



Autor	ANCOM
Persoană de contact	Costin MASILIEV
Cod document	2013/04/01/RO
Data publicării inițiale	24 aprilie 2013
Data ultimei modificări	-
Data încheierii procesului de consultare publică	27 mai 2013
Statut	Proiect
Acțiune așteptată	Răspuns

În temeiul prevederilor art. 3 lit. d), art. 10 alin. (1) pct. 1, art. 11 alin. (1) și art. 12 alin. (1) și (3) din Ordonanța de urgență a Guvernului nr. 22/2009 privind înființarea Autorității Naționale pentru Administrare și Reglementare în Comunicații, aprobată prin Legea nr. 113/2010, cu modificările și completările ulterioare, precum și ale art. 46 – 48 din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată cu modificări și completări, prin Legea nr. 140/2012,

**PREȘEDINTELE AUTORITĂȚII NAȚIONALE PENTRU ADMINISTRARE
ȘI REGLEMENTARE ÎN COMUNICAȚII**

emite prezenta:

DECIZIE

privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și raportarea incidentelor cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice

Art. 1. – Prezenta decizie are ca obiect stabilirea:

a) măsurilor tehnice și organizatorice care trebuie luate de furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului în vederea asigurării unui nivel adecvat al securității și integrității rețelelor și serviciilor de comunicații electronice;

b) circumstanțelor, formatului și procedurilor aplicabile notificării privind încălcarea securității sau pierderea integrității cu un impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice.

Art. 2. – În înțelesul prezentei decizii, următorii termeni se definesc astfel:

1. *securitatea și integritatea rețelelor și serviciilor de comunicații electronice* – capacitatea unei rețele sau a unui serviciu de comunicații electronice de a rezista evenimentelor, accidentale

sau rău intenționate, care pot compromite sau afecta continuitatea furnizării rețelelor și serviciilor la un nivel de performanță echivalent cu cel anterior producerii evenimentului;

2. *incident* – un eveniment care poate afecta sau amenința, direct sau indirect, securitatea și integritatea rețelelor și serviciilor de comunicații electronice;

3. *incident cu impact semnificativ* – acel incident care afectează un număr mai mare de 5.000 de conexiuni timp de cel puțin 60 de minute;

4. *măsuri de securitate* – mijloace (de natură administrativă, managerială, tehnică sau juridică) de management al riscurilor, incluzând politici, acțiuni, planuri, echipamente, facilități, proceduri, tehnici etc. menite să elimine sau să reducă riscurile privind securitatea și integritatea rețelelor sau a serviciilor de comunicații electronice.

Art. 3. – (1) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a lua toate măsurile de securitate adecvate pentru a administra riscurile la adresa securității rețelelor și serviciilor de comunicații electronice astfel încât să asigure un nivel de securitate corespunzător riscului identificat și să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor și rețelelor interconectate, având în vedere cele mai noi tehnologii și, acolo unde este cazul, de a colabora cu alți furnizori pentru implementarea acestor măsuri.

(2) Furnizorii de rețele publice de comunicații electronice au obligația de a lua toate măsurile de securitate necesare pentru a administra riscurile la adresa integrității rețelelor și serviciilor de comunicații electronice, în scopul garantării integrității rețelelor și al asigurării continuității furnizării serviciilor prin intermediul acestor rețele și, acolo unde este cazul, de a colabora cu alți furnizori pentru implementarea acestor măsuri.

(3) Măsurile minime de securitate pe care trebuie să le stabilească și să le implementeze furnizorii astfel încât să îndeplinească obligația prevăzută la alin. (1) și, după caz, cea prevăzută la alin. (2) vor viza cel puțin domeniile identificate în Anexa nr. 1.

(4) Furnizorii au obligația de a evalua și, dacă este cazul, de a actualiza măsurile prevăzute la alin. (3) ori de câte ori este necesar, însă cel puțin o dată la 12 luni.

