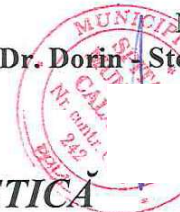




APROBAT,

.....  
Manager,  
Dr. Dorin - Stelian Niță



***STRATEGIA DE SECURITATE CIBERNETICĂ  
A SPITALULUI MUNICIPAL CALAFAT  
IN PERIOADA 2026-2031***

**1. SCOPUL**

Strategia de securitate cibernetică a Spitalului Municipal Calafat are scopul de a defini și de a menține un mediu cibernetic sigur, cu un înalt grad de reziliență și de încredere.

Totodată, Strategia de securitate cibernetică prezintă principiile, obiectivele și direcțiile principale de acțiune pentru cunoașterea, prevenirea și contracararea amenințărilor, vulnerabilităților și riscurilor la adresa securității cibernetică a instituției, în deplină concordanță cu natura activității sale specifice.

**2. DOMENIU APLICARE**

Strategia de securitate cibernetică a Spitalului Municipal Calafat acoperă toate activitățile specifice și se adresează întregului personal al instituției, tuturor partenerilor/ colaboratorilor, furnizorilor și terților, precum și pacienților/ clienților săi.

**3. DOCUMENTE DE REFERINȚĂ (REGLEMENTĂRI)**

**3.1. Reglementări internaționale**

- SR ISO/ CEI 27001: 2022 – Tehnologia informației. Tehnici de securitate. Sisteme de management a securității informației;
- SR EN ISO 9001:2015 – Sisteme de management al calității. Cerințe;
- SR ISO/ CEI 27002: 2022 - Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației;
- Directiva (UE) 2016/ 1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune;
- Regulamentul (UE) nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

**3.2. Legislație primară**

- HG nr. 1.321/2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022—2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022—2027;

- OUG nr.155, din 30.12.2024, privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil;
- Legea nr.124 din 7 iulie 2025 pentru aprobarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil;
- HG nr. 832 din 11 iulie 2024, privind aprobarea Strategiei naționale în domeniul inteligenței artificiale 2024-2027;
- Legea 362/ 2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice;
- Legea nr.182/2002, din 12 aprilie 2002, privind securitatea informațiilor clasificate;
- HG nr.585/2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România;
- HG nr. 781, din 25 iulie 2002 privind protecția informațiilor secrete de serviciu;
- Legea nr. 333, din 2003. privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor;
- Legea nr. 95/2006 privind reforma în domeniul sănătății, cu modificările și completările ulterioare;
- Legea nr. 273/2006 privind finanțele publice locale cu modificări și completări ulterioare;
- Legea nr. 500/2002 privind finanțele publice cu modificări și completări ulterioare;
- Legea nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public;
- Legea nr. 190/ 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/ 679 al Parlamentului European și al Consiliului.

### **3.3. Legislație secundară**

- Ordinul ministrului sănătății Nr. 446/2017, din 18 aprilie 2017, privind aprobarea Standardelor, Procedurii și metodologiei de evaluare și acreditare a spitalelor;
- OSGG 600/ 2018 – privind aprobarea Codului controlului intern managerial al entităților publice;
- Ordinul 1537/2018 privind stabilirea atribuțiilor principale ale responsabililor cu managementul calității din cadrul Ministerului Sănătății și unităților aflate în subordinea, coordonarea sau sub autoritatea acestuia pentru implementarea și gestionarea Sistemului de management al calității bazat pe standardul SR EN ISO 9001:2015, cu completările și modificările ulterioare.
- Ordinul Ministrului Sănătății și al Președintelui Autorității Naționale de Management al Calității în Sănătate nr. 1312/250/2020 privind organizarea și funcționarea structurii de management al calității serviciilor de sănătate în cadrul unităților sanitare cu paturi și serviciilor de ambulanță, în procesul de implementare a sistemului de management al calității serviciilor de sănătate și siguranței pacientului, cu modificările și completările ulterioare;
- OSGG 1.323/ 2020 – de aprobare a Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale ;
- Ghidul pentru implementarea măsurilor minime de securitate aplicabile OSE – DNSC;

### **3.4. Alte documente, inclusiv reglementări interne**

- Regulamentul intern (RI) al Spitalului Municipal Calafat;
- Regulamentul de organizare și funcționare (ROF) al Spitalului Municipal Calafat;

## 4. STRATEGIA DE SECURITATE CIBERNETICĂ

### 4.1. Introducere

Evoluția rapidă a domeniului tehnologic și dinamica amenințării cibernetice sunt condiții determinante pentru actualizarea și dezvoltarea permanentă a cadrului normativ instituțional pe componenta gestionării amenințărilor cibernetice și asigurării securității cibernetice.

