
ProDefence
NIS2 România
Conformare, securitate cibernetică și reziliență operațională
Directiva (UE) 2022/2555 • OUG nr. 155/2024 • Legea nr. 124/2025
Cadru de referință pentru entități esențiale și importante
EUROPEAN DIRECTIVE
NIS 2.0

Angheluș Alexandru

Expert în securitate cibernetică • Consultant NIS2 • Auditor acreditat de Directoratul Național de Securitate Cibernetică



Mesajul autorului

Implementarea cerințelor NIS2 nu înseamnă doar conformitate, ci consolidarea reală a capacității unei organizații de a preveni, detecta și răspunde la incidente cibernetice.

Măsurile de securitate, analiza riscurilor, responsabilitățile clare și documentarea corectă contribuie direct la reziliența operațională și la protejarea serviciilor esențiale.

NIS2 trebuie privită ca un cadru de maturizare: investiția de astăzi în guvernanță, procese și controale reduce impactul incidentelor de mâine și crește încrederea în organizație.

ProDefence

NIS2 ROMÂNIA

Securitate cibernetică. Reziliență digitală. Încredere în viitor.

Directiva NIS2 întărește securitatea rețelelor și a sistemelor informatice esențiale pentru o economie și o societate digitală rezilientă.

- Protejăm serviciile esențiale și cetățenii
- Consolidăm încrederea și continuitatea
- Construim împreună un viitor digital sigur



SECURITATE
Întărim apărarea împotriva amenințărilor cibernetice

REZILIENȚĂ
Asigurăm continuitatea serviciilor esențiale și a operațiunilor

CONFORMITATE
Aliniem la cerințele NIS2 și la cadrul european

RESPONSABILITATE
Clarificăm rolurile și responsabilitățile în întreaga organizație

TRANSPARENȚĂ
Îmbunătățim raportarea și schimbul de informații la nivel național și UE

COLABORARE
Parteneriat între sectorul public și privat pentru un ecosistem digital sigur

Împreună, construim o Românie digitală, sigură și rezilientă.

Ce este NIS2 și transpunerea directivei în România

Directiva (UE) 2022/2555 și cadrul de implementare în România

Repere: Directiva (UE) 2022/2555, OUG nr. 155/2024, Legea nr. 124/2025, Ordinul DNSC nr. 1/2025 și Ordinul DNSC nr. 2/2025

CE ESTE NIS2?

1. **Directivă europeană**
   - cadru comun de securitate cibernetică
   - pentru un nivel ridicat de reziliență
   - aplicabil în Uniunea Europeană
2. **Domeniu extins**
   - 18 sectoare critice
   - Anexa 1 și Anexa 2
   - mai multe entități decât NIS1
3. **Tipuri de entități**
   - entități esențiale
   - entități importante
   - criterii sectoriale și dimensionale
4. **Obligații principale**
   - gestionarea riscurilor
   - măsuri tehnice și organizatorice
   - raportarea incidentelor
5. **Guvernanță și responsabilitate**
   - implicarea managementului
   - continuitate și reziliență
   - control și audit

DE LA DIRECTIVA EUROPEANĂ LA IMPLEMENTAREA NAȚIONALĂ



14 decembrie 2022
– adoptarea NIS2

16 ianuarie 2023
– intrarea în vigoare

transpunere în legislația națională

TRANSPUNEREA ÎN ROMÂNIA

1. **Act normativ principal**
   - OUG nr. 155/2024
   - instituie cadrul național pentru securitatea cibernetică
2. **Aprobarea legislativă**
   - Legea nr. 124/2025
   - modificări și completări confirmă cadrul de aplicare
3. **Autoritate competentă**
   - DNSC
   - înregistrare și supraveghere
   - cooperare și notificare
4. **Legislație subsecventă**
   - Ordinul DNSC nr. 1/2025
   - procesul de notificare
   - transmiterea informațiilor
5. **Evaluare și risc**
   - Ordinul DNSC nr. 2/2025
   - criterii și praguri
   - evaluarea nivelului de risc
6. **Efecte pentru organizații**
   - verificarea încadrării
   - notificare către DNSC
   - conformare, audit, raportare

ELEMENTE-CHEIE

directivă UE | 18 sectoare | entități esențiale | entități importante | DNSC | OUG 155/2024

Schemă explicativă orientativă privind NIS2 și transpunerea directivei în România.

Rolul DNSC în NIS2 România

Autoritatea competentă pentru coordonare, notificare, supraveghere și răspuns la incidente

Repere: OUG nr. 155/2024, Legea nr. 124/2025, Ordinul DNSC nr. 1/2025, Ordinul DNSC nr. 2/2025 și Ordinul DNSC nr. 3/2025



1. Autoritate competentă

- aplică cadrul NIS2 în România
- coordonează implementarea
- stabilește mecanisme și proceduri

2. Înregistrare și încadrare

- primește notificările entităților
- analizează datele transmise
- emite decizia de încadrare / neîncadrare

3. Platforme și instrumente

- NIS2@RO pentru notificare
- ENIRE@RO pentru evaluarea riscului
- sprijină pentru autoevaluare și conformare

4. Supraveghere și control

- monitorizează respectarea obligațiilor
- verificare și control pe bază de risc
- poate solicita informații și dovezi

5. Raportare incidente și CSIRT

- primește notificările de incident
- coordonează răspunsul și schimbul de informații
- sprijină gestionarea incidentelor semnificative

6. Ghidare și cooperare

- publică ghiduri, ordine și repere
- cooperează cu autorități și entități relevante
- susține conștientizarea și implementarea

Ce înseamnă pentru organizații

notificare | încadrare | evaluare risc | raportare incidente | supraveghere

Schemă explicativă orientativă privind rolul DNSC în cadrul NIS2 România.

Rolul responsabilului NIS / responsabilului de securitate

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — implementare, monitorizare, raportare și coordonare

1 Coordonare implementare



- coordonează aplicarea măsurilor NIS2
- urmărește planul de implementare
- colaborează cu managementul și echipele tehnice

2 Monitorizare riscuri



- urmărește riscurile cibernetice relevante
- verifică evoluția vulnerabilităților și amenințărilor
- susține actualizarea registrului de riscuri

3 Comunicare cu DNSC



- punct de contact operațional
- transmite informații și clarificări
- susține notificările și schimbul de date

4 Urmărire incidente



- monitorizează gestionarea incidentelor
- coordonează escaladarea internă
- sprijină raportarea incidentelor semnificative

Responsabilul NIS transformă cerințele de securitate în acțiuni urmărite, documentate și coordonate operațional.

5 Evidențe și documentație



- menține dovezi, proceduri și registre
- organizează documentația de conformare
- asigură trasabilitatea măsurilor

6 Pregătire audit



- pregătește informațiile și dovezile pentru audit
- verifică stadiul măsurilor și controalelor
- susține remedierea deficiențelor

7 Raportare internă



- informează managementul periodic
- raportează progres, riscuri și blocaje
- sprijină deciziile privind prioritățile și resursele

Cum se vede rolul în practică

implementare → monitorizare → DNSC → incidente → documente → audit → raportare

Mesaj-cheie: Responsabilul NIS nu este doar un rol formal. El conectează managementul, operaționalul și obligațiile de conformare într-un flux continuu de coordonare și control.

ⓘ Schemă explicativă orientativă privind rolul responsabilului NIS / responsabilului de securitate în România.

