Autoritatea Națională pentru Administrare și Reglementare în Comunicații

Str. Delea Nouă nr.2, Sector 3, București, 030925 România
Tel: 0372 845 400 / 0372 845 454 Fax: 0372 845 402
ancom@ancom.ro www.ancom.ro

GHID DE RAPORTARE A INCIDENTELOR CU IMPACT SEMNIFICATIV ASUPRA REŢELELOR ŞI SERVICIILOR DE COMUNICAŢII ELECTRONICE (DISPONIBILITATE, CONFIDENŢIALITATE, INTEGRITATE SAU AUTENTICITATE)

Cuprins:

1. INTRODUCERE

În era digitală în continuă evoluție, rețelele și serviciile de comunicații electronice au devenit nu doar un aspect esențial al vieții cotidiene, ci și o coloană vertebrală a progresului tehnologic. Îndeplinind cerințele fundamentale pentru comunicație și informare, aceste entități au evoluat într-un suport esențial pentru tehnologii și aplicații aflate într-o creștere rapidă. În acest context, importanța lor transcendă cu mult sfera individuală, influențând nu doar activitățile de zi cu zi ale utilizatorilor, ci și dinamica afacerilor la nivel global.

Într-un mediu în care conectivitatea și schimbul rapid de informații sunt monedă curentă, inaccesibilitatea rețelelor și serviciilor de comunicații electronice devine sinonimă cu o stagnare a progresului. Consecințele devin vizibile în moduri diverse, afectând nu doar utilizatorii individuali, ci și întregi sectoare ale economiei naționale. De la industria financiară la sectorul energetic și la serviciile publice, toate depind de buna funcționare a infrastructurii de comunicații pentru a-și desfășura activitățile în mod eficient.

Aspectul critic al securității rețelelor și serviciilor devine astfel evidențiat într-un mod amplificat. Orice incident care amenință integritatea acestor infrastructuri poate genera consecințe negative în lanț, afectând nu doar furnizorii și utilizatorii direcți, ci și provocând turbulențe semnificative în întreaga economie.

Prin urmare, este esențial să dezvoltăm și să implementăm măsuri proactive pentru a gestiona și preveni potențialele amenințări la adresa securității comunicațiilor electronice. În acest context, ghidul pentru raportarea incidentelor devine un instrument vital, furnizând nu doar un cadru de intervenție în situații critice, ci și încurajând colaborarea între actorii implicați pentru a asigura o reziliență crescută în fața provocărilor din ce în ce mai sofisticate ale mediului digital. Astfel, acest ghid reprezintă o contribuție semnificativă la consolidarea și securizarea fundamentelor digitale ale societății contemporane.

2. CADRUL LEGAL

Dispozițiile Ordonanței de Urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată cu modificări și completări prin Legea nr. 140/2012, cu modificările și completările ulterioare, au fost actualizate pe baza Legii nr. 198 din 6 iulie 2022 pentru modificarea și completarea unor acte normative în domeniul comunicațiilor electronice și pentru stabilirea unor măsuri de facilitare a dezvoltării rețelelor de comunicații electronice[1]. Printre altele, au fost transpune în legislația națională prevederile Art. 40 din Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice[2] (denumit în continuare „EECC").

Conform Art. 46 din OUG nr. 111/2011:

„(1) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a notifica ANCOM, în cel mai scurt timp, cu privire la orice incident de securitate care are un impact semnificativ asupra rețelelor sau serviciilor.

(2) Amploarea impactului unui incident de securitate se determină ținând seama, în special, de următorii parametri, după caz:

a) numărul de utilizatori afectați de incidentul de securitate;

[1] https://legislatie.just.ro/Public/DetaliiDocumentAfis/257364

[2] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32018L1972

b) durata incidentului de securitate;
c) întinderea geografică a zonei afectate de incidentul de securitate;
d) măsura în care funcționarea rețelei sau a serviciului este afectată;
e) amploarea impactului asupra activităților economice și societale."

Prin Decizia președintelui ANCOM nr. 70/2024 privind securitatea rețelelor publice de comunicații electronice și a serviciilor de comunicații electronice destinate publicului a fost detaliată, printre altele, și modalitatea de raportare a incidentelor cu impact semnificativ asupra furnizării reţelelor şi serviciilor de comunicaţii electronice, inclusiv prin determinarea circumstanțelor, a formatului notificărilor şi condițiilor aplicabile în cazul cerințelor de notificare.

3. SCHEMA DE RAPORTARE

Pentru a putea realiza rapoartele anuale dar şi pentru statistici relevante, inclusiv pentru raportările către entităţi precum Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) sau Organismului Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice (BEREC) este nevoie de informații complete şi corecte, în conformitate cu reglementările în vigoare.

Modalitatea de notificare a incidentelor detailată în acest ghid va permite obținerea informațiilor de care experții ANCOM au nevoie în procesul de centralizare și analiză şi va evita solicitarea de informații suplimentare de la furnizori, în vederea clarificării informațiilor despre incidente.

În figura 1 este reprezentată schema de raportare a incidentelor către ANCOM.

