



2024/1774

25.6.2024

REGULAMENTUL DELEGAT (UE) 2024/1774 AL COMISIEI

din 13 martie 2024

de completare a Regulamentului (UE) 2022/2554 al Parlamentului European și al Consiliului în ceea ce privește standardele tehnice de reglementare care precizează instrumentele, metodele, procesele și politicile de gestionare a riscurilor TIC și cadrul simplificat de gestionare a riscurilor TIC

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 ⁽¹⁾, în special articolul 15 alineatul al patrulea paragraf și articolul 16 alineatul (3) al patrulea paragraf,

întrucât:

- (1) Regulamentul (UE) 2022/2554 acoperă o gamă largă de entități financiare care diferă în ceea ce privește dimensiunea, structura, organizarea internă și natura și complexitatea activităților lor și care, prin urmare, prezintă elemente de complexitate sau riscuri sporite sau reduse. Pentru a se asigura că această varietate este luată în considerare în mod corespunzător, orice cerință referitoare la politicile, procedurile, protocoalele și instrumentele de securitate TIC și la un cadru simplificat de gestionare a riscurilor TIC ar trebui să fie proporțională cu dimensiunea, structura, organizarea internă, natura și complexitatea entităților financiare respective, precum și cu riscurile aferente.
- (2) Din același motiv, entitățile financiare care fac obiectul Regulamentului (UE) 2022/2554 ar trebui să beneficieze de o anumită flexibilitate în ceea ce privește modul în care respectă orice cerință referitoare la politicile, procedurile, protocoalele și instrumentele de securitate TIC și la orice cadru simplificat de gestionare a riscurilor TIC. Din acest motiv, entităților financiare ar trebui să li se permită să utilizeze orice documentație pe care o au deja pentru a se conforma cerințelor în materie de documentație care decurg din cerințele respective. Prin urmare, ar trebui să se impună elaborarea, documentarea și punerea în aplicare a unor politici specifice de securitate TIC numai pentru anumite elemente esențiale, ținând seama, printre altele, de cele mai avansate practici și standarde din sector. În plus, pentru a acoperi aspectele tehnice specifice de punere în aplicare, este necesar să se elaboreze, să se documenteze și să se pună în aplicare proceduri de securitate TIC care să acopere aspectele tehnice specifice de punere în aplicare, inclusiv gestionarea capacității și a performanței, gestionarea vulnerabilităților și a corecțiilor, securitatea datelor și a sistemului, precum și jurnalizarea.
- (3) Pentru se a asigura punerea în aplicare corectă de-a lungul timpului a politicilor, procedurilor, protocoalelor și instrumentelor de securitate TIC menționate în titlul II capitolul I din prezentul regulament, este important ca entitățile financiare să atribuie și să mențină în mod corect orice roluri și responsabilități legate de securitatea TIC și să stabilească consecințele nerespectării politicilor sau procedurilor de securitate TIC.
- (4) Pentru a limita riscul de conflicte de interese, entitățile financiare ar trebui să asigure separarea sarcinilor atunci când atribuie roluri și responsabilități TIC.
- (5) Pentru asigurarea flexibilității și pentru simplificarea cadrului de control al entităților financiare, entitățile financiare nu ar trebui să aibă obligația de a elabora dispoziții specifice privind consecințele nerespectării politicilor, procedurilor și protocoalelor de securitate TIC menționate în titlul II capitolul I din prezentul regulament, în cazul în care astfel de dispoziții sunt deja stabilite în cadrul unei alte politici sau proceduri.

⁽¹⁾ JO L 333, 27.12.2022, p. 1, ELI: <http://data.europa.eu/eli/reg/2022/2554/oj>.

- (6) Într-un mediu dinamic, în care riscurile TIC evoluează în mod constant, este important ca entitățile financiare să își dezvolte setul de politici de securitate TIC pe baza celor mai avansate practici și, după caz, a standardelor definite la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului ^(*). Acest lucru ar trebui să le permită entităților financiare menționate în titlul II din prezentul regulament să rămână informate și pregătite într-un mediu în schimbare.
- (7) Pentru a-și asigura reziliența operațională digitală, entitățile financiare menționate în titlul II din prezentul regulament ar trebui, ca parte a politicilor, procedurilor, protocoalelor și instrumentelor lor de securitate TIC, să elaboreze și să pună în aplicare o politică de gestionare a activelor TIC, proceduri de gestionare a capacității și a performanței, precum și politici și proceduri pentru operațiunile TIC. Politicile și procedurile respective sunt necesare pentru a asigura monitorizarea statutului activelor TIC pe parcursul ciclului lor de viață, astfel încât activele respective să fie utilizate și întreținute în mod eficace (gestionarea activelor TIC). Aceste politici și proceduri ar trebui să asigure, de asemenea, optimizarea funcționării sistemelor TIC și faptul că performanța sistemelor TIC și a capacității îndeplinește obiectivele stabilite în materie de securitate a activității și a informațiilor (gestionarea capacității și a performanței). În cele din urmă, aceste politici și proceduri ar trebui să asigure gestionarea și funcționarea cotidiană eficace și fără probleme a sistemelor TIC (operațiunilor TIC), reducând astfel la minimum riscul de pierdere a confidențialității, integrității și disponibilității datelor. Prin urmare, aceste politici și proceduri sunt necesare pentru a asigura securitatea rețelelor, pentru a oferi garanții adecvate împotriva intruziunilor și a utilizării abuzive a datelor și pentru a menține disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor.
- (8) Pentru a asigura gestionarea adecvată a riscurilor legate de sistemele TIC moștenite, entitățile financiare ar trebui să înregistreze și să monitorizeze datele de încetare a serviciilor de asistență TIC furnizate de terți. Din cauza impactului pe care îl poate avea pierderea confidențialității, integrității și disponibilității datelor, entitățile financiare ar trebui să se concentreze asupra activelor sau sistemelor TIC care sunt esențiale pentru funcționarea activității operaționale atunci când înregistrează și monitorizează datele de expirare a serviciilor respective.
- (9) Controalele criptografice pot asigura disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor. Prin urmare, entitățile financiare menționate în titlul II din prezentul regulament ar trebui să identifice și să pună în aplicare astfel de controale printr-o abordare bazată pe riscuri. În acest scop, entitățile financiare ar trebui să creeze datele în cauză în repaus, în tranzit sau, dacă este necesar, în uz, pe baza rezultatelor unui proces care conține două elemente, și anume clasificarea datelor și o evaluare cuprinzătoare a riscurilor TIC. Având în vedere complexitatea criptării datelor în uz, entitățile financiare menționate în titlul II din prezentul regulament ar trebui să creeze datele în uz numai în cazul în care acest lucru ar fi adecvat, având în vedere rezultatele evaluării riscurilor TIC. Cu toate acestea, entitățile financiare menționate în titlul II din prezentul regulament ar trebui să poată, în cazul în care criptarea datelor în uz nu este fezabilă sau este prea complexă, să protejeze confidențialitatea, integritatea și disponibilitatea datelor în cauză prin alte măsuri de securitate TIC. Având în vedere evoluțiile tehnologice rapide din domeniul tehnicilor criptografice, entitățile financiare menționate în titlul II din prezentul regulament ar trebui să rămână la curent cu evoluțiile relevante în materie de criptare și să ia în considerare cele mai avansate practici și standarde. Entitățile financiare menționate în titlul II din prezentul regulament ar trebui, prin urmare, să urmeze o abordare flexibilă, bazată pe atenuarea și monitorizarea riscurilor, pentru a face față peisajului dinamic al amenințărilor criptografice, inclusiv al amenințărilor generate de progresele tehnologiilor cuantice.
- (10) Politicile, procedurile, protocoalele și instrumentele operaționale și de securitate a operațiunilor TIC sunt esențiale pentru a asigura confidențialitatea, integritatea și disponibilitatea datelor. Un aspect esențial este separarea strictă a mediilor de producție TIC de mediile în care sunt dezvoltate și testate sistemele TIC sau de alte medii care nu au legătură cu producția. Această separare ar trebui să servească drept măsură importantă de securitate TIC împotriva accesului neintenționat și neautorizat la datele din mediul de producție, a modificărilor și a ștergerilor acestora, care ar putea duce la perturbări majore ale activităților operaționale ale entităților financiare menționate în titlul II din prezentul regulament. Cu toate acestea, având în vedere practicile actuale de dezvoltare a sistemelor TIC, entităților financiare ar trebui să li se permită, în circumstanțe excepționale, să testeze în medii de producție, cu condiția să justifice o astfel de testare și să obțină aprobarea necesară.

(*) Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12, ELI: <http://data.europa.eu/eli/reg/2012/1025/oj>).

- (11) Evoluția rapidă inerentă peisajelor TIC, vulnerabilităților TIC și amenințărilor cibernetice necesită o abordare proactivă și cuprinzătoare pentru identificarea, evaluarea și abordarea vulnerabilităților TIC. Absența unei astfel de abordări ar putea duce la o expunere gravă la riscuri a entităților financiare, a clienților, a utilizatorilor sau a contrapărților acestora, ceea ce ar pune în pericol reziliența lor operațională digitală, securitatea rețelelor lor și disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor pe care politicile și procedurile de securitate TIC ar trebui să le protejeze. Entitățile financiare menționate în titlul II din prezentul regulament ar trebui, prin urmare, să identifice și să remedieze vulnerabilitățile mediului lor TIC și atât entitățile financiare, cât și furnizorii lor terți de servicii TIC ar trebui să adere la un cadru coerent, transparent și responsabil de gestionare a vulnerabilităților. Din același motiv, entitățile financiare ar trebui să monitorizeze vulnerabilitățile TIC utilizând resurse fiabile și instrumente automatizate, verificând dacă furnizorii terți de servicii TIC asigură luarea unor acțiuni prompte cu privire la vulnerabilitățile serviciilor TIC furnizate.
- (12) Gestionarea corecțiilor ar trebui să fie o parte esențială a politicilor și procedurilor de securitate TIC care, prin testare și implementare într-un mediu controlat, trebuie să soluționeze vulnerabilitățile identificate și să prevină perturbările cauzate de instalarea corecțiilor.
- (13) Pentru a asigura comunicarea în timp util și transparentă a potențialelor amenințări la adresa securității care ar putea avea un impact asupra entității financiare și a părților interesate ale acesteia, entitățile financiare ar trebui să stabilească proceduri pentru divulgarea responsabilă a vulnerabilităților TIC către clienți, contrapărți și public. La stabilirea procedurilor respective, entitățile financiare ar trebui să ia în considerare factori precum gravitatea vulnerabilității, impactul potențial al unei astfel de vulnerabilități asupra părților interesate și disponibilitatea unei soluții sau a unor măsuri de atenuare.
- (14) Pentru a permite atribuirea drepturilor de acces ale utilizatorilor, entitățile financiare menționate în titlul II din prezentul regulament ar trebui să stabilească măsuri ferme care să asigure identificarea unică a persoanelor și a sistemelor care vor avea acces la informațiile entității financiare. În caz contrar, entitățile financiare ar fi expuse riscului potențial de acces neautorizat, încălcări ale securității datelor și activități frauduloase, ceea ce ar compromite confidențialitatea, integritatea și disponibilitatea datelor financiare sensibile. Deși ar trebui să se permită în mod excepțional utilizarea conturilor generice sau partajate în circumstanțe specificate de entitățile financiare, entitățile financiare ar trebui să se asigure că își păstrează răspunderea pentru acțiunile efectuate prin intermediul acestor conturi. Fără această garanție, eventualii utilizatori răuvoitori ar putea să împiedice măsurile de investigare și măsurile corective, entitățile financiare devenind astfel vulnerabile la acțiuni răuvoitoare nedetectate sau la sancțiuni pentru neconformitate.
- (15) Pentru a gestiona progresul rapid din mediile TIC, entitățile financiare menționate în titlul II din prezentul regulament ar trebui să pună în aplicare politici și proceduri solide de gestionare a proiectelor TIC care să mențină disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor. Aceste politici și proceduri de gestionare a proiectelor TIC ar trebui să identifice elementele necesare pentru gestionarea cu succes a proiectelor TIC, inclusiv modificările, achizițiile, întreținerea și evoluțiile sistemelor TIC ale entității financiare, indiferent de metodologia de gestionare a proiectelor TIC aleasă de entitatea financiară. În contextul acestor politici și proceduri, entitățile financiare ar trebui să adopte practici și metode de testare care să corespundă nevoilor lor, respectând în același timp o abordare bazată pe riscuri și asigurând menținerea unui mediu TIC sigur, fiabil și rezilient. Pentru a garanta punerea în aplicare în condiții de siguranță a unui proiect TIC, entitățile financiare ar trebui să se asigure că personalul care lucrează în sectoare de activitate specifice sau desfășoară roluri specifice și care este influențat sau afectat de respectivul proiect TIC poate furniza informațiile și expertiza necesare. Pentru a asigura o supraveghere eficace, ar trebui să se prezinte organului de conducere rapoarte privind proiectele TIC, în special proiectele care afectează funcții critice sau importante și riscurile asociate acestora. Entitățile financiare ar trebui să adapteze frecvența și detaliile revizuirilor și rapoartelor sistematice și continue în funcție de importanța și dimensiunea proiectelor TIC în cauză.
- (16) Este necesar să se asigure că pachetele software pe care entitățile financiare menționate în titlul II din prezentul regulament le achiziționează și le dezvoltă sunt integrate în mod eficace și securizat în mediul TIC existent, în conformitate cu obiectivele stabilite în materie de securitate a activității și a informațiilor. Prin urmare, entitățile financiare ar trebui să evalueze în detaliu astfel de pachete software. În acest scop și pentru a identifica vulnerabilitățile și potențialele lacune în materie de securitate atât în cadrul pachetelor software, cât și al sistemelor TIC mai ample, entitățile financiare ar trebui să efectueze teste de securitate TIC. Pentru a evalua integritatea software-ului și pentru a se asigura că utilizarea software-ului respectiv nu prezintă riscuri de securitate TIC, entitățile financiare ar trebui, de asemenea, să revizuiască codurile sursă ale software-ului achiziționat, inclusiv, dacă este fezabil, ale software-ului brevetat furnizat de furnizorii terți de servicii TIC, utilizând metode de testare atât statice, cât și dinamice.

