UE

GUVERNUL REPUBLICII MOLDOVA
HOTĂRÂRE nr. _____
din _____
Cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice

În scopul executării prevederilor art. 11 și în temeiul art. 12 alin. (9) și al art. 14 alin. (2) din Legea nr. 48/2023 privind securitatea cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr. 151-153), Guvernul HOTĂRĂȘTE:

1. Prezenta Hotărâre transpune parțial Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555 în ceea ce privește cerințele tehnice și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică și specificarea suplimentară a cazurilor în care un incident este considerat semnificativ referitor la furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, precum și prestatorii de servicii de încredere, CELEX: 32024R2690, publicat în Jurnalul Oficial al Uniunii Europene L din 18 octombrie 2024.

2. Se aprobă Regulamentul cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice (se anexează).

3. Furnizorii esențiali de servicii, inclusiv operatorii obiectivelor de infrastructură critică:

3.1. vor asigura punerea în aplicare a prevederilor prezentei hotărâri în termen de 12 de luni din data intrării în vigoare a acesteia;

3.2. în termen 6 luni din data intrării în vigoare a prezentei hotărâri, în conformitate cu prevederile corespunzătoare ale anexei la prezenta hotărâre vor efectua analiza riscurilor la adresa securității rețelelor și sistemelor informatice proprii și vor aproba rapoarte în acest sens, precum și vor aproba planuri de tratare a riscurilor identificate și evaluate;

3.3. vor prezenta Agenției pentru Securitate Cibernetică raportul de evaluare a riscurilor și planul de tratare a riscurilor, în termen de 10 de zile din data aprobării acestora;

3.4. vor prezenta Agenției pentru Securitate Cibernetică, în termen de 18 de luni de la data intrării în vigoare a prezentei hotărâri raportul primei evaluări a

conformității cu cerințele prevăzute în anexa la prezenta hotărâre, efectuată de către o parte terță certificată în domeniul auditului securității informațiilor.

4. Furnizorii importanți de servicii:

4.1. vor asigura punerea în aplicare a prevederilor prezentei hotărâri în termen de 18 de luni din data intrării în vigoare a acesteia;

4.2. în termen 9 luni din data intrării în vigoare a prezentei hotărâri, în conformitate cu prevederile corespunzătoare ale anexei la prezenta hotărâre vor efectua analiza riscurilor la adresa securității rețelelor și sistemelor informatice proprii și vor aproba rapoarte în acest sens, precum și vor aproba planuri de tratare a riscurilor identificate și evaluate;

4.3. vor prezenta Agenției pentru Securitate Cibernetică, în termen de 10 de zile din data aprobării, rapoartele de evaluare a riscurilor și planurile de tratare a riscurilor;

4.4. vor prezenta Agenției pentru Securitate Cibernetică raportul primei evaluări a conformității cu cerințele prevăzute în anexa la prezenta hotărâre în termen de 24 de luni din data intrării în vigoare a prezentei hotărâri.

5. Agenția pentru Securitate Cibernetică:

5.1. în termen de 6 luni de la data publicării prezentei hotărâri, va asigura implementarea unor mecanisme, inclusiv prin utilizarea mijloacelor tehnice, destinate asigurării unui schimb direct, sistematic și imediat de informații în contextul realizării de către furnizorii de servicii a obligațiilor de raportare a incidentelor cibernetice cu impact semnificativ;

5.2. va acorda asistență consultativă furnizorilor de servicii, la solicitare, în procesul de evaluare a riscurilor

5.3. în termen de 12 luni de la data expirării termenului prevăzut la subpct. 3.4, va evalua nivelul de conformitate a furnizorilor esențiali de servicii și a operatorilor obiectivelor de infrastructură critică, inclusiv în baza rapoartelor de evaluare a riscurilor, a planurilor de tratare a riscurilor și a rapoartelor de evaluare a conformității, efectuate în temeiul subpunctelor 3.3 și, respectiv, 3.4, cu cerințele privind măsurile de securitate a rețelelor și sistemelor informatice, prevăzute în anexa la prezenta hotărâre, și va înainta recomandările corespunzătoare furnizorilor de servicii evaluați;

5.4. în termen de 18 luni de la data expirării termenului prevăzut la subpct. 4.4, va evalua nivelul de conformitate a furnizorilor importanți de servicii, inclusiv în baza rapoartelor de evaluare a riscurilor, a planurilor de tratare a riscurilor și a rapoartelor de evaluare a conformității, efectuate în temeiul subpunctelor 4.3 și, respectiv, 4.4, cu cerințele privind măsurile de securitate a rețelelor și sistemelor informatice, prevăzute în anexa la prezenta hotărâre, și va înainta recomandările corespunzătoare furnizorilor de servicii evaluați.

6. Se abrogă Hotărârea Guvernului nr. 201/2017 "Cu privire la aprobarea Cerințelor minime obligatorii de securitate cibernetică" (Monitorul Oficial al Republicii Moldova, 2017, nr. 109-118, art. 277).

7. Hotărârea Guvernului nr. 860/2024 cu privire identificarea furnizorilor de servicii (Monitorul Oficial al Republicii Moldova, 2024, nr. 548-551, art 999) se modifică după cum urmează:

7.1 Anexa nr. 1 se completează cu pct. 9^{1-} cu următorul cuprins:

„9^{1}. Actul administrativ de desemnare în calitate de furnizor de servicii, cât și notificarea privind intenția de desemnare în calitate de furnizor de servicii constituie informație cu acces limitat. Modul de prelucrare a informației precum și accesul la informația dată urmează a fi reglementat prin Ordinul Directorului Agenției pentru Securitate Cibernetică.”.

7.2 Punctul 10 din Anexa nr.3 va avea următorul cuprins:

„10. Lista constituie informație cu acces limitat. Modul de prelucrare a informației precum și accesul la listă urmează a fi reglementat prin Ordinul Directorului Agenției pentru Securitate Cibernetică.”.

8. Controlul executării prezentei hotărâri se pune în sarcina Ministerului Dezvoltării Economice și Digitalizării.

Prim-ministru

Contrasemnează

Viceprim-ministru, ministru al
dezvoltării economice și digitalizării

Anexă
la Hotărârea Guvernului nr.
din

REGULAMENTUL
cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice

Capitolul I. Dispoziții generale

1. Regulamentul cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice (în continuare - Regulament) are ca obiect de reglementare modul de aplicare a cerințelor privind măsurile de securitate a rețelelor și sistemelor informatice pe care le utilizează la prestarea serviciilor esențiale, procedura de notificare a incidentelor cibernetice cu impact semnificativ, condițiile specifice pentru unele tipuri de furnizori de servicii în care un incident cibernetic urmează a fi calificat ca fiind semnificativ, precum și modul de evaluare a echivalenței efectelor legislației care reglementează activitatea furnizorilor de servicii și/sau sectoarele şi subsectoarele critice stabilite prin Hotărârea Guvernului nr. 860/2023 cu privire la identificarea furnizorilor de servicii *(în continuare - legislație sectorială)* în raport cu cele ale Legii nr. 48/2023 privind securitatea cibernetică.

2. Prezentul Regulament se aplică furnizorilor de servicii identificați de către Agenția pentru Securitate Cibernetică (în continuare - Agenția) în conformitate cu Hotărârea Guvernului nr. 860/2024 „Cu privire la identificarea furnizorilor de servicii”.

3. În sensul prezentului Regulament noțiunile utilizate au înțelesul stabilit de Legea nr. 48/2023 privind securitatea cibernetică, Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat.

Capitolul II. Modul de aplicare a cerințelor privind măsurile de securitate a rețelelor și sistemelor informatice a furnizorilor de servicii în sectoarele critice

4. Furnizorii de servicii pot utiliza standarde și specificații tehnice naționale și internaționale, inclusiv europene, atunci când implementarea anumitor cerințe prevăzute în anexa la prezentul Regulament implică necesitatea unor informații mai detaliate.

5. În baza cerințelor prevăzute în anexa la prezentul Regulament, Agenția elaborează ghiduri de implementare și furnizează, orientări metodologice furnizorilor de servicii în sectoarele critice.

6. Furnizorii de servicii asigură un nivel de securitate a rețelelor și a sistemelor informatice corespunzător și proporțional riscurilor identificate atunci când implementează și aplică măsuri tehnice și organizatorice de gestionare a riscurilor în materie de securitate cibernetică.

7. Atunci când determină proporționalitatea măsurilor de securitate implementate pentru tratarea riscurilor identificate, furnizorii de servicii trebuie să țină cont în mod corespunzător de gradul lor de expunere la riscuri; de dimensiunea lor; de probabilitatea apariției unor incidente; de gravitatea acestora, inclusiv de impactul lor societal și economic.

8. În cazul în care anexa la prezentul Regulament prevede că o cerință a unei măsuri de gestionare a riscurilor în materie de securitate cibernetică se aplică dacă este adecvat, dacă este aplicabil sau în măsura în care este fezabil, iar în cazul în care un furnizor de servicii consideră că nu este adecvat, nu este aplicabil sau nu este fezabil să aplice astfel de cerințe, acesta documentează într-un mod inteligibil motivarea în acest sens, informând Agenția în termen de 10 zile din data documentării motivării de neimplementare a cerinței respective.

9. Furnizorii de servicii efectuează audituri externe privind securitatea informațiilor, în vederea determinării nivelului de conformitate cu cerințele privind măsurile de securitate a rețelelor și sistemelor informatice, prevăzute în anexa la prezentul Regulament, cel puțin o dată la trei ani sau ori de câte ori este necesar în conformitate cu cerințele stabilite de anexa la prezentul Regulament. Raportul de audit extern și rapoartele examinărilor independente, efectuate în conformitate cu secțiunea 2 a capitolului 2 din anexa la prezentul Regulament se prezintă Agenției în termen de o lună de la data efectuării.

10. Cerințele prevăzute în anexa la prezentul Regulament nu se aplică furnizorilor de servicii dacă măsurile de securitate implementate de furnizorul de servicii sunt conforme cu cerințele stabilite de standardul moldovenesc SM ISO/IEC 27001 sau standardul internațional ISO/IEC 27001 și furnizorul de servicii a prezentat Agenției un certificat valabil care confirmă conformitatea cu standardul respectiv. Îndeplinirea de către furnizorul de servicii a condițiilor stabilite de prezentul punct nu exclude dreptul Agenției de a efectua o evaluare a conformității acestui furnizor de servicii cu cerințele prevăzute în anexa la prezentul regulament în exercitarea funcției de supraveghere și control al modului în care sunt respectate prevederile cadrului normativ în domeniul securității cibernetice.

Capitolul III. Modul de evaluare a echivalenței efectelor obligațiilor de asigurare a securității cibernetice

11. Dacă legislația sectorială impune furnizorilor de servicii cerințe ale măsurilor de securitate a rețelelor și sistemelor informatice sau obligații de notificare

a incidentelor cibernetice semnificative cel puțin echivalente cu cele prevăzute de Legea nr. 48/2023 privind securitatea cibernetică și prezentul Regulament, furnizorii de servicii aplică prevederile legislației sectoriale.

12. Cerințele privind măsurile de securitate a rețelelor și sistemelor informatice sau obligațiile de notificare a incidentelor cibernetice semnificative din legile sectoriale sunt considerate echivalente în privința efectului cu cele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și prezentul Regulament, în cazul în care:

12.1. măsurile de gestionare a riscurilor în materie de securitate cibernetică sunt cel puțin echivalente în privința efectului cu cele prevăzute la articolul 11 alineatele (1) - (3) din Legea nr. 48/2023 privind securitatea cibernetică și prevederile prezentului Regulament;

12.2. legislația sectorială prevede accesul imediat, după caz automat și direct, al Agenției la notificările incidentelor cibernetice cu impact semnificativ și dacă obligațiile de notificare au un efect cel puțin echivalent cu cele prevăzute la articolul 12 din Legea nr. 48/2023 privind securitatea cibernetică.