Atacurile cibernetice, în special asupra serviciilor esențiale ori a infrastructurilor critice pot avea, datorită interconectivității, un impact major asupra serviciilor furnizate.

Strategia națională de securitate cibernetică, obligă Spitalul Municipal Calafat să dezvolte, să mențină și să implementeze propria Strategie de securitate cibernetică, document care va constitui temelia întregului cadru normativ instituțional privitor la securitatea cibernetică.

Strategia de securitate cibernetică se adresează întregului personal al Spitalului Municipal Calafat, inclusiv colaboratorilor și partenerilor, furnizorilor de servicii și echipamente IT&C, precum și pacienților, clienților, publicului și terților.

### 4.2. Principii

În vederea asigurării securității cibernetice a Spitalului Municipal Calafat trebuie respectate următoarele **principii**:

- Securitatea cibernetică a Spitalului Municipal Calafat este responsabilitatea tuturor actorilor implicați:
  - instituții ale administrației publice,
  - personalul desemnat pentru asigurarea securității cibernetice,
  - utilizatorii sistemului informatic al instituției,
  - furnizorii de servicii IT&C,
- Securitatea cibernetică sprijină funcționarea Spitalului Municipal Calafat;
- Securitatea cibernetică se bazează pe stabilirea unui cadru normativ și procedural adecvat;
- Securitatea cibernetică a Spitalului Municipal Calafat garantează:
  - menținerea unui spațiu cibernetic deschis, liber, stabil și sigur;
  - protejarea valorilor - politicile de securitate cibernetică vor asigura echilibrul între nevoia de creștere a securității în spațiul cibernetic și prezervarea dreptului la intimitate și alte valori și libertăți fundamentale ale cetățeanului și a statului de drept, în special în ceea ce privește libertatea de opinie, libertatea de exprimare, dreptul de a accesa și de a primi informații;
  - protejarea datelor cu caracter personal.

### 4.3. Viziunea

În concordanță cu Planul strategic de dezvoltare, Spitalul Municipal Calafat urmărește furnizarea de servicii medicale diversificate, de cea mai bună calitate, care să vină în intampinarea dezideratului nostru principal: « VINDECAREA BOLII SI RECUPERAREA TOTALA » sau în ultima situație « AMELIORAREA SIMPTOMATOLOGIEI » având în vedere permanent SATISFACTIA PACIENTULUI.

Evoluția digitală și cadrul normativ național și internațional reconfigurează provocările la adresa misiunii Spitalului Municipal Calafat, fiind create premisele dezvoltării capabilităților tehnologice și

implicat a infrastructurii IT&C prin implementarea unor soluții de nouă generație, interconectate, care să permită conjugarea eforturilor tuturor structurilor în vederea asigurării atribuțiilor instituționale.

Totodată, având în vedere locul și rolul Spitalului Municipal Calafat în furnizarea de servicii medicale de înaltă calitate, procesul de digitalizare a acestora se realizează în concordanță cu demersurile întreprinse la nivel național.

În acest context, problematica securității cibernetice cunoaște o diversificare accelerată a metodelor, tehnicilor și mijloacelor de asigurare a protecției infrastructurilor informatice, fapt care impune adoptarea unor măsuri și acțiuni actualizate, în baza diagnozelor și/sau prognozelor realizate.