- (17) Modificările, indiferent de amploarea lor, prezintă riscuri inerente și pot genera riscuri semnificative de pierdere a confidențialității, a integrității și a disponibilității datelor, ceea ce ar putea duce la perturbări grave ale activității. Pentru a proteja entitățile financiare de potențiale vulnerabilități și deficiențe TIC care le-ar putea expune unor riscuri semnificative, este necesar un proces riguros de verificare prin care să se confirme că toate modificările îndeplinesc cerințele de securitate TIC necesare. Entitățile financiare menționate în titlul II din prezentul regulament ar trebui, prin urmare, să dispună, ca element esențial al politicilor și procedurilor lor de securitate TIC, de politici și proceduri solide de gestionare a modificărilor TIC. Pentru a menține obiectivitatea și eficacitatea procesului de gestionare a modificărilor TIC, a preveni conflictele de interese și a se asigura că modificările TIC sunt evaluate în mod obiectiv, este necesar să se separe funcțiile responsabile de aprobarea modificărilor de funcțiile care solicită și pun în aplicare modificările respective. Pentru a asigura tranziții eficiente, punerea în aplicare controlată a modificărilor TIC și perturbări minime ale funcționării sistemelor TIC, entitățile financiare ar trebui să atribuie roluri și responsabilități clare care să asigure planificarea, testarea adecvată și calitatea modificărilor TIC. Pentru a se asigura că sistemele TIC continuă să funcționeze în mod eficiente și pentru ca entitățile financiare să dispună de o plasă de siguranță, entitățile financiare ar trebui, de asemenea, să elaboreze și să pună în aplicare proceduri alternative. Entitățile financiare ar trebui să identifice în mod clar aceste proceduri alternative și să atribuie responsabilități în așa fel încât să se asigure un răspuns rapid și eficient în cazul unor modificări TIC nereușite.
- (18) Pentru a detecta, gestiona și raporta incidentele legate de TIC, entitățile financiare menționate în titlul II din prezentul regulament ar trebui să instituie o politică privind incidentele legate de TIC care să cuprindă componentele unui proces de gestionare a incidentelor legate de TIC. În acest scop, entitățile financiare ar trebui să identifice toate contactele relevante din interiorul și din afara organizației care pot facilita coordonarea și punerea în aplicare corectă a diferitelor etape ale procesului respectiv. Pentru a optimiza detectarea incidentelor legate de TIC și răspunsul la acestea și pentru a identifica tendințele în ceea ce privește astfel de incidente, care reprezintă o sursă valoroasă de informații care le permite entităților financiare să identifice și să abordeze cauzele și problemele profunde într-un mod eficient, entitățile financiare ar trebui, în special, să analizeze în detaliu incidentele legate de TIC pe care le consideră a fi cele mai semnificative, printre altele din cauza reapariției lor periodice.
- (19) Pentru a garanta detectarea timpurie și eficientă a activităților anormale, entitățile financiare menționate în titlul II din prezentul regulament ar trebui să colecteze, să monitorizeze și să analizeze diferitele surse de informații și să aloce rolurile și responsabilitățile aferente. În ceea ce privește sursele interne de informații, jurnalele sunt o sursă extrem de relevantă, însă entitățile financiare nu ar trebui să se bazeze doar pe jurnale. În schimb, entitățile financiare ar trebui să ia în considerare informații mai ample pentru a include ceea ce este raportat de alte funcții interne, deoarece aceste funcții reprezintă adesea o sursă valoroasă de informații relevante. Din același motiv, entitățile financiare ar trebui să analizeze și să monitorizeze informațiile colectate din surse externe, inclusiv informațiile furnizate de furnizorii terți de servicii TIC cu privire la incidentele care le afectează sistemele și rețelele, precum și alte surse de informații pe care entitățile financiare le consideră relevante. În măsura în care aceste informații constituie date cu caracter personal, se aplică legislația Uniunii în materie de protecție a datelor. Datele cu caracter personal ar trebui să se limiteze la ceea ce este necesar pentru detectarea incidentului.
- (20) Pentru a facilita detectarea incidentelor legate de TIC, entitățile financiare ar trebui să păstreze dovezi ale incidentelor respective. Pentru a se asigura, pe de o parte, că astfel de dovezi sunt păstrate suficient de mult timp și, pe de altă parte, pentru a evita o sarcină de reglementare excesivă, entitățile financiare ar trebui să stabilească perioada de păstrare a datelor, ținând seama, printre altele, de caracterul critic al datelor și de cerințele de păstrare care decurg din dreptul Uniunii.
- (21) Pentru a se asigura că incidentele legate de TIC sunt detectate la timp, entitățile financiare menționate în titlul II din prezentul regulament ar trebui să considere criteriile identificate pentru declanșarea detectării incidentelor legate de TIC și răspunsurile la acestea ca fiind neexhaustive. În plus, deși entitățile financiare ar trebui să ia în considerare fiecare dintre aceste criterii, circumstanțele descrise în criterii nu ar trebui să aibă loc simultan, iar importanța serviciilor TIC afectate ar trebui luată în considerare în mod corespunzător pentru a declanșa procese de detectare a incidentelor legate de TIC și de răspuns la acestea.
- (22) Atunci când elaborează o politică de continuitate a activității TIC, entitățile financiare menționate în titlul II din prezentul regulament ar trebui să țină seama de componentele esențiale ale gestionării riscurilor TIC, inclusiv de strategiile de gestionare și comunicare a incidentelor legate de TIC, de procesul de gestionare a modificărilor TIC și de riscurile asociate furnizorilor terți de servicii TIC.

- (23) Este necesar să se stabilească setul de scenarii pe care entitățile financiare menționate în titlul II din prezentul regulament ar trebui să le ia în considerare atât pentru punerea în aplicare a planurilor de răspuns și de recuperare în domeniul TIC, cât și pentru testarea planurilor de continuitate a activității TIC. Aceste scenarii ar trebui să servească drept punct de plecare pentru ca entitățile financiare să analizeze atât relevanța și plauzibilitatea fiecărui scenariu, cât și necesitatea de a elabora scenarii alternative. Entitățile financiare ar trebui să se concentreze asupra scenariilor în care investițiile în măsuri de reziliență ar putea fi mai eficiente și mai eficace. Prin testarea transferurilor de la infrastructura TIC primară la orice capacitate redundantă, copie de rezervă și instalație redundantă, instituțiile financiare ar trebui să evalueze dacă respectiva capacitate, respectiva copie de rezervă și respectivele instalații funcționează în mod eficace pentru o perioadă de timp suficientă și să se asigure că funcționarea normală a infrastructurii TIC primare este restabilită în conformitate cu obiectivele de recuperare.
- (24) Este necesar să se stabilească cerințe pentru riscul operațional, în special cerințe privind gestionarea proiectelor și a modificărilor TIC și gestionarea continuității activității TIC, pe baza celor care se aplică deja contrapărților centrale, depozitarilor centrali de titluri de valoare și locurilor de tranzacționare în temeiul Regulamentelor (UE) nr. 648/2012 ⁽³⁾, (UE) nr. 600/2014 ⁽⁴⁾ și, respectiv, (UE) nr. 909/2014 ⁽⁵⁾ ale Parlamentului European și ale Consiliului.
- (25) Articolul 6 alineatul (5) din Regulamentul (UE) 2022/2554 impune obligația entităților financiare de a-și revizui cadrul de gestionare a riscurilor TIC și de a furniza autorității lor competente un raport cu privire la această revizuire. Pentru a le permite autorităților competente să prelucreze cu ușurință informațiile din rapoartele respective și pentru a garanta o transmitere adecvată a acestor informații, entitățile financiare ar trebui să transmită rapoartele în cauză într-un format electronic cu funcție de căutare.
- (26) Cerințele pentru entitățile financiare care fac obiectul cadrului simplificat de gestionare a riscurilor TIC menționat la articolul 16 din Regulamentul (UE) 2022/2554 ar trebui să se concentreze asupra domeniilor și elementelor esențiale care, având în vedere amploarea, riscurile, dimensiunea și complexitatea entităților financiare respective, reprezintă minimumul necesar pentru a asigura confidențialitatea, integritatea, disponibilitatea și autenticitatea datelor și serviciilor entităților financiare în cauză. În acest context, entitățile financiare respective ar trebui să dispună de un cadru intern de guvernanță și control cu responsabilități clare care să permită un cadru eficace și solid de gestionare a riscurilor. În plus, pentru a reduce sarcina administrativă și operațională, entitățile financiare respective ar trebui să elaboreze și să documenteze o singură politică, și anume o politică de securitate a informațiilor, care să specifice principiile și normele de nivel înalt necesare pentru a proteja confidențialitatea, integritatea, disponibilitatea și autenticitatea datelor și a serviciilor entităților financiare respective.
- (27) Dispozițiile prezentului regulament se referă la domeniul cadrului de gestionare a riscurilor TIC, prin detalierea elementelor specifice aplicabile entităților financiare în conformitate cu articolul 15 din Regulamentul (UE) 2022/2554 și prin elaborarea cadrului simplificat de gestionare a riscurilor TIC pentru entitățile financiare prevăzut la articolul 16 alineatul (1) din regulamentul respectiv. Pentru a asigura coerența dintre cadrul de gestionare a riscurilor TIC obișnuit și cel simplificat și având în vedere că dispozițiile respective ar trebui să devină aplicabile în același timp, este oportun ca dispozițiile respective să fie incluse într-un singur act legislativ.
- (28) Prezentul regulament are la bază proiectul de standarde tehnice de reglementare prezentat Comisiei de Autoritatea Bancară Europeană, Autoritatea Europeană de Asigurări și Pensii Ocupaționale și de Autoritatea Europeană pentru Valori Mobiliare și Piețe (autoritățile europene de supraveghere), în consultare cu Agenția Uniunii Europene pentru Securitate Cibernetică („ENISA”).