13. Atunci când se evaluează dacă cerințele legislației sectoriale privind măsurile de securitate a rețelelor și sistemelor informatice au un efect cel puțin echivalent cu cele prevăzute de Legea nr. 48/2023 privind securitatea cibernetică și prezentul regulament, cerințele legislației sectoriale trebuie:

13.1. cel puțin, să corespundă cerințelor prevederilor respective, să acopere toate problematicile prevăzute în anexa la prezentul Regulament sau să aibă un caracter mai detaliat pe fond;

13.2. să se refere la toate operațiunile și serviciile furnizorului de servicii în cauză, nu numai la anumite active sau servicii informatice critice pe care acesta le furnizează;

13.3. să cuprindă măsuri de securitate orientate spre asigurarea securității rețelelor și sistemelor informatice, inclusiv măsuri de securitate a hardware, firmware și software utilizate în activitatea furnizorului de servicii;

13.4. să abordeze în mod specific securitatea fizică și de mediu a rețelelor și a sistemelor informatice în caz de defectare a sistemelor, de erori umane, de acte ilegale sau de fenomene naturale.

14. Atunci când se evaluează dacă cerințele legislației sectoriale privind notificarea incidentelor semnificative de către furnizorul de servicii către Agenție au un efect cel puțin echivalent cu cele prevăzute de Legea nr. 48/2023 privind securitatea cibernetică și prezentul Regulament, trebuie să se țină cont de faptul că cerințele legislației sectoriale stabilesc cel puțin:

14.1. prevederi care să corespundă cerințelor din Legea 48/2023 privind securitatea cibernetică și prezentul Regulament sau să aibă un caracter mai detaliat pe fond;

14.2. obligativitatea raportării incidentelor cibernetice semnificative;

14.3. calificarea incidentelor cibernetice ca fiind semnificative, bazată pe condițiile minime stabilite la art. 12 alin. (5) din Legea 48/2023 privind securitatea cibernetică și dezvoltate de prezentul Regulament;

14.4. prevederi privind raportarea incidentelor în mai multe etape, care să cuprindă cel puțin: o notificare, corespunzătoare informării prevăzute la art. 12 alin. (1), o actualizare a notificării, corespunzătoare art. 12 alin. (3) și un raport final, corespunzător art. 12 alin. (8) din Legea nr. 48/2023 privind securitatea cibernetică;

14.5. conținutul obligației de raportare care să includă informațiile prevăzute la punctele 16-18;

14.6. asigurarea unui acces imediat prin mijloace automate și directe, care să asigure schimbul sistematic și imediat de informații cu Agenția.

Capitolul IV. Procedura de notificare a incidentelor cibernetice cu impact semnificativ

15. Pentru executarea obligațiilor stabilite de art. 12 din Legea nr. 48/2023 privind securitatea cibernetică, furnizorii de servicii prezintă Agenției o notificare a incidentului cibernetic, o actualizare a notificării și un raport final. Informațiile prezentate Agenției în condițiile art. 13 din Legea nr. 48/2023 sunt supuse cerințelor stabilite de prevederile prezentului capitol.

16. Notificarea trebuie să includă, atunci când există, informații privind suspiciunile că incidentul semnificativ este cauzat de acte ilegale sau presupus ilegale sau dacă există probabilitatea că acest incident ar putea avea un impact transfrontalier. Notificarea trebuie să includă informațiile strict necesare pentru a aduce la cunoștința Agenției incidentul semnificativ și pentru a permite furnizorului de servicii în cauză să solicite asistență, dacă este necesar.

17. Actualizarea notificării trebuie să includă o evaluare inițială a incidentului semnificativ, inclusiv a gravității și a impactului acestuia, precum și, dacă există, a indicatorilor de compromitere, precum și, atunci când există, o revizuire a informațiilor transmise în cadrul notificării.

18. Raportul final trebuie să includă o descriere detaliată a incidentului cibernetic, inclusiv a gravității și a impactului acestuia, tipul de amenințare și/sau de cauză principală care a declanșat sau este probabil să fi declanșat incidentul; măsurile de atenuare aplicate și în curs de aplicare și, dacă este cazul, o descriere a impactului transfrontalier al incidentului cibernetic.

19. În cazul în care la momentul prezentării raportului final incidentul cibernetic este în desfășurare, furnizorul de servicii prezintă la momentul respectiv un raport privind progresele înregistrate și un raport final în termen de o lună de la finalizarea gestionării incidentului.

20. În procesul gestionării incidentului cibernetic, la solicitarea Agenției, furnizorul de servicii prezintă actualizări ale informațiilor prezentate anterior sau, atunci când există, furnizează informații noi, relevante pentru procesul de gestionare a incidentului cibernetic și pentru asistența acordată de Agenție la solicitarea furnizorului de servicii.

21. Modelul actului și formatul informațiilor prezentate în cadrul interacțiunii dintre furnizorii de servicii și Agenție în procesul de realizare de către aceștia a obligațiilor de notificare a incidentelor cibernetice cu impact semnificativ se aprobă de directorul Agenției.

22. Incidentele care, în mod individual, nu sunt considerate drept un incident semnificativ în sensul art.12 alin. (5) din Legea nr.48/2023 privind securitatea cibernetică trebuie considerate toate împreună incidente recurente și calificate ca un unic incident cibernetic cu impact semnificativ, dacă îndeplinesc cumulativ următoarele condiții:

22.1. s-au produs cel puțin de două ori în decursul unei perioade de șase luni;

22.2. au aceeași cauză principală aparentă;

22.3. împreună au cauzat sau pot cauza pierderi financiare directe pentru furnizorul de servicii afectat care depășesc 5 % din cifra de afaceri anuală totală a acestuia aferentă exercițiului financiar anterior.

23. Nu sunt considerate a fi incidente cibernetice cu impact semnificativ întreruperile programate ale serviciului și consecințele planificate ale operațiunilor de întreținere programate, efectuate de către furnizorii de servicii sau de către terți în numele acestora.

24. Atunci când calculează numărul de utilizatori afectați de un incident cibernetic, furnizorii de servicii trebuie să țină cont cumulativ de următoarele elemente:

24.1. numărul de clienți care au un contract cu furnizorul de servicii care le acordă acces la rețeaua și la sistemele informatice ale furnizorului de servicii sau la serviciile oferite de rețeaua și de sistemele informatice respective sau accesibile prin intermediul acestora;

24.2. numărul de persoane fizice și juridice asociate clienților comerciali care utilizează rețeaua și sistemele informatice ale furnizorului de servicii sau serviciile oferite de rețeaua și de sistemele informatice respective sau accesibile prin intermediul acestora.

Capitolul V. Condiții specifice pentru determinarea impactului semnificativ al incidentelor cibernetice pentru unele tipuri de furnizori de servicii

25. În sensul art. 12 alin. (5) lit. d) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de servicii DNS, Registratorul național al domeniului de nivel superior .md, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate și furnizorii de servicii de securitate gestionate, furnizorii de piețe online, furnizorii de motoare de căutare online, furnizorii de platforme de servicii de socializare în rețea și prestatorii de servicii de încredere, prejudiciile urmează a fi calificate ca fiind considerabile, dacă sunt îndeplinite unul sau mai multe dintre următoarele criterii:

25.1. incidentul a cauzat sau poate cauza pierderi financiare directe pentru furnizorul de servicii afectat care depășesc 5 % din cifra de afaceri anuală totală a acestuia aferentă exercițiului financiar anterior;

25.2. incidentul a cauzat sau poate cauza exfiltrarea secretelor comerciale ale furnizorului de servicii, astfel cum acestea sunt definite la articolul 2 din Legea nr.384/2023 privind protecția secretelor comerciale;

25.3. incidentul a cauzat sau poate cauza decesul unei persoane fizice;

25.4. incidentul a cauzat sau poate cauza daune considerabile asupra sănătății unei persoane fizice;

25.5. s-a produs un acces reușit, presupus rău-intenționat și neautorizat, la rețelele și la sistemele informatice, care poate cauza perturbări operaționale grave furnizorului de servicii;

25.6. incidentul este recurent în sensul punctului 22;

25.7. incidentul îndeplinește, în mod corespunzător, cel puțin una dintre condițiile prevăzute la punctele 26-35.

26. În sensul art. 12 alin. (5) lit. a) și lit. b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de servicii DNS, un incident cibernetic urmează a fi considerat ca având impact semnificativ și atunci când intervine una sau mai multe dintre următoarele condiții:

26.1. un serviciu de rezolvare recursivă sau autoritară a numelor de domenii este complet indisponibil timp de peste 30 de minute, sau

26.2. pentru o perioadă care depășește o oră, timpul mediu de răspuns al unui serviciu de rezolvare recursivă sau autoritară a numelor de domenii la cererile DNS este mai mare de 10 secunde sau

26.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea serviciului de rezolvare autoritară a numelor de domenii este compromisă, cu excepția cazurilor în care datele cu mai puțin de 1 000 de nume de domenii gestionate de furnizorul de servicii DNS, care nu depășesc 1 % din numele de domenii gestionate de furnizorul de servicii DNS, nu sunt corecte din cauza unei configurări eronate.

27. În sensul art. 12 alin. (5) lit. a) și lit. b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește registrele de nume TLD, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

27.1. un serviciu de rezolvare autoritară a numelor de domenii este complet indisponibil;

27.2. pentru o perioadă care depășește o oră, timpul mediu de răspuns al unui serviciu de rezolvare autoritară a numelor de domenii la cererile DNS este mai mare de 10 secunde;

27.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de funcționarea tehnică a TLD este compromisă.

28. În sensul art. 12 alin. (5) lit. a) și lit. b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de servicii de cloud computing, un incident cibernetic urmează a fi considerat ca având impact semnificativ și atunci când intervine una sau mai multe dintre următoarele condiții:

28.1. un serviciu de cloud computing furnizat este complet indisponibil timp de peste 30 de minute;

28.2. disponibilitatea unui serviciu de cloud computing al unui furnizor de servicii de cloud computing este limitată, în cazul a peste 5 % dintre utilizatorii serviciului de cloud computing, pentru o durată care depășește o oră;

28.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unui serviciu de cloud computing este compromisă ca urmare a unei acțiuni presupus ilegale;

28.4. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unui serviciu de cloud computing este compromisă, cu un impact asupra a peste 5 % dintre utilizatorii serviciului respectiv de cloud computing.

29. În sensul art. 12 alin. (5) lit. a) și lit. b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de servicii de centre de date, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

29.1. un serviciu de centru de date al unui centru de date operat de furnizor este complet indisponibil;

29.2. disponibilitatea unui serviciu de centru de date al unui centru de date operat de furnizor este limitată pentru o durată care depășește o oră;

29.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unui serviciu de centru de date este compromisă ca urmare a unei acțiuni presupus ilegale;

29.4. accesul fizic la un centru de date gestionat de furnizor este compromis.

30. În sensul art. 12 alin. (5) lit. a) și lit. b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de rețele de furnizare de conținut, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

30.1. o rețea de furnizare de conținut este complet indisponibilă timp de peste 30 de minute;

30.2. disponibilitatea unei rețele de furnizare de conținut este limitată în cazul a peste 5 % dintre utilizatorii rețelei de furnizare de conținut pentru o durată care depășește o oră;

30.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unei rețele de furnizare de conținut este compromisă ca urmare a unei acțiuni presupus ilegale;

30.4. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unei rețele de furnizare de conținut este compromisă, cu un impact asupra a peste 5 % dintre utilizatorii respectivei rețele de furnizare de conținut.

