**Expunere de motive**
**la proiectul de Ordin al Directorului Directoratului Național de Securitate Cibernetică pentru aprobarea criteriilor și pragurilor de determinare a gradului de perturbare a unui serviciu și metodologia de evaluare a nivelului de risc al entităților**

## I. Context și cadru de reglementare

Directiva (UE) 2016/1148 (Directiva NIS) a avut drept scop consolidarea capacităților în materie de securitate cibernetică în întreaga Uniune Europeană, atenuarea amenințărilor la adresa rețelelor și sistemelor informatice utilizate pentru a furniza servicii esențiale în sectoare-cheie și asigurarea continuității acestor servicii atunci când se confruntă cu incidente, contribuind astfel la securitatea Uniunii Europene. Transpunerea acesteia în legislația națională s-a realizat prin emiterea Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, în prezent abrogată.

De la intrarea în vigoare a Directivei NIS s-au înregistrat progrese semnificative în ceea ce privește creșterea nivelului de reziliență cibernetică în Uniunea Europeană. Reexaminarea acesteia a arătat că prevederile sale au servit drept catalizator pentru abordarea instituțională și de reglementare a securității cibernetice în Uniunea Europeană, deschizând astfel calea pentru schimbări semnificative în domeniu. Cu toate acestea, reexaminarea Directivei NIS a evidențiat și deficiențe inerente care o împiedică să soluționeze în mod eficace provocările actuale și cele emergente în materie de securitate cibernetică.

În acest context a fost adoptată Directiva (UE) 2022/2555 (Directiva NIS2) care aduce ca noutate inclusiv reguli mai aplicate privitoare la procesele pe care entitățile trebuie să le urmeze în vederea conformării lor cu cerințele emise.

Prin Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil a fost realizată transpunerea Directivei NIS2 în legislația națională. În ceea ce privește caracteristicile de abordare a problematicilor la nivelul actului normativ menționat, precizăm că acesta prevede reguli mult mai aplicate, în special cu privire la procesul de identificare a entităților susceptibile a face parte din domeniul de aplicare al legii.

În acest sens, pe tot parcursul elaborării Ordonanței de urgență a Guvernului nr. 155/2024, s-a urmărit ca rezultatul final al aplicării legii asupra fiecărei entități vizate să fie proporțional cu caracteristicile acesteia. Pentru a putea atinge un astfel de obiectiv, a fost prevăzut un set de dispoziții specifice care să asigure o cartografiere cât mai clară a situației în care entitatea vizată se află la momentul analizării acesteia, cu posibilitatea actualizării acestor date în funcție de modificările pe care entitatea în cauză le suferă.

În vederea implementării dispozițiilor art. 9 - 10 și 18 din Ordonanța de urgență a Guvernului nr. 155/2024, în cadrul aceluiași act normativ a fost prevăzută în sarcina autorității responsabile obligația de a elabora cerințele specifice aplicării acestora.

## II. Scopul și obiectul reglementării

Prin prezentul proiect de ordin, Directoratul Național de Securitate Cibernetică, în continuare DNSC, realizează implementarea prevederilor art. 10 alin. (2) și ale art. 18 din Ordonanța de urgență a Guvernului nr. 155/2024, reglementând criteriile și pragurile de determinare a gradului de perturbare a unui serviciu, elemente procedurale privind evaluarea nivelului de risc al entităților, inclusiv valorile sectoriale pentru stabilirea nivelului de risc utilizate în evaluarea acestuia.

## III. Interpretarea generală și clarificarea acesteia

Prin intermediul proiectului de ordin se urmărește clarificarea cadrului de criterii și reguli privind procesul de identificare a entităților ca esențiale ori importante prin elemente suplimentare decât cele care țin de sector, tip de activitate și dimensiune, cât și evaluarea entităților din perspectiva riscurilor pe care acestea le pot genera la nivel societal în vederea stabilirii nivelului de complexitate a cerințelor privind măsurile de securitate pe care trebuie să le implementeze conform dispozițiilor art. 11 - 13 din Ordonanța de urgență a Guvernului nr. 155/2024.