⁽³⁾ Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului din 4 iulie 2012 privind instrumentele financiare derivate extrabursiere, contrapărțile centrale și registrele centrale de tranzacții (JO L 201, 27.7.2012, p. 1, ELI: <http://data.europa.eu/eli/reg/2012/648/oj>).

⁽⁴⁾ Regulamentul (UE) nr. 600/2014 al Parlamentului European și al Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 173, 12.6.2014, p. 84, ELI: <http://data.europa.eu/eli/reg/2014/600/oj>).

⁽⁵⁾ Regulamentul (UE) nr. 909/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind îmbunătățirea decontării titlurilor de valoare în Uniunea Europeană și privind depozitarii centrali de titluri de valoare și de modificare a Directivelor 98/26/CE și 2014/65/UE și a Regulamentului (UE) nr. 236/2012 (JO L 257, 28.8.2014, p. 1, ELI: <http://data.europa.eu/eli/reg/2014/909/oj>).

- (29) Comitetul comun al autorităților europene de supraveghere menționat la articolul 54 din Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului ⁽⁶⁾, la articolul 54 din Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului ⁽⁷⁾ și la articolul 54 din Regulamentul (UE) nr. 1095/2010 al Parlamentului European și al Consiliului ⁽⁸⁾ a efectuat consultări publice deschise cu privire la proiectul de standarde tehnice de reglementare pe care se bazează prezentul regulament, a analizat costurile și beneficiile potențiale ale standardelor propuse și a solicitat avizul Grupului părților interesate din domeniul bancar, instituit în conformitate cu articolul 37 din Regulamentul (UE) nr. 1093/2010, al Grupului părților interesate din domeniul asigurărilor și reasigurărilor și al Grupului părților interesate din domeniul pensiilor ocupaționale, instituite în conformitate cu articolul 37 din Regulamentul (UE) nr. 1094/2010, precum și al Grupului părților interesate din domeniul valorilor mobiliare și piețelor, instituit în conformitate cu articolul 37 din Regulamentul (UE) nr. 1095/2010.
- (30) În măsura în care prelucrarea datelor cu caracter personal este necesară pentru a respecta obligațiile prevăzute în prezentul act, ar trebui să se aplice pe deplin Regulamentele (UE) 2016/679 ⁽⁹⁾ și (UE) 2018/1725 ⁽¹⁰⁾ ale Parlamentului European și al Consiliului. De exemplu, principiul reducerii la minimum a datelor ar trebui respectat în cazul în care sunt colectate date cu caracter personal pentru a se asigura detectarea adecvată a incidentelor. Autoritatea Europeană pentru Protecția Datelor a fost, de asemenea, consultată cu privire la proiectul de text al prezentului act,

ADOPTĂ PREZENTUL REGULAMENT:

TITLUL I

PRINCIPIUL GENERAL

Articolul 1

Profilul general de risc și complexitatea

La elaborarea și punerea în aplicare a politicilor, procedurilor, protocoalelor și instrumentelor de securitate TIC menționate în titlul II și a cadrului simplificat de gestionare a riscurilor TIC menționat la titlul III, se iau în considerare dimensiunea și profilul general de risc al entității financiare, precum și natura, amploarea și elementele de complexitate sporită sau redusă ale serviciilor, activităților și operațiunilor sale, inclusiv elementele legate de:

- (a) criptare și criptografie;
- (b) securitatea operațiunilor TIC;
- (c) securitatea rețelor;

⁽⁶⁾ Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea Bancară Europeană), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/78/CE a Comisiei (JO L 331, 15.12.2010, p. 12, ELI: <http://data.europa.eu/eli/reg/2010/1093/oj>).

⁽⁷⁾ Regulamentul (UE) nr. 1094/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea Europeană de Asigurări și Pensii Ocupaționale) de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/79/CE a Comisiei (JO L 331, 15.12.2010, p. 48, ELI: <http://data.europa.eu/eli/reg/2010/1094/oj>).

⁽⁸⁾ Regulamentul (UE) nr. 1095/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea europeană pentru valori mobiliare și piețe), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/77/CE a Comisiei (JO L 331, 15.12.2010, p. 84, ELI: <http://data.europa.eu/eli/reg/2010/1095/oj>).

⁽⁹⁾ Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

⁽¹⁰⁾ Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

- (d) gestionarea proiectelor și a modificărilor TIC;
- (e) impactul potențial al riscului TIC asupra confidențialității, integrității și disponibilității datelor, precum și al perturbărilor asupra continuității și disponibilității activităților entității financiare.

TITLUL II

ARMONIZAREA SUPLIMENTARĂ A INSTRUMENTELOR, METODELOR, PROCESELOR ȘI POLITICILOR DE GESTIONARE A RISCURILOR TIC ÎN CONFORMITATE CU articolul 15 DIN REGULAMENTUL (UE) 2022/2554

CAPITOLUL I

Politice, procedurile, protocoalele și instrumentele TIC

Secțiunea 1

Articolul 2

Elementele generale ale politicilor, procedurilor, protocoalelor și instrumentelor de securitate TIC

(1) Entitățile financiare se asigură că politicile lor de securitate TIC, securitatea informațiilor și procedurile, protocoalele și instrumentele conexe, astfel cum sunt menționate la articolul 9 alineatul (2) din Regulamentul (UE) 2022/2554, sunt integrate în cadrul lor de gestionare a riscurilor TIC. Entitățile financiare stabilesc politicile, procedurile, protocoalele și instrumentele de securitate TIC prevăzute în prezentul capitol care:

- (a) asigură securitatea rețelelor;
 - (b) conțin măsuri de protecție împotriva intruziunilor și a utilizării necorespunzătoare a datelor;
 - (c) păstrează disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor, inclusiv prin utilizarea tehnicilor criptografice;
 - (d) garantează transmiterea precisă și promptă a datelor, fără perturbări majore și întârzieri nejustificate.
- (2) Entitățile financiare se asigură că politicile de securitate TIC menționate la alineatul (1):
- (a) sunt aliniate la obiectivele de securitate a informațiilor ale entității financiare incluse în strategia privind reziliența operațională digitală menționată la articolul 6 alineatul (8) din Regulamentul (UE) 2022/2554;
 - (b) indică data aprobării oficiale a politicilor de securitate TIC de către organul de conducere;
 - (c) conțin indicatori și măsuri pentru:
 - (i) monitorizarea punerii în aplicare a politicilor, procedurilor, protocoalelor și instrumentelor de securitate TIC;
 - (ii) înregistrarea excepțiilor de la punerea în aplicare respectivă;
 - (iii) asigurarea rezilienței operaționale digitale a entității financiare în cazul excepțiilor menționate la punctul (ii);
 - (d) specifică responsabilitățile personalului de la toate nivelurile pentru a asigura securitatea TIC a entității financiare;
 - (e) precizează consecințele nerespectării de către personalul entității financiare a politicilor de securitate TIC, în cazul în care alte politici ale entității financiare nu prevăd dispoziții în acest sens;
 - (f) oferă o listă a documentației care trebuie păstrată;

- (g) specifică modalitățile de separare a sarcinilor în contextul modelului celor trei linii de apărare sau al altui model intern de gestionare și control al riscurilor, după caz, pentru a evita conflictele de interese;
- (h) iau în considerare cele mai avansate practici și, dacă este cazul, standardele definite la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012;
- (i) identifică rolurile și responsabilitățile pentru elaborarea, punerea în aplicare și întreținerea politicilor, procedurilor, protocoalelor și instrumentelor de securitate TIC;
- (j) sunt revizuite în conformitate cu articolul 6 alineatul (5) din Regulamentul (UE) 2022/2554;
- (k) țin seama de modificările semnificative referitoare la entitatea financiară, inclusiv de modificările semnificative ale activităților sau proceselor entității financiare, ale peisajului amenințărilor cibernetice sau ale obligațiilor legale aplicabile.

Secțiunea 2

Articolul 3

Gestionarea riscurilor TIC

Entitățile financiare elaborează, documentează și pun în aplicare politici și proceduri de gestionare a riscurilor TIC care conțin toate elementele următoare:

- (a) o indicație a aprobării nivelului de toleranță la risc pentru riscurile TIC stabilit în conformitate cu articolul 6 alineatul (8) litera (b) din Regulamentul (UE) 2022/2554;
- (b) o procedură și o metodologie de efectuare a evaluării riscurilor TIC, care identifică
 - (i) vulnerabilitățile și amenințările care afectează sau pot afecta funcțiile operaționale sprijinite, sistemele TIC și activele TIC care sprijină funcțiile respective;
 - (ii) indicatorii cantitativi sau calitativi pentru a măsura impactul și probabilitatea apariției vulnerabilităților și amenințărilor menționate la punctul (i);
- (c) procedura de identificare, punere în aplicare și documentare a măsurilor de tratare a riscurilor TIC pentru riscurile TIC identificate și evaluate, inclusiv stabilirea măsurilor de tratare a riscurilor TIC necesare pentru a aduce riscurile TIC la nivelul de toleranță la risc menționat la litera (a);
- (d) pentru riscurile TIC reziduale care sunt încă prezente în urma punerii în aplicare a măsurilor de tratare a riscurilor TIC menționate la litera (c):
 - (i) dispoziții privind identificarea acestor riscuri TIC reziduale;
 - (ii) atribuirea rolurilor și a responsabilităților în ceea ce privește:
 - 1. acceptarea riscurilor TIC reziduale care depășesc nivelul de toleranță la risc al entității financiare menționat la litera (a);
 - 2. procesul de revizuire menționat la punctul (iv) de la prezenta literă (d);
 - (iii) elaborarea unui inventar al riscurilor TIC reziduale acceptate, inclusiv o justificare a acceptării acestora;
 - (iv) dispoziții privind revizuirea riscurilor TIC reziduale acceptate cel puțin o dată pe an, inclusiv:
 - 1. identificarea oricăror modificări ale riscurilor TIC reziduale;
 - 2. evaluarea măsurilor de atenuare disponibile;
 - 3. evaluarea măsurii în care motivele care justifică acceptarea riscurilor TIC reziduale sunt încă valabile și aplicabile la data revizuirii;
- (e) dispoziții privind monitorizarea:
 - (i) oricărei modificări a peisajului riscurilor TIC și amenințărilor cibernetice;
 - (ii) vulnerabilităților și amenințărilor interne și externe;
 - (iii) riscului TIC al entității financiare care permite detectarea promptă a modificărilor care ar putea afecta profilul său de risc TIC;

- (f) dispoziții privind un proces prin care să se asigure că se ține seama de orice modificare a strategiei de afaceri și a strategiei privind reziliența operațională digitală a entității financiare.

În sensul primului paragraf litera (c), procedura menționată la litera respectivă asigură:

- (a) monitorizarea eficacității măsurilor de tratare a riscurilor TIC care au fost puse în aplicare;
- (b) evaluarea măsurii în care au fost atinse nivelurile de toleranță la risc stabilite pentru entitatea financiară;
- (c) evaluarea măsurii în care entitatea financiară a întreprins acțiuni pentru a corecta sau a îmbunătăți măsurile respective, după caz.