31. În sensul art. 12 alin. (5) lit. a) și lit. b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de servicii gestionate și furnizorii de servicii de securitate gestionate, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

31.1. un serviciu gestionat sau un serviciu de securitate gestionat este complet indisponibil timp de peste 30 de minute;

31.2. disponibilitatea unui serviciu gestionat sau a unui serviciu de securitate gestionat este limitată în cazul a peste 5 % dintre utilizatorii serviciului pentru o durată care depășește o oră;

31.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unui serviciu gestionat sau a unui serviciu de securitate gestionat este compromisă ca urmare a unei acțiuni presupus ilegale;

31.4. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unui serviciu gestionat sau a unui serviciu de securitate gestionat este compromisă, cu un impact asupra a peste 5 % dintre utilizatorii respectivului serviciu gestionat sau ai respectivului serviciu de securitate gestionat.

32. În sensul art. 12 alin. (5) lit. a) și lit. b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de piețe online, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

32.1. o piață online este complet indisponibilă pentru peste 5 % dintre utilizatorii unei piețe online din Republica Moldova;

32.2. peste 5 % dintre utilizatorii din Republica Moldova a unei piețe online, sunt afectați de disponibilitatea limitată a respectivei piețe online;

32.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unei piețe online este compromisă ca urmare a unei acțiuni presupus ilegale;

32.4. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unei piețe online este compromisă, cu un impact asupra a peste 5 % dintre utilizatorii din Republica Moldova a respectivei piețe online.

33. În sensul art. 12 alin. (5) lit. a) și lit. b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de motoare de căutare online, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

33.1. un motor de căutare online este complet indisponibil pentru peste 5 % dintre utilizatorii din Republica Moldova a respectivului motor de căutare online;

33.2. peste 5 % dintre utilizatorii din Republica Moldova a unui motor de căutare online sunt afectați de disponibilitatea limitată a respectivului motor de căutare online;

33.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unui motor de căutare online este compromisă ca urmare a unei acțiuni presupus ilegale;

33.4. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unui motor de căutare online este compromisă, cu un impact asupra a peste 5 % dintre utilizatorii din Republica Moldova a respectivului motor de căutare online.

34. În sensul art. 12 alin. (5) lit. a) și lit. b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de platforme de servicii de socializare în rețea, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

34.1. o platformă de servicii de socializare în rețea este complet indisponibilă pentru peste 5 % dintre utilizatorii din Republica Moldova a respectivei platforme de servicii de socializare în rețea;

34.2. peste 5 % dintre utilizatorii din Republica Moldova a unei platforme de servicii de socializare în rețea sunt afectați de disponibilitatea limitată a respectivei platforme de servicii de socializare în rețea;

34.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unei platforme de servicii de socializare în rețea este compromisă ca urmare a unei acțiuni presupus ilegale;

34.4. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unei platforme de servicii de socializare în rețea este compromisă, cu un impact asupra a peste 5 % dintre utilizatorii din Republica Moldova a respectivei platforme de servicii de socializare în rețea.

35. În sensul art. 12 alin. (5) lit. a) și lit. b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește prestatorii de servicii de încredere, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

35.1. un serviciu de încredere este complet indisponibil timp de peste 20 de minute;

35.2. un serviciu de încredere este indisponibil pentru utilizatori sau beneficiari timp de peste o oră, calcul efectuat pe baza unei săptămâni calendaristice;

35.3. peste 1 % dintre utilizatorii sau beneficiarii din Republica Moldova sunt afectați de disponibilitatea limitată a unui serviciu de încredere;

35.4. accesul fizic la o zonă în care sunt situate rețelele și sistemele informatice și la care accesul este limitat la personalul de încredere al prestatorului de servicii de încredere este compromis sau protecția unui astfel de acces fizic este compromisă;

35.5. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate legate de furnizarea unui serviciu de încredere este compromisă, cu un impact asupra a peste 0,1 % dintre utilizatorii sau beneficiarii serviciului de încredere.

Anexă
la Regulamentul cu privire la modul de aplicare de către furnizorii de servicii a măsurilor de securitate a rețelelor și sistemelor informatice, aprobat prin Hotărârea Guvernului nr. _____ din

Cerințe privind măsurile de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii în sectoarele critice

Capitolul 1. Politica privind securitatea rețelelor și a sistemelor informatice

1. Furnizorii de servicii aprobă o politică privind securitatea rețelelor și a sistemelor informatice care trebuie să corespundă următoarelor cerințe:

1.1. stabilește abordarea furnizorilor de servicii în ceea ce privește gestionarea securității rețelelor și sistemelor lor informatice;

1.2. este adecvată și complementară strategiei de afaceri și obiectivelor furnizorului de servicii;

1.3. stabilește obiective în materie de securitate a rețelelor și a informațiilor;

1.4. include un angajament de îmbunătățire continuă a securității rețelelor și a sistemelor informatice;

1.5. include un angajament de a furniza resursele adecvate necesare pentru punerea sa în aplicare, inclusiv personalul, resursele financiare, procesele, instrumentele și tehnologiile necesare;

1.6. este comunicată angajaților relevanți și părților externe interesate relevante care iau cunoștință de aceasta;

1.7. stabilește rolurile, responsabilitățile și atribuțiile în conformitate cu punctul 3;

1.8. enumeră documentația care trebuie păstrată și durata păstrării documentației;

1.9. enumeră politicile tematice specifice;

1.10. stabilește indicatori și măsuri de monitorizare a punerii sale în aplicare și a stadiului actual al nivelului de maturitate al furnizorului de servicii în materie de securitate a rețelelor și a informațiilor;

1.11. precizează data aprobării oficiale de către organele de conducere ale furnizorului de servicii.

2. Politica privind securitatea rețelelor și sistemelor informatice este revizuită și, dacă este adecvat, actualizată de către organele de conducere cel puțin anual și atunci când apar incidente cibernetice cu impact semnificativ sau modificări

semnificative ale operațiunilor sau ale riscurilor. Rezultatul revizuirilor se documentează.

3. În cadrul politicii lor privind securitatea rețelelor și a sistemelor informatice furnizorii de servicii:

3.1. stabilesc responsabilitățile și atribuțiile pentru securitatea rețelelor și a sistemelor informatice și le atribuie roluri, le alocă în funcție de nevoile sale și le comunică organelor de conducere;

3.2. solicită personalului și părților terțe să aplice securitatea rețelelor și a sistemelor informatice în conformitate cu politica stabilită privind securitatea rețelelor și a informațiilor și cu politicile și procedurile tematice specifice ale furnizorului de servicii;

3.3. asigură raportarea cel puțin a unei persoane direct organelor de conducere cu privire la aspecte legate de securitatea rețelelor și a sistemelor informatice;

3.4. asigură, în funcție de dimensiunea sa, acoperirea securității rețelelor și a sistemelor informatice cu roluri sau sarcini specifice îndeplinite în plus față de cele existente;

3.5. asigură separarea sarcinilor și domeniilor de competență care intră în conflict, dacă este aplicabil.

4. Rolurile, responsabilitățile și atribuțiile se revizuiesc și, dacă este adecvat, se actualizează de către organele de conducere la intervale stabilite și atunci când apar incidente semnificative sau modificări semnificative ale operațiunilor sau ale riscurilor.

Capitolul 2. Politica de gestionare a riscurilor la adresa securității rețelelor și sistemelor informatice

Secțiunea 1. Cadrul de gestionare a riscurilor

5. Furnizorii de servicii efectuează și documentează evaluări ale riscurilor și, pe baza rezultatelor, stabilesc, pun în aplicare și monitorizează un plan de tratare a riscurilor. Rezultatele evaluării riscurilor și riscurile reziduale se acceptă de organele de conducere sau, dacă este aplicabil, de persoanele responsabile și care au autoritatea de a gestiona riscurile, cu condiția ca furnizorii de servicii să asigure raportarea adecvată către organele de conducere.

6. Furnizorii de servicii stabilesc proceduri de identificare, analiză, evaluare și tratare a riscurilor („procesul de gestionare a riscurilor în materie de securitate cibernetică”). Procesul de gestionare a riscurilor în materie de securitate cibernetică este parte integrantă a procesului general de gestionare a riscurilor furnizorului de

servicii, dacă este aplicabil. Ca parte a procesului de gestionare a riscurilor în materie de securitate cibernetică, furnizorii de servicii:

6.1. urmează o metodologie de gestionare a riscurilor;

6.2. stabilesc nivelul de toleranță la risc în conformitate cu apetitul la risc al furnizorului de servicii;

6.3. stabilesc și mențin criterii de risc relevante;

6.4. în conformitate cu o abordare care ține seama de toate riscurile, identifică riscurile la adresa securității rețelelor și a sistemelor informatice, și le documentează, în special în ceea ce privește părțile terțe, și riscurile care ar putea conduce la perturbări ale disponibilității, integrității, autenticității și confidențialității rețelelor și sistemelor informatice, inclusiv identificarea punctului unic de defecțiuni;

6.5. analizează riscurile la adresa securității rețelelor și a sistemelor informatice, inclusiv amenințările, probabilitatea, impactul și nivelul de risc, luând în considerare informațiile privind amenințările cibernetice și vulnerabilitățile;

6.6. evaluează riscurile identificate pe baza criteriilor de risc;

6.7. identifică și prioritizează opțiunile și măsurile adecvate de tratare a riscurilor;

6.8. monitorizează în permanență punerea în aplicare a măsurilor de tratare a riscurilor;

6.9. identifică cine are responsabilitatea punerii în aplicare a măsurilor de tratare a riscurilor și momentul în care acestea ar trebui puse în aplicare;

6.10. documentează măsurile de tratare a riscurilor alese într-un plan de tratare a riscurilor și motivele care justifică acceptarea riscurilor reziduale într-un mod inteligibil.

7. Atunci când identifică și ierarhizează opțiunile și măsurile adecvate de tratare a riscurilor, furnizorii de servicii țin seama de rezultatele evaluării riscurilor, de rezultatele procedurii de evaluare a eficacității măsurilor de gestionare a riscurilor în materie de securitate cibernetică, de costul punerii în aplicare în raport cu beneficiul preconizat, de clasificarea activelor menționată la capitolul 12 secțiunea 1 și de analiza impactului asupra activității menționată la punctul 40.

8. Furnizorii de servicii examinează și, dacă este adecvat, actualizează rezultatele evaluării riscurilor și planul de tratare a riscurilor la intervale stabilite și cel puțin o dată pe an și atunci când apar modificări semnificative ale operațiunilor, ale riscurilor sau incidente cibernetice cu impact semnificativ.

Secțiunea 2. Monitorizarea conformității

9. Furnizorii de servicii examinează periodic conformitatea cu politicile lor privind securitatea rețelelor și sistemelor informatice, cu politicile, normele și

standardele tematice specifice. Organele de conducere sunt informate cu privire la situația securității rețelelor și a informațiilor pe baza evaluărilor conformității, prin intermediul unor rapoarte periodice.

10. Furnizorii de servicii instituie un sistem eficace de raportare a conformității, care trebuie să fie adecvat structurilor lor, mediilor de operare și situației amenințărilor. Sistemul de raportare a conformității trebuie să fie în măsură să ofere organelor de conducere o imagine în cunoștință de cauză a situației curente a gestionării riscurilor de către furnizorii de servicii.

11. Furnizorii de servicii efectuează monitorizarea conformității la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor sau ale riscurilor.

Secțiunea 3. Examinarea independentă a securității informațiilor și rețelelor

12. Furnizorii de servicii examinează în mod independent abordarea în ceea ce privește gestionarea securității rețelelor și a sistemelor informatice și punerea în aplicare a acesteia, inclusiv în ceea ce privește persoanele, procesele și tehnologiile.

13. Furnizorii de servicii elaborează și mențin procese de efectuare a unor examinări independente, care sunt efectuate de persoane care dețin certificări în domeniul auditului securității informațiilor.. În cazul în care examinarea independentă este efectuată de membri ai personalului furnizorului de servicii, persoanele care efectuează examinarea nu trebuie să fie în linia ierarhică a personalului din domeniul examinat. În cazul în care dimensiunea furnizorului de servicii nu permite o astfel de separare a liniei ierarhice, furnizorul de servicii instituie măsuri alternative pentru a garanta imparțialitatea examinărilor.