În acest sens, proiectul de ordin stabilește, în primul rând, modalitatea de interpretare a dispozițiilor art. 9 lit. b) și c) din Ordonanța de urgență a Guvernului nr. 155/2024. Dispozițiile menționate se aplică acelor entități care, conform criteriului dimensiune, se încadrează în categoriile de întreprinderi mici și microîntreprinderi și care nu au fost identificate ca entități esențiale sau importante prin criteriile referitoare la apartenența la sector, subsector, tip de activitate derulată și/sau la dimensiune.

Precizăm că, astfel cum este prevăzut în proiectul de ordin pentru aprobarea cerințelor privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor, o entitate care este unic furnizor la nivel național al unui serviciu care face parte din lista de activități prevăzută în Anexa nr. 1 la Ordonanța de urgență a Guvernului nr. 155/2024, va fi identificată ca entitate esențială, iar o entitate care este unic furnizor la nivel național al unui serviciu care face parte din lista de activități prevăzută în Anexa nr. 2 la Ordonanța de urgență a Guvernului nr. 155/2024, va fi identificată ca entitate importantă.

În plus, subliniem și faptul că o entitate din sectoarele prevăzute în Anexele nr. 1 și 2 la Ordonanța de urgență a Guvernului nr. 155/2024 care a fost desemnată drept infrastructură informatică și de comunicații de interes național, în conformitate cu Legea nr. 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice și de comunicații de interes național și condițiile implementării rețelelor 5G, va fi identificată ca entitate esențială.

În vederea determinării gradului de perturbare pe care entitățile îl pot genera la nivelul societății, prezentul proiect de ordin detaliază o serie de praguri ce trebuie utilizate pentru a stabili impactul asupra fiecărei categorii de valori (sociale, economice și de securitate) ce poate fi afectată [prevăzute la art. 10 alin. (1) din Ordonanța de urgență a Guvernului nr. 155/2024]. De asemenea, această serie de praguri se utilizează și în stabilirea impactului asupra relațiilor de cooperare, prin analiza efectului extins asupra mai multor sectoare de importanță critică ori în plan transfrontalier, prin afectarea mai multor state. Astfel, în vederea determinării gradului de perturbare sunt utilizate mai multe categorii de impact (scăzut, mediu și ridicat). Aceste

categorii au menirea de a evalua importanța socială a entității și nivelul aferent de obligații, astfel cum acestea vor fi înscrise în cadrul ordinului privind măsurile de gestionare a riscurilor, pe care aceasta trebuie să le îndeplinească.

În vederea determinării categoriei de impact pe care entitatea îl poate genera, aceasta trebuie să ia în considerare efectul potențial maxim al compromiterii, blocării ori distrugerii complete a datelor, serviciului sau infrastructurii entității.

O variantă prin care acestea pot realiza autoevaluarea nivelului de impact este cea de utilizare a unor scenarii de situații de criză cibernetică, care trebuie să respecte următoarele condiții de definire a acestora (trebuie să fie respectate toate condițiile, simultan):

- utilizarea de vectori de amenințare plauzibili și relevanți pentru sectorul din care face parte;
- lipsa sau eșecul total al mecanismelor de protecție, prevenție, răspuns și back-up sau recuperare în caz de dezastru;
- imposibilitatea de a asigura continuitatea serviciilor esențiale prin metode alternative.

În cadrul utilizării scenariului, pentru evaluarea impactului se au de asemenea în vedere, după caz, efectele asupra serviciilor interdependente din alte sectoare sau state membre, cât și durata și amploarea geografică a perturbării produse până la repunerea în funcțiune a serviciului.

De asemenea, în vederea corectei aplicări a scenariului, entitatea va:

- identifica și inventaria serviciile și activele critice pentru desfășurarea activității;
- inventaria interdependențele interne (procese, sisteme IT&C) și externe (cu furnizori externi, parteneri, alte sisteme interconectate, utilități etc.);
- inventaria entitățile cu care este interconectată, în special din alte sectoare sau alte state membre.

