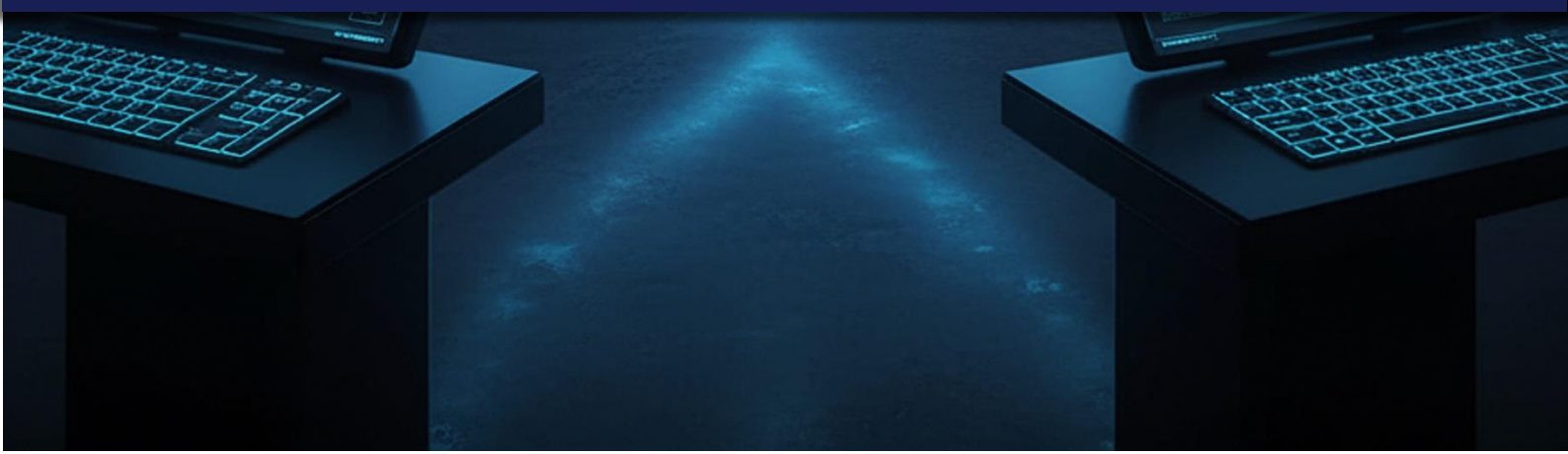
NIS2 și securitatea cibernetică în SECTORUL IT



NIS2 și securitatea cibernetică în sectorul IT și al platformelor digitale

Ghid orientativ pentru furnizori IT, platforme software, cloud, marketplace-uri și servicii digitale

1. Ce primești din acest document

Acest ghid este conceput pentru organizațiile din sectorul IT și al platformelor digitale și are rolul de a oferi:

- o **imagine clară a nivelului de risc specific sectorului IT și digital**;
- o **orientare generală privind aplicabilitatea cerințelor NIS2**;
- o înțelegere a **obligațiilor care pot apărea direct sau indirect**;
- o prezentare a **aspectelor care lipsesc frecvent în acest domeniu**;
- **recomandări clare și practice**, explicate pe înțelesul antreprenorilor și managerilor.

Documentul are caracter informativ și nu reprezintă o evaluare individuală a unei organizații.

2. De ce sectorul IT și al platformelor digitale este relevant pentru NIS2

Sectorul IT și cel al platformelor digitale joacă un rol transversal în economie, furnizând infrastructura și serviciile pe care se bazează majoritatea celorlalte domenii. O problemă de securitate în acest sector poate avea efecte în lanț, afectând simultan numeroși clienți și servicii critice.

Platformele software, serviciile cloud, marketplace-urile și furnizorii de infrastructură digitală operează sisteme expuse constant la internet, gestionează volume mari de date și sunt adesea integrate în procesele critice ale altor organizații.

3. Unde se poziționează, în general, sectorul IT față de NIS2

Directiva NIS2 acordă o atenție deosebită infrastructurilor și serviciilor digitale, având în vedere rolul lor de facilitatori pentru alte sectoare critice.