14. Rezultatele examinărilor independente, inclusiv rezultatele monitorizării conformității în temeiul secțiunii 2 și ale monitorizării și măsurării în conformitate cu capitolul 7, se raportează organelor de conducere. Furnizorul de servicii ia măsuri corective sau acceptă riscuri reziduale în conformitate cu criteriile de acceptare a riscurilor ale furnizorului de servicii.

15. Examinările independente se efectuează la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor sau ale riscurilor.

Capitolul 3. Gestionarea incidentelor

Secțiunea 1. Politica de gestionare a incidentelor

16. Furnizorii de servicii stabilesc și pun în aplicare o politică de gestionare a incidentelor cibernetice care stabilește rolurile, responsabilitățile și procedurile

pentru detectarea, analizarea, limitarea incidentelor sau răspunsul la incidente, redresarea în urma incidentelor, documentarea și raportarea în timp util a incidentelor. Politica respectivă trebuie să fie coerentă cu planul de asigurare a continuității activității și de recuperare în caz de dezastru menționat la capitolul 4 secțiunea 1.

17. Politica de gestionare a incidentelor cibernetice include:

17.1. un sistem de clasificare a incidentelor cibernetice care să fie în concordanță cu evaluarea și clasificarea evenimentelor, efectuate în temeiul punctului 28;

17.2. planuri de comunicare eficace, inclusiv pentru escaladare și raportare;

17.3. atribuirea rolurilor de detectare a incidentelor și de răspuns corespunzător în caz de incidente angajaților competenți;

17.4. documente care trebuie utilizate în cursul detectării incidentelor și al răspunsului la incidente, cum ar fi manuale de răspuns la incidente, grafice privind sesizarea nivelurilor competente, liste de contacte și modele.

18. Rolurile, responsabilitățile și procedurile stabilite în cadrul politicii sunt testate și revizuite și, dacă este adecvat, actualizate la intervale planificate și în urma unor incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor sau ale riscurilor.

Secțiunea 2. Monitorizare și jurnalizare

19. Furnizorii de servicii stabilesc proceduri și utilizează instrumente pentru monitorizarea și jurnalizarea activităților în rețelele și sistemele lor informatice pentru a detecta evenimentele care ar putea fi considerate incidente cibernetice și pentru a răspunde în consecință în vederea atenuării impactului.

20. În măsura în care este fezabil, monitorizarea trebuie să fie automată și să se efectueze fie în mod continuu, fie la intervale periodice, în funcție de capacitățile operaționale. Furnizorii de servicii își pun în aplicare activitățile de monitorizare într-un mod care să reducă la minimum rezultatele fals pozitive și fals negative.

21. Pe baza procedurilor menționate la punctul 19, furnizorii de servicii păstrează, documentează și revizuiesc jurnalele. Furnizorii de servicii întocmesc o listă a activelor care urmează să facă obiectul jurnalizării pe baza rezultatelor evaluării riscurilor efectuate potrivit secțiunii 1 a capitolului 2. Jurnalele includ dacă este adecvat:

21.1. traficul de rețea relevant la ieșire și la intrare;

21.2. crearea, modificarea sau eliminarea utilizatorilor rețelelor și sistemelor informatice ale furnizorului de servicii și extinderea permisiunilor;

21.3. accesul la sisteme și aplicații;

21.4. evenimente legate de autentificare;

21.5. toate accesurile privilegiate la sisteme și aplicații, precum și toate activitățile desfășurate de conturile administrative;

21.6. accesul sau modificările la fișierele configurației critice și la fișierele backup;

21.7. jurnale de evenimente și jurnale de la instrumente de securitate, cum ar fi antivirus, sisteme de detectare a intruziunilor sau firewall;

21.8. utilizarea resurselor sistemului, precum și performanța acestora;

21.9. accesul fizic la instalații;

21.10. accesul la echipamentele și dispozitivele lor de rețea și utilizarea acestora;

21.11. activarea, oprirea și întreruperea diferitelor jurnale;

21.12. evenimente de mediu.

22. Jurnalele sunt reexaminate periodic pentru a identifica orice tendință neobișnuită sau nedorită. Dacă este adecvat, furnizorii de servicii stabilesc valori corespunzătoare pentru pragurile de alarmă. În cazul în care valorile stabilite pentru pragul de alarmă sunt depășite, o alarmă urmează să se declanșeze, dacă este adecvat, în mod automat. Furnizorii de servicii se asigură că, în cazul declanșării unei alarme, se inițiază în timp util un răspuns calificat și adecvat.

23. Furnizorii de servicii păstrează jurnalele și realizează copii de rezervă ale acestora pentru o perioadă predefinită, dar nu mai mică de 6 luni, și le protejează împotriva accesului neautorizat sau a modificărilor neautorizate.

24. În măsura în care este fezabil, furnizorii de servicii se asigură că toate sistemele dispun de surse ale orei sincronizate pentru a putea corela jurnalele între sisteme pentru evaluarea evenimentelor. Furnizorii de servicii întocmesc și păstrează o listă a tuturor activelor jurnalizate și se asigură că sistemele de monitorizare și de jurnalizare sunt redundante. Disponibilitatea sistemelor de monitorizare și de jurnalizare este monitorizată independent de sistemele pe care le monitorizează.

25. Procedurile, precum și lista activelor jurnalizate sunt revizuite și, dacă este adecvat, actualizate la intervale regulate și după incidente cibernetice cu impact semnificativ.

Secțiunea 3. Raportarea evenimentelor

26. Furnizorii de servicii instituie un mecanism simplu care să le permită angajaților, furnizorilor și clienților lor să raporteze evenimentele suspecte.

27. Furnizorii de servicii comunică, dacă este adecvat, mecanismul de raportare a evenimentelor furnizorilor și clienților lor și își instruiesc periodic angajații cu privire la modul de utilizare a mecanismului.

Secțiunea 4. Evaluarea și clasificarea evenimentelor

28. Furnizorii de servicii evaluează evenimentele suspecte pentru a stabili dacă acestea constituie incidente și, în caz afirmativ, determină natura și gravitatea lor.

29. În sensul punctului 28, furnizorii de servicii acționează în modul următor:

29.1. efectuează evaluarea pe baza unor criterii predefinite, stabilite în prealabil, și a unei trieri pentru a stabili ordinea de prioritate a limitării și eradicării incidentelor;

29.2.evaluează trimestrial existența incidentelor recurente menționate la punctul 15 din Regulament;

29.3.examinează jurnalele corespunzătoare în scopul evaluării și clasificării evenimentelor;

29.4.instituie un proces de corelare și analiză a jurnalelor; și

29.5.reevaluează și reclasifică evenimentele în cazul în care devin disponibile noi informații sau după analizarea informațiilor disponibile anterior.

Secțiunea 5. Răspunsul la incidente

30. Furnizorii de servicii trebuie să răspundă la incidente în conformitate cu proceduri documentate și în timp util.

31. Procedurile de răspuns la incidente includ următoarele etape:

31.1. limitarea incidentului, pentru a preveni răspândirea consecințelor incidentului;

31.2. eradicarea, pentru a preveni continuarea sau reapariția incidentului;

31.3. redresarea în urma incidentului, dacă este necesar.

32. Furnizorii de servicii sunt obligați să stabilească planuri și proceduri de comunicare:

32.1. cu echipa de răspuns la incidentele cibernetice la nivel național a Agenției pentru Securitate Cibernetică în legătură cu notificarea incidentelor;

32.2. pentru comunicarea între membrii personalului furnizorului de servicii și pentru comunicarea cu părțile interesate relevante, externe furnizorului de servicii.

33. Furnizorii de servicii jurnalizează activitățile de răspuns la incidente în conformitate cu procedurile menționate la punctul 19 și înregistrează dovezile.

34. Furnizorii de servicii testează la intervale planificate procedurile lor de răspuns la incidente.

Secțiunea 6. Analizele post-incident

35. Dacă este adecvat, furnizorii de servicii efectuează analize post-incident după redresarea în urma incidentelor. Analizele post-incident identifică, atunci când este posibil, cauza principală a incidentului și au drept rezultat învățăminte documentate pentru a reduce apariția și consecințele incidentelor viitoare.

36. Furnizorii de servicii se asigură că analizele post-incident contribuie la îmbunătățirea abordării lor în ceea ce privește securitatea rețelelor și informațiilor, în ce privește măsurile de tratare a riscurilor și în ce privește procedurile de gestionare, detectare și răspuns la incidente.

37. Furnizorii de servicii trebuie să examineze la intervale planificate dacă incidentele au condus la analize post-incident.

Capitolul 4. Continuitatea activității și gestionarea crizelor

Secțiunea 1. Planul de continuitate a activității și de recuperare în caz de dezastru

38. Furnizorii de servicii stabilesc și mențin un plan de continuitate a activității și de recuperare în caz de dezastru care se aplică în caz de incidente cibernetice.

39. Operațiunile furnizorilor de servicii se restabilesc în conformitate cu planul de continuitate a activității și de recuperare în caz de dezastru. Planul se bazează pe rezultatele evaluării riscurilor și include, dacă este adecvat, următoarele:

39.1. scopul, domeniul de aplicare și publicul;

39.2. rolurile și responsabilitățile;

39.3. principalele contacte și canale de comunicare (interne și externe);

39.4. condițiile pentru activarea și dezactivarea planului;

39.5. ordinea de recuperare pentru operațiuni;

39.6. planuri de recuperare pentru operațiuni specifice, inclusiv obiective de recuperare;

39.7. resursele necesare, inclusiv copii de rezervă și redundanțe;

39.8. restabilirea și reluarea activităților în baza măsurilor temporare.

40. Furnizorii de servicii efectuează o analiză a impactului asupra activității pentru a evalua impactul potențial al perturbărilor grave asupra operațiunilor lor și, pe baza rezultatelor analizei impactului asupra activității, stabilesc cerințe de continuitate pentru rețelele și sistemele informatice.

41. Planul de continuitate a activității și planul de recuperare în caz de dezastru sunt testate și revizuite și, dacă este adecvat, actualizate la intervale planificate și în urma incidentelor cibernetice cu impact semnificativ sau a modificărilor semnificative ale operațiunilor sau ale riscurilor. Furnizorii de servicii se asigură că planurile includ învățămintele desprinse în urma unor astfel de teste.

Secțiunea 2. Gestionarea copiilor de rezervă și a redundanței

42. Furnizorii de servicii păstrează copii de rezervă ale datelor și furnizează suficiente resurse disponibile, inclusiv instalații, rețele și sisteme informatice și personal, pentru a asigura un nivel adecvat de redundanță.

43. Pe baza rezultatelor evaluării riscurilor și a planului de continuitate a activității, furnizorii de servicii stabilesc planuri de rezervă care includ următoarele:

43.1. timpii de recuperare;

43.2. asigurare privind caracterul complet și exactitudinea copiilor de rezervă, inclusiv a datelor de configurare și a datelor stocate în mediul serviciilor de cloud computing;

43.3. stocarea de copii de rezervă (online sau offline) într-un loc sau în locuri sigure, care nu se află în aceeași rețea cu sistemul și care se află la o distanță suficientă pentru a scăpa de orice daune cauzate de un dezastru la locul principal;

43.4. controale adecvate ale accesului fizic și logic la copiile de rezervă, în conformitate cu nivelul de clasificare a activelor;

43.5. restabilirea datelor din copiile de rezervă;

43.6. perioade de păstrare bazate pe cerințe comerciale și normative.