Acțiunile necesare a fi întreprinse vizează dezvoltarea următoarelor paliere:

- **prevenire și securizare** - cunoașterea amenințărilor, vulnerabilităților și riscurilor în vederea implementării permanente a măsurilor de actualizare a politicilor de securitate;
- **monitorizare și detecție** - dezvoltarea mecanismului de indexare, detectare, investigare și analiză a incidentelor și atacurilor informatice;
- **răspuns și contracarare** - adoptarea unor măsuri de răspuns la atacurile informatice;
- **documentare și atribuire** - creșterea capabilităților investigative pentru identificarea agresorilor cibernetici și atribuirea tehnică a atacurilor. În conceptul de securitate cibernetică sunt incluse totalitatea măsurilor întreprinse în vederea prevenirii și contracarării amenințărilor din spațiul cibernetic, inclusiv în ceea ce privește nivelul culturii de securitate a personalului propriu.
- **cunoaștere și prevenire** - pregătirea continuă pentru cunoașterea amenințărilor, modalităților de realizare și măsurilor minime de securizare;
- **detecție și semnalare** - adoptarea unor măsuri de identificare a elementelor suspecte și de raportare imediată.

#### 4.4. Misiunea

În acord cu misiunea instituțională definită în Planul strategic de dezvoltare, Spitalul Municipal Calafat își asumă:

- **îmbunătățirea calitatii actului medical și diversificarea serviciilor oferite populației, cu respectarea drepturilor pacienților și drepturilor cetățenilor;**
- **îmbunătățirea continuă a calității vieții pacienților, prin oferirea de servicii medicale profesionale, sigure și centrate pe nevoile acestora și**
- **asigurarea siguranței pacientului** (inclusiv a confidențialității datelor acestuia) prin folosirea:
  - de tehnologii avansate:
    - ✓ tehnică și echipamente medicale;
    - ✓ echipamente și sisteme IT&C;
  - de echipe de specialiști, dedicate.

Pentru furnizarea de servicii medicale profesionale, de cea mai înaltă calitate și sigure, Spitalul Municipal Calafat:

- va dezvolta și să asigure un sistem informatic și de comunicații (SIC) rezilient, accesibil și ușor de utilizat;
- va oferi pacienților, aparținătorilor acestora și celorlalți beneficiari ai serviciilor furnizate:
  - alegeri informate și servicii sigure, de înaltă calitate și echitabile, precum și
  - suport pentru servicii medicale integrate;

- va sprijini perfecționarea competențelor și motivarea angajaților în direcția utilizării rețelelor și sistemelor informatice instituționale în condiții de securitate cibernetică deplină;
- va asigura investiții adecvate, în securitatea cibernetică, în vederea furnizării neîntrerupte a serviciilor medicale preventive și curative.

Pentru aceasta, conform cerințelor standardelor de securitate cibernetică privitoare la sistemele informatice care asigură furnizarea serviciilor medicale Spitalul Municipal Calafat a instituit și aplică un **Sistem de Management al securității cibernetică**, în vederea asigurării:

- Securității datelor și informațiilor;
- Securității activelor/ resurselor informatice și de comunicații;
- Protecției datelor cu caracter personal.

#### 4.5. Declarația privind Strategia de securitate cibernetică

Spitalul Municipal Calafat este angajat deplin în:

- Dezvoltarea activității IT&C în acord cu nevoile și așteptările părților interesate (interne și externe);
- Asigurarea și furnizarea de servicii medicale integrate, aliniate la principiul ”îmbunătățirii continue”;
- Implicarea întregului personal în creșterea eficienței și calității serviciilor furnizate;
- Protejarea rețelelor și sistemelor informatice (NIS), precum și a datelor și informațiilor procesate în acestea de atacuri cibernetică;
- Asigurarea, consolidarea și promovarea rezilienței rețelelor și sistemelor informatice;
- Asigurarea unui mediu digital sigur, prin crearea, implementarea și adaptarea continua a unui cadru normativ intern în acord cu cerințele legislative și normative naționale și internaționale;
- Asigurarea Cooperării și colaborării, în domeniul securității NIS, cu părțile interesate și autoritățile desemnate ale statului;
- Promovarea culturii de securitate cibernetică în rândul angajaților proprii, furnizorilor și terților.

Conducerea Spitalului Municipal Calafat are în vedere îndeplinirea rolului deținut de instituție în sistemul național de sănătate și se preocupă, permanent, de menținerea, aplicarea și îmbunătățirea continua a eficacității sistemului de management la resurselor și infrastructurii IT&C pentru furnizarea de servicii medicale prompte, eficiente și de înaltă calitate, în vederea satisfacerii cerințelor pacienților, aparținătorilor, precum și a terților.