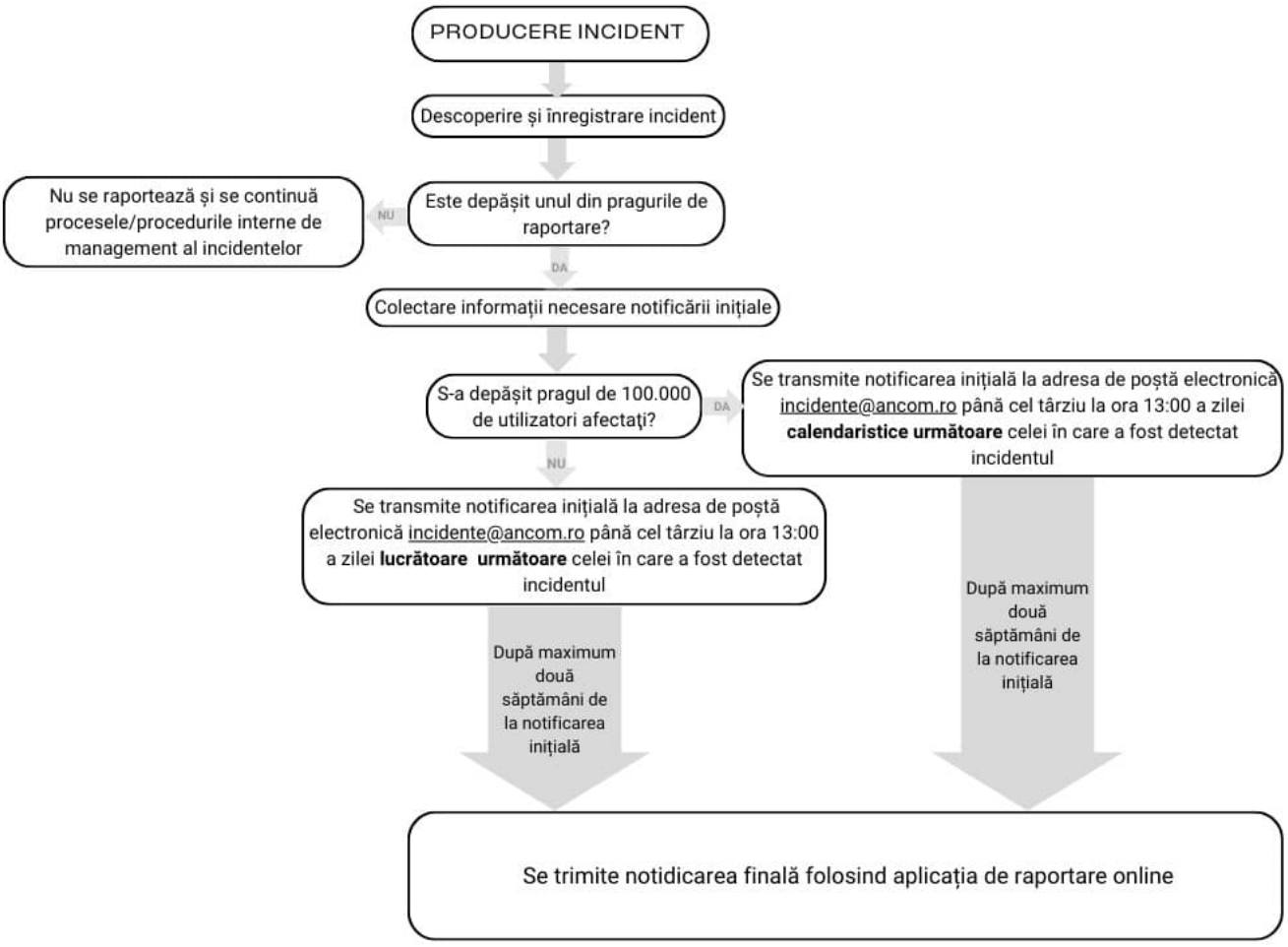

Figura 1

Având în vedere modificările induse de Decizia nr. 70/2024, menționăm şi în cuprinsul acestui ghid pragurile cantitative, precum şi pe cele calitative, praguri ce se vor folosi pentru notificarea incidentelor. Indiferent de tipul pragului depășit, fie el calitativ sau cantitativ, incidentele se notifică după schema de raportare evidențiată mai sus.

Astfel, un incident va fi notificat dacă se depășește cel puțin unul dintre următoarele praguri:

a) praguri cantitative:

(i) disponibilitate – afectarea, din perspectiva disponibilității rețelelor publice de comunicații electronice, a serviciilor de comunicații electronice destinate publicului, inclusiv a datelor stocate, transmise ori prelucrate sau a serviciilor aferente oferite de rețelele ori serviciile de comunicații electronice respective sau accesibile prin intermediul acestora, în cazul a 5.000 de utilizatori, timp de cel puțin 60 de minute sau în cazul în care se depășește pragul de 500.000 de „ore-utilizator";

(ii) autenticitate, integritate sau confidențialitate - sunt afectați cel puțin 5.000 de utilizatori, indiferent de durata incidentului.

b) praguri calitative:

(i) incidente care afectează, direct sau indirect, pe o perioadă de cel puțin 15 minute, rutarea comunicațiilor de urgență către Serviciul de urgență 112;

(ii) incidente cu impact transfrontalier;

(iii) incidente care afectează securitatea rețelelor și serviciilor altui furnizor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și îi cauzează acestuia un incident care are un impact semnificativ, în măsura în care această situație era cunoscută.

4. NOTIFICAREA INIŢIALĂ

Notificarea inițială semnalează faptul că a avut loc un incident cu impact semnificativ. Această notificare trebuie transmisă:

a) până cel târziu la ora 13:00 a zilei **lucrătoare următoare** celei în care a fost detectat incidentul, dacă incidentul a avut mai ***puțin*** de 100.000 de utilizatori afectați.

b) până cel târziu la ora 13:00 a zilei **calendaristice următoare** celei în care a fost detectat incidentul, dacă incidentul a avut mai ***mult*** de 100.000 de utilizatori afectați.

Notificarea inițială se transmite exclusiv pe email, la adresa incidente@ancom.ro, nefiind necesară conectarea la aplicația informatică pusă la dispoziție de ANCOM. Ea va cuprinde elementele disponibile la acel moment, dar cel puțin următoarele informații:

a) data şi ora detectării incidentului – se vor nota data şi ora la care a fost descoperit incidentul. Pot exista situații în care incidentul să fie descoperit la un anumit interval de la producerea lui efectivă, dar aceste detalii vor fi ulterior comunicate în cadrul notificării finale;

- b) serviciile şi/sau rețelele de comunicații electronice care sunt afectate de incident – se va nota tipul/tipurile de servicii afectat (ex: servicii de telefonie fixă, servicii de telefonie mobilă și SMS, servicii de internet fix şi transmisiuni de date fixe; servicii de internet mobil şi transmisiuni de date mobile, servicii NI-ICS etc.) şi tipul de rețea afectată (2G, 3G etc.), în funcţie de ce element al acesteia a fost impactat;

c) estimarea impactului incidentului:

c1) a ariei geografice afectate - se vor enumera județele afectate;

c2) a numărului de utilizatori afectați – se va nota numărul total de utilizatori afectați, cumulat pentru toate serviciile afectate;

c3) a efectelor incidentului asupra rețelelor şi serviciilor altor furnizori - se vor menționa denumirile altor furnizori afectaţi, pe piața națională de comunicații electronice sau pe cea din alt stat membru al Uniunii Europene, daca este cazul;

d) estimarea efectelor în ceea ce privește rutarea comunicațiilor de urgență către Serviciul de urgență 112 - se va specifica dacă apelurile de urgență către numărul unic 112 au putut fi efectuate din aria geografică afectată conform punctului c1) şi/sau dacă transmiterea informației de localizare aferente apelului 112 a fost afectată.

e) o descriere sumară a cauzei/cauzelor care a/au provocat incidentul – se va preciza dimensiunea afectată a securității (disponibilitate, autenticitate, integritate, confidențialitate). Se vor oferi informațiile în forma disponibilă la momentul notificării inițiale (ex: Incident provocat de probleme de transmisiuni în reţeaua unui partener. Incident provocat de probleme de alimentare cu energie electrică în reţeaua proprie. Incident provocat de probleme de secționare a fibrei optice în reţeaua proprie etc.).

f) estimarea graficului măsurilor de restabilire a furnizării rețelelor şi serviciilor de comunicații electronice în parametri normali de funcționare – se vor enumera succint şi cronologic pașii ce urmează să fie întreprinși în vederea remedierii incidentului. În situația în care incidentul s-a finalizat se vor enumera succint şi cronologic pașii întreprinși efectiv.

g) informațiile oferite de furnizor utilizatorilor, inclusiv îndrumări în vederea minimizării efectelor incidentului, dacă este cazul.