44. Furnizorii de servicii efectuează verificări periodice ale integrității copiilor de rezervă.

45. Pe baza rezultatelor evaluării riscurilor și a planului de continuitate a activității, furnizorii de servicii asigură disponibilitatea suficientă a resurselor prin redundanța, cel puțin parțială, a următoarelor:

45.1. rețele și sisteme informatice;

45.2. active, inclusiv instalații, echipamente și materiale;

45.3.personal care are responsabilitatea, atribuții și competența necesară;

45.4. canale de comunicare adecvate.

46. Dacă este adecvat, entitățile relevante se asigură că monitorizarea și ajustarea resurselor, inclusiv a instalațiilor, a sistemelor și a personalului, se întemeiază în mod corespunzător pe cerințele privind copiile de rezervă și redundanța.

47. Furnizorii de servicii testează periodic recuperarea copiilor de rezervă și a redundanțelor pentru a se asigura că, în condiții de recuperare, se pot baza pe acestea și că acoperă copiile, procesele și cunoștințele pentru realizarea unei recuperări efective. Furnizorii de servicii documentează rezultatele testelor și, dacă este necesar, iau măsuri corective.

Secțiunea 3. Gestionarea crizelor

48. Furnizorii de servicii instituie un proces de gestionare a crizelor.

49. Furnizorii de servicii se asigură că procesul de gestionare a crizelor abordează cel puțin următoarele elemente:

49.1. rolurile și responsabilitățile personalului și, dacă este adecvat, ale furnizorilor și ale prestatorilor de servicii, specificând alocarea rolurilor în situații de criză, inclusiv etapele specifice care trebuie urmate;

49.2. mijloace de comunicare adecvate între furnizorul de servicii și autoritățile competente relevante;

49.3. aplicarea unor măsuri adecvate pentru a asigura menținerea securității rețelelor și a sistemelor informatice în situații de criză.

50. În sensul subpunctului 49.2, fluxul de informații dintre furnizorul de servicii și autoritățile competente relevante include atât comunicările obligatorii, cum ar fi rapoartele privind incidentele și termenele aferente, cât și comunicările neobligatorii.

51. Furnizorii de servicii instituie un proces de gestionare și de utilizare a informațiilor primite de la Agenția pentru Securitate Cibernetică cu privire la incidente, vulnerabilități, amenințări sau posibile măsuri de atenuare.

52. Furnizorii de servicii testează, revizuiesc și, dacă este adecvat, actualizează planul de gestionare a crizelor în mod regulat sau în urma unor incidente cibernetice cu impact semnificativ sau a unor modificări semnificative ale operațiunilor sau riscurilor.

Capitolul 5. Securitatea lanțului de aprovizionare

53. Furnizorii de servicii instituie, implementează și aplică o politică de securitate a lanțului de aprovizionare care reglementează relațiile cu furnizorii și prestatorii lor de servicii direcți pentru a atenua riscurile identificate la adresa securității rețelelor și a sistemelor informatice. În cadrul politicii de securitate a lanțului de aprovizionare, furnizorii de servicii identifică rolul lor în lanțul de aprovizionare și îl comunică furnizorilor și prestatorilor lor de servicii direcți.

54. Ca parte a politicii de securitate a lanțului de aprovizionare menționată la punctul 53, furnizorii de servicii stabilesc criterii pentru selectarea și contractarea furnizorilor și a prestatorilor de servicii. Aceste criterii includ următoarele:

54.1. practicile în materie de securitate cibernetică ale furnizorilor și ale prestatorilor de servicii, inclusiv procedurile lor securizate de dezvoltare;

54.2. capacitatea furnizorilor și a prestatorilor de servicii de a respecta specificațiile în materie de securitate cibernetică stabilite de furnizorul de servicii;

54.3. calitatea și reziliența generală a produselor TIC (tehnologie a informației și comunicațiilor) și a serviciilor TIC și măsurile de gestionare a riscurilor în materie de securitate cibernetică încorporate în acestea, inclusiv riscurile și nivelul de clasificare a produselor TIC și a serviciilor TIC;

54.4. capacitatea furnizorului de servicii de a diversifica sursele de aprovizionare și de a limita dependența de furnizor, dacă este aplicabil.

55. Pe baza politicii de securitate a lanțului de aprovizionare și ținând seama de rezultatele evaluării riscurilor, furnizorii de servicii se asigură că contractele lor cu furnizorii și prestatorii de servicii specifică, dacă este adecvat, prin acorduri privind nivelul serviciilor următoarele :

55.1. cerințele în materie de securitate cibernetică pentru furnizori sau prestatorii de servicii, inclusiv cerințele în ceea ce privește securitatea achiziționării de servicii TIC sau de produse TIC prevăzute la capitolul 6 secțiunea 1;

55.2. cerințele privind sensibilizarea, competențele și formarea și, dacă este adecvat, certificările impuse angajaților furnizorilor sau ai prestatorilor de servicii;

55.3. cerințele privind verificarea antecedentelor angajaților furnizorilor și ai prestatorilor de servicii;

55.4. obligația furnizorilor și a prestatorilor de servicii de a notifica, fără întârzieri nejustificate, furnizorilor de servicii incidentele care prezintă un risc pentru securitatea rețelelor și a sistemelor informatice ale acestora;

55.5. dreptul de a efectua audituri sau dreptul de a primi rapoarte de audit;

55.6. obligația furnizorilor și a prestatorilor de servicii de a gestiona vulnerabilitățile care prezintă un risc pentru securitatea rețelelor și a sistemelor informatice ale entităților respective;

55.7. cerințe privind subcontractarea și, în cazul în care furnizorul de servicii permite subcontractarea, cerințe în materie de securitate cibernetică pentru subcontractanți în conformitate cu cerințele în materie de securitate cibernetică menționate la subpunctul 55.1.;

55.8. obligațiile furnizorilor și ale prestatorilor de servicii la rezilierea contractului, cum ar fi extragerea și distrugerea informațiilor obținute de către furnizori și prestatorii de servicii în exercitarea sarcinilor lor.

56. Furnizorii de servicii iau în considerare elementele menționate la punctul 54 ca parte a procesului de selecție a noilor furnizori și prestatori de servicii, precum și ca parte a procesului de achiziții publice menționat la capitolul 6 secțiunea 1.

57. Furnizorii de servicii trebuie să-și revizuiască politica de securitate a lanțului de aprovizionare și să monitorizeze, să evalueze și, dacă este necesar, să acționeze ca urmare a modificărilor aduse practicilor în materie de securitate cibernetică ale furnizorilor și ale prestatorilor de servicii, la intervale planificate și atunci când au loc modificări semnificative ale operațiunilor sau ale riscurilor ori incidente cibernetice cu impact semnificativ legate de furnizarea de servicii TIC sau care au un impact asupra securității produselor TIC de la furnizori și prestatorii de servicii.

58. În sensul punctului 57, furnizorii de servicii:

58.1. monitorizează periodic rapoartele privind punerea în aplicare a acordurilor privind nivelul serviciilor, dacă este aplicabil;

58.2.examinează incidentele legate de produsele TIC și de serviciile TIC de la furnizori și prestatori de servicii;

58.3. evaluează necesitatea unor examinări neprogramate și documentează constatările într-un mod inteligibil;

58.4. analizează riscurile prezentate de modificările legate de produsele TIC și de serviciile TIC de la furnizori și prestatori de servicii și, dacă este adecvat, iau măsuri de atenuare în timp util.

59. Furnizorii de servicii mențin și actualizează un registru al furnizorilor lor și al prestatorilor lor de servicii direcți, care include:

59.1. puncte de contact pentru fiecare furnizor și prestator de servicii direct;

59.2. o listă a produselor TIC, a serviciilor TIC și a proceselor TIC livrate furnizorului de servicii de către furnizorul sau de prestatorul de servicii direct.

Capitolul 6. Securitatea în achiziționarea, dezvoltarea și întreținerea rețelelor și a sistemelor informatice

Secțiunea 1. Securitatea în achiziționarea de servicii TIC sau de produse TIC

60. Furnizorii de servicii stabilesc și pun în aplicare, pe baza evaluării riscurilor efectuată potrivit capitolului 2, procese de gestionare a riscurilor care decurg din achiziționarea de servicii TIC sau de produse TIC de la furnizori sau prestatori de servicii pentru componente care sunt critice pentru securitatea rețelelor și a sistemelor informatice ale furnizorului de servicii pe parcursul întregului lor ciclu de viață.

61. Procesele menționate la punctul 60 trebuie să includă:

61.1. cerințe de securitate aplicabile serviciilor TIC sau produselor TIC care urmează să fie achiziționate;

61.2. cerințe privind actualizările de securitate pe întreaga durată de viață a serviciilor TIC sau a produselor TIC sau înlocuirea după încheierea perioadei de asistență;

61.3. informații care descriu componentele hardware și software utilizate în serviciile TIC sau în produsele TIC;

61.4. informații care descriu funcțiile de securitate cibernetică puse în aplicare ale serviciilor TIC sau ale produselor TIC și configurația necesară pentru funcționarea lor în condiții de siguranță;

61.5. asigurarea faptului că serviciile TIC sau produsele TIC respectă cerințele de securitate în conformitate cu subpunctul 61.1.;

61.6. metode de validare a conformității serviciilor TIC sau a produselor TIC livrate cu cerințele de securitate declarate, precum și documentarea rezultatelor validării.

62. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează procesele la intervale planificate și atunci când apar incidente semnificative.

Secțiunea 2. Ciclul de viață al dezvoltării securizate

63. Înainte de a dezvolta o rețea și un sistem informatic, inclusiv un software, furnizorii de servicii stabilesc norme pentru dezvoltarea securizată de rețele și sisteme informatice și le aplică atunci când dezvoltă rețele și sisteme informatice la nivel intern sau atunci când externalizează dezvoltarea rețelelor și a sistemelor informatice. Normele acoperă toate etapele dezvoltării, inclusiv specificațiile, proiectarea, dezvoltarea, punerea în aplicare și testarea.

64. În sensul punctului 63, furnizorii de servicii:

64.1. efectuează o analiză a cerințelor de securitate în etapele referitoare la specificațiile și proiectarea oricărui proiect de dezvoltare sau de achiziție întreprins de furnizorul de servicii sau în numele acestuia;

64.2. aplică principii de creare de sisteme securizate și principii de programare securizată oricărei activități de dezvoltare de sisteme informatice, cum ar fi promovarea securității cibernetice din faza de proiectare, a arhitecturilor de tip „încredere zero”;

64.3. stabilesc cerințe de securitate privind mediile de dezvoltare;

64.4. instituie și pun în aplicare procese de testare a securității în ciclul de viață al dezvoltării;

64.5. selectează, protejează și gestionează în mod corespunzător datele privind testele de securitate;

64.6. sanitizează și anonimizează datele privind testele în conformitate cu evaluarea riscurilor.

65. În cazul în care dezvoltarea rețelelor și a sistemelor informatice este externalizată, furnizorul de servicii aplică și politicile și procedurile menționate la capitolul 5 și secțiunea 1 din prezentul capitol.

66. Furnizorii de servicii își revizuiesc și, dacă este necesar, își actualizează normele de dezvoltare securizată la intervale planificate.

Secțiunea 3. Gestionarea configurației

67. Furnizorii de servicii iau măsurile adecvate pentru a stabili, a documenta, a pune în aplicare și a monitoriza configurațiile, inclusiv configurațiile de securitate ale hardware-ului, software-ului, serviciilor și rețelelor.

68. În acest scop, furnizorii de servicii:

68.1. stabilesc și asigură securitatea configurațiilor pentru hardware, software, servicii și rețele;

68.2. stabilesc și pun în aplicare procese și instrumente pentru a asigura respectarea configurațiilor securizate stabilite pentru hardware, software, servicii și rețele, pentru sistemele nou instalate, precum și pentru sistemele aflate în funcțiune pe durata lor de viață.

69. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează configurațiile la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor sau ale riscurilor.