Secțiunea 3

Gestionarea activelor TIC

Articolul 4

Politica de gestionare a activelor TIC

- (1) Ca parte a politicilor, procedurilor, protocoalelor și instrumentelor de securitate TIC menționate la articolul 9 alineatul (2) din Regulamentul (UE) 2022/2554, entitățile financiare elaborează, documentează și pun în aplicare o politică privind gestionarea activelor TIC.
- (2) Politica privind gestionarea activelor TIC menționată la alineatul (1):
 - (a) dispune monitorizarea și gestionarea ciclului de viață al activelor TIC identificate și clasificate în conformitate cu articolul 8 alineatul (1) din Regulamentul (UE) 2022/2554;
 - (b) impune entității financiare să țină evidența tuturor elementelor următoare:
 - (i) identificatorul unic al fiecărui activ TIC;
 - (ii) informații privind localizarea, fizică sau logică, a tuturor activelor TIC;
 - (iii) clasificarea tuturor activelor TIC menționate la articolul 8 alineatul (1) din Regulamentul (UE) 2022/2554;
 - (iv) identitatea proprietarilor activelor TIC;
 - (v) funcțiile sau serviciile operaționale sprijinite de activul TIC;
 - (vi) cerințele de continuitate a activității TIC, inclusiv obiectivele privind timpul de recuperare și punctul de recuperare;
 - (vii) dacă activul TIC poate fi sau este expus la rețele externe, inclusiv la internet;
 - (viii) legăturile și interdependențele dintre activele TIC și funcțiile operaționale care utilizează fiecare activ TIC;
 - (ix) după caz, pentru toate activele TIC, datele de expirare ale serviciilor de asistență periodice, extinse și personalizate oferite de furnizorul terț de servicii TIC, după care activele TIC respective nu mai beneficiază de asistență din partea furnizorului lor sau a unui furnizor terț de servicii TIC;
 - (c) pentru entitățile financiare, altele decât microîntreprinderile, impune obligația entităților financiare respective de a ține evidența informațiilor necesare pentru efectuarea unei evaluări specifice a riscurilor TIC cu privire la toate sistemele TIC existente menționate la articolul 8 alineatul (7) din Regulamentul (UE) 2022/2554.

Articolul 5

Procedura de gestionare a activelor TIC

- (1) Entitățile financiare elaborează, documentează și pun în aplicare o procedură de gestionare a activelor TIC.

(2) Procedura de gestionare a activelor TIC menționată la alineatul (1) specifică criteriile de efectuare a evaluării caracterului critic al activelor informaționale și al activelor TIC care sprijină funcțiile operaționale. Această evaluare ia în considerare:

- (a) riscul TIC legat de funcțiile operaționale respective și de dependențele acestora de activele informaționale sau de activele TIC;
- (b) modul în care pierderea confidențialității, a integrității și a disponibilității unor astfel de active informaționale și active TIC ar afecta procesele operaționale și activitățile entităților financiare.

Secțiunea 4

Criptarea și criptografia

Articolul 6

Criptarea și controalele criptografice

(1) Ca parte a politicilor, procedurilor, protocoalelor și instrumentelor de securitate TIC menționate la articolul 9 alineatul (2) din Regulamentul (UE) 2022/2554, entitățile financiare elaborează, documentează și pun în aplicare o politică privind criptarea și controalele criptografice.

(2) Entitățile financiare elaborează politica privind criptarea și controalele criptografice menționată la alineatul (1) pe baza rezultatelor unei clasificări aprobate a datelor și a unei evaluări a riscurilor TIC. Politica respectivă conține norme pentru toate elementele următoare:

- (a) criptarea datelor în repaus și în tranzit;
- (b) criptarea datelor în uz, dacă este necesar;
- (c) criptarea conexiunilor la rețeaua internă și a traficului cu părțile externe;
- (d) gestionarea cheilor criptografice menționată la articolul 7, prin stabilirea de norme privind utilizarea corectă, protecția și ciclul de viață al cheilor criptografice.

În sensul literei (b), în cazul în care criptarea datelor în uz nu este posibilă, entitățile financiare prelucrează datele în uz într-un mediu separat și protejat sau iau măsuri echivalente pentru a asigura confidențialitatea, integritatea, autenticitatea și disponibilitatea datelor.

(3) Entitățile financiare includ în politica privind criptarea și controalele criptografice menționată la alineatul (1) criterii pentru selectarea tehnicilor criptografice și a practicilor de utilizare, ținând seama de cele mai avansate practici și de standardele definite la articolul 2 alineatul (1) din Regulamentul (UE) nr. 1025/2012, precum și de clasificarea activelor TIC relevante stabilită în conformitate cu articolul 8 alineatul (1) din Regulamentul (UE) 2022/2554. Entitățile financiare care nu sunt în măsură să adere la cele mai avansate practici sau standarde sau să utilizeze cele mai fiabile tehnici adoptă măsuri de atenuare și monitorizare care asigură reziliența la amenințările cibernetice.

(4) Entitățile financiare includ în politica privind criptarea și controalele criptografice menționată la alineatul (1) dispoziții privind actualizarea sau modificarea, dacă este necesar, a tehnologiei criptografice pe baza evoluțiilor în materie de criptanaliză. Aceste actualizări sau modificări asigură faptul că tehnologia criptografică rămâne rezilientă la amenințările cibernetice, astfel cum se prevede la articolul 10 alineatul (2) litera (a). Entitățile financiare care nu sunt în măsură să actualizeze sau să modifice tehnologia criptografică adoptă măsuri de atenuare și monitorizare care asigură reziliența la amenințările cibernetice.

(5) Entitățile financiare includ în politica privind criptarea și controalele criptografice menționată la alineatul (1) o cerință de a înregistra adoptarea măsurilor de atenuare și de monitorizare adoptate în conformitate cu alineatele (3) și (4) și de a furniza o explicație motivată în acest sens.

Articolul 7

Gestionarea cheilor criptografice

- (1) Entitățile financiare includ în politica de gestionare a cheilor criptografice menționată la articolul 6 alineatul (2) litera (d) cerințe pentru gestionarea cheilor criptografice pe parcursul întregului lor ciclu de viață, inclusiv generarea, reînnoirea, stocarea, realizarea de copii de rezervă, arhivarea, extragerea, transmiterea, retragerea, revocarea și distrugerea cheilor criptografice respective.
- (2) Entitățile financiare identifică și pun în aplicare controale pentru a proteja cheile criptografice pe parcursul întregului lor ciclu de viață împotriva pierderii, accesului neautorizat, divulgării și modificării. Entitățile financiare concep controalele criptografice pe baza rezultatelor unei clasificări aprobate a datelor și a unei evaluări a riscurilor TIC.
- (3) Entitățile financiare elaborează și pun în aplicare metode de înlocuire a cheilor criptografice în caz de pierdere sau în cazul în care aceste chei sunt compromise sau deteriorate.
- (4) Entitățile financiare creează și mențin un registru pentru toate certificatele și dispozitivele de stocare a certificatelor cel puțin pentru activele TIC care sprijină funcții critice sau importante. Entitățile financiare actualizează registrul respectiv.
- (5) Entitățile financiare asigură reînnoirea promptă a certificatelor înainte de expirarea acestora.

Secțiunea 5

Securitatea operațiunilor TIC

Articolul 8

Politicele și procedurile pentru operațiunile TIC

- (1) Ca parte a politicilor, procedurilor, protocoalelor și instrumentelor de securitate TIC menționate la articolul 9 alineatul (2) din Regulamentul (UE) 2022/2554, entitățile financiare elaborează, documentează și pun în aplicare politici și proceduri de gestionare a operațiunilor TIC. Politicile și procedurile respective specifică modul în care entitățile financiare operează, monitorizează, controlează și restaurează activele TIC, inclusiv documentarea operațiunilor TIC.
- (2) Politicile și procedurile pentru operațiunile TIC menționate la alineatul (1) conțin toate elementele următoare:
 - (a) o descriere a activelor TIC, care include toate elementele următoare:
 - (i) cerințe privind instalarea, întreținerea, configurarea și dezinstalarea în condiții de siguranță a unui sistem TIC;
 - (ii) cerințe privind gestionarea activelor informaționale utilizate de activele TIC, inclusiv prelucrarea și manipularea acestora, atât în mod automatizat, cât și manual;
 - (iii) cerințe privind identificarea și controlul sistemelor TIC moștenite;
 - (b) controlul și monitorizarea sistemelor TIC, inclusiv toate elementele următoare:
 - (i) cerințe legate de copiile de rezervă și restaurarea sistemelor TIC;
 - (ii) cerințe privind programarea în timp, ținând seama de interdependențele dintre sistemele TIC;
 - (iii) protocoale privind informațiile din pista de audit și jurnalul sistemului;
 - (iv) cerințe pentru a se asigura că efectuarea auditului intern și a altor teste reduce la minimum perturbările activităților operaționale;
 - (v) cerințe privind separarea mediilor de producție TIC de mediile de dezvoltare, testare și alte medii care nu au legătură cu producția;
 - (vi) cerințe privind efectuarea dezvoltării și a testării în medii separate de mediul de producție;
 - (vii) cerințe privind efectuarea dezvoltării și a testării în medii de producție;

- (c) tratarea erorilor legate de sistemele TIC, inclusiv toate elementele următoare:
 - (i) proceduri și protocoale privind tratarea erorilor;
 - (ii) persoanele de contact pentru asistență și pentru escaladare, inclusiv persoanele de contact pentru asistență externă în cazul unor probleme operaționale sau tehnice neprevăzute;
 - (iii) procedurile de repornire, reactivare și recuperare a sistemului TIC care trebuie utilizate în caz de perturbări ale sistemului TIC.

În sensul literei (b) punctul (v), separarea ia în considerare toate componentele mediului, inclusiv conturile, datele sau conexiunile, astfel cum se prevede la articolul 13 primul paragraf litera (a).

În sensul literei (b) punctul (vii), politicile și procedurile menționate la alineatul (1) prevăd că situațiile în care se efectuează testarea într-un mediu de producție sunt clar identificate, motivate, realizate pe perioade limitate de timp și aprobate de funcția relevantă în conformitate cu articolul 16 alineatul (6). Entitățile financiare asigură disponibilitatea, confidențialitatea, integritatea și autenticitatea sistemelor TIC și a datelor de producție în timpul activităților de dezvoltare și testare în mediul de producție.

Articolul 9

Gestionarea capacității și a performanței

(1) Ca parte a politicilor, procedurilor, protocoalelor și instrumentelor de securitate TIC menționate la articolul 9 alineatul (2) din Regulamentul (UE) 2022/2554, entitățile financiare elaborează, documentează și pun în aplicare proceduri de gestionare a capacității și a performanței pentru următoarele:

- (a) identificarea cerințelor în materie de capacitate ale sistemelor lor TIC;
- (b) aplicarea optimizării resurselor;
- (c) procedurile de monitorizare pentru menținerea și îmbunătățirea:
 - (i) disponibilității datelor și a sistemelor TIC;
 - (ii) eficienței sistemelor TIC;
 - (iii) prevenirii deficitelor de capacitate TIC.

(2) Procedurile de gestionare a capacității și a performanței menționate la alineatul (1) asigură faptul că entitățile financiare iau măsurile adecvate pentru a ține seama de particularitățile sistemelor TIC cu procese lungi sau complexe de achiziție sau de aprobare sau ale sistemelor TIC care necesită multe resurse.

Articolul 10

Gestionarea vulnerabilităților și a corecțiilor

(1) Ca parte a politicilor, procedurilor, protocoalelor și instrumentelor de securitate TIC menționate la articolul 9 alineatul (2) din Regulamentul (UE) 2022/2554, entitățile financiare elaborează, documentează și pun în aplicare proceduri de gestionare a vulnerabilităților.

- (2) Procedurile de gestionare a vulnerabilităților menționate la alineatul (1):
 - (a) identifică și actualizează resursele de informații relevante și fiabile pentru a consolida și a menține gradul de conștientizare cu privire la vulnerabilități;
 - (b) asigură efectuarea scanării automate de vulnerabilități și a evaluărilor cu privire la activele TIC, frecvența și domeniul de aplicare al acestor activități fiind proporționale cu clasificarea stabilită în conformitate cu articolul 8 alineatul (1) din Regulamentul (UE) 2022/2554 și cu profilul general de risc al activului TIC;

- (c) verifică dacă:
 - (i) furnizorii terți de servicii TIC gestionează vulnerabilitățile legate de serviciile TIC furnizate entității financiare;
 - (ii) respectivii furnizori de servicii raportează entității financiare, în timp util, cel puțin vulnerabilitățile critice, precum și statisticile și tendințele;
- (d) monitorizează utilizarea:
 - (i) bibliotecilor terțe, inclusiv a bibliotecilor cu sursă deschisă, utilizate de serviciile TIC care sprijină funcții critice sau importante;
 - (ii) serviciilor TIC dezvoltate chiar de entitatea financiară ori personalizate sau dezvoltate în mod specific pentru entitatea financiară de către un furnizor terț de servicii TIC;
- (e) stabilesc proceduri pentru divulgarea responsabilă a vulnerabilităților către clienți, contrapărți și publicul larg;
- (f) acordă prioritate implementării corecțiilor și a altor măsuri de atenuare care abordează vulnerabilitățile identificate;
- (g) monitorizează și verifică remediarea vulnerabilităților;
- (h) impun înregistrarea oricărei vulnerabilități detectate care afectează sistemele TIC și monitorizarea soluționării acesteia.