În cazul furnizorilor care au mai mult de 5.000 de utilizatori, notificarea inițială se va transmite de către una dintre persoanele responsabile de notificarea incidentelor. Aceste persoane sunt comunicate în conformitate cu Art. 7. În cazul furnizorilor care au sub

5.000 de utilizatori, notificarea inițială se va transmite de către reprezentantul legal sau de către un împuternicit al acestuia, care va transmite în același timp și dovada calității de împuternicit al furnizorului. În ambele situații primirea notificării inițiale pe email este confirmată prin transmiterea automată a unui mesaj la adresa expeditorului notificării.

În situația în care furnizorul deține toate informațiile necesare notificării finale în termenul în care trebuia să transmită notificarea inițială, acesta poate să completeze direct formularul aferent notificării finale prin intermediul aplicației online.

5. NOTIFICAREA FINALĂ

Transmiterea notificării finale trebuie realizată în termen de maximum două săptămâni de la detectarea incidentului folosind aplicația online de raportare[3]. Această notificare se transmite exclusiv prin completarea informațiilor în aplicația informatică pusă la dispoziție de ANCOM. Câmpurile se vor completa după cum urmează:

1) **furnizor** – denumirea furnizorului ce raportează incidentul se va completa automat pe baza credenţialelor utilizate la conectarea în aplicație.

2) **data şi ora producerii incidentului**, precum şi **data şi ora detectării incidentului**. – se vor completa cu valorile aferente momentului producerii şi detectării incidentului în concordanță cu valorile ce se regăsesc în sistemele proprii de monitorizare a incidentelor de securitate.

3) **dimensiunea afectată a securității** – se va selecta una dintre cele 4 dimensiuni:

[3] Se va adăuga linkul de la aplicație

disponibilitate[4], autenticitate[5], integritate[6], confidențialitate[7].

4) **incident repetitiv** – se va selecta în funcţie de tipul incidentului. Un incident repetitiv se definește ca acel incident de securitate care are un impact semnificativ şi care cumulează următoarele 3 caracteristici: afectează aceleași resurse (ex: același router, aceeași stație de bază); are aceeași cauză; a mai fost raportat în precedentele 12 luni. În cazul în care incidentul ce se raportează nu îndeplinește cumulat condițiile anterior amintite, atunci se va selecta opțiunea NU. Altfel, se va bifa în calendar data precedentei apariții.

5) **praguri depășite/incidentul a afectat** – se vor selecta toate variantele aplicabile incidentului semnificativ în cauză dintre cele 6 opțiuni predefinite:

a) mai mult de 5.000 de utilizatori timp de cel puțin 60 de minute

b) mai mult de 500.000 de „ore-utilizator"

- *incidentele care afectează disponibilitatea sunt raportabile folosind pragul de număr*

[4] ISO/IEC 27000:2018 definește **disponibilitatea** ca fiind proprietatea de a fi accesibil și utilizabil la cerere, de o entitate autorizată. Disponibilitatea asigură că informația sau sistemele sunt gata să răspundă (să fie „disponibile") nevoilor utilizatorilor legitimi, în momentul în care aceștia solicită. Aceasta implică și continuitatea serviciilor și se poate asocia cu fiabilitatea sistemului (având în vedere că poate fi impactată de elemente care nu sunt neapărat rău-intenționate, cum ar fi lucrări programate, actualizări de sistem, defecțiuni hardware, erori umane, calamități naturale, incendii, cutremure, după cum pot exista și cauze rău-intenționate cum sunt atacuri cibernetice, DDoS etc.). Disponibilitatea asigură faptul că nu există refuzul accesului autorizat la elemente ale rețelei, informații stocate, fluxuri de informații, servicii şi aplicații, refuz care poate apărea datorită evenimentelor cu impact asupra rețelei. Măsurile de securitate pot include elemente cum ar fi redundanța, back-up, recuperare în caz de dezastru, virtualizare etc. Disponibilitatea reprezintă proprietatea rețelelor publice de comunicații electronice, a serviciilor de comunicații electronice destinate publicului, inclusiv a datelor stocate, transmise ori prelucrate, a serviciilor aferente oferite de respectivele rețele, sau accesibile prin intermediul acestora, de a fi accesibile și utilizabile la cerere de persoane, procese, sisteme care sunt autorizate în acest sens.

[5] ISO/IEC 27000:2018 definește **autenticitatea** ca fiind proprietatea ca o entitate să fie ceea ce pretinde că este, definiția fiind preluată de ENISA în ghidul Technical Guideline on Security Measures Under the EECC, 4th Edition, July 2021. Autenticitatea reprezintă proprietatea rețelelor publice de comunicații electronice, a serviciilor de comunicații electronice destinate publicului, inclusiv a datelor stocate, transmise ori prelucrate sau a serviciilor aferente oferite de respectivele rețele, sau accesibile prin intermediul acestora, de a fi veritabile, verificabile, de încredere, existând certitudinea în validitatea transmisiei datelor, a conținutului sau a entităților ce comunică.

[6] ISO/IEC 27000:2018 definește **integritatea** ca fiind proprietatea acurateței și deplinătății. Recomandarea ITU X.800 (03/91) definește integritatea (integritatea datelor) ca fiind proprietatea ca datele să nu fie alterate, modificate sau distruse într-un mod neautorizat. Obiectivul în acest caz este de a se preveni ca datele să fie alterate, modificate, utilizate în mod ilicit de entități neautorizate, adică să fie asigurată integritatea lor. Trebuie acordată atenție astfel încât datele să nu fie modificate nici în cazul tranzitului (având în vedere interconectarea rețelelor). Integritatea datelor asigură corectitudinea sau acuratețea datelor, fiind proprietatea care demonstrează caracterul nemodificat al acestora, confirmând faptul că datele trimise, primite sau stocate nu sunt modificate sau distruse într-o manieră neautorizată. Pe de altă parte, integritatea este capacitatea sistemului de a-şi păstra atributele specifice din punct de vedere al performanței și funcționalității. Măsurile de securitate pot include elemente cum ar fi proceduri de backup și restaurare, criptare, controlul versiunii, controlul accesului utilizatorilor, software privind detecția erorilor etc. Astfel, integritatea reprezintă proprietatea rețelelor publice de comunicații electronice, a serviciilor de comunicații electronice destinate publicului, inclusiv a datelor stocate, transmise ori prelucrate sau a serviciilor aferente oferite de respectivele rețelele, sau accesibile prin intermediul acestora, de a nu fi alterate, modificate, distruse într-un mod neautorizat, ilicit, existând certitudinea acurateței și deplinătății.

