NIS2 și securitatea cibernetică în alte CATEGORII DE ORGANIZAȚII

NIS2 și obligațiile de securitate cibernetică pentru alte categorii de organizații

Ghid orientativ pentru furnizori de servicii, companii non-critice, platforme online și organizații din afara sectoarelor NIS2 clasice

1. Ce primești din acest document

Acest ghid este conceput pentru organizațiile care **nu se încadrează clar într-un sector NIS2 clasic**, dar care pot avea **obligații de securitate cibernetică și digitală** ca urmare a:

- rolului în **lanțuri de aprovizionare**;
- relațiilor contractuale cu entități NIS2;
- operării de **platforme online, aplicații sau magazine online**;
- procesării de **date importante sau sensibile**.

Documentul oferă:

- o **imagine clară a riscurilor tipice** pentru această categorie;
- o **orientare realistă privind NIS2 (indirect)**;
- o prezentare a **altor reglementări aplicabile**;
- **recomandări practice**, explicate pe înțelesul antreprenorilor.

Documentul are caracter informativ și nu reprezintă o evaluare individuală.

2. De ce această categorie este relevantă pentru NIS2 și securitatea digitală

Un număr mare de organizații consideră că NIS2 nu li se aplică deoarece:

- sunt de dimensiuni mici sau medii;
- nu operează infrastructuri critice;
- nu activează într-un sector explicit menționat în directivă.

În practică, multe dintre aceste organizații **devin relevante indirect** pentru NIS2 și pentru alte regimuri de conformare digitală, deoarece furnizează servicii, tehnologii sau date către entități reglementate.

3. Poziționarea generală față de NIS2

Pentru majoritatea organizațiilor din această categorie:

- **NIS2 nu se aplică direct**;
- **NIS2 se poate aplica indirect**, prin lanțul de aprovizionare;
- pot exista **alte obligații legale relevante**, chiar și în absența NIS2.

Această poziționare este frecvent întâlnită în practică și este important de înțeles corect pentru a evita riscuri comerciale și legale.

4. NIS2 – aplicabilitate indirectă prin lanțul de aprovizionare

Chiar dacă o organizație nu este entitate NIS2, poate avea obligații indirecte atunci când:

- are contracte cu entități supuse NIS2;
- furnizează servicii IT, software, mentenanță, suport sau consultanță;
- operează aplicații sau platforme utilizate de entități critice;

- are acces la date sau sisteme ale unor entități NIS2.

În aceste situații, entitățile NIS2 sunt obligate să își securizeze lanțul de aprovizionare și transferă cerințele către furnizori prin:

- clauze contractuale;
- cerințe minime de securitate;
- audituri și evaluări periodice.

5. Situația organizațiilor care doresc să lucreze cu entități NIS2

Chiar și în lipsa unui contract actual, organizațiile care **intenționează să colaboreze** cu entități NIS2 trebuie să țină cont de faptul că:

- cerințele de securitate sunt verificate încă din faza de selecție;
- lipsa unor măsuri minime poate duce la excluderea din proceduri;
- conformarea de bază devine un avantaj competitiv.

În acest context, securitatea cibernetică nu este doar o obligație, ci și un criteriu comercial.

6. Alte obligații digitale relevante (în afara NIS2)

Chiar dacă NIS2 nu se aplică direct sau indirect, multe organizații din această categorie sunt supuse altor reglementări, precum:

- **GDPR** – dacă sunt procesate date cu caracter personal;
- cerințe privind **securitatea platformelor online și aplicațiilor**;
- obligații asociate **comerțului electronic**;
- cerințe impuse de autorități naționale în domeniul digital (de exemplu, ADR);
- obligații privind protecția datelor comerciale sau confidențiale.

Neconformarea poate conduce la amenzi, restricții operaționale sau pierderea încrederii clienților.

7. Riscurile tipice pentru această categorie de organizații

Riscurile frecvent întâlnite includ:

- pierderea contractelor cu parteneri mari;
- breșe de date și incidente de securitate;
- sancțiuni pentru neconformare cu reglementări digitale;
- impact reputațional negativ;
- dificultăți în extinderea activității.

Aceste riscuri sunt adesea subestimate de organizațiile mici și medii.

8. Ce lipsește frecvent în această categorie

În practică, se observă frecvent:

- lipsa unei abordări structurate de securitate;
- confuzie între NIS2, GDPR și alte reglementări;
- măsuri tehnice minime inexistente sau neuniform implementate;
- lipsa documentației și a responsabilităților clare.

9. Ce se așteaptă, în mod realist, de la aceste organizații

Așteptările sunt proporționale cu dimensiunea și rolul organizației.

În mod realist, se așteaptă:

- un nivel minim de securitate cibernetică;
- capacitatea de a proteja datele gestionate;
- disponibilitatea de a respecta cerințe contractuale;

- reacție adecvată în cazul incidentelor.

10. Recomandări generale, aplicabile majorității organizațiilor

Pentru majoritatea organizațiilor din această categorie, sunt recomandate:

- clarificarea rolului în lanțul de aprovizionare;
- implementarea unor măsuri minime de securitate;
- înțelegerea obligațiilor digitale aplicabile;
- pregătirea pentru cerințe contractuale viitoare.

11. Ce NU este obligatoriu

Pentru a evita interpretările eronate:

- nu este obligatorie certificarea ISO;
- nu este impus un anumit furnizor sau produs;
- NIS2 nu se aplică automat tuturor organizațiilor.

12. Concluzie și pași următori

Acest ghid oferă o bază de orientare pentru organizațiile care nu se încadrează direct în sectoarele NIS2, dar care pot avea obligații indirecte sau alte cerințe digitale aplicabile. Pentru clarificarea exactă a situației unei organizații concrete, este recomandată o analiză dedicată, adaptată activităților desfășurate.