#### 4.6. Obiectivele privind securitatea cibernetică

- Consolidarea cadrului normativ și procedural instituțional
- Rețele și sisteme informatice sigure și reziliente
- Creșterea capacității de răspuns
- Educație și conștientizare
- Cooperare interinstituțională

#### 4.7. Planul de acțiune strategic

**Planul de acțiune strategic** acționează ca un ”ghid procedural” care, pentru atingerea/ îndeplinirea fiecăruia dintre obiectivele strategice ale Spitalului Municipal Calafat, va specifica, cel puțin:

- măsurile stabilite pentru asigurarea un mediu digital sigur
- principalele acțiuni planificate

- participanții
- responsabilul/ coordonatorul acțiunilor și
- termenul de implementare.

#### 4.8. Bugetul pentru securitatea cibernetică

Bugetul pentru securitate cibernetică își propune să asigure resursele financiare necesare pentru implementarea:

- **Planului de acțiune strategic și a**
- **Obiectivelor și direcțiilor de acțiune privind securitatea cibernetică.**

**Bugetul pentru securitatea cibernetică** trebuie să îndeplinească următoarele **caracteristici**:

- să fie conform cu politicile, cerințele legislative și de reglementare, ordinele și deciziile relevante în determinarea bugetului pentru securitate cibernetică, astfel încât să asigure disponibilitatea tehnologiilor și instrumentelor de securitate cibernetică;
- să fie precis, rațional și să includă toate cheltuielile preconizate pentru asigurarea securității cibernetică;
- să se bazeze pe ciclul bugetar anual al Spitalului Municipal Calafat;
- să fie supus revizuirii regulate în conformitate cu politicile și procedurile Spitalului Municipal Calafat.

#### Componentele bugetare

Bugetul pentru securitate cibernetică va fi compus din:

- **Bugetul pentru operarea funcției de securitate cibernetică, inclusiv:**
  - Costuri cu resursele umane
  - Costuri cu serviciile de consultanță
  - Costuri cu tehnologia
  - Alte costuri.
- **Bugetul pentru inițiativele și programele de securitate cibernetică, inclusiv:**
  - Costuri unice pentru configurarea funcției de securitate cibernetică și a proceselor aferente pentru implementarea Strategiei de securitate cibernetică.
  - Costuri recurente care acoperă măsurile de securitate cibernetică (de exemplu, gestionarea securității cibernetică, monitorizarea, raportarea, conformitate, audituri de securitate, etc.)
  - Costul programelor specializate de dezvoltare a competențelor și al instruirilor necesare pentru personalul de securitate cibernetică, cum ar fi cursuri de instruire și conferințe.
  - Costuri de externalizare.

## 4. RESPONSABILITĂȚI

4.1. **Forurile decizionale ale Spitalului Municipal Calafat** au următoarele responsabilități:

- stabilesc și aprobă **Strategia de securitate cibernetică**;
- asigură disponibilitatea resurselor (financiare, tehnologice și umane) necesare pentru aplicarea Strategiei de securitate cibernetică, precum și a politicilor și procedurilor de securitate IT&C;

- comunică importanța unei gestionări eficiente a securității cibernetice.

#### 4.2. Managerul Spitalului Municipal Calafat:

- aprobă **Strategia de securitate cibernetică**;
- aprobă **Planul de acțiune pentru implementarea Strategiei de Securitate Cibernetică**;
- alocă, cu eficiență, resursele financiare, tehnologice și umane necesare aplicării Strategiei de securitate cibernetică;

#### 4.3. Responsabilul cu securitatea rețelelor și sistemelor informatice (RSRSI)/ Responsabilul IT&C (angajat al organizației sau angajat al unui furnizor de servicii IT&C) are următoarele responsabilități:

- propune revizuirii/ modificării/ actualizării ale **Strategiei de securitate cibernetică**;
- elaborează **Planul de acțiune pentru implementarea Strategiei de securitate cibernetică** și monitorizează îndeplinirea acestuia;
- elaborează și propune spre aprobare politici și proceduri operaționale de securitate în conformitate cu Strategia de securitate cibernetică;
- propune **Bugetul pentru securitate cibernetică** care să asigure resursele financiare necesare pentru implementarea **Planului de acțiune pentru implementarea Strategiei de securitate cibernetică**.