[7] ISO/IEC 27000:2018 definește **confidențialitatea** ca fiind proprietatea ca informația să nu fie făcută disponibilă sau dezvăluită către persoane, entități sau procese neautorizate . Confidențialitatea informației înseamnă ca aceasta să fie protejată pentru a nu fi expusă accesului unor părți neautorizate, astfel încât entitățile neautorizate să nu aibă acces la informații la care nu au acest drept de acces. Confidențialitatea datelor protejează datele de accesări neautorizate. Dintre măsurile privind protecția confidențialității putem aminti criptarea, verificarea biometrică, utilizarea parolelor, autentificarea prin mai multe etape etc. Prin urmare, confidențialitatea reprezintă proprietatea rețelelor publice de comunicații electronice, a serviciilor de comunicații electronice destinate publicului, prin care asigură ca datele stocate, transmise ori prelucrate sau a serviciilor aferente oferite de respectivele rețelele, sau accesibile prin intermediul acestora, să fie făcute disponibile sau dezvăluite doar către persoane, entități sau procese autorizate.

de utilizatori şi timp (mai mult de 5.000 de utilizatori timp de cel puțin 60 de minute) sau pragul de „ore-utilizator”.

Pragul „ore–utilizator” se calculează folosind formula:

Ore-utilizator = (Număr de utilizatori afectați x durată incident, exprimată în minute) / 60

c) autenticitatea, integritatea sau confidențialitatea - mai mult de 5.000 de utilizatori

- incidentele care afectează autenticitatea, integritatea sau confidențialitatea sunt raportabile folosind doar pragul de număr de utilizatori (mai mult de 5.000 de utilizatori), indiferent de durata incidentului.

d) rutarea comunicațiilor de urgență către Serviciul de urgență 112, pentru cel puțin 15 minute

- incidentele care afectează direct sau indirect, pe o perioadă de cel puțin 15 minute, rutarea comunicațiilor de urgență către Serviciul de urgență 112 trebuie raportate. Problemele la care facem referire sunt doar acele incidente ce afectează segmentele de transport şi interconectare ale reţelei, cu impact asupra comunicaţiilor de urgentă. Pentru clarificare, incidentele care afectează serviciul de comunicații de voce și, implicit, apelarea către numărul unic pentru apeluri de urgență 112 nu vor fi raportate conform acestui prag, ci conform pragului cantitativ.

e) securitatea reţelelor şi serviciilor altui furnizor

- incidentele care afectează securitatea rețelelor și serviciilor unui furnizor partener și îi provoacă acestuia un incident care are un impact semnificativ, trebuie raportate, indiferent dacă este atins sau nu un prag cantitativ în rețeaua proprie.

Acest prag se referă la furnizorii care pun la dispoziție elemente ale reţelei proprii, spre utilizare unui alt furnizor. În acest sens, furnizorul care deține acele elemente de reţea are obligația de a notifica ANCOM, selectând acest prag, în momentul în care îi provoacă partenerului său un incident. În majoritatea cazurilor ANCOM va informa furnizorul de existența acestui caz, menționând şi numărul de utilizatori afectați ai partenerului său. În acest caz, furnizorul care deține elementele de reţea va raporta coordonatele incidentului conform datelor din sistemul său de monitorizare a incidentelor de securitate (ex: data şi ora vor fi cele din acest sistem, iar nu data şi ora primirii informării din partea ANCOM).

f) a avut impact transfrontalier

- incidentele care afectează utilizatori ai unor furnizori de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului din afara granițelor României, trebuie raportate. În măsura în care, în urma unui incident de securitatea din reţeaua proprie, furnizorii primesc notificări din parte unor furnizori din afara granițelor României, conform cărora că au suferit un incident cu impact semnificativ, aceştia au obligația de a raporta ANCOM un astfel de incident.

6) **impact incident**

a) numărul de utilizatori afectați - se vor completa valorile numerice corespunzătoare fiecărui serviciu afectat dintre cele 10 tipuri de servicii predefinite:

- Internet la puncte fixe;
- Internet la puncte mobile;
- Comunicații interpersonale bazate pe numere, la puncte fixe (inclusiv cele nomade/independente de locație);
- Comunicații interpersonale bazate pe numere, la puncte mobile (inclusiv MVNO);
- Comunicații interpersonale care nu se bazează pe numere;
- Transmisiuni de date;
- Linii închiriate;
- Programe de televiziune;
- Programe de radiodifuziune sonoră

- Retransmisia serviciilor de programe media audiovizuale liniare;
- M2M (Machine-to-machine)[8];
- Alte tipuri de servicii decât cele de dinainte.

Determinarea numărului de utilizatori afectaţi se va face astfel:
- în cazul **serviciilor furnizate prin intermediul reţelelor fixe**, utilizatorii afectaţi se vor determina în funcţie de numărul de conexiuni afectate;
- în cazul **serviciilor de linii închiriate**: o conexiune afectată este aferentă unui segment terminal de linie închiriată;
- în cazul serviciilor de **comunicații interpersonale care nu se bazează pe numere**: utilizatorii se vor determina în funcţie de numărul de utilizatori activi posibil afectaţi;
- în cazul **serviciilor furnizate prin intermediul reţelelor mobile**, utilizatorii afectaţi se vor determina în funcţie de numărul de cartele SIM active afectate[9];

NOTA: În cazul serviciilor furnizate prin intermediul unor rețele publice mobile terestre, furnizorul va estima numărul de cartele SIM active afectate.

a) În cazul incidentelor care afectează ***stații de bază şi echipamente de transmisiuni***, se va folosi următoarea metodologie:

În momentul apariției unui incident se identifică celulele afectate.

Traficul total pierdut la nivelul tuturor celulelor afectate ($T_{pierdut}$), pe fiecare serviciu (voce, internet şi date), se consideră a fi traficul înregistrat în săptămâna anterioară, în același interval de timp în care a avut loc incidentul (ziua și intervalul orar), la nivelul acelor celule.

Traficul total înregistrat la nivelul rețelei (T_{retea}) se consideră a fi suma traficului din toate celulele din rețea în intervalul de timp respectiv (ziua și intervalul orar) din săptămâna anterioară producerii incidentului.

Numărul de cartele SIM afectate se calculează astfel:

$$N_{cartele\ SIM\ afectate} = N_{ds} \frac{T_{pierdut}}{T_{retea}}$$

N_{ds} reprezintă numărul de cartele SIM active pe respectivul serviciu la nivelul furnizorului, conform raportării în baza Deciziei președintelui ANCOM nr. 333/2013 privind raportarea unor date statistice de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului.

În calculul traficului total pierdut se are în vedere atât traficul originat, cât şi traficul terminat la nivelul celulelor afectate. Algoritmul propus se va aplica tuturor tipurilor de servicii la puncte mobile.

b) În cazul incidentelor care afectează ***echipamente din reţeaua centrală***, estimarea

[8] Machine-to-machine (M2M) - un serviciu care implică un transfer automat de date și informații între dispozitive sau aplicații bazate pe software, cu o interacțiune umană limitată sau fără interacțiune umană.