Responsabilitățile managementului sub NIS2

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — guvernanță, responsabilitate, resurse, supraveghere și raportare

1 Aprobarea măsurilor



- aprobarea politicilor
- aprobarea măsurilor tehnice, organizatorice și operaționale
- validarea direcției de conformare

2 Asumarea riscurilor



- înțelegerea riscurilor cibernetice
- acceptarea riscurilor reziduale
- decizii informate privind tratamentul riscurilor

3 Alocarea bugetului



- resurse financiare
- resurse umane
- investiții în securitate
- suport pentru implementare

4 Supravegherea implementării



- monitorizarea progresului
- urmărirea planului de măsuri
- verificarea termenelor și a responsabililor

Managementul nu are un rol simbolic. Sub NIS2, conducerea aprobă, susține, supraveghează și răspunde pentru implementarea măsurilor.

7 Raportare către autorități



- susținerea notificării și raportării
- transmiterea informațiilor relevante
- cooperarea cu DNSC și autoritățile competente

5 Instruire



- formarea conducerii
- susținerea instruirii personalului
- dezvoltarea culturii de securitate cibernetică

6 Răspundere



- responsabilitatea managementului
- obligația de implicare
- consecințe pentru lipsa conformării

Cum se reflectă implicarea managementului

decizie → resurse → implementare → monitorizare → raportare

Mesaj-cheie: Fără implicarea reală a conducerii, conformarea NIS2 rămâne formală și vulnerabilă.

Schemă explicativă orientativă privind responsabilitățile managementului sub NIS2 în România.

Cele 18 sectoare NIS2 explicate vizual

Hartă vizuală a sectoarelor acoperite în România

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — Anexa nr. 1 și Anexa nr. 2

Anexa nr. 1 – Sectoare de înaltă criticitate

11 sectoare



1. Energie



2. Transport



3. Bănci



4. Infrastructuri ale pieței financiare



5. Sănătate



6. Apă potabilă



7. Ape uzate



8. Infrastructură digitală



9. Management servicii TIC (B2B)



10. Administrație publică



11. Spațiu

Anexa nr. 2 – Alte sectoare critice

7 sectoare



12. Servicii postale și curierat



13. Gestionarea deșeurilor



14. Substanțe chimice



15. Alimente



16. Producție / fabricare



17. Furnizori digitali



18. Cercetare

Ce contează pentru încadrare



sectorul și tipul serviciului



dimensiunea organizației



rol critic / furnizor unic



criterii speciale prevăzute de lege



Mesaj-cheie: NIS2 acoperă 18 sectoare, dar încadrarea unei organizații se stabilește în funcție de sector, serviciul prestat, dimensiune și criteriile speciale aplicabile.



Schemă explicativă orientativă pentru domeniul de aplicare NIS2 în România.

Criteriile dimensionale NIS2

Micro, mică, medie si mare întreprindere – cum contează în NIS2 România

Repere: OUG nr. 155/2024, Legea nr. 124/2025, Legea nr. 346/2004 — art. 8 și art. 9

Clasificarea dimensională

1 Microîntreprindere



- mai puțin de 10 angajați
- cifră de afaceri anuală netă ≤ 2 mil. euro
- și/sau bilanț total ≤ 2 mil. euro

de regulă, nu intră prin criteriul dimensional, dar poate intra în cazuri speciale

2 Întreprindere mică



- mai puțin de 50 angajați
- cifră de afaceri anuală netă ≤ 10 mil. euro
- și/sau bilanț total ≤ 10 mil. euro

în mod obișnuit, nu intră doar prin dimensiune; se verifică și excepțiile

3 Întreprindere mijlocie



- mai puțin de 250 angajați
- cifră de afaceri anuală netă ≤ 50 mil. euro
- și/sau bilanț total ≤ 43 mil. euro

poate intra sub NIS2 în anumite sectoare sau situații speciale

4 Întreprindere mare



- depășește pragurile întreprinderii mijlocii
- peste 250 angajați sau peste pragurile financiare
- categoria cel mai frecvent vizată de NIS2

în multe situații, reprezintă baza încadrării în anexele NIS2

Praguri de încadrare

angajați → cifră de afaceri → bilanț → categoria întreprinderii → verificare NIS2

Excepții importante

- încadrarea NIS2 nu depinde exclusiv de dimensiune
- unele entități pot intra și sub pragurile IMM
- se verifică sectorul, serviciul prestat și rolul organizației
- dimensiunea este un filtru de bază, nu singurul criteriu

Cazuri speciale NIS2

- furnizor unic al unui serviciu esențial
- impact semnificativ asupra siguranței, sănătății sau ordinii publice
- risc sistemic sau impact transfrontalier
- importanță națională ori regională
- anumite entități pot fi vizate indiferent de dimensiune

Exemple orientative

- administrație publică centrală
- entități critice identificate
- furnizori DNS / registre TLD
- prestatori de servicii de încredere calificați
- anumite entități din comunicații electronice și servicii de securitate gestionate

Mesaj-cheie

În NIS2, dimensiunea contează, dar nu decide singură. După stabilirea categoriei micro / mică / medie / mare, trebuie analizate și sectorul, serviciul prestat și situațiile speciale prevăzute de lege.

Schemă explicativă orientativă pentru clasificarea dimensională relevantă în evaluarea încadrării NIS2 în România.

Excepțiile de la criteriul dimensional

Când o organizație se poate încadra sub NIS2 chiar dacă nu este medie sau mare

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — art. 5, art. 6, art. 9, art. 10

1. Furnizor unic



- singurul furnizor al unui serviciu esențial
- întreruperea poate afecta activități critice
- relevanță poate justifica încadrarea

2. Serviciu critic



- serviciu esențial pentru societate sau economie
- importanța serviciului contează mai mult decât dimensiunea
- se analizează rolul real al entității

3. Impact sistemic



- perturbarea poate produce efecte în lanț
- impact asupra sectoarelor critice sau asupra publicului
- criterii relevante pentru încadrare

4. Risc transfrontalier



- perturbarea poate avea efecte în alte state membre
- relevanță pentru servicii cu interdependențe europene
- riscul extins poate susține încadrarea

Dimensiunea NU este singurul criteriu

În anumite situații speciale încadrarea se poate face și sub pragurile IMM.

5. Administrație publică



- anumite entități de administrație publică intră prin natura rolului lor
- nu se aplică exclusiv logica de dimensiune comercială
- analiza se face conform cadrului legal aplicabil

6. Infrastructură digitală



- anumite entități din infrastructura digitală pot fi vizate special
- relevanța serviciilor furnizate este esențială
- se verifică subsectorul și tipul entității

7. Decizie autoritate competentă



- DNSC poate identifica entități pe baza criteriilor speciale
- se evaluează rolul, impactul și riscul
- rezultatul poate fi încadrarea ca entitate esențială sau importantă

Cum se analizează excepția



sectorul și serviciul



rolul organizației



impactul potențial



criterii speciale art. 9–10



decizie de încadrare

Mesaji-cheie:

În NIS2 România, o organizație nu este exclusă automat doar pentru că nu este medie sau mare.
Dacă are rol critic, impact semnificativ sau se află într-o situație specială, poate intra sub incidența legii.

Schemă explicativă orientativă privind excepțiile de la criteriul dimensional în evaluarea încadrării NIS2 în România.

Verificarea încadrării NIS2 în România

Flux dedicat identificării entităților care intră sau nu sub incidența OUG nr. 155/2024.

Repere: OUG nr. 155/2024, Legea nr. 124/2025, Anexele 1 și 2, criterii DNSC



1. Identificarea sectorului

- sector de activitate
- anexa 1 / anexa 2
- domeniu critic / suplimentar



2. Verificarea serviciului prestat

- serviciu prevăzut de OUG 155/2024
- relevanță pentru economie / societate
- delimitarea serviciilor vizate



3. Criterii dimensionale

- număr de angajați
- cifră de afaceri / bilanț
- micro / mică / mijlocie / mare



4. Rol critic / unic furnizor

- unic furnizor în România
- impact major al perturbării
- rol critic în lanțul de servicii



5. Excepții și particularități

- administrație publică centrală / regională
- entități vizate prin criterii speciale
- cazuri care necesită analiză suplimentară



Rezultatul verificării

Se încadrează sau nu sub incidența NIS2?