#### 4.4. Șefii structurilor/ entităților organizatorice sunt responsabili pentru:

- implementarea de zi cu zi a:
  - Strategiei de securitate cibernetică,
  - Planului de acțiune pentru implementarea Strategiei de securitate cibernetică;
  - politicilor și procedurilor operaționale de securitate aferente strategiei;
- asigurarea că obiectivele și direcțiile de acțiune stabilite în Strategia de securitate cibernetică sunt implementate și aplicate în mod corespunzător și de către tot personalul din subordine,
- asigurarea resurselor necesare pentru ca Strategia de securitate cibernetică să fie aplicată în mod corespunzător în zona lor de responsabilitate.

#### 4.5. Utilizatorii autorizați ai sistemelor (angajați și terți care acționează într-o modalitate similară, cum ar fi furnizori de servicii) sunt responsabili pentru:

- cunoașterea și respectarea Strategiei de securitate cibernetică.

#### 4.6. Colaboratorii și angajații furnizorilor de servicii au următoarele responsabilități:

- respectă Strategia de securitate cibernetică a Spitalului Municipal Calafat, pe timpul derulării contractului.

## 5. DEFINIȚII ALE TERMENILOR

| Nr. crt. | Termenul              | Definiția și/sau, dacă este cazul, actul care definește termenul  |
|----------|-----------------------|---|
| 1.       | Managementul riscului | Un proces complex, continuu și flexibil de identificare, evaluare și contracarare a riscurilor la adresa securității cibernetice, bazat pe utilizarea unor tehnici și instrumente complexe, pentru prevenirea pierderilor de orice natură |

| Nr. crt. | Termenul                              | Definiția și/sau, dacă este cazul, actul care definește termenul   |
|----------|---------------------------------------|--|
| 2.       | Apărare cibernetică                   | Acțiune care are în vedere obiectivele domeniului, respectiv: <ul style="list-style-type: none"> <li>➤ asigurarea managementului incidentelor de securitate;</li> <li>➤ detectarea și tratarea incidentelor de securitate care afectează securitatea rețelelor și sistemelor informatice.</li> </ul>   |
| 3.       | Securitatea cibernetică               | Starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic ale resurselor și serviciilor publice sau private din spațiul cibernetic;  |
| 4.       | Securitatea informației               | Păstrarea confidențialității, integrității și a disponibilității informației;<br>În plus, pot fi implicate de asemenea și alte proprietăți precum autenticitatea, responsabilitatea, nerepudierea și fiabilitatea.   |
| 5.       | Rețea și sistem informatic            | <p>Înseamnă:</p> <ol style="list-style-type: none"> <li>1. O <b>rețea de comunicații electronice</b> respectiv: <ul style="list-style-type: none"> <li>• <b>sistemele de transmisie</b>, bazate sau nu pe o infrastructură permanentă sau pe o capacitate de administrare centralizată, și, acolo unde este cazul, echipamentele de comutare sau rutare și alte resurse, inclusiv elementele de rețea care nu sunt active, care permit transportul semnalelor prin cablu, prin unde radio, prin mijloace optice ori alte mijloace electromagnetice, incluzând rețelele de comunicații electronice prin satelit, rețelele terestre fixe, cu comutare de circuite și cu comutare de pachete, inclusiv internet, și mobile,</li> <li>• <b>rețelele electrice</b>, în măsura în care sunt utilizate pentru transmiterea de semnale,</li> <li>• <b>rețelele utilizate pentru transmisia serviciilor media audiovizuale și</b></li> <li>• <b>rețelele de televiziune prin cablu</b>, indiferent de tipul de informație transmisă</li> </ul> </li> <li>2. Orice <b>dispozitiv</b> sau <b>ansamblu de dispozitive interconectate</b> sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor digitale cu ajutorul unui program informatic;</li> <li>3. <b>Datele digitale</b> stocate, prelucrate, recuperate sau transmise de elementele unei rețele sau unui sistem informatic, în vederea funcționării, utilizării, protejării și întreținerii lor;</li> </ol> |
| 6.       | Resurse informatice și de comunicații | Toate dispozitivele de tipărire/imprimare, dispozitive de afișare, unități de stocare și toate activitățile asociate stației de lucru/ calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze email-uri, să navigheze pe site-uri web, capabil să transmită, stocheze, administreze date și informații în format electronic, incluzând, dar fără a se limita la: servere, calculatoare personale, laptop-uri, smartphone-uri, sisteme de procesare distribuită, echipament de laborator și medical conectat la rețea și controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante și alte accesorii. La acestea se adaugă procedurile, echipamentele, facilitățile, programele și datele care sunt proiectate, construite, puse în funcțiune (operaționale) și menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afișa și transmite informația.   |
| 7.       | Confidențialitate                     | Proprietatea ca informația să nu fie făcută disponibilă sau divulgată unor persoane, entități, sau procese neautorizate.   |
| 8.       | Integritate                           | Proprietatea de a proteja acuratețea și completitudinea resurselor.  |