În sensul literei (b), entitățile financiare efectuează cel puțin o dată pe săptămână scanarea automată de vulnerabilități și evaluările activelor TIC pentru activele TIC care sprijină funcții critice sau importante.

În sensul literei (c), entitățile financiare solicită furnizorilor terți de servicii TIC să investigheze vulnerabilitățile relevante, să stabilească cauzele principale și să pună în aplicare măsuri de atenuare adecvate.

În sensul literei (d), entitățile financiare monitorizează, după caz, în colaborare cu furnizorul terț de servicii TIC, versiunea și posibilele actualizări ale bibliotecilor terțe. În cazul activelor sau componentelor TIC gata de utilizare (*off-the-shelf*) ale activelor TIC achiziționate și utilizate în operarea serviciilor TIC care nu sprijină funcții critice sau importante, entitățile financiare monitorizează, în măsura posibilului, utilizarea bibliotecilor terțe, inclusiv a bibliotecilor cu sursă deschisă.

În sensul literei (f), entitățile financiare iau în considerare caracterul critic al vulnerabilității, clasificarea stabilită în conformitate cu articolul 8 alineatul (1) din Regulamentul (UE) 2022/2554 și profilul de risc al activelor TIC afectate de vulnerabilitățile identificate.

(3) Ca parte a politicilor, procedurilor, protocoalelor și instrumentelor de securitate TIC menționate la articolul 9 alineatul (2) din Regulamentul (UE) 2022/2554, entitățile financiare elaborează, documentează și pun în aplicare proceduri privind gestionarea corecțiilor.

- (4) Procedurile de gestionare a corecțiilor menționate la alineatul (3):
 - (a) identifică și evaluează, în măsura posibilului, corecțiile și actualizările de software și hardware disponibile cu ajutorul instrumentelor automatizate;
 - (b) identifică procedurile de urgență pentru corectarea și actualizarea activelor TIC;
 - (c) testează și implementează corecțiile și actualizările de software și hardware menționate la articolul 8 alineatul (2) litera (b) punctele (v), (vi) și (vii);
 - (d) stabilesc termene pentru instalarea corecțiilor și actualizărilor de software și hardware, precum și proceduri de escaladare în cazul în care aceste termene nu pot fi respectate.

Articolul 11

Securitatea datelor și a sistemului

(1) Ca parte a politicilor, procedurilor, protocoalelor și instrumentelor de securitate TIC menționate la articolul 9 alineatul (2) din Regulamentul (UE) 2022/2554, entitățile financiare elaborează, documentează și pun în aplicare o procedură privind securitatea datelor și a sistemului.

(2) Procedura de securitate a datelor și a sistemului menționată la alineatul (1) conține toate elementele următoare legate de securitatea datelor și a sistemelor TIC, în conformitate cu clasificarea stabilită conform articolului 8 alineatul (1) din Regulamentul (UE) 2022/2554:

- (a) restricțiile de acces menționate la articolul 21 din prezentul regulament, care sprijină cerințele de protecție pentru fiecare nivel de clasificare;
- (b) identificarea unui configurații de referință securizate pentru activele TIC care reduce la minimum expunerea activelor TIC respective la amenințările cibernetice și măsuri prin care se verifică periodic dacă setările de referință respective sunt implementate în mod eficace;
- (c) identificarea măsurilor de securitate pentru a se asigura că numai software-ul autorizat este instalat în sistemele TIC și în dispozitivele de punct final;
- (d) identificarea măsurilor de securitate împotriva codurilor dăunătoare;
- (e) identificarea măsurilor de securitate pentru a se asigura că se utilizează numai medii de stocare a datelor, sisteme și dispozitive de punct final autorizate pentru transferul și stocarea datelor entității financiare;
- (f) următoarele cerințe pentru a se asigura utilizarea în condiții de siguranță a dispozitivelor de punct final portabile și a dispozitivelor de punct final neportabile private:
 - (i) cerința de a utiliza o soluție de gestionare pentru a gestiona de la distanță dispozitivele de punct final și a șterge de la distanță datele entității financiare;
 - (ii) cerința de a utiliza mecanisme de securitate care nu pot fi modificate, eliminate sau ocolite de membrii personalului sau de furnizorii terți de servicii TIC în mod neautorizat;
 - (iii) cerința de a utiliza dispozitive amovibile de stocare a datelor numai în cazul în care riscul TIC rezidual rămâne în limitele nivelului de toleranță la risc al entității financiare menționat la articolul 3 primul paragraf litera (a);
- (g) procesul de ștergere în condiții de siguranță a datelor, aflate în sediile entității financiare sau stocate extern, pe care entitatea financiară nu mai are nevoie să le colecteze sau să le stocheze;
- (h) procesul de eliminare sau scoatere din uz în condiții de siguranță a dispozitivelor de stocare a datelor, aflate în sediile entității financiare sau stocate extern, care conțin informații confidențiale;
- (i) identificarea și punerea în aplicare a unor măsuri de securitate pentru a preveni pierderea și scurgerile de date pentru sistemele și dispozitivele de punct final;
- (j) punerea în aplicare a unor măsuri de securitate pentru a se asigura că telemunca și utilizarea dispozitivelor de punct final private nu au un impact negativ asupra securității TIC a entității financiare;
- (k) pentru activele sau serviciile TIC operate de un furnizor terț de servicii TIC, identificarea și punerea în aplicare a cerințelor de menținere a rezilienței operaționale digitale, în conformitate cu rezultatele clasificării datelor și ale evaluării riscurilor TIC.

În sensul literei (b), configurația de referință securizată menționată la litera respectivă ține seama de cele mai avansate practici și tehnici adecvate prevăzute în standardele definite la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012.

În sensul literei (k), entitățile financiare iau în considerare următoarele:

- (a) punerea în aplicare a setărilor recomandate de vânzător cu privire la elementele operate de entitatea financiară;
- (b) o alocare clară a rolurilor și responsabilităților în materie de securitate a informațiilor între entitatea financiară și furnizorul terț de servicii TIC, în conformitate cu principiul responsabilității depline a entității financiare pentru furnizorul său terț de servicii TIC, astfel cum se menționează la articolul 28 alineatul (1) litera (a) din Regulamentul (UE) 2022/2554, și pentru entitățile financiare menționate la articolul 28 alineatul (2) din regulamentul respectiv și în conformitate cu politica entității financiare privind utilizarea serviciilor TIC care sprijină funcții critice sau importante;
- (c) necesitatea de a asigura și de a menține competențe adecvate în cadrul entității financiare în ceea ce privește gestionarea și securitatea serviciului utilizat;
- (d) măsuri tehnice și organizatorice pentru a reduce la minimum riscurile legate de infrastructura utilizată de furnizorul terț de servicii TIC pentru serviciile sale TIC, ținând seama de cele mai avansate practici și de standardele definite la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012.

*Articolul 12***Jurnalizarea**

- (1) Ca parte a măsurilor de protecție împotriva intruziunilor și a utilizării abuzive a datelor, entitățile financiare elaborează, documentează și pun în aplicare proceduri, protocoale și instrumente de jurnalizare.
- (2) Procedurile, protocoalele și instrumentele de jurnalizare menționate la alineatul (1) conțin toate elementele următoare:
- (a) identificarea evenimentelor care urmează să fie înregistrate în jurnale, perioada de păstrare a jurnalelor și măsurile de asigurare a securității și de gestionare a datelor din jurnal, având în vedere scopul pentru care sunt create jurnalele;
 - (b) alinierea nivelului de detaliu al jurnalelor la scopul și utilizarea acestora pentru a permite detectarea eficace a activităților anormale, astfel cum se menționează la articolul 24;
 - (c) cerința de a înregistra în jurnal evenimentele legate de toate elementele următoare:
 - (i) controlul accesului logic și al accesului fizic, astfel cum se menționează la articolul 21, și gestionarea identității;
 - (ii) gestionarea capacității;
 - (iii) gestionarea modificărilor;
 - (iv) operațiunile TIC, inclusiv activitățile legate de sistemele TIC;
 - (v) activitățile de trafic în rețea, inclusiv performanța rețelei TIC;
 - (d) măsuri de protecție a sistemelor de jurnalizare și a informațiilor din jurnale împotriva manipulării frauduloase, a ștergerii și a accesului neautorizat în repaus, în tranzit și, dacă este cazul, în uz;
 - (e) măsuri de detectare a unei defecțiuni a sistemelor de jurnalizare;
 - (f) fără a aduce atingere niciunei cerințe de reglementare aplicabile în temeiul dreptului Uniunii sau al dreptului intern, sincronizarea ceasurilor fiecăruia dintre sistemele TIC ale entității financiare pe baza unei surse de indicare a timpului de referință fiabile și documentate.

În sensul literei (a), entitățile financiare stabilesc perioada de păstrare, ținând seama de obiectivele în materie de securitate a activității și a informațiilor, de motivul înregistrării evenimentului în jurnal și de rezultatele evaluării riscurilor TIC.

*Secțiunea 6***Securitatea rețelelor***Articolul 13***Gestionarea securității rețelelor**

Ca parte a garanțiilor care asigură securitatea rețelelor împotriva intruziunilor și a utilizării abuzive a datelor, entitățile financiare elaborează, documentează și pun în aplicare politici, proceduri, protocoale și instrumente privind gestionarea securității rețelelor, inclusiv toate elementele următoare:

- (a) segregarea și segmentarea sistemelor și rețelelor TIC, ținând seama de:
 - (i) caracterul critic sau importanța funcției pe care o sprijină sistemele și rețelele TIC respective;
 - (ii) clasificarea stabilită în conformitate cu articolul 8 alineatul (1) din Regulamentul (UE) 2022/2554;
 - (iii) profilul general de risc al activelor TIC care utilizează sistemele și rețelele TIC respective;
- (b) documentarea tuturor conexiunilor la rețea și fluxurilor de date ale entității financiare;
- (c) utilizarea unei rețele separate și specializate pentru gestionarea activelor TIC;
- (d) identificarea și punerea în aplicare a controalelor accesului la rețea pentru a preveni și a detecta conexiunile la rețeaua entității financiare prin orice dispozitiv sau sistem neautorizat sau orice punct final care nu îndeplinește cerințele de securitate ale entității financiare;

- (e) criptarea conexiunilor la rețea care trec prin rețele corporative, rețele publice, rețele naționale, rețele terțe și rețele fără fir, pentru protocoalele de comunicare utilizate, ținând seama de rezultatele clasificării aprobate a datelor, de rezultatele evaluării riscurilor TIC și de criptarea conexiunilor de rețea menționate la articolul 6 alineatul (2);
- (f) proiectarea rețelelor în conformitate cu cerințele de securitate TIC stabilite de entitatea financiară, ținând seama de cele mai avansate practici pentru a asigura confidențialitatea, integritatea și disponibilitatea rețelei;
- (g) securizarea traficului de rețea între rețelele interne și internet și alte conexiuni externe;
- (h) identificarea rolurilor și responsabilităților și a etapelor pentru specificarea, punerea în aplicare, aprobarea, modificarea și revizuirea regulilor firewall și a filtrelor de conexiuni;
- (i) efectuarea de revizuiți ale arhitecturii rețelei și ale modului în care este concepută securitatea rețelei o dată pe an și periodic pentru microîntreprinderi, pentru a se identifica potențialele vulnerabilități;
- (j) măsurile de izolare temporară, dacă este necesar, a subrețelelor și a componentelor și dispozitivelor de rețea;
- (k) implementarea unei configurații de referință securizate pentru toate componentele rețelei și întărirea rețelei și a dispozitivelor de rețea, în conformitate cu eventualele instrucțiuni ale furnizorului, după caz, precum și cu standardele definite la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012 și cu cele mai avansate practici;
- (l) procedurile de limitare, blocare și închidere a sistemului și a sesiunilor la distanță după o anumită perioadă de inactivitate;
- (m) pentru acordurile de servicii de rețea:
 - (i) identificarea și specificarea măsurilor TIC și de securitate a informațiilor, a nivelurilor serviciilor și a cerințelor de gestionare a tuturor serviciilor de rețea;
 - (ii) dacă aceste servicii sunt furnizate de un furnizor de servicii TIC intragrup sau de furnizori terți de servicii TIC.