NU se încadrează



În afara sferei NIS2



Opțional: implementare voluntară a măsurilor de securitate cibernetică

SE încadrează



Entitate esențială sau importantă



Pas următor: notificarea către DNSC

Elemente analizate



sector



serviciu



dimensiune



criticitate



excepții

ⓘ Schemă explicativă orientativă pentru evaluarea încadrării NIS2 în România.

Fluxul complet de notificare către DNSC

Pașii oficiali de notificare pentru entitățile vizate de NIS2 în România.

Repere: OUG nr. 155/2024, Legea nr. 124/2025, Ordinul DNSC nr. 1/2025



1. Generarea formularului

- prin Platforma NIS2@RO
- sau Instrumentul NIS
- formular standard de notificare



2. Completarea datelor entității

- denumire, CUI, sediu
- sector / serviciu vizat
- date de contact



3. Completarea responsabilului NIS

- persoană desemnată
- funcție și date contact
- rol de coordonare



4. Transmiterea către DNSC

- trimitere electronică
- în termenul legal
- max. 30 zile



5. Confirmarea primirii

- DNSC confirmă recepția
- în termenul de 5 zile
- număr de referință



6. Solicitări de clarificare

- dacă sunt necesare
- completări / documente
- răspuns din partea entității



7. Decizie de încadrare

- analiza notificării
- entitate esențială / importantă
- sau neîncadrare



Rezultatul notificării

Încadrare sau neîncadrare în sfera NIS2

NU se încadrează



În afara sferei NIS2



Opțional: implementare voluntară a măsurilor de securitate cibernetică

SE încadrează



Entitate esențială sau importantă



Pas următor: evaluarea nivelului de risc și continuarea conformării

Elemente transmise



date entitate



serviciu



responsabil NIS



formular



clarificări

Schemă explicativă orientativă pentru procesul de notificare către DNSC.

Diferența între entitate esențială și entitate importantă

Comparație orientativă în cadrul NIS2 România

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — art. 5, art. 6, art. 11–15, art. 46–49

Entitate esențială



1 Criterii de clasificare
- administrație publică centrală
- entități critice și entități identificate conform art. 9
- DNS, TLD, prestatori de servicii de încredere calificați
- întreprinderi mari din Anexa 1
- anumite entități mijlocii: comunicații electronice și servicii de securitate gestionate



2 Nivelul obligațiilor
- aceleași obligații de bază NIS2: măsuri tehnice, operaționale și organizatorice
- evaluare de risc, audit, raportare incidente
- autoevaluare anuală a maturității
- plan de măsuri pentru remedierea deficiențelor în 30 de zile de la autoevaluare



3 Nivelul de risc
- criticitate mai ridicată
- impact potențial major asupra serviciilor esențiale
- expunere mai mare la risc sistemic, public sau transfrontalier



4 Nivelul de control
- supraveghere și control mai extinse
- măsuri corective, termene-limită, monitorizare
- pentru neconformare gravă pot exista măsuri suplimentare



5 Audit
- audit obligatoriu în funcție de nivelul de risc
- DNSC poate dispune audit ad-hoc
- rezultate transmise către DNSC



6 Raportare
- raportare fără întârziere nejustificată a incidentelor semnificative
- raportare prin PNRISC
- pot exista și notificări către destinatarii serviciilor



7 Responsabilitate managerială
- managementul aprobă măsurile și supraveghează implementarea
- răspundere pentru nerespectare
- desemnarea responsabilului NIS
- pentru entitățile esențiale, responsabilul are cerințe mai stricte de autoritate și independență

Entitate importantă



1 Criterii de clasificare
- entități mari și mijlocii din Anexa 1 și Anexa 2
- se aplică atunci când nu sunt încadrate ca esențiale
- pot include anumite entități din comunicații electronice sau servicii de încredere, dacă nu sunt esențiale



2 Nivelul obligațiilor
- aceleași obligații de bază NIS2: măsuri tehnice, operaționale și organizatorice
- evaluare de risc, audit, raportare incidente
- autoevaluare anuală a maturității
- remedierea deficiențelor rămâne obligatorie



3 Nivelul de risc
- criticitate importantă, dar de regulă sub nivelul entităților esențiale
- impact semnificativ, însă de obicei mai redus sistemic
- nivelul concret de risc se evaluează individual



4 Nivelul de control
- supraveghere mai țintită
- control activ mai ales la incident, indicii de neconformare sau măsuri dispuse
- DNSC poate solicita informații și dovezi



5 Audit
- audit obligatoriu în funcție de nivelul de risc
- DNSC poate dispune audit ad-hoc
- rezultate transmise către DNSC



6 Raportare
- raportare fără întârziere nejustificată a incidentelor semnificative
- raportare prin PNRISC
- pot exista și notificări către destinatarii serviciilor



7 Responsabilitate managerială
- managementul aprobă măsurile și supraveghează implementarea
- răspundere pentru nerespectare
- desemnarea responsabilului NIS
- cerințele specifice sunt, în general, mai puțin accentuate decât la entitățile esențiale



Mesaj-cheie

Obligațiile de bază sunt similare pentru ambele categorii, însă entitățile esențiale au, în general, un nivel mai ridicat de criticitate și un regim de supraveghere mai sever.



Schemă comparativă orientativă pentru NIS2 România. Pentru încadrare și aplicare concretă, analiza se face în raport cu OUG 155/2024, Legea 124/2025 și actele DNSC.

Organizație sub NIS2, dar neînregistrată la DNSC

Ce înseamnă neînregistrarrea: expunere, riscuri, sancțiuni și consecințe operaționale

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — art. 18, art. 48¹, 60



1. Obligația legală există

- entitățile vizate trebuie să notifice DNSC
- înregistrarea se face în max. 30 de zile
- faptul că nu te înregistrezi nu te scoate din sfera NIS2



2. Expunere directă

- DNSC poate identifica entitatea din oficiu
- poate exista sesizare privind sustragerea de la notificare
- începe verificarea încalcării și a obligațiilor



3. Riscuri de conformare

- nu intri controlat în fluxul de evaluare
- întârzii evaluarea nivelului de risc
- întârzii autoevaluarea și planul de măsuri



4. Măsuri și control

- DNSC poate solicita informații și dovezi
- poate dispune măsuri de remediere
- poate impune termene și chiar audit ad-hoc



5. Amenzi și sancțiuni

- neîndeplinirea obligației de notificare este contravenție
- importantă: 1.000–300.000 lei
- esențială: 1.500–500.000 lei
- alte încălcări grave ulterioare pot atrage sancțiuni mult mai mari





Mesaj-cheie:

Neînregistrarea nu înseamnă invizibilitate, ci vulnerabilitate și risc.



6. Impact real

- expunere juridică și reputațională
- presiune asupra managementului
- risc operațional mai mare în caz de incident
- lipsa pregătirii poate costa mai mult decât conformarea

Ce poate urma


identificare


control


măsuri



amendă


conformare întârziată

ⓘ Schemă explicativă orientativă privind riscurile neînregistrării la DNSC pentru entitățile aflate sub incidența NIS2 în România.