| Nr. crt. | Termenul                                  | Definiția și/sau, dacă este cazul, actul care definește termenul   |
|----------|---|--|
| 9.       | Disponibilitate                           | Proprietatea de a fi accesibil și utilizabil la cerere de către o entitate autorizată.   |
| 10.      | Securitatea fizică                        | Domeniul securității care prezintă atât măsuri pentru prevenire cât și pentru împiedicarea atacatorilor să aibă acces la obiective, resurse sau informații și recomandări privind proiectarea infrastructurii pentru a opune rezistență la actele ostile.  |
| 11.      | Protecție                                 | Acțiune care are în vedere obiectivele domeniului, respectiv: <ul style="list-style-type: none"> <li>➤ asigurarea securității rețelelor și sistemelor informatice,</li> <li>➤ securitatea fizică și a persoanei;</li> <li>➤ administrarea și mentenanța resurselor rețelelor și sistemelor informatice;</li> <li>➤ controlul accesului la elementele/ componentele rețelelor și sistemelor informatice.</li> </ul> |
| 12.      | Atac                                      | Încercare de a distruge, a expune, a modifica, a dezactiva, a fura sau a obține accesul neautorizat sau a utiliza în mod neautorizat o resursă.  |
| 13.      | Amenințare                                | Cauză potențială a unui incident nedorit care poate produce daune unui sistem sau organizației.  |
| 14.      | Vulnerabilitate                           | Slăbiciune a unei resurse sau a unui mijloc de control care poate fi exploatată de o amenințare.   |
| 15.      | Spațiul cibernetic                        | Mediul virtual, generat de infrastructurile cibernetice, incluzând conținutul informațional procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta.  |
| 16.      | Eveniment privind securitatea informației | Fapt identificat în legătură cu starea unui sistem, a unui serviciu, sau a unei rețele indicând o posibilă încălcare a politicii de securitate a informației, un eșec al mijloacelor de control sau o situație ignorată anterior dar care poate fi relevantă din punct de vedere al securității.   |
| 17.      | Incident privind securitatea informației  | Unul sau o serie de evenimente privind securitatea informației nedorite sau neprevăzute care au o probabilitate semnificativă de compromitere a operațiunilor de business și de amenințare a securității informației.  |
| 18.      | Reziliența infrastructurilor cibernetice  | Capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic și de a reveni la starea de normalitate   |

### 5.1. Abrevieri ale termenilor

| Nr. crt. | Abrevierea | Termenul abreviat   |
|----------|------------|---|
| 1.       | ISO        | Organizația Internațională pentru Standardizare                                     |
| 2.       | CEI        | Comisia Electrotehnică Internațională   |
| 3.       | SR         | Standard român  |
| 4.       | UE         | Uniunea Europeană   |
| 5.       | NIS        | Network and Information Security (în română Securitatea rețelei și a informațiilor) |
| 6.       | SIC        | Sistem Informatic și de Comunicații   |
| 7.       | IT&C       | Tehnologia Informațiilor și Comunicațiilor  |
| 8.       | DNCS       | Directoratul Național de Securitate Cibernetică                                     |
| 9.       | RI         | Regulamentul intern   |
| 10.      | ROF        | Regulamentul de organizare și funcționare   |

Elaborat,

Şef Serviciu RU-Juridic, Statistica-Informatică

C

F

1

Rețelelor și Sistemelor Informatice  
t SRL

M