În funcție de dimensiune, tipul serviciilor și aria de impact:

- unele organizații IT pot fi **entități NIS2** (esențiale sau importante);
- multe organizații IT **nu intră direct sub incidența NIS2**, dar sunt afectate indirect prin relațiile contractuale și rolul în lanțul de aprovizionare.

Încadrarea exactă depinde de natura serviciilor digitale furnizate și de scala acestora.

4. NIS2 – aplicabilitate directă în sectorul IT și digital

În mod uzual, pot intra sub incidența directă a NIS2:

- furnizori de servicii cloud și centre de date;
- furnizori de servicii DNS;
- operatori de infrastructuri digitale critice;

- platforme digitale de dimensiuni mari, cu impact semnificativ.

Pentru aceste organizații, NIS2 introduce obligații privind:

- managementul riscurilor de securitate cibernetică;
- securitatea serviciilor digitale furnizate;
- reziliența operațională;
- raportarea incidentelor de securitate.

Nu toate firmele IT sau platformele software sunt automat entități NIS2.

5. NIS2 – aplicabilitate indirectă și lanțul de aprovizionare

Majoritatea organizațiilor IT și digitale sunt implicate în lanțurile de aprovizionare ale unor entități critice, chiar dacă ele însele nu sunt entități NIS2.

Obligații indirecte pot apărea atunci când:

- serviciile IT sunt utilizate de entități NIS2;
- platformele software sunt integrate în procese critice;
- furnizorii IT au acces la date sensibile sau sisteme esențiale.

În aceste cazuri, cerințele de securitate sunt frecvent impuse contractual și pot include audituri sau cerințe minime obligatorii.

6. Alte obligații digitale relevante pentru sectorul IT și platforme

Pe lângă NIS2, organizațiile din acest sector pot fi supuse și altor cadre de reglementare, precum:

- obligații privind securitatea platformelor online și a aplicațiilor;
- cerințe impuse de autorități naționale în domeniul digital (de exemplu, ADR);
- obligații privind protecția datelor și confidențialitatea;

- reglementări privind comerțul electronic și serviciile digitale.

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

7. Riscurile tipice în sectorul IT și al platformelor digitale

Riscurile frecvent întâlnite în acest sector includ:

- atacuri cibernetice asupra aplicațiilor și infrastructurii;
- breșe de date și expunerea informațiilor sensibile;
- atacuri de tip DDoS asupra platformelor online;
- compromiterea lanțului de aprovizionare software.

Aceste riscuri pot afecta simultan un număr mare de clienți și utilizatori.

8. Ce lipsește frecvent în sectorul IT și digital

În practică, sunt des întâlnite:

- lipsa unei abordări structurate de management al riscurilor;
- securitate insuficient integrată în ciclul de dezvoltare software;
- dependență excesivă de furnizori terți fără evaluare adecvată;
- planuri insuficiente de răspuns la incidente.

9. Ce se așteaptă, în mod realist, de la organizațiile din acest sector

Așteptările sunt proporționale cu dimensiunea și rolul fiecărei organizații în ecosistemul digital.

În mod realist, se așteaptă:

- implementarea unor măsuri de securitate de bază;
- gestionarea riscurilor asociate serviciilor digitale;

- capacitatea de a detecta și gestiona incidentele;
- transparență față de clienți și parteneri.

10. Recomandări generale pentru sectorul IT și platforme digitale

Pentru majoritatea organizațiilor din domeniu, sunt recomandate:

- evaluarea periodică a riscurilor de securitate;
- integrarea securității în dezvoltarea și operarea serviciilor;
- gestionarea atentă a furnizorilor și partenerilor;
- pregătirea pentru incidente de securitate cibernetică.

11. Ce NU este obligatoriu

Pentru a evita confuziile frecvente:

- nu este obligatorie certificarea ISO;
- nu este impus un anumit furnizor sau tehnologie;
- nu este necesară externalizarea completă a securității IT.

12. Concluzie și pași următori

Acest ghid oferă o imagine generală asupra cerințelor și riscurilor din sectorul IT și al platformelor digitale. Pentru stabilirea obligațiilor exacte și a măsurilor necesare într-un caz concret, este recomandată o analiză dedicată, adaptată specificului organizației.