Organizație sub NIS2, dar fără implementarea măsurilor

Ce înseamnă lipsa implementării: expunere, riscuri, sancțiuni și consecințe operaționale

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — art. 11, art. 12, art. 14, art. 48, art. 60



1. Obligațiile există

- măsuri tehnice, operaționale și organizatorice
- gestionarea riscurilor de securitate cibernetică
- autoevaluare, remediere și dovezi de conformare



2. Expunere directă

- vulnerabilități rămase neadresate
- probabilitate mai mare de incidente
- afectarea serviciilor și a continuității



3. Riscuri de conformare

- întârzieri la evaluare și autoevaluare
- lipsa planurilor și a măsurilor corective
- presiune crescută în cazul unui control





4. Măsuri și control

- DNSC poate solicita informații și dovezi
- poate dispune măsuri și termene-limită
- poate impune audit ad-hoc și remediere



5. Amenzi și sancțiuni

- neimplementarea măsurilor poate fi contravenție
- importantă: până la 7.000.000 EUR sau 1,4% CA globală
- esențială: până la 10.000.000 EUR sau 2% CA globală
- se aplică valoarea cea mai mare, în limitele legale



Mesaj-cheie:
Fără implementare, organizația rămâne expusă, controlabilă și sancționabilă.



6. Impact real

- impact juridic, reputațional și contractual
- presiune asupra managementului
- costul incidentelor poate depăși costul conformării

Ce poate urma


deficiențe


control


măsuri impuse



amendă


conformare sub presiune

Schemă explicativă orientativă privind riscurile neimplementării măsurilor NIS2 în România.

Evaluarea nivelului de risc NIS2

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — art. 10 și art. 11

1 Identificarea activelor



- active IT și OT relevante
- sisteme, aplicații, date, echipamente
- servicii esențiale și procese critice

2 Identificarea amenințărilor



- atacuri cibernetice și erori umane
- întreruperi, sabotaj, scurgeri de date
- amenințări interne și externe

3 Vulnerabilități



- puncte slabe tehnice sau organizatorice
- configurări greșite, lipsa patching-ului
- controale insuficiente sau lipsă

4 Probabilitate



- cât de posibil este incidentul
- frecvență, expunere, atractivitate
- context operațional și istoric

Nivelul de risc

Probabilitate × Impact

Evaluarea se bazează pe active, amenințări, vulnerabilități și efectele potențiale asupra serviciilor.

5 Impact



- efect asupra serviciilor și operațiunilor
- impact financiar, juridic, reputațional
- efect asupra siguranței și continuității

6 Nivel de risc



- combinarea probabilității cu impactul
- scăzut / mediu / ridicat / critic
- se stabilește prioritatea de tratament

Exemplu de logică

activ critic + amenințare relevantă + vulnerabilitate exploatabilă = risc mai mare

7 Prioritizare măsuri



- măsuri preventive și corective
- remedierea vulnerabilităților critice
- plan de acțiune și termene

Cum se calculează și se folosește rezultatul



Mesaj-cheie: Evaluarea riscului nu este doar un exercițiu formal. Ea ajută organizația să înțeleagă unde este expusă și ce măsuri trebuie prioritizate pentru a proteja serviciile esențiale.

ⓘ Schemă explicativă orientativă privind evaluarea nivelului de risc în cadrul NIS2 România.

Registrul de riscuri NIS2

Structura unui registru de riscuri pentru gestionarea și monitorizarea riscurilor în cadrul NIS2 România

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — analiză, evaluare, tratament, responabilitate și urmărire



1. Activ afectat

- sistem / serviciu / proces / date
- activ critic sau suport
- ce trebuie protejat



2. Amenințare

- atac cibernetic / eroare / întrerupere
- sursă internă sau externă
- scenariu de materializare



3. Vulnerabilitate

- punct slab tehnic sau procedural
- control insuficient
- condiție exploatabilă



4. Probabilitate

- cât de posibil este riscul
- frecvență / expunere / context
- scor estimat

Registrul de riscuri

centralizează informațiile esențiale despre fiecare risc și permite prioritizarea, tratamentul și urmărirea lui până la remediere sau acceptare.



5. Impact

- efect asupra serviciilor
- impact operațional, juridic, reputațional
- severitate estimată



6. Nivel risc

- probabilitate × impact
- scăzut / mediu / ridicat / critic
- prioritate de tratament



7. Măsuri

- control existent sau propus
- măsuri preventive și corective
- reducerea riscului



8. Responsabil

- persoană / echipă desemnată
- owner al riscului
- responsabil de implementare



9. Termen

- dată țintă
- etapă / milestone
- termen de revizuire

Cum se citește registrul



Mesaj-cheie: Un registru de riscuri bine structurat ajută organizația să vadă clar ce este expus, cât de grav este riscul și cine trebuie să acționeze, până când.

De la risc la plan de măsuri

Cum se transformă evaluarea de risc într-un plan de conformare în cadrul NIS2 România

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — evaluare, remediere, implementare și raportare

1 Risc identificat



- vulnerabilitate
- amenințare
- expunere
- impact asupra serviciului

2 Control lipsă



- lipsa unei politici
- control tehnic insuficient
- proces neimplementat
- monitorizare inexistentă

3 Măsură propusă



- măsură tehnică, organizatorică sau operațională
- remediere clar definită

4 Responsabil



- desemnarea persoanei / echipei responsabile
- ownership clar

Riscul evaluat trebuie transformat în măsuri concrete

Planul de măsuri leagă evaluarea, responsabilitatea și implementarea.

5 Termen



- termen de implementare
- prioritate
- calendar

6 Buget



- resurse necesare
- cost estimat
- achiziții
- servicii externe

7 Status implementare



- neînceput
- în lucru
- parțial implementat
- finalizat

8 Raportare



- raportare internă
- raport către management
- dovadă de implementare
- raportare către autoritate unde este cazul

Fluxul transformării riscului într-un plan de măsuri



Mesaj-cheie: Evaluarea riscului este utilă doar dacă rezultatul ei este tradus într-un plan clar, urmărit și documentat până la implementare.

Schemă explicativă orientativă privind transformarea riscurilor identificate în plan de măsuri în cadrul NIS2 România.

Gap Analysis NIS2

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — cerințe, controale, maturitate, risc și remediere



1. Cerință legală

- obligație NIS2 aplicabilă
- articol / cerință relevantă
- măsură tehnică, operațională sau organizatorică
- criteriu de verificare



2. Control existent

- măsură deja implementată
- dovezi și documentație
- control funcțional și verificabil
- reduce parțial sau total riscul



3. Control parțial

- implementare incompletă
- acoperire limitată
- lipsesc proceduri, dovezi sau testare
- necesită consolidare



4. Control lipsă

- cerință neacoperită
- măsură inexistentă
- vulnerabilitate procedurală sau tehnică
- gap cu impact direct asupra conformării

Gap Analysis arată unde cerințele NIS2 nu sunt acoperite complet și ce trebuie remediat pentru conformare.



5. Nivel de maturitate

- inițial / de bază / mediu / avansat
- grad de formalizare
- nivel de repetabilitate
- capacitate de monitorizare și îmbunătățire



6. Risc asociat

- impact asupra serviciilor
- probabilitate de incident
- expunere juridică și operațională
- prioritate de tratament

Logica analizei

cerință NIS2 + stare actuală + maturitate + risc = priorități de remediere



7. Acțiune corectivă

- măsură recomandată
- responsabil desemnat
- termen de implementare
- rezultat urmărit

Fluxul Gap Analysis

cerință → control → gap → maturitate → risc → acțiune

Mesaj-cheie: Gap Analysis nu înseamnă doar identificarea lipsurilor, ci transformarea lor în acțiuni concrete, prioritizate și asumate.

Planul de remediere NIS2

De la risc identificat la conformare și implementare

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — evaluare, remediere, implementare și raportare

1. Risc identificat



- scenariu de risc identificat
- activ / proces / serviciu afectat
- cauză și expunere
- nivel de risc estimat

2. Control lipsă



- control inexistent sau insuficient
- cerință NIS2 neacoperită
- vulnerabilitate procedurală sau tehnică
- cauză rădăcină identificată

3. Măsură propusă



- măsură tehnică, operațională sau organizatorică
- acțiune clar definită
- corelare cu riscul și controlul lipsă
- rezultat urmărit: reducerea riscului

4. Responsabil



- persoană / echipă responsabilă
- ownership clar
- rol de coordonare și execuție
- implicarea managementului, unde este cazul

5. Termen



- data de început
- termen de implementare
- prioritizare pe urgență
- etape intermediare / milestone-uri

Riscul evaluat trebuie transformat în măsuri concrete, asumate, finanțate și urmărite până la implementare.