[9] O cartelă SIM activă este considerată orice cartelă SIM pe bază de abonament, respectiv orice cartelă SIM preplătită utilizată în mod efectiv cel puțin o dată, în sensul că a fost efectuat/recepționat un apel sau a fost trimis un SMS/MMS ori de pe care au fost utilizate servicii de transmisiuni de date cel puțin o dată în perioada de raportare determinată în baza Deciziei președintelui ANCOM nr. 333/2013 privind raportarea unor date statistice de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului.

numărului de utilizatori afectaţi va reflecta numărul de cartele SIM deservite de echipamentul respectiv.

NOTA: A se avea în vedere şi faptul că un serviciu nu trebuie să fie complet nefuncțional pentru a determina apariția unui incident. În acest sens, vor fi furnizate în continuare două exemple de conjuncturi punctuale pentru a evidenția situațiile incluse în această categorie:

- nefuncționarea serviciului de translatare nume de domenii în adrese IP – serviciul de acces la internet funcționează; cu toate acestea utilizatorii nu pot accesa anumite pagini de internet.
- probleme de interconectare pentru apelurile de voce – utilizatorii nu pot efectua apeluri în anumite reţele, deși, în altele o pot face.

b) durata incidentului – Se va specifica intervalul de timp dintre momentul în care serviciul începe să se degradeze sau s-a întrerupt și momentul în care acesta este restabilit la parametrii inițiali. Timpul va fi exprimat în minute. În situația unui incident ce afectează autenticitatea, integritatea sau confidențialitatea, durata va fi măsurată ca intervalul de timp dintre ora (estimată) a producerii breșei de securitate și ora rezolvării sau încheierii acesteia.

c) aria/răspândirea geografică - se vor specifica: numărul de județe afectate, denumirea județelor afectate, precum şi numele localităților (la nivel de UAT, inclusiv codul SIRUTA).

7) **descriere incident** - se va completa cu orice informații şi detalii relevante disponibile. Descrierea va fi sub formă de text şi va cuprinde, în mod obligatoriu, cel puțin următoarele elemente:

a) succesiunea evenimentelor care au dus la incident;

b) cauza incidentului (atât cauza principală, cât şi cea subsecventă, incluzând şi cauzele tehnice);

c) tehnologia/protocolul echipamentelor afectate de incident;

d) resursele afectate de incident;

e) localizarea echipamentelor afectate în cadrul rețelei;

f) nivelul la care componentele au fost afectate;

g) dacă a existat impact pe apelarea serviciului de urgență 112.

În continuare vor fi oferite îndrumări în ceea ce privește completarea câmpului descriere incident.

a) Succesiunea evenimentelor - va indica desfășurarea cronologică a ceea ce s-a petrecut în mod concret pe parcursul evenimentului raportat. Se dorește detalierea succesiunii evenimentelor, pentru a putea avea o imagine detaliată a ceea ce s-a întâmplat. De exemplu: se va specifica modul în care a apărut incidentul, ce anume l-a produs, ce a fost afectat punctual, se acțiuni au fost întreprinse pentru a remedia incidentul, cum s-a soluționat incidentul.

b) Cauza incidentului - incidentele vor fi clasificate în conformitate cu următoarele categorii de cauze principale:

b1) **Acțiune rău intenționată** - de exemplu: atac cibernetic[10], vandalism, furt de date, furt de echipamente, furt de cabluri, acces neautorizat la echipamente de rețea, platforme, aplicații (software), baze de date, atacuri de tip DoS sau DDoS, efectuare de modificări neautorizate

[10] Conform definiției prezente **Strategia de Securitate cibernetică a** României, **atacul cibernetic** este reprezentat orice acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică.

ale sistemelor şi datelor, sabotaj și care se soldează cu afectarea funcționării anumitor resurse.
b2) **Eroare de sistem** – de exemplu: eroare software datorată programării defectuoase ale software-lui din vina producătorului aplicației, defect hardware, procedură elaborată greșit.
b3) **Eroare umană**: de exemplu: acțiuni ale personalului intern precum: configurare sau dezvoltare și operare defectuoasă a echipamentelor de rețea, platformelor, aplicațiilor (software), aplicarea eronată a procedurilor.
b4) **Fenomene naturale** – de exemplu: incidente cauzate de dezastre şi fenomene naturale ori condiții meteo nefavorabile precum: ninsori abundente, furtuni, temperaturi excesive, cutremure, inundații, incendii, alunecări de teren, fenomene meteorologice spațiale, acțiuni ale rozătoarelor.
b5) **Cauză externă/Parte terță/Probleme electrice** - de exemplu: discontinuitate în alimentarea cu energie electrică datorată furnizorului/distribuitorului, șocuri de energie electrică datorate furnizorului/distribuitorului;
b6) **Cauză externă/Parte terță/Accident** - de exemplu: secționare de fibră optică de către terți în mod accidental, accident auto.
b7) **Cauză externă/Parte terță/Cauză necunoscută** – cauza incidentului nu a putut fi determinată.

Descrierea incidentului va include şi cauzele tehnice ale acestuia. Se vor utiliza cele ce se aplică incidentului în cauză:

- ascultarea convorbirilor
- atac de tip DDoS
- congestie element de rețea
- cutremur
- defecțiune hardware
- deturnarea traficului din rețea
- disfuncționalități sisteme backup energie electrică
- eroare software
- exploatarea unei vulnerabilități
- furt de identitate
- furt element de rețea
- gheață
- incendiu
- indisponibilitate sistem climatizare
- interferențe electromagnetice
- inundație
- înlocuire echipament defect sau upgrade de echipament, efectuate greșit
- întrerupere furnizare energie electrică
- malware sau virus
- nefuncționarea sistemelor suport
- ninsori abundente
- oprire de urgență a unui echipament
- phishing
- probleme procedurale
- secționare fibră optică
- supratensiune
- update software efectuat greșit
- vânt puternic

c) Tehnologia/protocolul echipamentelor afectate de incident – se vor alege opțiunile corespunzătoare din lista următoare:

- cablu
- email
- eMBB
- fibră optică
- GPRS/EDGE
- GSM
- LTE
- MTC
- mMTC
- protocol de mesagerie instant
- protocol de semnalizare
- PSTN
- UMTS
- URLLC
- VoIP
- Web/App

d) Resursele afectate de incident - se vor alege opțiunile corespunzătoare din lista următoare:

- aplicații
- cabinete stradale/containere
- cabluri aeriene/stâlpi
- cabluri subterane/conducte/camere de tragere
- centre de comutație în reţele fixe (centrală locală/de tranzit/națională/internațională, soft switch, server de gestiune a abonaților)
- centre de comutație în reţele mobile (MSC, SGSN, GGSN, PGW, SGW, ePDG, EPC, 5GC etc.)
- centre de retransmisie a programelor media (head-end, inclusiv amplificatoare, distribuitoare, etc.)
- centru de mesagerie mobilă (SMSC, MMSC)
- clădiri şi sisteme de securitate fizică
- componente/platforme de servicii (IPTV, VoIP, IMS, STP, SCP etc.)
- dispozitive pentru rețea inteligentă (IN)
- echipament terminal de rețea (repetor radio, modem, router etc.)
- linkuri radio
- noduri de transmisiuni (echipamente de modulație/demodulație, echipamente de multiplexare/demultiplexare pe tehnologie SDH, PDH, DWDM, hub radio etc.)
- puncte de interconectare(IXP, POI etc.)
- regiştri de utilizatori şi de localizare în reţele mobile (HLR, VLR, HSS, AuC şi similare etc.)
- servere de adresare (DHCP, DNS)
- SIM/eSIM
- sistem de taxare și mediere (PCRF)
- sisteme de climatizare
- sisteme de retenție a datelor şi interceptare legală a comunicaţiilor
- sisteme de securitate logică (IDS, IPS, VPN, firewall)
- sisteme suport operațional (OSS şi BSS)
- stații de bază și controlere mobile (BTS, BSC, NodeB, eNodeB, gNodeB, RNC etc.)/piloni
- stocare in cloud
- surse de alimentare (acumulatori, generatoare, dispozitive încărcare acumulatori, convertoare etc.)

- surse de energie electrică de backup
- switch-uri și routere
- alte resurse

e) Localizarea echipamentelor afectare în cadrul rețelei - se va alege opțiunea corespunzătoare din lista următoare:

- interconectare - legătura fizică și logică realizată între rețele publice de comunicații electronice care permite comunicarea dintre utilizatorii rețelelor sau accesul la servicii; serviciile pot fi furnizate de către părțile implicate sau de către terțe părți care au acces la rețeaua respectivă; interconectarea este o formă specifică de acces realizată de operatorii de rețele publice de comunicații (de exemplu IXP-ul se află în această categorie);
- reţea centrală (Core network) – este centrul rețelei care furnizează servicii utilizatorilor conectați la aceasta prin rețeaua de acces.
- reţea de acces (Acces network) – cuprinde accesul individual al utilizatorilor la rețelele și serviciile de comunicații electronice (de exemplu stațiile de bază se află în această categorie).
- reţea de transport/transmisiuni – cuprinde infrastructura dedicată transmiterii eficiente a datelor între diverse puncte şi include canale de transmisie (cum ar fi cabluri de fibră optică sau unde radio), echipamente de rutare și comutare pentru direcționarea traficului, protocoale de comunicare care stabilesc regulile de transmitere, și mecanisme de management al traficului.

*** Suplimentar, se va specifica şi numele localității la nivel de UAT şi codul SIRUTA unde sunt situate resursele afectate.

f) Nivelul la care componentele au fost afectate - se vor alege opțiunile corespunzătoare din lista următoare:

- nivel logic - face referire la componentele software ale echipamentelor.
- nivel fizic - face referire la componentele hardware ale echipamentelor.
- nivel suport - face referire la componentele suport ale echipamentelor precum cele utilizate pentru alimentarea cu energie electrică, echipamente auxiliare (de alimentare de backup cu energie electrică (grup electrogen, baterie/UPS etc.), sisteme de monitorizare și control al temperaturii (cooler, aer condiționat etc.), instalații electrice (cabluri electrice, siguranțe, întrerupătoare, transformatoare etc.) deținute de furnizor etc.

8) **acțiunile de răspuns -** se va completa cu măsurile de securitate implementate până la momentul producerii incidentului și descrierea detaliată a acțiunilor de răspuns, inclusiv momentele de timp în care au fost acestea realizate. De exemplu, se vor detalia acțiunile întreprinse pentru a aduce serviciul la un nivel acceptabil, precum şi pentru a restabili serviciul la parametrii inițiali în cazul afectării disponibilității, acțiunile întreprinse în ceea ce privește limitarea pierderii suplimentare a datelor, evaluarea pierderilor survenite prin colectarea faptelor și evaluarea riscurilor, inclusiv a potențialelor prejudicii aduse persoanelor afectate, în cazul afectării autenticității, integrității sau confidențialității. Se vor menționa alte autorități care au fost contactate și acțiunile de informare a persoanelor implicate în incident, dacă este cazul.

În cazul în care cauza incidentului este „Cauză externă/Parte terță/Probleme electrice" se vor specifica durata de back-up electric fix calculată în sensul Art. 4, alin. 3 din Decizia nr. 70/2024, respectiv durata aferenta capacității de back-up instalate efectiv. În eventualitatea epuizării resursei de back-up înainte de remedierea cauzei incidentului, se va menționa durata reală/măsurată de

funcționare a sistemului de back-up.

9) **măsurile luate sau planificate pentru a împiedica producerea unui incident similar inclusiv momentul când acestea au fost/vor fi luate, precum şi lecțiile învățate -** se va completa cu descrierea detaliată a acțiunilor realizate pentru a minimiza nivelul de risc şi pentru a preîntâmpina reapariția incidentului (de exemplu: revizuire măsuri de securitate şi proceduri, renegociere SLA-uri, instruiri de personal, achiziție de echipamente sau sisteme de back-up etc.), precum şi momentul când au fost luate sau când vor fi luate aceste măsuri. Acest câmp va conține și informații despre lecțiile învățate - aceasta presupune realizarea unui bilanț al incidentului, ajungerea la sursa problemei (root cause), cum și de ce s-a întâmplat, evaluarea a cât de bine a funcționat planul de răspuns la incident pentru a rezolva problema și identificarea îmbunătățirilor care trebuie făcute.

10) **alți furnizori de reţele şi servicii de comunicaţii electronice afectați -** se va selecta una dintre cele 2 opțiuni prezente în aplicația informatică (DA/NU). În situația în care sunt afectați și alți furnizori se va specifica denumirea furnizorul afectat de incidentul în cauză.

11) **persoana de contact:** se vor completa datele de contact (nume, prenume, număr telefon de contact, e-mail) ale persoanei responsabile cu furnizarea clarificărilor de natură tehnică, în cazul în care va fi nevoie. În cazul în care persoana care poate oferi mai multe detalii tehnice despre incident este aceeași cu persoana desemnata conform Art. 7, din Decizia nr. 70/2024, adică persoana responsabilă de notificarea incidentelor, acest câmp nu se mai completează.

În anumite cazuri, este posibil ca furnizorii să nu dețină, la momentul transmiterii notificării finale toate informațiile privind incidentul care a afectat securitatea rețelelor şi serviciilor de comunicații electronice. În acest caz, furnizorii vor transmite în termenul legal de 2 săptămâni datele pe care le dețin şi, ulterior, în termen de maximum 4 săptămâni de la detectarea incidentului vor transmite şi elementele lipsă printr-o notificare suplimentară. Această notificare presupune completarea elementelor lipsă în câmpurile corespunzătoare din notificarea finală transmisă anterior.