Art.4. – (1) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a transmite Autorității Naționale pentru Administrare și Reglementare în Comunicații, denumită în continuare *ANCOM*, o notificare privind existența unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice.

(2) În aplicarea alin. (1), furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a transmite *ANCOM*, o primă

notificare, în termen de 6 ore de la detectarea incidentului cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice.

(3) Notificarea inițială prevăzută la alin. (2) se transmite de către una din persoanele responsabile prevăzute la art. 6, ca înscris în formă electronică la adresa de poștă electronică incidente@ancom.org.ro, și va cuprinde cel puțin următoarele elemente:

- a) ora descoperirii incidentului;
- b) serviciile și/sau rețelele care sunt afectate de incident;
- c) estimarea ariei geografice afectate, a numărului de conexiuni afectate, precum și a efectelor incidentului asupra furnizării rețelelor și serviciilor de către alți furnizori, pe piața națională de comunicații electronice sau pe cea din alt stat membru al Uniunii Europene;
- d) estimarea efectelor în ceea ce privește apelarea numărului unic pentru apeluri de urgență 112;
- e) o descriere sumară a cauzei/cauzelor care a/au provocat incidentul;
- f) estimarea graficului de restabilire a furnizării rețelelor și serviciilor de comunicații electronice în parametrii normali de funcționare;
- g) îndrumările oferite de furnizor utilizatorilor în vederea minimizării efectelor incidentului, dacă este cazul;
- h) informațiile oferite publicului cu privire la existența unui incident, modalitatea de comunicare și ora la care au fost comunicate informațiile, dacă este cazul;
- i) toate aspectele/elementele care pot permite ANCOM să decidă dacă informarea publicului privind incidentul este sau nu în interesul public;
- j) datele de contact (nume, prenume, număr de telefon, număr de fax, adresă de poștă electronică) ale persoanei/persoanelor care poate/pot da mai multe informații privind incidentul.

(4) Este considerată dată a transmiterii înscrisului în formă electronică data confirmării primirii de către ANCOM a acestui înscris. ANCOM asigură fără întârziere și în mod automat confirmarea primirii înscrisului în formă electronică transmis la adresa de poștă electronică incidente@ancom.org.ro.

(5) În situația în care confirmarea primirii unui înscris în formă electronică nu s-a realizat în condițiile alin. (4), este considerată dată a transmiterii data la care înscrisul în formă electronică a fost trimis, în măsura în care această dată poate fi determinată cu certitudine.

(6) În aplicarea alin. (1), furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a transmite ANCOM o notificare finală privind existența unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice, în termen de două săptămâni de la detectarea acestuia, completând formularul-tip de raportare prevăzut în Anexa nr. 2, cu respectarea instrucțiunilor de completare specificate în Anexa nr. 3.

(7) În cazul în care, la momentul transmiterii notificării finale prevăzute la alin. (6), furnizorii nu au disponibile toate informațiile prevăzute în formularul-tip de raportare, aceștia au obligația de a transmite o notificare suplimentară cu informațiile respective, completând formularul-tip de raportare prevăzut în Anexa nr. 2, imediat ce acestea sunt disponibile, dar nu mai târziu de 3 săptămâni de la detectarea incidentului cu impact semnificativ.

(8) Notificarea finală și notificarea suplimentară prevăzute la alin. (6), respectiv alin. (7), se transmit către sediul central din municipiul București sau către structura teritorială a ANCOM în raza căreia se situează sediul ori domiciliul furnizorului, în unul dintre următoarele moduri:

a) prin depunere, personal sau de către un reprezentant al furnizorului, sub luare de semnătură;

b) printr-un serviciu poștal;

c) ca înscris în formă electronică la adresa de poștă electronică incidente@ancom.org.ro, căruia i s-a încorporat, atașat sau i s-a asociat logic o semnătură electronică extinsă, bazată pe un certificat calificat nesuspendat sau nerevocat la momentul respectiv și generată cu ajutorul unui dispozitiv securizat de creare a semnăturii electronice.