6. Buget



- cost estimat
- resurse necesare
- cost intern / extern
- aprobare bugetară

7. Status implementare



- planificat
- în lucru
- parțial implementat
- finalizat / întârziat

8. Raportare



- progres și dovezi de implementare
- raport intern către management
- actualizare plan de măsuri
- raportare către autoritate, unde este cazul

Fluxul planului de remediere



Mesaj-cheie: Un plan de remediere eficient transformă constatările în acțiuni clare, urmărite și documentate până la reducerea reală a riscului.

Schemă explicativă orientativă privind structura unui plan de remediere NIS2 în România.

Măsurile minime de securitate NIS2

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — măsuri tehnice, operaționale și organizatorice



1. Politici de securitate

- politici aprobate și actualizate
- reguli pentru protecția sistemelor și datelor
- roluri și responsabilități clare
- revizuire periodică



2. Managementul incidentelor

- detectare, analiză și răspuns
- proceduri de escaladare
- lecții învățate și remediere
- coordonare internă și externă



3. Continuitate

- plan de continuitate și recuperare
- scenarii de întrerupere
- teste periodice de reziliență
- menținerea serviciilor esențiale



4. Securitatea lanțului de aprovizionare

- evaluarea furnizorilor critici
- cerințe de securitate contractuale
- monitorizarea dependențelor
- controlul riscurilor externe

Măsurile NIS2 trebuie aplicate coerent, proporțional cu riscul și susținute prin dovezi, procese și responsabilități clare.



5. Control acces

- acces pe baza nevoii de a cunoaște
- scenuri individuale și privilegii controlate
- autentificare puternică
- revizuirea accesurilor



6. Criptare

- protecția datelor în tranzit și la stocare
- folosirea mecanismelor adecvate de criptare
- gestionarea cheilor
- protejarea comunicațiilor sensibile



7. Backup

- copii de siguranță regulate
- copii izolate / protejate
- testarea restaurării
- protejarea integrității backup-ului



8. Instruire

- conștientizare pentru întreg personalul
- instruire pe roluri și responsabilități
- exerciții și simulări
- reducerea erorii umane



9. Raportare

- raportare internă rapidă
- notificarea incidentelor relevante
- evidențe și documentare
- informarea managementului și a autorităților, unde este cazul

Domeniile minime de control

politici ⇒ incidente ⇒ continuitate ⇒ furnizori ⇒ acces ⇒ criptare ⇒ backup ⇒ instruire ⇒ raportare

Mesaj-cheie: Conformarea NIS2 nu înseamnă o singură măsură, ci un set minim de controale care trebuie implementate, testate și îmbunătățite continuu.

ⓘ Schemă explicativă orientativă privind măsurile minime de securitate NIS2 în România.

Documentația necesară pentru conformare NIS2

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — guvernanță, evaluare, măsuri, continuitate, incidente și audit

1. Politici de securitate



- Politica de securitate a informației
- Roluri și responsabilități
- Principii și reguli de securitate
- Aliniere la cerințele NIS2

2. Proceduri



- Proceduri operaționale și tehnice
- Managementul schimbărilor
- Gestionarea accesului
- Managementul furnizorilor și terților

3. Registru riscuri



- Identificarea și descrierea riscurilor
- Evaluarea probabilității și impactului
- Nivelul de risc și prioritizare
- Revizuire și actualizare periodică

4. Plan de măsuri



- Măsuri de tratare a riscurilor
- Acțiuni, responsabili și termene
- Resurse și buget
- Monitorizare și status implementare

Conformarea NIS2 se bazează pe documente clare, actualizate și susținute prin dovezi.

5. Plan de continuitate



- Analiza impactului (BIA)
- Strategii de continuitate
- Planuri de recuperare și proceduri de testare
- Teste, revizuiri și îmbunătățiri

6. Plan de răspuns la incidente



- Proceduri de detectare și raportare
- Clasificarea și gestionarea incidentelor
- Comunicări interne și externe
- Învățături și îmbunătățiri

8. Rapoarte audit



- Rapoarte audit intern/extern
- Constatări și recomandări
- Planuri de acțiune
- Evidența remedierilor

9. Dovezi implementare



- Dovezi tehnice și operaționale
- Capturi, loguri, configurări
- Procese-verbale și aprobări
- Alte dovezi relevante

Cum se vede dosarul de conformare



Mesaj-cheie: Documentația nu este doar formală. Ea demonstrează controlul, trasabilitatea și nivelul real de pregătire al organizației.

Schemă explicativă orientativă privind documentația necesară pentru conformare NIS2 în România.

NIS2 ca proces continuu, nu acțiune unică

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — guvernanță, evaluare, implementare, monitorizare și îmbunătățire continuă



CICLUL NIS2: DE LA PLANIFICARE LA ÎMBUNĂTĂȚIRE CONTINUĂ



Mesaj-cheie:

NIS2 trebuie tratat ca un proces continuu de identificare, evaluare, implementare, verificare și îmbunătățire, nu ca o acțiune singulară.

ⓘ Schemă explicativă orientativă privind conformarea continuă NIS2 în România.

Managementul incidentelor NIS2

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — detectare, răspuns, raportare și remediere

1 Detectare



- identificarea evenimentului
- alertă din monitorizare / utilizator / furnizor
- confirmarea existenței incidentului

2 Analiză



- evaluarea naturii și cauzei
- sisteme și servicii afectate
- severitate și impact estimat

3 Izolare



- limitarea propagării
- segmentarea sistemelor afectate
- măsuri imediate de contenție

4 Eradicare



- eliminarea cauzei incidentului
- înlăturarea codului malițios / accesului neautorizat
- corectarea vulnerabilităților exploatate

Managementul incidentelor leagă detecția, răspunsul, comunicarea și îmbunătățirea continuă.

5 Recuperare



- restaurarea serviciilor
- validarea integrității sistemelor
- revenire controlată în producție

6 Comunicare



- coordonare internă
- informarea managementului și echipelor relevante
- comunicare cu partenerii, unde este cazul

8 Post-incident review



- lecții învățate
- analiză cauză rădăcină
- actualizare proceduri și controale

7 Raportare



- notificarea incidentului conform procedurilor
- raportare către DNSC / PNRISC, unde este cazul
- evidență a etapelor și măsurilor aplicate

Fluxul operațional al incidentului



Mesaj-cheie: Un management eficient al incidentelor reduce impactul operațional, susține raportarea corectă și transformă fiecare incident într-o oportunitate de consolidare a securității.

Schemă explicativă orientativă privind managementul incidentelor NIS2 în România.

Fluxul de raportare a incidentelor către DNSC

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — raportarea incidentelor, PNRISC, remediere și învățare

1 Detectarea incidentului



- identificarea evenimentului de securitate
- alertă din monitorizare / utilizator / furnizor
- confirmarea faptului că există un incident

2 Clasificare severitate



- evaluarea impactului asupra serviciilor
- analizarea afectării confidențialității, integrității și disponibilității
- stabilirea prioritații și a nivelului de severitate

3 Notificare timpurie



- informare rapidă către DNSC
- transmitere prin canalele aplicabile / PNRISC
- comunicarea elementelor esențiale cunoscute la momentul inițial

4 Raport intermediar



- actualizarea situației pe măsură ce apar date noi
- descrierea evoluției incidentului
- măsuri de limitare și impact estimat

Raportarea incidentelor nu înseamnă doar notificare. Ea leagă detecția, analiza, comunicarea, remedierea și îmbunătățirea continuă.