În sensul literei (h), entitățile financiare efectuează revizuirea regulilor firewall și a filtrelor de conexiuni în mod regulat, în conformitate cu clasificarea stabilită conform articolului 8 alineatul (1) din Regulamentul (UE) 2022/2554 și cu profilul general de risc al sistemelor TIC implicate. Pentru sistemele TIC care sprijină funcții critice sau importante, entitățile financiare verifică adecvarea regulilor firewall existente și a filtrelor de conectare cel puțin o dată la 6 luni.

Articolul 14

Securitatea informațiilor în tranzit

(1) Ca parte a garanțiilor de menținere a disponibilității, autenticității, integrității și confidențialității datelor, entitățile financiare elaborează, documentează și pun în aplicare politici, proceduri, protocoale și instrumente pentru protejarea informațiilor în tranzit. Entitățile financiare asigură, în special, toate elementele următoare:

- (a) disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor în timpul transmiterii în rețea și stabilirea unor proceduri de evaluare a conformității cu aceste cerințe;
- (b) prevenirea și detectarea scurgerilor de date și transferul securizat de informații între entitatea financiară și părțile externe;
- (c) punerea în aplicare, documentarea și revizuirea periodică a cerințelor privind acordurile de confidențialitate sau de nedivulgare care reflectă nevoile entității financiare de protecție a informațiilor, atât pentru personalul entității financiare, cât și pentru terți.

(2) Entitățile financiare elaborează politicile, procedurile, protocoalele și instrumentele pentru protejarea informațiilor în tranzit menționate la alineatul (1) pe baza rezultatelor clasificării aprobate a datelor și a evaluării riscurilor TIC.

Secțiunea 7

Gestionarea proiectelor și a modificărilor TIC

Articolul 15

Gestionarea proiectelor TIC

- (1) Ca parte a garanțiilor de menținere a disponibilității, autenticității, integrității și confidențialității datelor, entitățile financiare elaborează, documentează și pun în aplicare o politică de gestionare a proiectelor TIC.
- (2) Politica de gestionare a proiectelor TIC menționată la alineatul (1) specifică elementele care asigură gestionarea eficace a proiectelor TIC legate de achiziționarea, întreținerea și, după caz, dezvoltarea sistemelor TIC ale entității financiare.
- (3) Politica de gestionare a proiectelor TIC menționată la alineatul (1) include toate elementele următoare:
- (a) obiectivele proiectelor TIC;
 - (b) guvernanta proiectelor TIC, inclusiv rolurile și responsabilitățile;
 - (c) planificarea, calendarul și etapele proiectelor TIC;
 - (d) evaluarea riscurilor proiectelor TIC;
 - (e) etapele relevante;
 - (f) cerințele privind gestionarea modificărilor;
 - (g) testarea tuturor cerințelor, inclusiv a cerințelor de securitate, și a procesului de aprobare corespunzător atunci când se implementează un sistem TIC în mediul de producție.
- (4) Politica de gestionare a proiectelor TIC menționată la alineatul (1) asigură punerea în aplicare securizată a proiectelor TIC prin furnizarea informațiilor și a expertizei necesare din domeniul de activitate sau funcțiile afectate de proiectul TIC.
- (5) În conformitate cu evaluarea riscurilor proiectelor TIC menționată la alineatul (3) litera (d), politica de gestionare a proiectelor TIC menționată la alineatul (1) prevede că elaborarea și progresele proiectelor TIC care au un impact asupra funcțiilor critice sau importante ale entității financiare și riscurile asociate acestora trebuie raportate organului de conducere după cum urmează:
- (a) individual sau agregat, în funcție de importanța și dimensiunea proiectelor TIC;
 - (b) periodic și, dacă este necesar, de fiecare dată când un eveniment impune acest lucru.

Articolul 16

Achiziționarea, dezvoltarea și întreținerea sistemelor TIC

- (1) Ca parte a garanțiilor de menținere a disponibilității, autenticității, integrității și confidențialității datelor, entitățile financiare elaborează, documentează și pun în aplicare o politică aplicabilă achiziționării, dezvoltării și întreținerii sistemelor TIC. Această politică:
- (a) identifică practicile și metodologiile de securitate legate de achiziționarea, dezvoltarea și întreținerea sistemelor TIC;
 - (b) impune identificarea:
 - (i) specificațiilor tehnice și a specificațiilor tehnice TIC, astfel cum sunt definite la articolul 2 punctele 4 și 5 din Regulamentul (UE) nr. 1025/2012;
 - (ii) cerințelor referitoare la achiziționarea, dezvoltarea și întreținerea sistemelor TIC, cu un accent deosebit pe cerințele de securitate TIC și pe aprobarea acestora de către funcția operațională relevantă și de către proprietarul activelor TIC în conformitate cu mecanismele de guvernanta internă ale entității financiare;

- (c) specifică măsurile de atenuare a riscului de modificare neintenționată sau de manipulare intenționată a sistemelor TIC în timpul dezvoltării, întreținerii și implementării sistemelor TIC respective în mediul de producție.

(2) Entitățile financiare elaborează, documentează și pun în aplicare o procedură de achiziționare, dezvoltare și întreținere a sistemelor TIC pentru testarea și aprobarea tuturor sistemelor TIC înainte de utilizarea acestora și după întreținere, în conformitate cu articolul 8 alineatul (2) litera (b) punctele (v), (vi) și (vii). Nivelul de testare este proporțional cu caracterul critic al procedurilor operaționale și al activelor TIC în cauză. Testarea este concepută în așa fel încât să se poată verifica dacă noile sisteme TIC sunt adecvate pentru a funcționa conform așteptărilor, inclusiv calitatea software-ului dezvoltat la nivel intern.

În plus față de cerințele prevăzute la primul paragraf, contrapărțile centrale implică, după caz, în conceperea și efectuarea testelor menționate la primul paragraf:

- (a) membrii compensatori și clienții;
- (b) contrapărțile centrale interoperabile;
- (c) alte părți interesate.

În plus față de cerințele prevăzute la primul paragraf, depozitarii centrali de titluri de valoare implică, după caz, în conceperea și efectuarea testelor menționate la primul paragraf:

- (a) utilizatorii;
- (b) furnizorii de utilități critice și de servicii critice;
- (c) alți depozitari centrali de titluri de valoare;
- (d) alte infrastructuri ale pieței;
- (e) orice alte instituții cu care depozitarii centrali de titluri de valoare au identificat interdependențe în politica lor de continuitate a activității.

(3) Procedura menționată la alineatul (2) conține efectuarea revizuirilor codurilor sursă care acoperă atât testarea statică, cât și testarea dinamică. Testarea respectivă include teste de securitate pentru sistemele și aplicațiile expuse la internet în conformitate cu articolul 8 alineatul (2) litera (b) punctele (v), (vi) și (vii). Entitățile financiare:

- (a) identifică și analizează vulnerabilitățile și anomaliile codului sursă;
- (b) adoptă un plan de acțiune pentru a aborda aceste vulnerabilități și anomalii;
- (c) monitorizează punerea în aplicare a planului de acțiune respectiv.

(4) Procedura menționată la alineatul (2) conține testarea de securitate a pachetelor software cel târziu în etapa de integrare, în conformitate cu articolul 8 alineatul (2) litera (b) punctele (v), (vi) și (vii).

(5) Procedura menționată la alineatul (2) prevede că:

- (a) mediile care nu au legătură cu producția stochează numai date de producție anonimizate, pseudonimizate sau randomizate;
- (b) entitățile financiare trebuie să protejeze integritatea și confidențialitatea datelor în mediile care nu au legătură cu producția.

(6) Prin derogare de la alineatul (5), procedura menționată la alineatul (2) poate prevedea că datele de producție sunt stocate numai pentru situații de testare specifice, pentru perioade limitate de timp și în urma aprobării de către funcția relevantă și a raportării acestor situații către funcția de gestionare a riscurilor TIC.

(7) Procedura menționată la alineatul (2) conține punerea în aplicare a unor controale menite să protejeze integritatea codului sursă al sistemelor TIC care sunt dezvoltate intern sau care sunt dezvoltate de către un furnizor terț de servicii TIC și livrate entității financiare de către un furnizor terț de servicii TIC.

(8) Procedura menționată la alineatul (2) prevede că software-ul brevetat și, dacă este fezabil, codul sursă care este furnizat de furnizorii terți de servicii TIC sau care provine din proiecte cu sursă deschisă trebuie analizate și testate în conformitate cu alineatul (3) înainte de implementarea lor în mediul de producție.

(9) Alineatele (1)-(8) de la prezentul articol se aplică, de asemenea, sistemelor TIC dezvoltate sau gestionate de utilizatori din afara funcției TIC, utilizând o abordare bazată pe riscuri.

Articolul 17

Gestionarea modificărilor TIC

(1) Ca parte a garanțiilor pentru menținerea disponibilității, autenticității, integrității și confidențialității datelor, entitățile financiare includ în procedurile de gestionare a modificărilor TIC menționate la articolul 9 alineatul (4) litera (e) din Regulamentul (UE) 2022/2554, în ceea ce privește toate modificările aduse componentelor software, hardware sau firmware, sistemelor sau parametrilor de securitate, toate elementele următoare:

- (a) o verificare a îndeplinirii cerințelor de securitate TIC;
- (b) mecanisme de asigurare a independenței funcțiilor care aprobă modificările și a funcțiilor responsabile cu solicitarea și punerea în aplicare a modificărilor respective;
- (c) o descriere clară a rolurilor și responsabilităților pentru a se asigura că:
 - (i) modificările sunt specificate și planificate;
 - (ii) o tranziție adecvată este concepută;
 - (iii) modificările sunt testate și finalizate într-un mod controlat;
 - (iv) există o asigurare a calității efectivă;
- (d) documentația și comunicarea detaliilor modificării, inclusiv:
 - (i) scopul și domeniul de aplicare ale modificării;
 - (ii) calendarul de punere în aplicare a modificării;
 - (iii) rezultatele preconizate;
- (e) identificarea procedurilor și responsabilităților de rezervă, inclusiv a procedurilor și responsabilităților pentru abandonarea modificărilor sau recuperarea în urma modificărilor care nu au fost puse în aplicare cu succes;
- (f) proceduri, protocoale și instrumente de gestionare a modificărilor de urgență care oferă garanții adecvate;
- (g) proceduri pentru documentarea, reevaluarea, evaluarea și aprobarea modificărilor de urgență după punerea lor în aplicare, inclusiv soluții alternative și corecții;
- (h) identificarea impactului potențial al unei modificări asupra măsurilor de securitate TIC existente și o evaluare a necesității de a adopta măsuri suplimentare de securitate TIC.

(2) După ce aduc modificări semnificative sistemelor lor TIC, contrapărțile centrale și depozitarii centrali de titluri de valoare își supun sistemele TIC unor teste stricte prin simularea condițiilor de criză.

Contrapărțile centrale implică, după caz, în conceperea și efectuarea testelor menționate la primul paragraf:

- (a) membrii compensatori și clienții;
- (b) contrapărțile centrale interoperabile;
- (c) alte părți interesate;

Depozitarii centrali de titluri de valoare implică, după caz, în conceperea și efectuarea testelor menționate la primul paragraf:

- (a) utilizatorii;
- (b) furnizorii de utilități critice și de servicii critice;

- (c) alți depozitari centrali de titluri de valoare;
- (d) alte infrastructuri ale pieței;
- (e) orice alte instituții cu care depozitarii centrali de titluri de valoare au identificat interdependențe în politica lor de continuitate a activității TIC.