(9) Este considerată dată a transmiterii, după caz, data înscrierii în registrul general de intrare-ieșire a corespondenței al ANCOM, data confirmării primirii documentelor la sediul central al ANCOM printr-un serviciu poștal cu confirmare de primire sau data confirmării primirii înscrisului în formă electronică.

(10) Formularul-tip de raportare prevăzut la alin. (6) poate fi obținut de la sediul central, de la orice structură teritorială sau de pe pagina de internet a ANCOM.

(11) Începând cu data de 1 ianuarie 2014, transmiterea notificării finale și a notificării suplimentare prevăzute la alin. (6), respectiv, alin. (7), se va realiza exclusiv prin intermediul unei aplicații disponibile pe pagina de internet a ANCOM, ca înscris în formă electronică, căruia i s-a încorporat, atașat sau i s-a asociat logic o semnătură electronică extinsă, bazată pe un certificat calificat nesuspendat sau nerevocat la momentul respectiv și generată cu ajutorul unui dispozitiv securizat de creare a semnăturii electronice.

Art.5. – (1) Ca urmare a primirii notificării inițiale prevăzute la art. 4 alin. (2) și atunci când consideră că este în interesul public, ANCOM poate informa publicul cu privire la existența unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice, prin intermediul paginii de internet a ANCOM sau poate solicita furnizorului să informeze publicul în acest sens.

(2) La solicitarea ANCOM, furnizorul de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului are obligația de a asigura informarea

publicului cu privire la existența situației prevăzute la alin. (1), cel puțin prin una dintre următoarele modalități:

- a) prin intermediul unei secțiuni speciale pe propria pagină de internet;
- b) prin canalul propriu de televiziune;
- c) prin intermediul poștei electronice;
- d) prin intermediul serviciului de mesagerie scurtă;
- e) prin mass-media.

(3) Atunci când incidentul semnificativ care face obiectul notificării inițiale prevăzute la art. 4 alin. (2) poate afecta furnizarea rețelelor și serviciilor de către un furnizor din alt stat membru al Uniunii Europene, pe baza informațiilor colectate, ANCOM decide cu privire la informarea autorității de reglementare din respectivul stat și a Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor, denumită în continuare *ENISA*, cu privire la acest incident.

(4) ANCOM transmite anual un raport succint Comisiei Europene și ENISA cu privire la notificările primite potrivit art. 4 alin. (6), respectiv, art. 4 alin. (7).

Art.6. – Furnizorii de rețele publice de comunicații electronice sau servicii de comunicații electronice destinate publicului au obligația de a transmite ANCOM datele de contact ale persoanelor responsabile de raportarea incidentelor cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice, în termen de 5 zile de la intrarea în vigoare a prezentei decizii, precum și orice modificare a acestor date, în termen de 5 zile de la survenirea modificărilor.

Art.7. – Anexele nr. 1 - 3 fac parte integrantă din prezenta decizie.

Art.8. – (1) Prezenta decizie se publică în Monitorul Oficial al României, Partea I și intră în vigoare la 3 zile de la data publicării, cu excepția prevederilor art. 3 care intră în vigoare la data de 1 ianuarie 2014.

(2) Furnizorii de rețele publice de comunicații electronice sau servicii de comunicații electronice destinate publicului au obligația de a transmite ANCOM, în termen de 30 de zile de la data intrării în vigoare a prezentei decizii, câte o notificare privind fiecare incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice care a avut loc în anul 2013, până la data intrării în vigoare a prezentei decizii, completând formularul-tip de raportare prevăzut în Anexa nr. 2, cu respectarea instrucțiunilor de completare din Anexa nr. 3.

PREȘEDINTE,
MARIUS CĂTĂLIN MARINESCU

București, 2013

Nr.