5 Raport final



- descriere completă a incidentului
- cauză, impact și perioada afectată
- măsuri aplicate și stadiul remedierii

6 Lecții învățate



- analiza cauzelor și a vulnerabilităților exploatate
- identificarea punctelor slabe de proces sau control
- concluzii pentru prevenirea recurenței

7 Actualizare măsuri



- îmbunătățirea controalelor și procedurilor
- actualizarea planurilor, registrelor și instruirii
- urmărirea implementării măsurilor corective

Cum curge procesul de raportare



Mesaj-cheie: Un proces bun de raportare ajută organizația să răspundă rapid, să comunice corect cu DNSC și să transforme incidentul într-o sursă de

NIS2 pentru administrația publică

Cum se aplică securitatea cibernetică în instituțiile și autoritățile publice din România

Repere: OUG nr. 155/2024, Legea nr. 124/2025 – guvernanță, risc, continuitate, raportare și responsabilitate



1. Cine este vizat

- autorități și instituții publice relevante
- servicii publice esențiale
- sisteme și servicii critice



2. De ce este important

- protecția serviciilor publice
- continuitate operațională
- protecția datelor
- încrederea cetățenilor



3. Guvernanță și management

- rolul conducerii
- aprobarea măsurilor
- alocarea resurselor
- supravegherea implementării



4. Evaluarea riscurilor

- active
- amenințări
- vulnerabilități
- impact
- prioritizare

Administrația publică trebuie să trateze conformarea NIS2 ca pe un proces continuu de guvernanță, gestionare a riscurilor, implementare, raportare și îmbunătățire.



5. Măsuri esențiale

- politici
- control acces
- backup
- criptare
- management incidente
- securitatea furnizorilor



6. Raportarea incidentelor

- detectare
- clasificare
- notificare timpurie
- raport intermediar
- raport final



7. Responsabilul NIS / securitate

- coordonare implementare
- comunicare cu DNSC
- evidențe
- raportare internă
- pregătire audit



8. Documentație și dovezi

- politici și proceduri
- registru riscuri
- plan de măsuri
- plan de continuitate
- rapoarte și dovezi



9. Audit și îmbunătățire

- verificări
- interviuri
- neconformități
- recomandări
- remediere
- reevaluare periodică

Cum se aplică NIS2 în administrația publică

guvernanță » risc » măsuri » incidente » documente » audit » îmbunătățire

Mesaj-cheie: NIS2 în administrația publică înseamnă servicii mai reziliente, procese mai bine controlate și responsabilitate reală pentru securitatea cibernetică.

NIS2 PENTRU ENERGIE

Securitate cibernetică pentru un sector energetic sigur, rezilient și sustenabil.

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — analiză, evaluare, tratament, responsabilitate și urmărire

1. DE CE ESTE IMPORTANT NIS2 ÎN ENERGIE



- protejează infrastructura critică de energie (producție, transport, distribuție)
- previne întreruperile și impactul asupra populației și economiei
- asigură conformitatea legală și încrederea în sectorul energetic

2. CE VIZEAZĂ NIS2 ÎN ENERGIE



- operatori de servicii esențiale și furnizori de servicii digitale
- sisteme IT, OT și ICS/SCADA
- date operaționale și de clienți
- lanțul de aprovizionare critic
- comunicații și servicii suport

3. ACTIVE CRITICE



- sisteme SCADA/ICS și RTU
- rețele de comunicații energetice
- sisteme de management al energiei
- baze de date și aplicații critice
- echipamente și infrastructuri fizice și logică
- personal și know-how

4. RISCURI PRINCIPALE



- atacuri cibernetice asupra OT/ICS
- ransomware și malware
- compromiterea datelor și a informațiilor operaționale
- atacuri asupra lanțului de aprovizionare
- erori umane și phishing

NIS2 ÎN ENERGIE

Consolidăm securitatea cibernetică a sistemului energetic pentru a asigura continuitatea furnizării energiei, protejarea datelor și a infrastructurilor critice și pentru a sprijini tranziția energetică în condiții de siguranță.

5. MĂSURI ESENȚIALE



- managementul riscurilor
- controlul accesului și al identităților
- segmentarea rețelelor OT/IT
- monitorizare și detecție continuă
- backup și planuri de continuitate
- patch management și hardening
- instruirea personalului

6. RĂSPUNS LA INCIDENTE



- detectarea rapidă și corelare evenimente
- izolare și limitarea impactului
- comunicare internă și externă
- raportare către DNSC în 24h
- recuperare și lecții învățate

7. GUVERNANȚĂ ȘI RESPONSABILITĂȚI



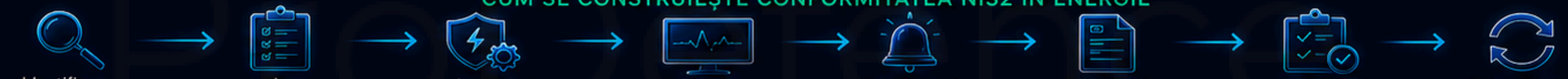
- conducerea își asumă responsabilitatea
- desemnarea responsabiiului NIS
- politici și proceduri documentate
- evaluări și audituri periodice
- colaborare cu autoritățile și operatorii critici

8. BENEFICII



- continuitatea și fiabilitatea serviciilor
- reducerea impactului incidentelor
- conformitate legală și evitarea sancțiunilor
- protejarea reputației și încrederii
- susținerea tranziției energetice sigure

CUM SE CONSTRUIEȘTE CONFORMITATEA NIS2 ÎN ENERGIE





Securitate. Continuitate. Încredere. Energie pentru viitor.

NIS2 PENTRU SĂNĂTATE

Securitate cibernetică pentru servicii de sănătate esențiale, pacienți protejați, sisteme reziliente

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — analiză, evaluare, tratament, responsabilitate și urmărire

1. CE ESTE NIS2 PENTRU SĂNĂTATE?

- Protejează serviciile esențiale de sănătate și datele pacienților
- Crește reziliența și continuitatea actului medical
- Respectă cerințele legale și reduce riscul de sancțiuni și incidente majore

2. CE VIZEAZĂ?

- Unități sanitare publice și private
- Laboratoare, imagistică, ambulatorii
- Furnizori de servicii IT și dispozitive medicale conectate
- Platforme și aplicații de telemedicină

3. OBIECTIVE NIS2 ÎN SĂNĂTATE

- ✓ Continuitatea serviciilor medicale critice
- ✓ Protecția datelor cu caracter personal
- ✓ Detectarea și răspunsul rapid la incidente
- ✓ Creșterea rezilienței cibernetice
- ✓ Cooperare și schimb de informații

4. ACTIVI CRITICI

- EHR / HIS / PACS
- Dispozitive medicale conectate (IoT / IoMT)
- Sisteme de laborator și farmacie
- Rețele, cloud, backup
- Date pacienți și personal

5. RISCURI PRINCIPALE

- Ransomware și întreruperi de servicii
- Acces neautorizat și scurgeri de date
- Vulnerabilități în dispozitive medicale
- Erori umane și phishing
- Atacuri în lanțul de aprovizionare

6. MĂSURI ESENȚIALE

- Managementul riscurilor
- Controlul accesului și al identităților
- Criptarea datelor și comunicațiilor
- Backup și recuperare sigură
- Segmentarea rețelei și monitorizare
- Managementul vulnerabilităților

7. RĂSPUNS LA INCIDENTE

- Plan de răspuns la incidente
- Detectare, analiză, izolare
- Comunicarea internă și externă
- Raportare către DNSC în 24h
- Lecții învățate și îmbunătățire

8. RESPONSABILITĂȚI CHEIE

- Conducerea: guvernanță și alocarea resurselor
- Responsabil cu securitatea (RSSI)
- DPO: protecția datelor pacienților
- Personalul medical și administrativ
- Furnizori și parteneri critici

NIS2 ÎN SĂNĂTATE

Sisteme sigure.
Date protejate.
Pacienți în siguranță.