Secțiunea 8

Articolul 18

Securitatea fizică și de mediu

(1) Ca parte a garanțiilor de menținere a disponibilității, autenticității, integrității și confidențialității datelor, entitățile financiare specifică, documentează și pun în aplicare o politică de securitate fizică și de mediu. Entitățile financiare concep această politică în funcție de peisajul amenințărilor cibernetice, în conformitate cu clasificarea stabilită în conformitate cu articolul 8 alineatul (1) din Regulamentul (UE) 2022/2554 și având în vedere profilul general de risc al activelor TIC și al activelor informaționale accesibile.

(2) Politica de securitate fizică și de mediu menționată la alineatul (1) include toate elementele următoare:

- (a) o trimitere la secțiunea din politica privind controlul drepturilor de gestionare a accesului menționată la articolul 21 primul paragraf litera (g);
- (b) măsuri de protecție a sediilor, a centrelor de date ale entității financiare și a zonelor sensibile desemnate identificate de entitatea financiară în care sunt situate activele TIC și activele informaționale împotriva atacurilor, a accidentelor și a amenințărilor și pericolelor de mediu;
- (c) măsuri de securizare a activelor TIC, atât în interiorul, cât și în afara sediului entității financiare, ținând seama de rezultatele evaluării riscurilor TIC legate de activele TIC relevante;
- (d) măsuri de asigurare a disponibilității, autenticității, integrității și confidențialității activelor TIC, a activelor informaționale și a dispozitivelor de control al accesului fizic ale entității financiare prin asigurarea întreținerii adecvate;
- (e) măsuri de menținere a disponibilității, autenticității, integrității și confidențialității datelor, inclusiv:
 - (i) o politică de tip birou curat pentru documente;
 - (ii) o politică de tip ecran curat pentru unitățile de prelucrare a informațiilor.

În sensul literei (b), măsurile de protecție împotriva amenințărilor și pericolelor de mediu sunt proporționale cu importanța sediilor, a centrelor de date și a zonelor sensibile desemnate și cu caracterul critic al operațiunilor sau al sistemelor TIC situate în acestea.

În sensul literei (c), politica de securitate fizică și de mediu menționată la alineatul (1) conține măsuri de asigurare a unei protecții adecvate a activelor TIC nesupravegheate.

CAPITOLUL II

Politica de resurse umane și controlul accesului

Articolul 19

Politica de resurse umane

Entitățile financiare includ în politica lor de resurse umane sau în alte politici relevante toate elementele următoare legate de securitatea TIC:

- (a) identificarea și atribuirea oricăror responsabilități specifice în materie de securitate TIC;
- (b) cerințe aplicabile membrilor personalului entității financiare și al furnizorilor terți de servicii TIC care utilizează sau accesează activele TIC ale entității financiare astfel încât:
 - (i) să fie informați cu privire la politicile, procedurile și protocoalele de securitate TIC ale entității financiare și să adere la acestea;
 - (ii) să aibă cunoștință de canalele de raportare instituite de entitatea financiară pentru detectarea comportamentului anormal, inclusiv, după caz, canalele de raportare instituite în conformitate cu Directiva (UE) 2019/1937 a Parlamentului European și a Consiliului ⁽¹⁾;
 - (iii) pentru membrii personalului, să returneze entității financiare, la încetarea contractului de muncă, toate activele TIC și activele informaționale corporale aflate în posesia lor care aparțin entității financiare.

Articolul 20

Gestionarea identității

- (1) Ca parte a controlului pe care îl exercită asupra drepturilor de gestionare a accesului, entitățile financiare elaborează, documentează și pun în aplicare politici și proceduri de gestionare a identității care asigură identificarea și autentificarea unică a persoanelor fizice și a sistemelor care accesează informațiile entităților financiare pentru a permite alocarea drepturilor de acces ale utilizatorilor în conformitate cu articolul 21.
- (2) Politicile și procedurile de gestionare a identității menționate la alineatul (1) conțin toate elementele următoare:
- (a) fără a aduce atingere articolului 21 primul paragraf litera (c), se atribuie o identitate unică corespunzătoare unui cont de utilizator unic fiecărui membru al personalului entității financiare sau fiecărui membru al personalului furnizorilor terți de servicii TIC care accesează activele informaționale și activele TIC ale entității financiare;
 - (b) un proces de gestionare a ciclului de viață pentru identități și conturi care gestionează crearea, modificarea, revizuirea și actualizarea, dezactivarea temporară și închiderea tuturor conturilor.

În sensul literei (a), entitățile financiare păstrează evidențe ale tuturor identităților atribuite. Evidențele respective se păstrează în urma unei reorganizări a entității financiare sau după încetarea relației contractuale, fără a aduce atingere cerințelor de păstrare prevăzute în dreptul Uniunii și în dreptul intern aplicabil.

În sensul literei (b), entitățile financiare implementează, atunci când este fezabil și adecvat, soluții automatizate pentru procesul de gestionare a identității pe durata ciclului de viață.

Articolul 21

Controlul accesului

Ca parte a controlului pe care îl exercită asupra drepturilor de gestionare a accesului, entitățile financiare elaborează, documentează și pun în aplicare o politică ce conține toate elementele următoare:

- (a) atribuirea drepturilor de acces la activele TIC pe baza principiului necesității de a cunoaște, al necesității de a utiliza și al celor mai mici privilegii, inclusiv pentru accesul la distanță și de urgență;
- (b) separarea sarcinilor pentru a preveni accesul nejustificat la datele critice sau a preveni alocarea combinațiilor de drepturi de acces care ar putea fi utilizate pentru eludarea controalelor;
- (c) o dispoziție privind răspunderea utilizatorului, prin limitarea, în măsura posibilului, a utilizării conturilor de utilizator generice și partajate și prin asigurarea faptului că utilizatorii sunt identificabili pentru acțiunile pe care le efectuează în sistemele TIC în orice moment;

⁽¹⁾ Directiva (UE) 2019/1937 a Parlamentului European și a Consiliului din 23 octombrie 2019 privind protecția persoanelor care raportează încălcări ale dreptului Uniunii (JO L 305, 26.11.2019, p. 17, ELI: <http://data.europa.eu/eli/dir/2019/1937/oj>).

- (d) o dispoziție privind restricțiile de acces la activele TIC, care să stabilească controalele și instrumentele de prevenire a accesului neautorizat;
- (e) proceduri de gestionare a conturilor pentru acordarea, modificarea sau revocarea drepturilor de acces pentru conturile de utilizator și conturile generice, inclusiv pentru conturile de administrator generice, care conțin dispoziții privind toate elementele următoare:
 - (i) atribuirea rolurilor și a responsabilităților pentru acordarea, revizuirea și revocarea drepturilor de acces;
 - (ii) atribuirea accesului privilegiat, a accesului în situații de urgență și a accesului cu drepturi de administrator pe baza principiului necesității de a utiliza sau ad-hoc pentru toate sistemele TIC;
 - (iii) retragerea drepturilor de acces fără întârzieri nejustificate la încetarea contractului de muncă sau atunci când accesul nu mai este necesar;
 - (iv) actualizarea drepturilor de acces în cazul în care sunt necesare modificări și cel puțin o dată pe an pentru toate sistemele TIC, altele decât sistemele TIC care sprijină funcții critice sau importante și cel puțin o dată la 6 luni pentru sistemele TIC care sprijină funcții critice sau importante;
- (f) metode de autentificare care includ toate elementele următoare:
 - (i) utilizarea unor metode de autentificare proporționale cu clasificarea stabilită în conformitate cu articolul 8 alineatul (1) din Regulamentul (UE) 2022/2554 și cu profilul general de risc al activelor TIC și luând în considerare cele mai avansate practici;
 - (ii) utilizarea unor metode de autentificare puternice în conformitate cu cele mai avansate practici și tehnici pentru accesul de la distanță la rețeaua entității financiare, pentru accesul privilegiat și pentru accesul la active TIC care sprijină funcții critice sau importante sau la active TIC accesibile publicului;
- (g) măsuri de control al accesului fizic care includ:
 - (i) identificarea și înregistrarea persoanelor fizice autorizate să aibă acces la sedii, centre de date și zone sensibile desemnate identificate de entitatea financiară în care sunt situate activele TIC și informaționale;
 - (ii) acordarea drepturilor de acces fizic la activele TIC esențiale numai persoanelor autorizate, în conformitate cu principiul necesității de a cunoaște și al celor mai mici privilegii și ad-hoc;
 - (iii) monitorizarea accesului fizic la sedii, centre de date și zone sensibile desemnate identificate de entitatea financiară în care sunt se află activele TIC și/sau informaționale;
 - (iv) revizuirea drepturilor fizice de acces pentru a se asigura că se revocă prompt drepturile de acces inutile.

În sensul literei (e) punctul (i), entitățile financiare stabilesc perioada de păstrare, ținând seama de obiectivele în materie de securitate a activității și a informațiilor, de motivele înregistrării evenimentului în jurnal și de rezultatele evaluării riscurilor TIC.

În sensul literei (e) punctul (ii), entitățile financiare utilizează, în măsura posibilului, conturi specifice pentru îndeplinirea sarcinilor administrative legate de sistemele TIC. Atunci când este fezabil și adecvat, entitățile financiare implementează soluții automatizate pentru gestionarea accesului privilegiat.

În sensul literei (g) punctul (i), identificarea și jurnalizarea sunt proporționale cu importanța sediilor, a centrelor de date și a zonelor sensibile desemnate și cu caracterul critic al operațiunilor sau al sistemelor TIC situate în acestea.

În sensul literei (g) punctul (iii), monitorizarea este proporțională cu clasificarea stabilită în conformitate cu articolul 8 alineatul (1) din Regulamentul (UE) 2022/2554 și cu caracterul critic al zonei accesate.

CAPITOLUL III

Detectarea incidentelor legate de tic și răspunsul la acestea

Articolul 22

Politica de gestionare a incidentelor legate de TIC

Ca parte a mecanismelor de detectare a activităților anormale, inclusiv a problemelor de performanță a rețelelor TIC și a incidentelor legate de TIC, entitățile financiare elaborează, documentează și pun în aplicare o politică privind incidentele legate de TIC prin care:

- (a) documentează procesul de gestionare a riscurilor TIC menționat la articolul 17 din Regulamentul (UE) 2022/2554;
- (b) stabilesc o listă a contactelor relevante cu funcțiile interne și cu părțile interesate externe care sunt direct implicate în securitatea operațiunilor TIC, inclusiv în ceea ce privește:
 - (i) detectarea și monitorizarea amenințărilor cibernetice;
 - (ii) detectarea activităților anormale;
 - (iii) gestionarea vulnerabilităților;
- (c) instituie, pun în aplicare și operează mecanisme tehnice, organizaționale și operaționale pentru a sprijini procesul de gestionare a incidentelor legate de TIC, inclusiv mecanisme care permit detectarea rapidă a activităților și comportamentelor anormale în conformitate cu articolul 23 din prezentul regulament;
- (d) păstrează toate dovezile referitoare la incidentele legate de TIC pentru o perioadă care nu este mai lungă decât ceea ce este necesar în scopurile pentru care sunt colectate datele și care este proporțională cu caracterul critic al funcțiilor operaționale, al proceselor de sprijin și al activelor TIC și informaționale afectate, în conformitate cu articolul 15 din Regulamentul delegat (UE) 2024/1772 al Comisiei ⁽¹²⁾ și cu orice cerință de păstrare aplicabilă în temeiul dreptului Uniunii;
- (e) instituie și pun în aplicare mecanisme de analiză a incidentelor semnificative sau recurente legate de TIC și a tiparelor în ceea ce privește numărul și apariția incidentelor legate de TIC.

În sensul literei (d), entitățile financiare păstrează dovezile menționate la litera respectivă în condiții de securitate.

Articolul 23

Detectarea activităților anormale și criterii pentru detectarea incidentelor legate de TIC și răspunsul la acestea

(1) Entitățile financiare stabilesc roluri și responsabilități clare pentru a detecta și a răspunde în mod eficace la incidentele legate de TIC și la activitățile anormale.