Secțiunea 4. Gestionarea schimbărilor, reparații și întreținere

70. Furnizorii de servicii aplică proceduri de gestionare a schimbărilor pentru a controla modificările aduse rețelelor și sistemelor informatice. Dacă este aplicabil, procedurile trebuie să fie în concordanță cu politicile generale privind gestionarea schimbărilor ale furnizorului de servicii.

71. Procedurile de gestionare a schimbărilor se aplică noilor versiuni, modificărilor și modificărilor de urgență ale oricărui software și hardware în exploatare și modificărilor configurației. Procedurile respective asigură faptul că modificările respective sunt documentate și, pe baza evaluării riscurilor, sunt testate și evaluate având în vedere impactul potențial înainte de a fi puse în aplicare.

72. În cazul în care procedurile obișnuite de gestionare a schimbărilor nu au putut fi urmate din cauza unei urgențe, furnizorul de servicii documentează rezultatul modificării și explicația motivului pentru care procedurile nu au putut fi urmate.

73. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează procedurile la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor sau ale riscurilor.

Secțiunea 5. Teste de securitate

74. Furnizorii de servicii stabilesc, implementează și aplică o politică și proceduri pentru testele de securitate.

75. Furnizorii de servicii:

75.1. stabilesc, pe baza evaluării riscurilor, necesitatea, sfera, frecvența și tipul testelor de securitate;

75.2. efectuează teste de securitate în conformitate cu o metodologie de testare documentată, care acoperă componentele identificate în cadrul unei analize a riscurilor ca fiind relevante pentru operarea în condiții de siguranță;

75.3. documentează tipul, sfera, ora și rezultatele testelor, inclusiv evaluarea criticalității și acțiunile de atenuare pentru fiecare constatare;

75.4. aplică măsuri de atenuare în cazul constatărilor critice.

76. Furnizorii de servicii își revizuiesc și, dacă este adecvat, își actualizează politicile privind testele de securitate la intervale planificate.

Secțiunea 6. Gestionarea corecțiilor de securitate

77. Furnizorii de servicii specifică și aplică proceduri coerente cu procedurile de gestionare a modificărilor, precum și cu gestionarea vulnerabilităților, gestionarea riscurilor și cu alte proceduri de gestionare relevante, pentru a se asigura că:

77.1. corecțiile de securitate se aplică într-un termen rezonabil de la data la care devin disponibile;

77.2. corecțiile de securitate se testează înainte de a fi aplicate în sistemele de producție;

77.3. corecțiile de securitate provin din surse de încredere și sunt verificate din punctul de vedere al integrității;

77.4. în cazurile în care o corecție nu este disponibilă sau nu se aplică în temeiul punctului 78, se pun în aplicare măsuri suplimentare și se acceptă riscuri reziduale.

78. Furnizorii de servicii pot alege să nu aplice corecții de securitate atunci când dezavantajele aplicării corecțiilor de securitate sunt mai mari decât beneficiile în materie de securitate cibernetică. Furnizorii de servicii documentează și justifică în mod corespunzător motivele unei astfel de decizii.

Secțiunea 7. Securitatea rețelelor

79. Furnizorii de servicii iau măsurile adecvate pentru a-și proteja rețelele și sistemele informatice împotriva amenințărilor cibernetice.

80. În acest sens, furnizorii de servicii:

80.1. documentează arhitectura rețelei într-un mod inteligibil și actualizat;

80.2. stabilesc și aplică controale pentru a-și proteja domeniile rețelei interne împotriva accesului neautorizat;

80.3. configurează controale pentru a preveni accesul și comunicarea în rețea care nu sunt necesare pentru funcționarea furnizorului de servicii;

80.4. stabilesc și aplică controale pentru accesul de la distanță la rețele și la sistemele informatice, inclusiv accesul prestatorilor de servicii;

80.5. nu utilizează în alte scopuri sistemele folosite pentru administrarea punerii în aplicare a politicii de securitate;

80.6. interzic sau dezactivează în mod explicit conexiunile și serviciile care nu sunt necesare;

80.7. dacă este adecvat, permit exclusiv accesul la rețelele și sistemele sale informatice prin intermediul unor dispozitive autorizate de furnizorul de servicii;

80.8. permit conectarea prestatorilor de servicii numai după o cerere de autorizare și pentru o perioadă stabilită, cum ar fi durata unei operațiuni de întreținere;

80.9. stabilesc comunicarea între sisteme distincte numai prin canale de încredere care sunt izolate prin separare logică, criptografică sau fizică de alte canale de comunicare și garantează identificarea punctelor lor finale și protecția datelor canalului împotriva modificării sau divulgării;

80.10. adoptă un plan de punere în aplicare pentru tranziția completă către protocoale de comunicare la nivel de rețea de ultimă generație într-un mod sigur, adecvat și treptat și stabilesc măsuri de accelerare a acestei tranziții;

80.11. adoptă un plan de punere în aplicare pentru implementarea unor standarde moderne de comunicații prin e-mail convenite la nivel internațional și interoperabile pentru a securiza comunicațiile prin e-mail în vederea atenuării vulnerabilităților legate de amenințările privind e-mailuri și stabilesc măsuri pentru accelerarea unei astfel de implementări;

80.12. aplică cele mai bune practici pentru securitatea DNS și pentru securitatea rutării pe internet și pentru igiena rutării traficului care provine din rețea și care este destinat acesteia.

81. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează aceste măsuri la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor sau ale riscurilor.

Secțiunea 8. Segmentarea rețelei

82. Furnizorii de servicii segmentează sistemele în rețele sau zone în conformitate cu rezultatele evaluării riscurilor. Furnizorii de servicii își segmentează sistemele și rețelele de sistemele și rețelele terților.

83. În acest scop, furnizorii de servicii:

83.1. iau în considerare relația funcțională, logică și fizică, inclusiv localizarea, dintre sisteme și servicii fiabile;

83.2. acordă acces la o rețea sau la o zonă pe baza unei evaluări a cerințelor sale de securitate;

83.3. păstrează sistemele care sunt critice pentru funcționarea furnizorului de servicii sau pentru siguranță în zone securizate;

83.4. instalează o zonă demilitarizată în cadrul rețelelor lor de comunicare pentru a asigura o comunicare securizată care provine de la rețelele lor sau este destinată acestora;

83.5. restricționează accesul și comunicațiile dintre zone și în interiorul acestora la cele necesare pentru funcționarea furnizorului de servicii sau pentru siguranță;

83.6. separă rețeaua dedicată administrării rețelelor și sistemelor informatice de rețeaua operațională a furnizorului de servicii;

83.7. separă canalele de administrare a rețelei de alte tipuri de trafic de rețea;

83.8. separă sistemele de producție pentru serviciile furnizorului de servicii de sistemele utilizate pentru dezvoltare și testare, inclusiv copii de rezervă.

84. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează segmentarea rețelei la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor sau ale riscurilor.

Secțiunea 9. Protecția împotriva software-ului rău-intenționat și neautorizat

85. Furnizorii de servicii își protejează rețelele și sistemele informatice împotriva software-ului rău-intenționat și neautorizat.

86. În acest scop, furnizorii de servicii pun în aplicare, în special, măsuri de detectare sau de prevenire a utilizării programelor informatice rău-intenționate sau neautorizate. Furnizorii de servicii se asigură, dacă este adecvat, că rețelele și sistemele lor informatice sunt echipate cu software de detectare și răspuns, care este actualizat periodic în conformitate cu evaluarea riscurilor și cu acordurile contractuale cu furnizorii.

Secțiunea 10. Gestionarea și divulgarea vulnerabilităților

87. Furnizorii de servicii obțin informații cu privire la vulnerabilitățile tehnice din rețelele și sistemele lor informatice, evaluează expunerea lor la astfel de vulnerabilități și iau măsurile adecvate pentru gestionarea vulnerabilităților.

88. În acest sens, furnizorii de servicii:

88.1. monitorizează informațiile privind vulnerabilitățile prin canale adecvate, cum ar fi anunțurile echipelor de răspuns la incidente cibernetice, inclusiv a echipei de răspuns la incidente cibernetice la nivel național a Agenției pentru Securitate Cibernetică, ale altor autorități competente sau informațiile furnizate de furnizori sau de prestatorii de servicii;

88.2. efectuează, dacă este adecvat**,** scanări ale vulnerabilității și consemnează rezultatele scanărilor, la intervale planificate;

88.3. abordează, fără întârzieri nejustificate, vulnerabilitățile identificate ca fiind critice pentru operațiunile sale;

88.4. se asigură că gestionarea vulnerabilităților este compatibilă cu procedurile lor de gestionare a modificărilor, de gestionare a corecțiilor de securitate, de gestionare a riscurilor și de gestionare a incidentelor;

88.5. stabilesc o procedură pentru divulgarea vulnerabilităților în conformitate cu politica națională coordonată aplicabilă în materie de divulgare a vulnerabilităților.

89. Atunci când acest lucru este justificat de impactul potențial al vulnerabilității, furnizorii de servicii creează și pun în aplicare un plan de atenuare a

vulnerabilității. În alte cazuri, furnizorii de servicii documentează și justifică motivul pentru care vulnerabilitatea nu necesită remediere.

90. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează la intervale planificate canalele pe care le utilizează pentru monitorizarea informațiilor privind vulnerabilitatea.

Capitolul 7. Politici și proceduri pentru a evalua eficacitatea măsurilor de gestionare a riscurilor în materie de securitate cibernetică

91. Furnizorii de servicii stabilesc, implementează și aplică o politică și proceduri pentru a evalua dacă măsurile de gestionare a riscurilor în materie de securitate cibernetică luate sunt puse în aplicare și menținute în mod eficace.

92. Politica și procedurile menționate la punctul 91 trebuie să țină cont de rezultatele evaluării riscurilor și de incidentele cibernetice cu impact semnificativ din trecut. Furnizorii de servicii stabilesc:

92.1. măsurile de gestionare a riscurilor în materie de securitate cibernetică ce urmează să fie monitorizate și măsurate, inclusiv procese și controale;

92.2. metodele pentru monitorizare, măsurare, analiză și evaluare, dacă acest lucru se aplică, pentru a se asigura rezultate valide;

92.3. momentul în care trebuie efectuate monitorizarea și măsurarea;

92.4. persoana/entitatea responsabilă de monitorizarea și măsurarea eficacității măsurilor de gestionare a riscurilor în materie de securitate cibernetică;

92.5. momentul în care trebuie analizate și evaluate rezultatele monitorizării și măsurării;

92.6. persoana/entitatea responsabilă de analiza și evaluarea acestor rezultate.

93. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează politicile și procedurile la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor sau ale riscurilor.

Capitolul 8. Practici de bază în materie de igienă cibernetică și formare în domeniul securității cibernetice

Secțiunea 1. Sensibilizare și practici de bază în materie de igienă cibernetică

94. Furnizorii de servicii se asigură că angajații lor, inclusiv membrii organelor de conducere, precum și furnizorii și prestatorii de servicii direcți sunt sensibilizați cu privire la riscuri, sunt informați cu privire la importanța securității cibernetice și aplică practici de igienă cibernetică.

95. În acest scop, furnizorii de servicii oferă angajaților lor, inclusiv membrilor organelor de conducere, precum și furnizorilor și prestatorilor de servicii direcți, dacă este adecvat, un program de sensibilizare, care:

95.1. este programat în timp, astfel încât activitățile să fie repetate și să acopere noii angajați;

95.2. este stabilit în conformitate cu politica de securitate a rețelelor și a informațiilor, cu politicile tematice specifice și cu procedurile relevante privind securitatea rețelelor și a informațiilor;

95.3. acoperă amenințările cibernetice relevante, măsurile existente de gestionare a riscurilor în materie de securitate cibernetică, punctele de contact și resursele pentru obținerea de informații și consiliere suplimentare cu privire la aspectele legate de securitatea cibernetică, precum și practicile de igienă cibernetică pentru utilizatori.