9. DOCUMENTAȚIE NECESARĂ

- Politici și proceduri de securitate
- Registru de riscuri și plan de tratament
- Plan de continuitate a activității
- Plan de răspuns la incidente
- Evidențe instruire și conștientizare
- Rapoarte audit și testare periodică

10. BENEFICII

- Servicii medicale disponibile și sigure
- Încredere sporită a pacienților
- Conformare legală și reducerea riscurilor
- Reducerea impactului financiar al incidentelor
- Reputație și parteneriate consolidate

CICLUL NIS2 ÎN SĂNĂTATE

IDENTIFICARE
Identifică activele, procesele și riscurile critice

→

EVALUARE
Evaluează impactul și probabilitatea riscurilor

→

IMPLEMENTARE
Implementează măsuri de securitate și controale

→

MONITORIZARE
Monitorizează continuu sistemele și amenințările

→

RAPORTARE
Raportează incidentele către DNSC și conducere

→

AUDIT
Evaluează periodic conformitatea și eficacitatea

→

ÎMBUNĂTĂȚIRE
Îmbunătățește continuu măsurile și procesele

→

REEVALUARE PERIODICĂ
Reevaluează riscurile la intervale regulate sau după incidente

MESAJ-CHEIE: Securitatea cibernetică în sănătate nu este doar o cerință legală, ci o responsabilitate față de fiecare pacient. Un sistem sănătos este un sistem care funcționează în siguranță.

ÎMPREUNĂ PROTEJĂM SĂNĂTATEA.
Conformitate. Reziliență. Încredere.

NIS2 PENTRU UTILITĂȚI

Securitate cibernetică pentru servicii esențiale de apă, canalizare, energie termică, salubritate, iluminat public și alte servicii de utilitate publică

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — analiză, evaluare, tratament, responsabilitate și urmărire

1. DE CE ESTE IMPORTANT NIS2 PENTRU UTILITĂȚI

- asigură continuitatea serviciilor esențiale pentru comunități
- reduce impactul incidentelor asupra sănătății publice și mediului
- crește reziliența și încrederea cetățenilor

2. CE VIZEAZĂ NIS2 ÎN UTILITĂȚI

- operatori de servicii esențiale de utilități
- sisteme IT, OT și ICS/SCADA
- date operaționale și de clienți
- lanțul de aprovizionare și serviciile terțe critice
- infrastructuri fizice și logice

3. ACTIVE CRITICE

- SCADA, PLC, HMI și RTU
- rețele de comunicații industriale
- stații, pompe, rezervoare, rețele
- servere, baze de date și aplicații
- echipamente de teren și infrastructuri suport
- personal și know-how

4. RISCURI PRINCIPALE

- atacuri ransomware și malware
- acces neautorizat la sisteme OT
- compromiterea disponibilității serviciilor
- atacuri asupra lanțului de aprovizionare
- erori umane și phishing

NIS2 ÎN UTILITĂȚI

Asigură un cadru robust de management al securității cibernetice pentru a proteja infrastructurile critice, a menține serviciile esențiale și a răspunde eficient la incidente, contribuind la reziliența și sustenabilitatea comunităților.

5. MĂSURI ESENȚIALE

- managementul riscurilor
- controlul accesului și al identităților
- securizarea rețelelor OT/IT
- monitorizare și detecție continuă
- backup și planuri de continuitate
- managementul vulnerabilităților
- instruirea personalului

6. RĂSPUNS LA INCIDENTE

- detectare rapidă și analiză
- izolarea sistemelor afectate
- comunicare internă și externă
- raportare către DNSC în 24h
- recuperare și lecții învățate

7. GUVERNANȚĂ ȘI RESPONSABILITĂȚI

- conducerea își asumă responsabilitatea
- desemnarea responsabilului NIS
- politici și proceduri documentate
- evaluări și audituri periodice
- colaborare cu autoritățile și furnizorii critici

8. BENEFICII

- servicii continue și sigure pentru cetățeni
- reducerea impactului incidentelor
- conformitate legală și evitarea sancțiunilor
- protejarea mediului și a sănătății publice
- creșterea încrederii și a reputației

CUM SE CONSTRUIEȘTE CONFORMITATEA NIS2 ÎN UTILITĂȚI

1. identificare active și riscuri
2. evaluare și prioritizare
3. implementare măsuri
4. monitorizare continuă
5. detectare și răspuns
6. raportare către DNSC
7. audit și revizuire periodică
8. îmbunătățire continuă

MESAJ-CHEIE: Utilitățile sunt fundamentul vieții de zi cu zi, NIS2 asigură protecția acestor servicii esențiale împotriva amenințărilor cibernetice și reziliența comunităților pe termen lung.

ProDefence

NIS2 PENTRU FURNIZORI IT ȘI DIGITALI

Securitate cibernetică puternică. Servicii digitale de încredere. Reziliență pentru clienții tăi și pentru economie.

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — analiză, evaluare, tratament, responsabilitate și urmărire

1. DE CE ESTE IMPORTANT NIS2 PENTRU FURNIZORII IT ȘI DIGITALI

- ești parte din lanțuri critice digitale ale clienților esențiali
- incidentul tău poate avea impact asupra multor organizații
- crește încrederea clienților și conformitatea contractelor
- diferențiator competitiv și acces la piețe reglementate

2. CE VIZEAZĂ NIS2 PENTRU FURNIZORII IT

- securitatea serviciilor gestionate (SaaS, PaaS, IaaS, cloud, hosting, colocation)
- dezvoltare software sigură și DevSecOps
- managementul datelor și al identităților
- terți și lanțul de aprovizionare IT
- continuitatea serviciilor digitale critice
- transparență și raportare a incidentelor

3. ACTIVE CRITICE ȘI SERVICII DIGITALE

- platforme și aplicații critice
- infrastructură cloud și rețele
- baze de date și date cu caracter personal / sensibile
- API, integrări și servicii gestionate
- medii de dezvoltare și CI/CD
- suport și servicii pentru clienți

4. RISCURI PRINCIPALE

- ransomware și atacuri asupra lanțului de aprovizionare (supply chain)
- exploatări de vulnerabilități în aplicații, API și cloud
- scurgeri de date și acces neautorizat
- erori de configurare și credențiale slabe
- întreruperi de servicii și indisponibilitate

NIS2 PENTRU FURNIZORI IT ȘI DIGITALI

Construiește un sistem de management al securității cibernetice care protejează serviciile digitale, datele și clienții, asigură conformitatea legală și contractuală și susține reziliența și continuitatea afacerii.

5. MĂSURI ESENȚIALE

- managementul riscurilor și al securității
- controlul accesului și al identităților (IAM)
- securizarea dezvoltării și testării (SSDLC)
- monitorizare 24/7 și detecție în timp real
- backup, recuperare și disaster recovery
- criptarea datelor și protecția informațiilor
- training și conștientizare pentru personal

6. RĂSPUNS LA INCIDENTE

- detectare rapidă și analiză
- izolare și limitarea impactului
- comunicare internă și cu clienții
- raportare către DNSC în 24h
- recuperare și lecții învățate

7. GUVERNANȚĂ ȘI RESPONSABILITĂȚI

- conducerea își asumă responsabilitatea
- desemnarea responsabilului NIS
- politici și proceduri documentate
- evaluări și audituri periodice
- colaborare cu autoritățile și clienții critici

8. BENEFICII

- încrederea clienților și partenerilor
- conformitate legală și contractuală
- reducerea incidentelor și a costurilor
- reziliență operațională și continuitate
- avantaj competitiv și acces la piețe noi

CUM SE CONSTRUIEȘTE CONFORMITATEA NIS2

identificare active și riscuri → evaluare și prioritizare → implementare măsuri → monitorizare continuă → detecție și răspuns → raportare către DNSC → audit și revizuire periodică → îmbunătățire continuă

MESAJ-CHEIE: Ca furnizor IT și digital, securitatea ta este fundația serviciilor tale.
NIS2 te ajută să livrezi servicii sigure, să protejezi datele clienților și să construiești un viitor digital rezilient.

