
# NIS2 și securitatea cibernetică în SECTORUL POȘTĂ ȘI CURIERAT

# NIS2 și securitatea cibernetică în sectorul poștă și curierat

**Ghid orientativ pentru operatori poștali, firme de curierat și servicii de livrare**

## 1. Ce primești din acest document

Acest ghid este conceput pentru organizațiile din sectorul poștal și de curierat și are rolul de a oferi:

- o **imagine clară a nivelului de risc specific sectorului poștă & curierat**;
- 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**, formulate pe înțelesul managementului și al antreprenorilor.

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

## 2. De ce sectorul poștă & curierat este relevant pentru NIS2

Sectorul poștal și de curierat joacă un rol esențial în funcționarea economiei moderne, asigurând circulația documentelor, bunurilor și coletelor pentru persoane fizice, companii și instituții publice. Perturbarea acestor servicii poate afecta lanțurile de aprovizionare, comerțul electronic și serviciile publice.

Operatorii din acest sector utilizează sisteme informatice complexe pentru gestionarea comenzilor, urmărirea coletelor, optimizarea rutelor și interacțiunea cu clienții, fiind expuși constant la riscuri cibernetice.

## 3. Unde se poziționează, în general, sectorul poștă & curierat față de NIS2

Directiva NIS2 include serviciile poștale și de curierat printre domeniile vizate, în special în cazul operatorilor de dimensiuni mari sau cu rol semnificativ în economie.

În funcție de dimensiune, volum de activitate și rol:

- unii operatori poștali și de curierat pot fi **entități NIS2**;
- multe firme de curierat sau livrare **nu intră direct sub incidența NIS2**, dar pot avea obligații indirecte relevante.

Încadrarea exactă depinde de amploarea serviciilor furnizate.

## 4. NIS2 – aplicabilitate directă în sectorul poștă & curierat

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

- operatori poștali naționali;
- companii de curierat de mari dimensiuni;
- furnizori de servicii de livrare cu impact major asupra comerțului și serviciilor publice.

Pentru aceste entități, NIS2 introduce obligații privind:

- managementul riscurilor de securitate cibernetică;
- protejarea sistemelor informatice critice;
- asigurarea continuității serviciilor;
- raportarea incidentelor de securitate.

Nu toate firmele de curierat sau livrare sunt automat entități NIS2.

## 5. NIS2 – aplicabilitate indirectă și lanțul de aprovizionare

Sectorul poștal și de curierat este strâns integrat cu alte sectoare critice, precum comerțul electronic, administrația publică și serviciile financiare.

Obligații indirecte pot apărea atunci când organizațiile:

- furnizează servicii către entități NIS2;
- gestionează date sau sisteme pentru clienți reglementați;
- sunt parte din lanțuri logistice critice.

În aceste cazuri, cerințele de securitate sunt adesea stabilite prin contracte și politici ale partenerilor mari.

## 6. Alte obligații digitale relevante pentru sectorul poștă & curierat

Pe lângă NIS2, organizațiile din acest sector pot fi supuse și altor cerințe, precum:

- obligații privind protecția datelor cu caracter personal;
- cerințe privind securitatea platformelor online și aplicațiilor;
- reglementări asociate comerțului electronic;
- cerințe impuse de autorități naționale în domeniul digital.

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

## 7. Riscurile tipice în sectorul poștă & curierat

Riscurile frecvent întâlnite includ:

- atacuri cibernetice asupra sistemelor de urmărire și livrare;
- indisponibilitatea platformelor de comandă;
- compromiterea datelor clienților;
- perturbarea operațiunilor logistice.

Impactul poate fi semnificativ din punct de vedere operațional și reputațional.

## 8. Ce lipsește frecvent în sectorul poștă & curierat

În practică, sunt frecvent identificate:

- măsuri insuficiente de securitate a aplicațiilor;
- lipsa unei abordări structurate de management al riscurilor;
- proceduri incomplete de răspuns la incidente;
- responsabilități neclare privind securitatea IT.

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

Așteptările sunt proporționale cu dimensiunea și rolul organizației.

În mod realist, se așteaptă:

- măsuri de securitate adaptate volumului de date procesate;
- gestionarea riscurilor digitale;
- capacitatea de a preveni și gestiona incidente;
- respectarea cerințelor contractuale ale partenerilor.

## 10. Recomandări generale pentru sectorul poștă & curierat

Pentru majoritatea organizațiilor din domeniu, sunt recomandate:

- evaluarea periodică a riscurilor cibernetice;
- protejarea sistemelor critice și a datelor clienților;
- clarificarea responsabilităților interne;
- pregătirea pentru incidente de securitate și întreruperi operaționale.

## 11. Ce NU este obligatoriu

Pentru a evita confuziile:

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

## 12. Concluzie și pași următori

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