În desfășurarea scenariului, entitatea va evalua toate categoriile de impact care îi sunt aplicabile, luând în considerare specificul activității sale și analiza interdependențelor și va stabili, conform prevederilor prezentului proiect de ordin, valorile de prag sau măsura în care se încadrează în nivelurile prevăzute în cadrul anexei nr. 1 la proiectul de ordin.

- Reiterăm faptul că măsurile de securitate de orice fel, existente la nivelul entității, sunt irelevante pentru scopul acestei analize care nu are ca obiect stabilirea nivelului de maturitate cibernetică a organizației.

Autoevaluarea gradului de perturbare trebuie realizată și transmisă către DNSC, atunci când entitatea se încadrează în situațiile menționate mai sus, și va fi utilizată în cadrul procesului de identificare a entităților.

Astfel, recomandăm ca autoevaluarea să se realizeze pe bază de scenarii, sens în care, la momentul transmiterii acesteia către DNSC, să se atașeze și documente relevante în atestarea datelor furnizate.

Criteriile și pragurile pentru determinarea impactului prevăzute în cadrul anexei nr. 1 la prezentul proiect de ordin sunt utilizate și în cadrul etapei de evaluare a nivelului de risc al entității.

Cel mai înalt nivel de impact identificat la orice categorie de impact determină nivelul după care va fi evaluată categoria în care se încadrează entitatea.

Evaluarea nivelului de risc este destinată tuturor entităților care fac obiectul legii, cu excepția celor cărora li se aplică Regulamentul (UE) 2022/2.554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1.060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1.011 (Regulamentul DORA) și al furnizorilor de servicii DNS, registrele de nume TLD, furnizorilor de servicii de cloud computing, furnizorilor de servicii de centre de date, furnizorilor de rețele de furnizare de conținut, furnizorilor de servicii gestionate, furnizorilor de servicii de securitate gestionate, furnizorilor de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, precum și prestatorilor de servicii de încredere.

Metodologia de evaluare a nivelului de risc a fost elaborată pentru a asigura proporționalitatea măsurilor de securitate cibernetică ce vor fi impuse prin puterea legii entităților identificate drept esențiale și importante, luând în calcul nivelul de risc reprezentat de acestea în plan societal. În acest sens, nivelul de risc este influențat în principal de factori precum sectorul din care face parte entitatea și dimensiunea acesteia.

DNSC stabilește profilul de risc pentru fiecare sector, conținând valorile aferente modului de manifestare predilectă a fiecărui tip de atac, impactul acestuia, dar și probabilitatea riscurilor rezultate corespunzător derulării fiecărui tip de atac de către fiecare tip de atacator.

Entitățile preiau profilul de risc corespunzător sectorului din care fac parte, corelat cu dimensiunea proprie. În situația în care acestea reprezintă o excepție de la profilul de risc sectorial, pot solicita, temeinic justificat, modificarea nivelului de impact sau probabilitate a riscurilor. Entitatea va trebui să aducă argumente distinct, pentru fiecare valoare pentru care solicită modificarea, susținute cu date concrete.

Precizăm că implementarea de controale pentru gestionarea riscurilor la nivel de entitate nu este relevantă din perspectiva valorii de risc în acest context deoarece evaluarea nivelului de risc nu conține valorile reziduale ale riscurilor, ci valorile absolute ale acestora.

Astfel, scopul evaluării este cel de determinare a profilului de risc al entității pentru a stabili totalitatea controalor de gestionare a riscurilor care trebuie să fie impementate de către entitate. În acest sens, două entități de același tip pot avea un profil de risc similar, însă niveluri de maturitate a securității cibernetice diferite. În această situație, cele două entități vor implementa același set de cerințe privind măsurile de securitate, dar ecartul dintre situația actuală și starea de conformitate cu cerințele prevăzute de Ordonanța de urgență a Guvernului nr. 155/2024 va fi diferit.