96. Dacă este adecvat, programul de sensibilizare este testat din punctul de vedere al eficacității. Programul de sensibilizare este actualizat și oferit la intervale planificate, ținând seama de modificările practicilor de igienă cibernetică, precum și de situația actuală a amenințărilor și de riscurile pentru furnizorul de servicii.

Secțiunea 2. Formare în domeniul securității

97. Furnizorii de servicii identifică angajații ale căror roluri necesită seturi de competențe și expertiză relevante în materie de securitate și se asigură că aceștia beneficiază de formare periodică privind securitatea rețelelor și a sistemelor informatice.

98. Furnizorii de servicii stabilesc, implementează și aplică un program de formare în conformitate cu politica de securitate a rețelelor și a informațiilor, cu politicile tematice specifice și cu alte proceduri relevante privind securitatea rețelelor și a informațiilor, care stabilește nevoile de formare pentru anumite roluri și funcții pe baza unor criterii.

99. Formarea trebuie să fie relevantă pentru funcția postului angajatului, iar eficacitatea sa trebuie evaluată. Formarea ia în considerare măsurile de securitate instituite și acoperă următoarele aspecte:

99.1. instrucțiuni privind configurarea și funcționarea în condiții de siguranță a rețelei și a sistemelor informatice, inclusiv a dispozitivelor mobile;

99.2. informare cu privire la amenințările cibernetice cunoscute;

99.3. formare cu privire la comportamentul care trebuie adoptat atunci când au loc evenimente relevante pentru securitate.

100. Furnizorii de servicii aplică cursuri de formare membrilor personalului care se transferă în posturi sau roluri noi care necesită seturi de competențe și expertiză relevante în materie de securitate.

101. Programul se actualizează și se desfășoară periodic, ținând seama de politicile și normele aplicabile, de rolurile și responsabilitățile atribuite, precum și de amenințările cibernetice cunoscute și de evoluțiile tehnologice.

Capitolul 9. Criptografie

102. Furnizorii de servicii stabilesc, implementează și aplică o politică și proceduri legate de criptografie, cu scopul de a asigura utilizarea adecvată și eficace a criptografiei pentru a proteja confidențialitatea, autenticitatea și integritatea datelor în conformitate cu clasificarea activelor furnizorului de servicii și cu rezultatele evaluării riscurilor efectuate în conformitate cu prezentele cerințe.

103. Politica și procedurile cu privire la criptografie urmează să stabilească:

103.1. tipul, puterea și calitatea măsurilor criptografice necesare pentru a proteja activele furnizorului de servicii, inclusiv datele în repaus și datele în tranzit;

103.2. pe baza subpct.103.1, protocoalele sau familiile de protocoale de adoptat, precum și algoritmii criptografici, puterea de criptare, soluțiile criptografice și practicile de utilizare care urmează să fie aprobate și care sunt necesare pentru a fi utilizate în cadrul furnizorului de servicii, urmând, dacă este adecvat, o abordare bazată pe agilitate criptografică;

103.3. abordarea furnizorului de servicii în ceea ce privește gestionarea cheilor, inclusiv, dacă este adecvat, metodele pentru:

103.3.1. generarea de chei diferite pentru sistemele și aplicațiile criptografice;

103.3.2. emiterea și obținerea de certificate de cheie publică;

103.3.3. distribuirea cheilor către entitățile vizate, inclusiv modul de activare a cheilor atunci când sunt primite;

103.3.4. stocarea cheilor, inclusiv modul în care utilizatorii autorizați obțin acces la chei;

103.3.5. modificarea sau actualizarea cheilor, inclusiv norme privind momentul și modul de modificare a cheilor;

103.3.6. gestionarea cheilor compromise;

103.3.7. revocarea cheilor, inclusiv modul de retragere sau dezactivare a cheilor;

103.3.8. recuperarea cheilor pierdute sau corupte;

103.3.9. crearea de copii de rezervă sau arhivarea cheilor;

103.3.10. distrugerea cheilor;

103.3.11. jurnalizarea și auditarea activităților legate de gestionarea cheilor;

103.3.12. stabilirea datelor de activare și dezactivare a cheilor, astfel încât cheile să poată fi utilizate numai pentru perioada de timp specificată, în conformitate cu normele organizației privind gestionarea cheilor.

104. Furnizorii de servicii revizuiesc și, dacă este adecvat, își actualizează politicile și procedurile la intervale planificate, ținând seama de stadiul de dezvoltare al criptografiei.

Capitolul 10. Securitatea resurselor umane

Secțiunea 1. Securitatea resurselor umane

105. Furnizorii de servicii se asigură că angajații lor și furnizorii și prestatorii lor de servicii direcți, dacă este aplicabil, înțeleg și își asumă responsabilitățile în materie de securitate, astfel cum este adecvat pentru serviciile oferite și postul ocupat și în conformitate cu politica furnizorului de servicii privind securitatea rețelelor și a sistemelor informatice.

106. Cerința menționată la punctul 105 include:

106.1. mecanisme prin care să se asigure că toți angajații, furnizorii și prestatorii de servicii direcți, dacă acest lucru este aplicabil, înțeleg și urmează practicile standard de igienă cibernetică pe care furnizorul de servicii le aplică în conformitate cu capitolul 8 secțiunea 1;

106.2. mecanisme prin care să se asigure că toți utilizatorii cu acces administrativ sau privilegiat cunosc și acționează în conformitate cu rolurile, responsabilitățile și atribuțiile lor;

106.3. mecanisme prin care să se asigure că membrii organelor de conducere înțeleg și acționează în conformitate cu rolul, responsabilitățile și atribuțiile lor în ceea ce privește securitatea rețelelor și a sistemelor informatice;

106.4. mecanisme de angajare a personalului calificat pentru rolurile respective, cum ar fi verificările referințelor, proceduri de verificare, validarea certificărilor sau teste scrise.

107. Furnizorii de servicii revizuiesc alocarea personalului în roluri specifice, astfel cum este descris în politica privind securitatea rețelelor și sistemelor informatice, precum și gradul de mobilizare al resurselor umane în această privință, la intervale planificate și cel puțin o dată pe an. Furnizorii de servicii actualizează alocarea dacă este necesar.

Secțiunea 2. Verificarea antecedentelor

108. Furnizorii de servicii se asigură că se efectuează, în măsura în care este fezabil, verificări ale antecedentelor angajaților lor și, dacă este aplicabil, ale furnizorilor și prestatorilor lor de servicii direcți, în conformitate cu punctul 21, în cazul în care este necesar pentru rolul, responsabilitățile și autorizările lor.

109. În sensul punctului 108, furnizorii de servicii:

109.1. instituie criterii care stabilesc rolurile, responsabilitățile și atribuțiile care sunt exercitate numai de către persoane cărora le-au fost verificate antecedentele;

109.2. se asigură că verificările se efectuează pentru aceste persoane înainte ca ele să înceapă să exercite aceste roluri, responsabilități și atribuții, care țin seama de actele cu putere de lege, normele administrative și etica aplicabile în raport cu cerințele comerciale, clasificarea activelor menționată în capitolul 12 secțiunea 1 și rețelele și sistemele informatice care urmează să fie accesate, precum și cu riscurile percepute.

110. Furnizorii de servicii trebuie să revizuiască și, dacă este adecvat, actualizează politica la intervale planificate și o actualizează dacă este necesar.

Secțiunea 3. Procedura în caz de încetare sau modificare a raporturilor de muncă

111. Furnizorii de servicii se asigură că responsabilitățile și sarcinile în materie de securitate a rețelelor și a sistemelor informatice care rămân valabile după încetarea sau după modificarea raportului de muncă al angajaților lor sunt definite și puse în aplicare prin contract.

112. În sensul punctului 111, furnizorii de servicii trebuie să includă în termenii și condițiile de muncă, în contractul sau în acordul persoanei în cauză responsabilitățile și sarcinile care sunt încă valabile după încetarea raportului de muncă sau a contractului, cum ar fi clauzele de confidențialitate.

Secțiunea 4. Procesul disciplinar

113. Furnizorii de servicii instituie, comunică și mențin un proces disciplinar pentru gestionarea încălcărilor politicilor de securitate a rețelelor și a sistemelor informatice. Procesul ține seama de cerințele juridice, statutare, contractuale și comerciale relevante.

114. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează procesul disciplinar la intervale planificate și atunci când este necesar ca urmare a unor schimbări legislative sau a unor modificări semnificative ale operațiunilor sau ale riscurilor.

Capitolul 11. Controlul accesului

Secțiunea 1. Politica de control al accesului

115. Furnizorii de servicii stabilesc, documentează și pun în aplicare politici de control al accesului logic și fizic pentru accesul la rețelele și sistemele lor

informatice, pe baza cerințelor comerciale, precum și a cerințelor de securitate a rețelelor și a sistemelor informatice.

116. Politicile menționate la punctul 115 trebuie:

116.1. să abordeze accesul persoanelor, inclusiv al personalului, al vizitatorilor și al entităților externe, cum ar fi furnizorii și prestatorii de servicii;

116.2. să abordeze accesul rețelelor și al sistemelor informatice;

116.3. să asigure faptul că accesul este acordat numai utilizatorilor care au fost autentificați în mod corespunzător.

117. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează politicile la intervale planificate și atunci când apar incidente semnificative sau modificări semnificative ale operațiunilor sau ale riscurilor.

Secțiunea 2. Gestionarea drepturilor de acces

118. Furnizorii de servicii trebuie să acorde, să modifice, să elimine și să documenteze drepturile de acces la rețele și la sistemele informatice în conformitate cu politica de control al accesului menționată în secțiunea 1 al prezentului capitol.

119. Furnizorii de servicii:

119.1 atribuie și revocă drepturi de acces pe baza principiilor necesității de a cunoaște, privilegiului minim și separării sarcinilor;

119.2 se asigură că drepturile de acces sunt modificate în mod corespunzător la încetarea sau modificarea raportului de muncă;

119.3 se asigură că accesul la rețele și la sistemele informatice este autorizat de către persoanele relevante;

119.4 se asigură că drepturile de acces abordează în mod corespunzător accesul terților, cum ar fi vizitatorii, furnizorii și prestatorii de servicii, în special prin limitarea drepturilor de acces în ceea ce privește sfera și durata acestora;

119.5 țin un registru al drepturilor de acces acordate;

119.6 aplică jurnalizarea gestionării drepturilor de acces.

120. Furnizorii de servicii revizuiesc drepturile de acces la intervale planificate și le modifică pe baza schimbărilor organizaționale, precum și documentează rezultatele revizuirii, inclusiv modificările necesare ale drepturilor de acces.

Secțiunea 3. Conturile privilegiate și conturile de administrare a sistemului

121. Furnizorii de servicii mențin politici de gestionare a conturilor privilegiate și a conturilor de administrare a sistemului ca parte a politicii de control al accesului menționate la punctul 11.1.

122. Politicile menționate la punctul 121:

122.1. instituie proceduri riguroase de identificare, autentificare, cum ar fi autentificarea multifactorială, și de autorizare pentru conturile privilegiate și conturile de administrare a sistemului;

122.2. creează conturi specifice care să fie utilizate exclusiv pentru operațiunile de administrare a sistemului, cum ar fi instalarea, configurarea, gestionarea sau întreținerea;

122.3. individualizează și restricționează privilegiile de administrare a sistemului în cea mai mare măsură posibilă;

122.4. prevăd faptul că sunt utilizate conturile de administrare a sistemului numai pentru conectarea la sistemele de administrare a sistemului.

123. Furnizorii de servicii revizuiesc drepturile de acces aferente conturilor privilegiate și conturilor de administrare a sistemului la intervale planificate și le modifică pe baza schimbărilor organizaționale și documentează rezultatele revizuirii, inclusiv modificările necesare ale drepturilor de acces.

Secțiunea 4. Sisteme de administrare

124. Furnizorii de servicii restricționează și controlează utilizarea sistemelor de administrare a sistemului în conformitate cu politica de control al accesului.