Domeniile vizate de măsurile minime de securitate

I. Politica de securitate și managementul riscului

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

- 1) să stabilească o politică de securitate adecvată;
- 2) să stabilească un management al riscului care:
 - a) să stabilească domeniul de aplicare, precum și criteriile de bază necesare procesului de management al riscului (criteriul de evaluare a riscului, criteriul de stabilire a impactului, criteriul de acceptare a riscului);
 - b) să identifice riscurile, prin identificarea resurselor furnizorului în cauză, amenințărilor, vulnerabilităților, măsurilor existente și a consecințelor pe care pierderea/încălcarea securității le-ar putea avea asupra resurselor;
 - c) să estimeze riscurile prin evaluarea impactului pe care îl poate avea concretizarea unei amenințări care exploatează o vulnerabilitate a unei resurse și prin evaluarea probabilității de apariție a incidentelor;
 - d) să evalueze riscul;
 - e) să evalueze opțiunile de tratare a riscului, să selecteze măsuri pentru tratarea riscului cu fixarea obiectivelor acestor măsuri și să justifice riscurile acceptate care nu îndeplinesc criteriul de acceptare a riscului.
- 3) să stabilească o structură adecvată a rolurilor și responsabilităților în asigurarea securității și integrității rețelelor și serviciilor;
- 4) să stabilească o politică cu privire la cerințele de securitate pentru achiziționarea de produse și servicii de la terțe părți și pentru asigurarea întreținerii sau gestiunii de către terțe părți a produselor și serviciilor (servicii IT, software, interconectare, baze de date, facilități asociate etc).

II. Securitatea resurselor umane

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

- 1) să efectueze controale de verificare de fond a candidaților pentru angajare, a contractorilor și a terților în conformitate cu legile aplicabile, reglementări și etică, proporționale cu riscurile percepute;
- 2) să se asigure că personalul său are cunoștințe suficiente de securitate și este instruit permanent cu privire la securitatea și integritatea rețelelor și serviciilor;
- 3) să stabilească un proces corespunzător de gestionare a schimbărilor de personal sau a modificărilor de roluri și responsabilități;
- 4) să stabilească un proces disciplinar pentru angajații care produc o încălcare a securității și integrității rețelelor sau serviciilor de comunicații electronice.

III. Securitatea și integritatea rețelelor, a facilităților asociate și a informațiilor

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

- 1) să stabilească o securitate fizică adecvată a rețelei și a infrastructurii asociate (stabilirea și menținerea unor măsuri care să protejeze în mod corespunzător împotriva accesului fizic neautorizat, distrugerilor provocate de incendii, inundații, cutremure, explozii, tulburări publice și alte forme de dezastru naturale sau provocate de oameni);
- 2) să stabilească o securitate adecvată a utilităților suport, cum ar fi furnizarea de energie electrică, combustibil sau răcirea echipamentelor;
- 3) să stabilească măsuri de securitate adecvate pentru accesul (logic) la rețea și la sistemele informatice;
- 4) să stabilească măsuri de securitate adecvate pentru a asigura protecția rețelelor și serviciilor de comunicații electronice împotriva codurilor cu potențial dăunător, codurilor mobile neautorizate și a atacurilor informatice, inclusiv DoS/DDoS.

IV. Managementul operațiunilor

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

- 1) să stabilească proceduri operaționale și responsabilități adecvate;
- 2) să stabilească proceduri privind managementul schimbărilor efectuate în rețeaua de comunicații electronice și în software-urile de aplicații;
- 3) să stabilească proceduri de gestionare a resurselor astfel încât disponibilitatea și starea acestora să fie verificată.