ⓘ Schemă explicativă orientativă privind aplicarea NIS2 pentru furnizorii IT și digitali din România.

Lanțul de aprovizionare și furnizorii critici

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — furnizori critici, cerințe de securitate, monitorizare și continuitate

1. Identificare furnizori



- furnizori IT, OT și servicii suport
- prestatori esențiali pentru operațiuni
- dependente directe și indirecte

2. Clasificare criticitate



- impact asupra serviciilor esențiale
- nivel de dependență operațională
- furnizor critic / important / suport

3. Verificare contractuală



- clauze de securitate
- obligații de notificare incidente
- SLA, audit și responsabilități

4. Cerințe de securitate



- controale minime aplicabile
- acces securizat și protecția datelor
- continuitate și backup

Gestionarea furnizorilor critici reduce riscul de propagare a incidentelor și întărește reziliența organizației.

5. Monitorizare



- evaluări periodice
- urmărirea riscurilor și vulnerabilităților
- revizuirea performanței de securitate

6. Audit furnizor



- verificarea conformării
- dovezi, documentație și teste
- remedierea neconformităților

7. Plan de continuitate



- scenarii de întrerupere
- furnizori alternativi / redundanță
- măsuri de răspuns și recuperare

Cum se gestionează lanțul de aprovizionare

furnizori → criticitate → contract → cerințe → monitorizare → audit → continuitate

Mesaj-cheie: Securitatea lanțului de aprovizionare nu înseamnă doar selecția furnizorilor, ci control continuu, cerințe clare și pregătire pentru disfuncționalități.

Schemă explicativă orientativă privind gestionarea furnizorilor critici și a lanțului de aprovizionare în cadrul NIS2 România.

Auditul NIS2 — ce verifică auditorul

Repere: OUG nr. 155/2024, Legea nr. 124/2025 — verificare, conformare, dovezi și remediere

1. 1. Documentație



- politici și proceduri
- registru de riscuri
- planuri și registre
- documente de conformare

2. 2. Controale tehnice



- configurări și protecții
- control acces și autentificare
- backup, criptare, monitorizare
- vulnerabilități și patching

3. 3. Controale organizaționale



- roluri și responsabilități
- guvernanță și procese
- managementul incidentelor
- continuitate și furnizori

4. 4. Interviuri



- management
- responsabil NIS / securitate
- echipe operaționale
- verificarea aplicării în practică

Auditorul verifică dacă măsurile NIS2 sunt implementate, susținute prin dovezi și funcționează în practică.

5. 5. Dovezi



- capturi, loguri, rapoarte
- procese-verbale și aprobări
- evidențe de instruire
- probe ale implementării

6. 6. Neconformități



- cerințe neacoperite
- controale insuficiente
- lipsă dovezi
- gap-uri procedurale sau tehnice

8. 8. Raport final



- constatări
- nivel de conformare
- riscuri și impact
- concluzii și acțiuni următoare

7. 7. Recomandări



- măsuri corective
- prioritizare după risc
- responsabili și termene
- plan de remediere

Cum curge auditul

documente → controale → interviuri → dovezi → neconformități → recomandări → raport

Mesaj-cheie: **Auditul NIS2** nu verifică doar existența documentelor, ci și eficiența reală a măsurilor, trasabilitatea și capacitatea organizației de a demonstra conformarea.

Schemă explicativă orientativă privind verificările realizate în cadrul unui audit NIS2 în România.

NIS2 ÎN ROMÂNIA

Securitate cibernetică. Reziliență digitală. Încredere în viitor.

Aplicarea Directivei NIS2 este mai mult decât o obligație legală – este un angajament comun pentru o Românie digitală, sigură și pregătită pentru provocările viitorului.



PROTEJĂM
Serviciile esențiale și cetățenii împotriva riscurilor cibernetice.

COLABORĂM
Împreună, public și privat, pentru un ecosistem digital sigur.

INVESTIM
În tehnologie, oameni și procese pentru reziliență pe termen lung.

INOVĂM
Digitalizarea responsabilă deschide drumul către o economie competitivă.

ACȚIONĂM
Astăzi, pentru a construi încrederea de mâine.

REZILIENȚA CIBERNETICĂ ESTE FORȚA ROMÂNIEI DIGITALE

Fiecare organizație contează.
Fiecare decizie contează.
Împreună, facem România mai sigură.



PRINCIPII CARE NE GHIDEAZĂ

Responsabilitate
Fiecare actor își asumă rolul în securitatea cibernetică.

Transparență
Informații clare și raportare pentru decizii mai bune.

Proporționalitate
Măsuri adaptate la riscuri, pentru eficiență și sustenabilitate.

Îmbunătățire continuă
Învățăm, ne adaptăm și evoluăm constant în fața amenințărilor.

ÎMPREUNĂ, CONSTRUIM O ROMÂNIE DIGITALĂ, SIGURĂ ȘI REZILIENTĂ.

NIS2 nu este doar despre tehnologie. Este despre încredere, responsabilitate și viitor.

ProDefence

Expertiză, securitate cibernetică și suport specializat pentru organizații



1 Consultanță în implementarea NIS2

- evaluare și încadrare
- planificare și conformare
- suport pentru implementare

2 Audit de securitate

- verificarea măsurilor și controalelor
- identificarea neconformităților
- recomandări și raportare

3 Scanare de vulnerabilități și teste de penetrare

- identificarea vulnerabilităților
- validarea expunerilor reale
- sprijin pentru remediere

4 Investigații privind infracțiuni informatice

- fraude informatice
- spionaj cibernetic
- ransomware și analiză incidente

5 Cursuri de educație cibernetică

- instruire pentru management și angajați
- conștientizare și prevenție
- cultură de securitate cibernetică

ProDefence oferă expertiză specializată pentru **prevenție, conformare, investigație** și **reziliență cibernetică.**

www.prodefence.ro

ProDefence

EUROPEAN DIRECTIVE
NIS 2.0

Prodefence & CysNis

Expertiză și suport pentru implementarea **NIS2** în România

Prodefence oferă expertiză în evaluare, conformare și securitate cibernetică, iar CysNis susține organizațiile printr-o platformă dedicată implementării NIS2. Împreună, transformă obligațiile de conformare într-un proces clar, structurat și ușor de urmărit.



- Evaluare și încadrare
- Planificare și implementare
- Monitorizare și documentare
- Conformare și reziliență

» **Consultanță + platformă dedicată = un parcurs NIS2 mai clar și mai eficient**

www.prodefence.ro | www.cysnis.eu

REZILIENȚA
ÎNCEPE CU NOI.

NIS2 nu este doar o obligație. Este un angajament pentru protejarea a ceea ce contează: oameni, servicii esențiale și viitorul digital al României.

Conformitatea este punctul de plecare.
Reziliența este destinația.
Împreună, construim un ecosistem digital mai sigur, mai matur și mai pregătit pentru provocările de mâine.



Fiecare decizie conștientă de astăzi construiește o România digitală puternică și sigură.
Viitorul se protejează. Astăzi.

ProDefence

Ghid NIS2 România
Conformitate • Reziliență • Securitate

Resurse, bune practici și instrumente pentru o România digitală mai sigură.
www.cysnis.eu

www.prodefence.ro | contact@prodefence.ro

© 2026 Prodefence. Toate drepturile rezervate.