6. RAPORTAREA UNUI INCIDENT FOLOSIND APLICAŢIA ONLINE

Conform Deciziei președintelui ANCOM nr. 70/2024, transmiterea notificării finale şi după caz a celei suplimentare se realizează exclusiv prin intermediul aplicației disponibile pe pagina de internet a ANCOM, ca înscris în formă electronică căruia i s-a încorporat, atașat ori asociat logic o semnătură electronică extinsă, bazată pe un certificat calificat nesuspendat sau nerevocat la data transmiterii și generată cu ajutorul unui dispozitiv securizat de creare a semnăturii electronice, prevederile Deciziei președintelui Autorității Naționale pentru Administrare şi Reglementare în Comunicații nr. 336/2013 privind mijloacele şi modalitatea de transmitere a unor documente, date sau informații către Autoritatea Națională pentru Administrare şi Reglementare în Comunicații şi privind modificarea Deciziei președintelui Autorității Naționale pentru Comunicații nr. 77/2009 privind obligațiile de informare a utilizatorilor finali de către furnizorii de servicii de comunicații electronice destinate publicului fiind aplicabile în mod corespunzător.

Astfel, formularul de raportare a incidentelor cu impact semnificativ aferent notificării finale trebuie completat de către furnizorul de rețele şi servicii de comunicații electronice prin intermediul aplicației online SSCPDS - Sistemul Software de Colectare şi Prelucrare a Datelor Statistice (https://statistica.ancom.ro/sscpds/index.faces). Aplicația este accesibilă din pagina principală a site-ului ANCOM (http://www.ancom.ro), apăsând

butonul *Raportează*.

Pentru autentificare, se folosesc datele (numele de utilizator şi parola) utilizate de reprezentantul furnizorului pentru completarea datelor statistice ce trebuie raportate ANCOM.

Pentru informații privind accesul în aplicație, autentificarea şi gestionarea profilului utilizatorului, funcția de administrare a persoanelor autorizate, completarea datelor, semnarea electronică a formularelor, se recomandă consultarea manualului pentru utilizator FRSCE disponibil în format electronic pe pagina principală a aplicației.

ANEXA 1 GLOSAR DE TERMENI

Stații de bază și controlere mobile

BTS (Base Transceiver Station) este o stație de bază de emisie-recepție din rețeaua de telefonie mobilă situată în partea de acces, care asigură comunicarea wireless între echipamentele de utilizator (UE) și rețea.
BSC (Base Station Controller) este controlerul stației de bază și realizează, în partea de acces a rețelelor mobile, controlul BTS-urilor. De obicei, un BSC are zeci sau chiar sute de BTS-uri aflate sub controlul său.
NodeB este stația de bază de emisie-recepție în rețele de telefonie mobilă UMTS echivalentă cu BTS utilizată în GSM;
eNodeB (Evolved NodeB) este stația de bază de emisie-recepție în rețele de telefonie mobilă LTE.
gNodeB (Next generation NodeB) este o componentă critică a arhitecturii rețelelor fără fir 5G. În lumea 5G, gNodeB este similar cu BTS în 2G, NodeB în 3G și eNodeB în 4G.
RNC (Radio Network Controller) este controlerul de rețea radio din rețeaua de acces mobil UMTS (UTRAN) și este responsabil pentru controlul NodeB-urilor care sunt conectate la acesta. RNC realizează managementul resurselor radio, unele dintre funcțiile de gestionare a mobilității și este punctul în care se face criptarea datelor înainte de a fi trimise la și de la telefonul mobil al utilizatorului.
MME (Mobility Management Entity) este nodul de control cheie pentru rețeaua de acces LTE. Acesta este responsabil pentru procedura de urmărire și paging, inclusiv retransmisia în modul de așteptare (idle) al UE (echipament de utilizator).
ANDSF (Access Network Discovery and Selection Function) este situat în rețeaua centrală LTE și ajută echipamentul utilizatorului (UE) să descopere rețele de acces non- 3GPP, cum ar fi Wi-Fi sau WiMAX - care pot fi utilizate pentru comunicații de date în plus față de rețele de acces 3GPP (cum ar fi HSPA sau LTE) și pentru a oferi UE regulile de conectare la aceste rețele.
PCRF (Policy and Charging Rules Function) realizează stabilirea normelor de politică într-o rețea multimedia. PCRF joacă un rol central în rețelele IP de ultimă generație.

Centre de comutație în rețele mobile

MSC (Mobile Switching Centre) este centrul de comutare a unei rețele de telefonie mobilă și are interfețe către BSC-uri, HLR, VLR și alte MSC-uri. MSC asigură comutarea apelurilor, managementul mobilității și servicii mobile pentru UE aflate în roaming în interiorul zonei pe care o deservește (voce, servicii fax, date, SMS, transferare a apelurilor).
SGSN (Serving GPRS Support Node) realizează transportul pachetelor de date de la și către stațiile de bază din aria sa geografică de acoperire.
GGSN (Gateway GPRS Support Node) realizează legătura între rețeaua GPRS (General Packet Radio Service) și rețelele externe cu comutație de pachete.
PGW/PDN GW (Public Data Network Gateway): GW-ul PDN oferă conectivitate UE la rețelele externe de pachete de date, fiind punctul de intrare și ieșire al traficului pentru UE. PGW aplică politica de securitate și realizează filtrarea de pachete pentru fiecare utilizator, suport pentru taxare, interceptarea legală și screening-ul de pachete. Un alt rol cheie al PGW este de a acționa ca ancoră pentru mobilitatea între tehnologiile 3GPP și non-3GPP.
SGW (Serving Gateway) rutează și redirecționează pachetele de date de utilizator, în timp ce se comportă ca ancora de mobilitate pentru planul de utilizator în timpul handover-ului între eNodeB-uri și ca ancoră pentru mobilitatea între LTE și alte tehnologii 3GPP.
EPC (Evolved Packet Core) este un cadru pentru furnizarea de servicii convergente de voce și de date pe o rețea 4G Long-Term Evolution (LTE).
ePDG (Evolved Packet Data Gateway) securizează transmisia datelor dintre UE-uri

conectate la EPC (Evolved Packet Core) peste rețele non 3GPP nesecurizate.

Registri de localizare

HLR (Home Location Register) este baza de date centrală într-o rețea mobilă care conține informații despre fiecare abonat care este autorizat să acceseze/să se conecteze la rețeaua centrală GSM.
VLR (Visitor Location Register) este baza de date a abonaților rețelei mobile din aria de acoperire a MSC-ului. Fiecare stație de bază din rețea este deservită de câte un VLR.
HSS (Home Subscriber Server) este baza de date ce conține profilurile abonaților și serviciile la care aceștia au acces. HSS realizează funcția de autentificare și autorizare a abonaților și poate furniza informații privind localizarea și IP-ul acestora.
AuC (Authentication Centre) este o componentă a rețelei ce realizează funcția de autentificare/validare a informațiilor de securitate a cartelelor SIM ce încearcă să se conecteze la rețea.