V. Managementul incidentelor

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

- 1) să stabilească procese și proceduri pentru managementul incidentelor care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice (care să vizeze raportarea internă, evaluarea, răspunsul la incidente și escaladarea acestuia), inclusiv prin definirea rolurilor și responsabilităților;
- 2) să stabilească un sistem de detectare a incidentelor;
- 3) să stabilească o procedură adecvată de raportare a incidentelor către ANCOM, precum și către alte autorități responsabile, precum și să stabilească planuri de comunicare a incidentelor către alte părți externe (furnizori de rețele și servicii de comunicații electronice afectați, media, clienți, parteneri de afaceri etc.).

VI. Managementul continuității afacerii

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

- 1) să stabilească o strategie pentru asigurarea continuității furnizării rețelelor și serviciilor de comunicații electronice în situațiile generate de perturbări grave ale funcționării rețelei sau serviciului;
- 2) să dețină capacități de implementare a strategiei de continuitate și să stabilească planuri de continuitate și de recuperare.

VII. Monitorizare, testare și audit

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

- 1) să stabilească politici de monitorizare a sistemelor, precum și politici privind jurnalele de sistem;
- 2) să stabilească politici pentru testarea, inclusiv prin exerciții, a planurilor de continuitate și de recuperare în cazul perturbărilor grave ale funcționării rețelei sau serviciului;
- 3) să stabilească politici pentru testarea echipamentelor, sistemelor și software-lor, în special înainte de conectarea/punerea lor în funcțiune;
- 4) să stabilească o politică adecvată pentru evaluarea și testarea securității tuturor resurselor (echipamente, sisteme și software etc.);
- 5) să stabilească o politică pentru monitorizarea conformității și pentru audit, cu un proces de raportare a conformității și de rezolvare a deficiențelor constatate în timpul auditului.

FORMULAR DE RAPORTARE A INCIDENTELOR CARE AU AFECTAT SECURITATEA ȘI INTEGRITATEA REȚELELOR ȘI SERVICIILOR DE COMUNICAȚII ELECTRONICE

1. Furnizor:

2. Data și ora

2.1 Data și ora la care s-a produs incidentul Data: _____ Ora: _____

2.2 Data și ora la care s-a descoperit incidentul Data: _____ Ora: _____

3. Impactul incidentului și tipul cauzei

3.1 Serviciul/serviciile afectate:

- Servicii de telefonie destinate publicului:
- Servicii de telefonie furnizate prin intermediul unor rețele publice fixe sau cu mobilitate limitată
 - Servicii de telefonie furnizate prin intermediul unor rețele publice mobile terestre
 - Servicii de telefonie furnizate prin intermediul unor rețele publice cu transmisie prin satelit
 - Servicii de transport apeluri
- Servicii de linii închiriate
- Servicii de transmisiuni de date (inclusiv VPN):
- La puncte fixe
 - Cu mobilitate limitată
 - SMS (numai în cazul rețelelor celulare)
 - Mobil (inclusiv MVNO)
- Servicii de acces la Internet:
- Dial-up (numai pentru bucla locală)
 - Conexiuni permanente la punct fix
 - Conexiuni radio mobile (inclusiv MVNO)
- Retransmisia serviciilor de programe media audiovizuale liniare către utilizatorii finali:
- Cu acces fix prin satelit (tip DTH)
 - Cu acces mobil prin satelit (tip S-DAB/DVB-S)
 - Terestre cu acces la punct fix tip CATV, DVB-C/Mx, IPTV etc.
 - Terestre dedicate tip T-DAB/DVB-T
 - Radio Celulare Publice (tip Mobile TV)
- Alte servicii de comunicații electronice
- Servicii de radiocomunicații mobile profesionale
 - Comunicații voce
 - Mesagerie radio
 - Transmisii de date, telex
 - Localizare, poziționare
 - Alte tipuri de servicii
 - Servicii de comunicații electronice care permit servicii de voce
 - Servicii de comunicații electronice care permit accesul la servicii de conținut
 - Alte tipuri de servicii decât cele de mai sus

3.2 Parametrii de impact:

Numărul de conexiuni afectate de incident per serviciu:

Resursele/echipamentele afectate:

Durata incidentului:

Aria/răspândirea geografică:

Impactul asupra apelurilor de urgență:

3.3 Descrierea incidentului:**3.4 Tipul cauzei incidentului:**

- Eroare umană
- Eroare de sistem
- Fenomen natural
- Acțiune rău intenționată
- Cauză externă/parte terță

3.5 Mai multe informații despre cauza incidentului:**4. Alte informații despre incident****4.1 Acțiuni de răspuns la incident (inclusiv momentul când au fost luate):**

4.2 Măsurile luate sau planificate pentru a împiedica producerea unui incident similar/eliminarea cauzei incidentului (inclusiv momentul când au fost/vor fi luate):

4.3 Alți furnizori de rețele și servicii de comunicații electronice afectați:

4.4 Alte observații:

**Instrucțiuni de completare a formularului de raportare a incidentelor
care au afectat securitatea și integritatea rețelelor și serviciilor
de comunicații electronice**

1. Furnizor	
Se va completa cu denumirea furnizorului care trimite raportul către ANCOM.	
2. Data și ora	
2.1 Data și ora la care s-a produs incidentul	Se vor completa data și ora la care s-a produs incidentul, respectiv la care s-a descoperit incidentul.
2.2 Data și ora la care s-a descoperit incidentul	
3. Impactul incidentului și tipul cauzei	
3.1 Servicii afectate de incident:	
Se va/vor bifa serviciul/serviciile a căror furnizare a fost afectată de incident.	
3.2 Parametrii de impact:	
Numărul de conexiuni afectate de incident per serviciu	<p>Se va specifica numărul total de conexiuni afectate de incident pentru fiecare serviciu afectat în parte.</p> <p>O conexiune reprezintă:</p> <ul style="list-style-type: none"> - în cazul serviciilor de acces la internet la puncte fixe: o conexiune de acces la internet; - în cazul serviciilor de transmisiuni de date la puncte fixe: o conexiune de acces la servicii de transmisiuni de date; - în cazul serviciilor de telefonie la punct fix: o linie telefonică alocată unui abonat de către un furnizor prin intermediul propriei rețele publice fixe pe care o operează sau prin rețeaua publică fixă a unui terț; un abonat poate avea alocate una sau mai multe linii de acces; - în cazul serviciilor de telefonie, acces la internet și transmisiuni de date furnizate prin intermediul rețelelor radio mobile celulare: o cartelă SIM activă; - în cazul serviciilor de retransmisie a programelor media audiovizuale liniare: o conexiune de retransmisie a programelor media audiovizuale. <p>În cazul serviciilor furnizate prin intermediul unor rețele publice mobile terestre, furnizorul va estima numărul posibilibilor utilizatori afectați ținând cont de utilizarea normală a sistemelor afectate (exemplu: dacă o stație de bază care deservește în medie 1000 de utilizatori/SIM pe oră este inactivă timp de o oră, impactul acestui incident va fi estimat la 1000 de conexiuni).</p>
Resursele/echipamentele afectate	<p>Se vor specifica resursele/echipamentele afectate de incident. Ca și exemplu, este prezentată în continuare o listă de resurse ce pot fi afectate:</p> <ul style="list-style-type: none"> - stații de bază pentru PLMN (BSC, BTS, RNC, NodeB etc.); - rețea locală (cabluri de cupru, fibră etc.); - cabinete stradale; - echipamente de comutare sau rutare (comutatoare de rețea, routere, multiplexoare etc.) - noduri de transmisiuni; - centre de comutație; - centre de mesaje; - registre de utilizatori (HLR, VLR, AuC, Home Subscriber Server etc.); - backbone; - interconectări; - echipamente pentru alimentarea de rezervă cu energie electrică (baterii, generatoare); - sisteme de alimentare cu energie electrică.