125. În acest scop, furnizorii de servicii:

125.1. utilizează sisteme de administrare a sistemului numai în scopul administrării sistemului și nu pentru alte operațiuni;

125.2. separă în mod logic astfel de sisteme de aplicațiile software care nu sunt utilizate în scopul administrării sistemului;

125.3. protejează accesul la sistemele de administrare a sistemului prin autentificare și criptare.

Secțiunea 5. Identificare

126. Furnizorii de servicii gestionează întregul ciclu de viață al identităților rețelelor și sistemelor informatice și ale utilizatorilor acestora.

127. În acest scop, furnizorii de servicii:

127.1. stabilesc identități unice pentru rețele și sisteme informatice și pentru utilizatorii acestora;

127.2. asociază identitatea utilizatorilor cu o singură persoană;

127.3. asigură supravegherea identităților rețelei și sistemelor informatice;

127.4. aplică jurnalizarea gestionării identităților.

128. Furnizorii de servicii permit identitățile atribuite mai multor persoane, cum ar fi identitățile comune, numai în cazul în care acestea sunt necesare din motive comerciale sau operaționale și fac obiectul unui proces de aprobare și al unei

documentări explicite. Furnizorii de servicii țin seama de identitățile atribuite mai multor persoane în cadrul de gestionare a riscurilor de securitate cibernetică.

129. Furnizorii de servicii revizuiesc periodic identitățile pentru rețele și sisteme informatice și ale utilizatorilor acestora și, dacă nu mai sunt necesare, le dezactivează fără întârziere.

Secțiunea 6. Autentificare

130. Furnizorii de servicii pun în aplicare proceduri și tehnologii de autentificare securizată bazate pe restricții de acces și pe politica privind controlul accesului.

131. În acest scop, furnizorii de servicii:

131.1. se asigură că puterea autentificării este adecvată pentru clasificarea activului care urmează să fie accesat;

131.2. controlează alocarea către utilizatori și gestionarea informațiilor secrete de autentificare printr-un proces care să asigure confidențialitatea informațiilor, inclusiv consilierea personalului cu privire la gestionarea adecvată a informațiilor de autentificare;

131.3. solicită modificarea acreditărilor de autentificare inițial, la intervale predefinite și în cazul în care se suspectează că respectivele acreditări au fost compromise;

131.4. solicită resetarea acreditărilor de autentificare și blocarea utilizatorilor după un număr predefinit de încercări nereușite de conectare;

131.5. pun capăt sesiunilor inactive după o perioadă prestabilită de inactivitate; și

131.6. solicită acreditări separate pentru a obține acces privilegiat sau a avea acces la conturi administrative.

132. Furnizorii de servicii utilizează, în măsura în care este fezabil, metode de autentificare de ultimă generație, în conformitate cu riscul evaluat asociat și cu clasificarea activului care urmează să fie accesat, precum și informații de autentificare unice.

133. Furnizorii de servicii revizuiesc procedurile și tehnologiile de autentificare la intervale planificate.

Secțiunea 7. Autentificarea multifactor

134. Furnizorii de servicii se asigură că utilizatorii sunt autentificați prin factori de autentificare multipli sau prin mecanisme de autentificare continuă pentru accesarea rețelelor și a sistemelor informatice ale furnizorului de servicii, dacă este adecvat, în conformitate cu clasificarea activului care urmează să fie accesat.

135. Furnizorii de servicii se asigură că puterea autentificării este adecvată pentru clasificarea activului care urmează să fie accesat.

Capitolul 12. Gestionarea activelor

Secțiunea 1. Clasificarea activelor

136. Furnizorii de servicii stabilesc niveluri de clasificare a tuturor activelor, inclusiv a informațiilor, care intră în domeniul de aplicare al rețelelor și sistemelor lor informatice corespunzătoare nivelului de protecție necesar.

137. În acest scop furnizorii de servicii:

137.1. stabilesc un sistem de niveluri de clasificare a activelor;

137.2. asociază tuturor activelor un nivel de clasificare, bazat pe cerințe de confidențialitate, integritate, autenticitate și disponibilitate, pentru a indica protecția necesară în funcție de sensibilitatea, criticalitatea, riscul și valoarea lor comercială;

137.3. aliniază cerințele privind disponibilitatea activelor la obiectivele de livrare și de recuperare stabilite în planurile lor de continuitate a activității și de recuperare în caz de dezastru.

138. Furnizorii de servicii efectuează revizuiri periodice ale nivelurilor de clasificare a activelor și le actualizează, dacă este adecvat.

Secțiunea 2. Gestionarea activelor

139. Furnizorii de servicii stabilesc, implementează și aplică o politică pentru gestionarea corespunzătoare a activelor, inclusiv a informațiilor, în conformitate cu politica lor de securitate a rețelelor și a informațiilor și comunică politica privind gestionarea corespunzătoare a activelor oricărei persoane care utilizează sau gestionează aceste active.

140. Politica de gestionare a activelor:

140.1. acoperă întregul ciclu de viață al activelor, inclusiv achiziționarea, utilizarea, depozitarea, transportul și eliminarea;

140.2. prevede norme privind utilizarea în condiții de siguranță, depozitarea în condiții de siguranță, transportul în condiții de siguranță și ștergerea și distrugerea iremediabilă a activelor;

140.3. prevede că transferul trebuie să aibă loc în condiții de siguranță, în funcție de tipul de activ care urmează să fie transferat.

141. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează politica la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor sau ale riscurilor.

Secțiunea 3. Politica privind suporturile amovibile

142. Furnizorii de servicii stabilesc, implementează și aplică o politică de gestionare a suporturilor de stocare amovibile și o comunică angajaților lor și părților terțe care gestionează suporturi de stocare amovibile în incintele furnizorului de servicii sau în alte locuri în care suporturile amovibile sunt conectate la rețelele și sistemele informatice ale furnizorului de servicii.

143. Politica de gestionare a suporturilor de stocare amovibile:

143.1. prevede o interdicție tehnică de conectare a suporturilor amovibile, cu excepția cazului în care există un motiv organizațional pentru utilizarea acestora;

143.2. prevede dezactivarea autoexecutării din aceste suporturi și scanarea suporturilor pentru coduri rău-intenționate înainte de a fi utilizate în sistemele furnizorului de servicii;

143.3. prevede măsuri de control și protecție a dispozitivelor portabile de stocare care conțin date în timpul tranzitului și al stocării;

143.4. dacă este adecvat, prevede măsuri pentru utilizarea tehnicilor criptografice pentru a proteja datele de pe suporturile de stocare amovibile.

144. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează politica la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor sau ale riscurilor.

Secțiunea 4. Inventarul activelor

145. Furnizorii de servicii elaborează și mențin un inventar complet, exact, actualizat și consecvent al activelor lor. Furnizorii de servicii înregistrează modificările aduse înregistrărilor din inventar într-un mod care să poată fi urmărit.

146. Granularitatea inventarului activelor trebuie să fie la un nivel adecvat nevoilor furnizorilor de servicii. Inventarul include următoarele:

146.1. lista operațiunilor și a serviciilor și descrierea acestora;

146.2. lista rețelelor și a sistemelor informatice și a altor active asociate care sprijină operațiunile și serviciile entităților relevante.

147. Furnizorii de servicii trebuie să revizuiască și să actualizeze periodic inventarul și activele lor și să documenteze istoricul modificărilor.

148. Furnizorii de servicii stabilesc, implementează și aplică proceduri care garantează că activele lor, aflate în custodia personalului, sunt depozitate, restituite sau eliminate la încetarea raportului de muncă și documentează depozitarea, returnarea și eliminarea activelor respective.

149. În cazul în care nu este posibilă depozitarea, returnarea sau eliminarea activelor, furnizorii de servicii se asigură că activele nu mai pot accesa rețelele și sistemele informatice ale acestora în conformitate cu politica pentru gestionarea corespunzătoare a activelor, prevăzută la secțiunea 2 din prezentul capitol.

Capitolul 13. Securitatea mediului și fizică

Secțiunea 1. Utilități de sprijin

150. Furnizorii de servicii previn pierderea, deteriorarea sau compromiterea rețelelor și a sistemelor informatice sau întreruperea funcționării acestora din cauza defectării și perturbării utilităților de sprijin.

151. În acest scop, furnizorii de servicii, dacă este adecvat:

151.1. protejează instalațiile împotriva întreruperii alimentării cu energie electrică și a altor perturbări cauzate de defecțiuni în ceea ce privește utilitățile de sprijin, cum ar fi energia electrică, telecomunicațiile, alimentarea cu apă, gazele, apele uzate, ventilarea și aerul condiționat;

151.2. iau în considerare utilizarea redundanței în ceea ce privește serviciile de utilități;

151.3. protejează serviciile de utilități pentru energie electrică și telecomunicații, care transportă date sau furnizează rețele și sisteme informatice, împotriva interceptării și a deteriorării;

151.4. monitorizează serviciile de utilități menționate la subpct. 151.3 și raportează personalului intern sau extern competent evenimentele din afara pragurilor minime și maxime de control menționate la subpunctul 154.2 care afectează serviciile de utilități;

151.5. încheie contracte pentru aprovizionarea de urgență cu servicii corespunzătoare, cum ar fi pentru combustibilul pentru alimentarea cu energie electrică în situații de urgență;

151.6. asigură eficacitatea continuă, monitorizează, întreține și testează alimentarea rețelelor și a sistemelor informatice necesare pentru funcționarea serviciului oferit, în special energia electrică, controlul temperaturii și umidității, telecomunicațiile și conexiunea la internet.

152. Furnizorii de servicii testează, revizuiesc și, dacă este adecvat, actualizează măsurile de protecție în mod regulat sau în urma unor incidente cibernetice cu impact semnificativ sau a unor modificări semnificative ale operațiunilor sau ale riscurilor.

Secțiunea 2. Protecția împotriva amenințărilor fizice și de mediu

153. Furnizorii de servicii previn sau reduc consecințele evenimentelor generate de amenințări fizice și de mediu, cum ar fi dezastrele naturale și alte amenințări intenționate sau neintenționate, pe baza rezultatelor evaluării riscurilor.

154. În acest scop, furnizorii de servicii, dacă este adecvat:

154.1. concep și pun în aplicare măsuri de protecție împotriva amenințărilor fizice și de mediu;

154.2. determină pragurile minime și maxime de control pentru amenințările fizice și de mediu;

154.3. monitorizează parametrii de mediu și raportează personalului intern sau extern competent evenimentele din afara pragurilor minime și maxime de control menționate la subpct.154.2.

155. Furnizorii de servicii testează, revizuiesc și, dacă este adecvat, actualizează măsurile de protecție împotriva amenințărilor fizice și de mediu în mod regulat sau în urma unor incidente cu impact semnificativ sau a unor modificări semnificative ale operațiunilor sau ale riscurilor.

Secțiunea 3. Controlul perimetrului și al accesului fizic

156. Furnizorii de servicii previn și monitorizează accesul fizic neautorizat la rețelele și sistemele lor informatice, precum și deteriorarea acestora și interferențele cu acestea.

157. În acest scop, furnizorii de servicii:

157.1. pe baza evaluării riscurilor, stabilesc și utilizează perimetre de securitate pentru a proteja zonele în care sunt situate rețelele și sistemele informatice și alte active asociate;

157.2. protejează zonele menționate la subpct.157.1 prin controale de intrare și puncte de acces adecvate;

157.3.concep și pun în aplicare securitatea fizică pentru birouri, încăperi și instalații;

157.4. își monitorizează permanent incintele pentru a depista accesul fizic neautorizat.

158. Furnizorii de servicii testează, revizuiesc și, dacă este adecvat, actualizează măsurile de control al accesului fizic în mod regulat sau în urma unor incidente cu impact semnificativ sau a unor modificări semnificative ale operațiunilor sau ale riscurilor.