Centre de mesagerie mobilă

SMSC (Short Message Service Centre) este centrul serviciului de mesagerie scurtă ce stochează, redirecționează, modifică și transmite mesaje SMS.
MMSC (Multimedia Messaging Service Centre) este centrul serviciului de mesagerie multimedia ce stochează, redirecționează, modifică și transmite mesaje MMS.

Routere şi switch-uri IP

DSLAM (Digital Subscriber Line Access Multiplexer) este un echipament din rețeaua de acces care conectează mai multe interfețe de linii digitale de abonat (DSL) la un canal de comunicații digitale de mare viteză folosind tehnici de multiplexare.
BRAS rutează traficul către și dinspre dispozitive de acces broadband precum DSLAM în rețeaua unui ISP.
Metro router este un sistem de rutare a traficului în rețele de acoperire metropolitană.
Metro switch este un dispozitiv care realizează interconectarea diferitelor segmente din rețele de acoperire metropolitană.
EDGE routers sunt routere situate la marginea rețelei IP a furnizorului.
IP PBX (Private Branch Exchange) este un sistem de rutare și comutare a apelurilor telefonice într-o rețea de telefonie IP.
Core routers sunt routere situate în rețeaua centrală (core) a furnizorului.

Echipamente din noduri de transmisiune

SDH (Synchronous Digital Hierarchy) sunt protocoale standardizate care transferă în mod sincron mai multe fluxuri digitale de biți pe fibră optică.
PDH (Plesiochronous Digital Hierarchy) este o tehnologie folosită în rețelele de telecomunicații pentru a transporta cantități mari de date prin rețele digitale de mari dimensiuni.
DWDM (Dense/Wavelength-Division Multiplexing) este o tehnologie prin care se multiplexează un număr de semnale purtătoare optice pe o singură fibră optică utilizând lungimi de undă diferite (de exemplu culori) de lumină laser. Această tehnică permite comunicații bidirecționale peste un fir de fibre.

Puncte de interconectare

IXP (Internet eXchange Point) este o infrastructură fizică prin care furnizorii de servicii de acces la Internet (ISP) realizează transfer de trafic IP între rețelele lor.
POI (Point Of Interconnection) este un punct în rețeaua furnizorului de comunicații

electronice de interconectare cu alte rețele.

Servere de adresare

DHCP (Dynamic Host Configuration Protocol) este un protocol și un serviciu care alocă o adresă IP sistemelor din rețea.

DNS (Domain Name System) este un sistem distribuit de denumire a computerelor, serviciilor sau oricăror alte resurse conectate la Internet sau rețea privată. Acesta asociază diferite informații cu nume de domenii alocate fiecărei entități participante.

Sisteme de securitate

IDS (Intrusion Detection System) este sistemul de detectare a intruziunilor care este utilizat pentru identificarea unor încercări de intruziuni, intruziuni ce au sau au avut loc și eventual pentru răspunsul la intruziuni în rețele și sisteme informatice.

IPS (Intrusion Prevention System) este sistemul de prevenire a intruziunilor care este utilizat pentru identificarea și prevenirea unor încercări de intruziuni sau intruziuni ce au loc în rețele și sisteme informatice.

AAA (authentication, authorization and accounting or auditability) se referă la o arhitectură de securitate a sistemelor distribuite în cadrul căreia se autentifică identitatea utilizatorului, se acordă acces acestuia și în final se menține o înregistrare a accesului acestuia pentru taxare și auditare.

LDAP (Lightweight Directory Access Protocol) este un protocol de accesare și administrare a directorului cu informații privind utilizatorii și drepturile de acces ale acestora. De obicei, LDAP este utilizat pentru a găsi rapid informații despre un anumit utilizator în directoare cu foarte mulți utilizatori.

VPN (Virtual Private Network) conectează componentele și resursele unei rețele private prin intermediul unei rețele publice.

Firewall este un sistem de securitate al rețelei, de tip software sau hardware, care controlează traficul ce iese și intră în rețea analizând pachetele de date și determinând pe baza unui set de reguli de securitate dacă acestea pot pătrunde în rețea sau nu.

Componente/Platforme de servicii

IPTV (Internet Protocol TeleVision) este o platformă de servicii prin care se transmit programe audio-vizuale într-o rețea care se bazează pe IP.

VoIP (Voice over IP) este o platformă prin care se oferă servicii de transmitere a semnalelor vocale prin rețele IP.

IMS (IP Multimedia Subsystem) este o platformă în rețelele de generație viitoare prin care se pot oferi servicii multimedia fixe sau mobile.

STP (Signal Transfer Point) este o componentă a rețelelor inteligente (de telefonie fixă și mobilă) care comută mesajele SS7 între SEP-uri (Signalling End-Point) și alte STP- uri.

SCP (Service Control Point) este o componentă standard a rețelelor inteligente (de telefonie fixă și mobilă) utilizată pentru administrarea serviciilor oferite în aceste rețele.

OSS (Operations Support Systems) și **BSS** (Business Support Systems) sunt platforme informatice utilizate de furnizorii de servicii de comunicații electronice în scopul administrării propriilor rețele. Aceste platforme realizează funcții precum managementul, inventarierea și configurarea rețelei. De asemenea, se mai ocupă cu managementul rețelei în cazul incidentelor.

MTC (Mobile Terminating Call) este o componentă esențială a sistemului de telecomunicații mobile care permite efectuarea de apeluri de voce și de date către un dispozitiv mobil. MTC se referă la un apel inițiat din rețeaua părții apelante către dispozitivul mobil al destinatarului.

mMTC (Massive Machine-Type Communications) reprezintă unul dintre cele trei domenii de bază ale serviciilor 5G. Acesta a fost creat special pentru a permite colectarea simultană a unui volum uriaș de pachete mici de date de la un număr mare de dispozitive.

eMBB (Enhanced Mobile Broadband) este un concept 5G care se concentrează asupra vitezei, capacității și mobilității pentru a permite noi utilizări mobile, cum ar fi streamingul video de înaltă definiție și realitatea augmentată (AR) și realitatea virtuală (VR) imersivă în mișcare.

URLLC (Ultra-Reliable and Low-Latency Communications) este o caracteristică esențială a 5G care permite comunicații de înaltă fiabilitate și latență redusă pentru aplicații critice, cum ar fi automatizarea fabricilor, conducerea autonomă și realitatea virtuală/aumentată.

5GC (5G Core) este o parte fundamentală a rețelei 5G pentru: îmbunătățirea experienței utilizatorului final (UX) simplificarea operațiunilor de rețea, creșterea agilității de creare a serviciilor, îmbunătățirea capacităților rețelei.