aplicate și impactul transfrontalier.

7

Raportarea Voluntară și Vulnerabilități

Raportarea Voluntară

Entitățile pot raporta voluntar:

- Incidente și amenințări cibernetice
- Incidente evitate la limită

Nu impune obligații suplimentare

Raportarea Vulnerabilităților

Orice persoană poate raporta DNSC vulnerabilități în termen de 48 ore de la identificare.

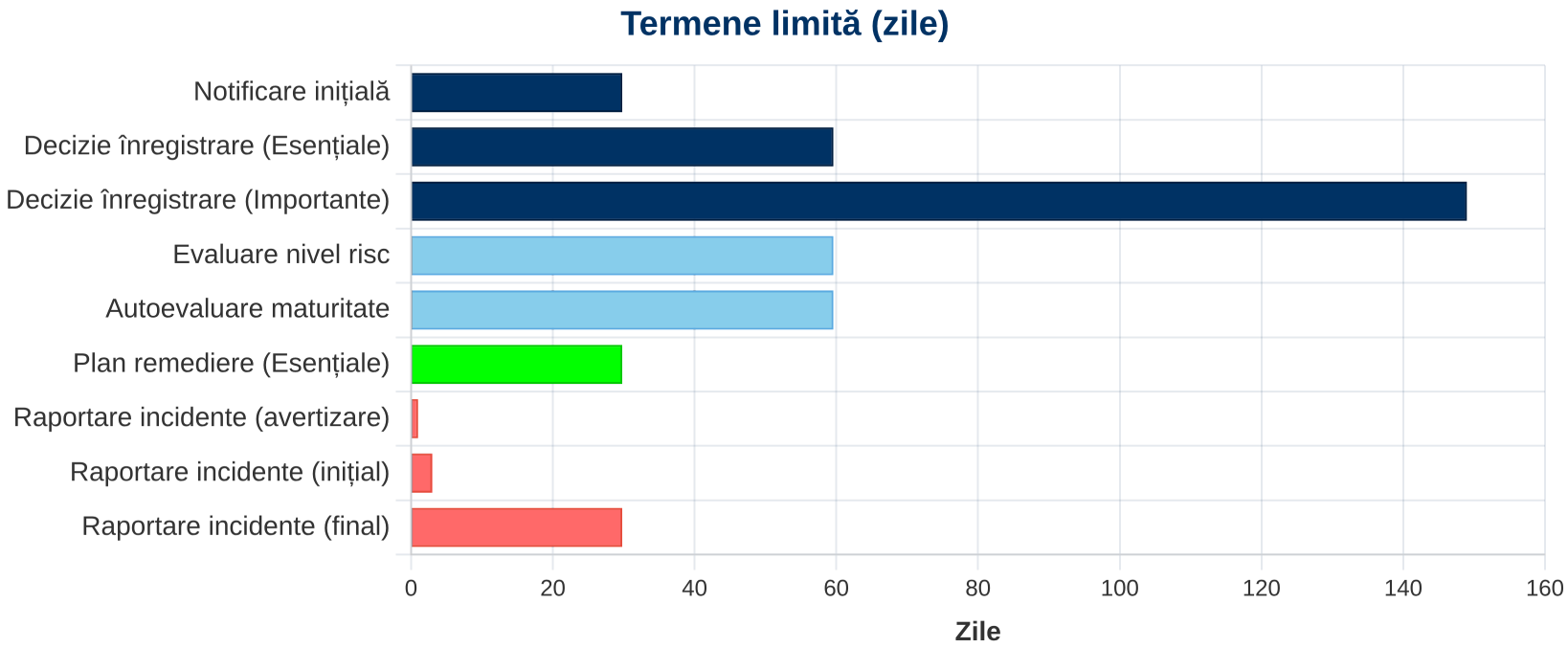
- Primirea și remedierea vulnerabilităților
- Cooperarea cu DNSC

Obligații pentru Entități

Entitățile esențiale/importante trebuie să instituie procese de management al vulnerabilităților TIC și să publice modalitățile de contact pentru raportare.

Cronologia Obligațiilor

Termene Cheie pentru Conformitate



Notificare și Înregistrare
Evaluare și Raportare
Remediere și Audit
Incidente și Vulnerabilități

** Termenele sunt calculate de la momentul de referință specificat în OUG nr. 155/2024*

Securitate Cibernetică

Protejarea Infrastructurii Digitale

Puncte Cheie de Reținut

- Notificarea inițială trebuie realizată în cel mult 30 de zile de la intrarea în vigoare a OUG
- Actualizarea informațiilor din notificare: 15 zile pentru date de identificare, 90 zile pentru alte informații
- Raportarea incidentelor semnificative: avertizare în 24h, raport inițial în 72h, raport final în 30 zile