Durata incidentului	Se va specifica intervalul de timp dintre momentul în care serviciul începe să se degradeze sau s-a întrerupt, până în momentul în care acesta este restabilit la parametrii inițiali. Timpul va fi exprimat în minute.
Aria/răspândirea geografică	Se va specifica regiunea geografică afectată de incident (ex: regiunea, județele, localitățile).
Impactul asupra apelurilor de urgență	Se va specifica modul în care au fost afectate comunicațiile către Sistemul național unic pentru apeluri de urgență.
3.3 Descrierea incidentului:	
Se va completa cu orice informații și detalii disponibile privind apariția, dezvoltarea, impactul incidentului și modalitatea în care au fost afectate resursele/echipamentele.	
3.4 Tipul cauzei incidentului:	
Se va/vor bifa cauza/cauzele incidentului: eroare umană, eroare de sistem, fenomen natural, acțiune rău intenționată și cauză externă/parte terță. De obicei, categoria cauză externă/parte terță poate fi corelată cu una din celelalte 4 cauze (de exemplu: în cazul unui cablu de fibră optică distrus în urma unor lucrări de construcție, cauzele incidentului vor fi eroare umană și cauză externă/parte terță). Unele incidente pot avea o cauză inițială și una subsecventă, incidentele apărând în urma unei succesiuni de evenimente sau factori (exemplu: în cazul unui incident datorat unei alimentări defectuoase cu energie electrică – suprasarcină care produce o defectare a unui echipament al furnizorului, cauza inițială este eroare de sistem al unui echipament al furnizorului de utilități și cauză externă/parte terță, iar cauza subsecventă este eroare de sistem – defecțiune hardware al unui echipament de comunicații electronice). În acest caz, furnizorul va bifa cauza inițială.	
3.5 Mai multe informații despre cauza incidentului:	
Câmpul va cuprinde descrierea detaliată a cauzei incidentului, inclusiv vulnerabilitățile exploatate. În cazul incidentelor apărute în urma unei succesiuni de evenimente, furnizorul va oferi atât detalii privind cauza inițială, cât și despre cauza/cauzele subsecvente.	
4. Alte informații despre incident	
4.1 Acțiuni de răspuns la incident (inclusiv momentul când au fost luate):	
Câmpul va cuprinde descrierea detaliată a: - măsurilor de securitate implementate până la momentul producerii incidentului în vederea minimizării riscului incidentului; - acțiunilor întreprinse și a măsurilor adoptate pentru a restabili serviciul la parametrii inițiali în cazul în care incidentul afectează doar calitatea serviciului (nu există întreruperi în furnizarea serviciului); - acțiunilor întreprinse și a măsurilor adoptate pentru a aduce serviciul la un nivel acceptabil, precum și pentru a restabili serviciul la parametrii inițiali în cazul întreruperii furnizării serviciului, inclusiv momentele de timp în care au fost acestea realizate.	
4.2 Măsurile luate sau planificate pentru a împiedica producerea unui incident similar/eliminarea cauzei incidentului (inclusiv momentul când au fost/vor fi luate):	
Câmpul va cuprinde descrierea detaliată a acțiunilor realizate pentru a minimiza nivelul de risc și pentru a preîntâmpina reparația incidentului (ex: revizuire măsuri de securitate și proceduri, renegociere SLA-uri, instruire de personal, achiziție de echipamente sau sisteme de backup etc), precum și momentul când au fost luate sau când vor fi luate aceste măsuri.	
4.3 Alți furnizori de rețele și servicii de comunicații electronice afectați:	
Acest câmp se completează cu detalii despre furnizorul și resursele/serviciile acestuia afectate de incidentul în cauză, inclusiv cazurile în care furnizori din alte state membre ale Uniunii Europene au fost afectați. De asemenea, se descrie modul de colaborare cu alți furnizori în vederea soluționării incidentului, inclusiv acțiunile comune de răspuns la incident.	
4.4 Alte observații:	
Acest câmp se completează cu orice alte detalii sau observații care nu au fost incluse în câmpurile de mai sus.	