(2) Mecanismul de detectare rapidă a activităților anormale, inclusiv a problemelor legate de performanța rețelei TIC și a incidentelor legate de TIC, astfel cum este menționat la articolul 10 alineatul (1) din Regulamentul (UE) 2022/2554, le permite entităților financiare:

- (a) să colecteze, să monitorizeze și să analizeze toate elementele următoare:
 - (i) factorii interni și externi, incluzând cel puțin jurnalele colectate în conformitate cu articolul 12 din prezentul regulament, informațiile de la funcțiile operaționale și funcțiile TIC, precum și orice problemă raportată de utilizatorii entității financiare;
 - (ii) potențialele amenințări cibernetice interne și externe, ținând seama de scenariile utilizate în mod obișnuit de actorii care generează amenințări și de scenariile bazate pe activitatea de colectare a informațiilor privind amenințările;

⁽¹²⁾ Regulamentul delegat (UE) 2024/1772 al Comisiei din 13 martie 2024 de completare a Regulamentului (UE) 2022/2554 al Parlamentului European și al Consiliului în ceea ce privește standardele tehnice de reglementare care precizează criteriile de clasificare a incidentelor legate de TIC și a amenințărilor cibernetice, stabilesc pragurile de semnificație și detaliile rapoartelor privind incidentele majore (JO L, 2024/1772, 25.6.2024 ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj)

- (iii) notificarea, de către un furnizor terț de servicii TIC al entității financiare, a incidentelor legate de TIC care sunt detectate în sistemele și rețelele TIC ale furnizorului terț de servicii TIC și care ar putea afecta entitatea financiară;
- (b) să identifice activitățile și comportamentele anormale și să pună în aplicare instrumente care generează alerte pentru activități și comportamente anormale, cel puțin pentru activele TIC și activele informaționale care sprijină funcții critice sau importante;
- (c) să acorde prioritate alertelor menționate la litera (b) pentru a permite gestionarea incidentelor legate de TIC detectate în termenul de soluționare prevăzut, astfel cum este specificat de entitățile financiare, atât în timpul programului de lucru, cât și în afara acestuia;
- (d) să înregistreze, să analizeze și să evalueze, în mod automat sau manual, informațiile relevante privind toate activitățile și comportamentele anormale.

În sensul literei (b), instrumentele menționate la litera respectivă conțin instrumente care generează alerte automate bazate pe reguli predefinite pentru identificarea anomaliilor care afectează exhaustivitatea și integritatea surselor de date sau colectarea jurnalelor.

- (3) Entitățile financiare protejează orice înregistrare a activităților anormale împotriva manipulării frauduloase și a accesului neautorizat în repaus, în tranzit și, dacă este cazul, în uz.
- (4) Entitățile financiare înregistrează într-un jurnal, pentru fiecare activitate anormală detectată, toate informațiile relevante care permit:
 - (a) identificarea datei și a orei apariției activității anormale;
 - (b) identificarea datei și a orei detectării activității anormale;
 - (c) identificarea tipului de activitate anormală.
- (5) Entitățile financiare iau în considerare toate criteriile următoare pentru a declanșa procesele de detectare a incidentelor legate de TIC și de răspuns la acestea, astfel cum sunt menționate la articolul 10 alineatul (2) din Regulamentul (UE) 2022/2554:
 - (a) indicii din care să reiasă că este posibil ca o activitate răuvoitoare să fi fost desfășurată într-un sistem sau într-o rețea TIC sau că este posibil ca sistemul sau rețeaua TIC să fi fost compromis(ă);
 - (b) pierderile de date detectate în legătură cu disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor;
 - (c) impactul negativ detectat asupra tranzacțiilor și operațiunilor entității financiare;
 - (d) indisponibilitatea sistemelor și a rețelelor TIC.
- (6) În sensul alineatului (5), entitățile financiare iau în considerare, de asemenea, caracterul critic al serviciilor afectate.

CAPITOLUL IV

Gestionarea continuității activității TIC

Articolul 24

Componentele politicii de continuitate a activității TIC

- (1) Entitățile financiare includ în politica lor de continuitate a activității TIC menționată la articolul 11 alineatul (1) din Regulamentul (UE) 2022/2554 toate elementele următoare:
 - (a) o descriere a:
 - (i) obiectivelor politicii de continuitate a activității TIC, inclusiv a relației dintre continuitatea activității TIC și continuitatea generală a activității, ținând seama de rezultatele analizei impactului asupra activității (AIA) menționate la articolul 11 alineatul (5) din Regulamentul (UE) 2022/2554;
 - (ii) domeniului de aplicare al măsurilor, planurilor, procedurilor și mecanismelor de asigurare a continuității activității TIC, inclusiv al limitărilor și excluderilor;
 - (iii) intervalului de timp care urmează să fie acoperit de măsurile, planurile, procedurile și mecanismele de asigurare a continuității activității TIC;

- (iv) criteriilor de activare și dezactivare a planurilor de continuitate a activității TIC, a planurilor de răspuns și de recuperare în domeniul TIC și a planurilor de comunicare în situații de criză;
- (b) dispoziții privind:
 - (i) guvernanta și organizarea punerii în aplicare a politicii de continuitate a activității TIC, inclusiv rolurile, responsabilitățile și procedurile de escaladare, asigurându-se că sunt disponibile resurse suficiente;
 - (ii) alinierea dintre planurile de continuitate a activității TIC și planurile generale de continuitate a activității, cel puțin în ceea ce privește toate elementele următoare:
 - 1. scenariile de defecțiuni posibile, inclusiv scenariile menționate la articolul 26 alineatul (2) din prezentul regulament;
 - 2. obiectivele în materie de recuperare, specificându-se că entitatea financiară trebuie să fie în măsură să recupereze operațiunile funcțiilor sale critice sau importante după perturbări respectând un obiectiv privind timpul de recuperare și un obiectiv privind punctul de recuperare;
 - (iii) elaborarea, ca parte a acestor planuri, a unor planuri de continuitate a activității TIC în cazul unor perturbări grave ale activității și stabilirea priorităților în rândul acțiunilor de continuitate a activității TIC utilizând o abordare bazată pe riscuri;
 - (iv) elaborarea, testarea și revizuirea planurilor de răspuns și de recuperare în domeniul TIC, în conformitate cu articolele 25 și 26 din prezentul regulament;
 - (v) examinarea eficacității măsurilor, planurilor, procedurilor și mecanismelor de asigurare a continuității activității TIC puse în aplicare, în conformitate cu articolul 26 din prezentul regulament;
 - (vi) alinierea politicii de continuitate a activității TIC la:
 - 1. politica de comunicare menționată la articolul 14 alineatul (2) din Regulamentul (UE) 2022/2554;
 - 2. măsurile de comunicare și de comunicare în caz de criză menționate la articolul 11 alineatul (2) litera (e) din Regulamentul (UE) 2022/2554.
- (2) În plus față de cerințele menționate la alineatul (1), contrapărțile centrale se asigură că politica lor de continuitate a activității TIC:
 - (a) conține un timp maxim de recuperare pentru funcțiile critice care nu depășește 2 ore;
 - (b) ține seama de legăturile externe și de interdependențele din cadrul infrastructurilor financiare, inclusiv de locurile de tranzacționare care realizează compensarea prin intermediul contrapărții centrale, de sistemele de decontare și de plată a titlurilor de valoare și de instituțiile de credit utilizate de contrapartea centrală sau de o contraparte centrală legată;
 - (c) impune instituirea unor mecanisme care:
 - (i) asigură continuitatea funcțiilor critice sau importante ale contrapărții centrale pe baza scenariilor de dezastru;
 - (ii) mențin o unitate de prelucrare secundară capabilă să asigure continuitatea funcțiilor critice sau importante ale contrapărții centrale în mod identic cu unitatea de prelucrare principală;
 - (iii) mențin sau asigură accesul imediat la un sediu de activitate secundar, pentru a permite personalului să asigure continuitatea serviciului în cazul în care sediul de activitate principal nu este disponibil;
 - (iv) iau în considerare necesitatea unor unități de prelucrare suplimentare, în special în cazul în care diversitatea profilurilor de risc ale unității principale și ale celei secundare nu oferă suficiente asigurări că obiectivele de continuitate a activității contrapărții centrale vor fi îndeplinite în toate scenariile.

În sensul literei (a), contrapărțile centrale finalizează procedurile și plățile de sfârșit de zi la momentul și în ziua cerute, în toate circumstanțele.

În sensul literei (c) punctul (i), măsurile menționate la litera respectivă abordează disponibilitatea resurselor umane adecvate, intervalele de timp maxime de indisponibilitate a funcțiilor critice, precum și transferul automat și recuperarea într-un sediu secundar.

În sensul literei (c) punctul (ii), unitatea de prelucrare secundară menționată la litera respectivă trebuie să aibă un profil de risc geografic diferit de cel al unității principale.

(3) În plus față de cerințele menționate la alineatul (1), depozitarii centrali de titluri de valoare se asigură că politica lor de continuitate a activității TIC:

- (a) ține seama de orice legătură și interdependență cu utilizatorii, utilitățile critice și furnizorii de servicii critice, alți depozitari centrali de titluri de valoare și alte infrastructuri de piață;
- (b) impune mecanismelor de asigurare a continuității activității TIC să garanteze că obiectivul privind timpul de recuperare pentru funcțiile critice sau importante nu depășește 2 ore.

(4) În plus față de cerințele menționate la alineatul (1), locurile de tranzacționare se asigură că politica lor de continuitate a activității TIC garantează că:

- (a) tranzacționarea poate fi reluată în termen de 2 ore de la producerea unui incident perturbator sau într-un termen apropiat de acesta;
- (b) volumul maxim de date care pot fi pierdute prin orice serviciu informatic al locului de tranzacționare după un incident perturbator este aproape zero.

Articolul 25

Testarea planurilor de continuitate a activității TIC

(1) Atunci când testează planurile de continuitate a activității TIC în conformitate cu articolul 11 alineatul (6) din Regulamentul (UE) 2022/2554, entitățile financiare iau în considerare analiza impactului asupra activității (AIA) a entității financiare și evaluarea riscurilor TIC menționată la articolul 3 alineatul (1) litera (b) din prezentul regulament.

(2) Entitățile financiare evaluează, prin testarea planurilor de continuitate a activității TIC menționate la alineatul (1), dacă sunt în măsură să asigure continuitatea funcțiilor lor critice sau importante. Această testare:

- (a) este efectuată pe baza unor scenarii de testare care simulează potențiale perturbări, inclusiv a unui set adecvat de scenarii grave, dar plauzibile;
- (b) conține testarea serviciilor TIC furnizate de furnizori terți de servicii TIC, după caz;
- (c) pentru entitățile financiare, altele decât microîntreprinderile, astfel cum sunt menționate la articolul 11 alineatul (6) al doilea paragraf din Regulamentul (UE) 2022/2554, conține scenarii de transferuri de la infrastructura TIC primară la capacitățile redundante, copiile de rezervă și instalațiile redundante;
- (d) este concepută în așa fel încât să conteste ipotezele pe care se bazează planurile de continuitate a activității, inclusiv mecanismele de guvernare și planurile de comunicare în situații de criză;
- (e) conține proceduri de verificare a capacității personalului entităților financiare, a furnizorilor terți de servicii TIC, a sistemelor TIC și a serviciilor TIC de a răspunde în mod adecvat la scenariile avute în vedere în mod corespunzător în conformitate cu articolul 26 alineatul (2).

În sensul literei (a), entitățile financiare includ întotdeauna în testare scenariile avute în vedere pentru elaborarea planurilor de continuitate a activității.

În sensul literei (b), entitățile financiare iau în considerare în mod corespunzător scenarii legate de insolvența sau disfuncționalitățile furnizorilor terți de servicii TIC sau de riscurile politice din jurisdicțiile furnizorilor terți de servicii TIC, după caz.

În sensul literei (c), testarea verifică cel puțin dacă funcțiile critice sau importante pot fi operate în mod corespunzător pentru o perioadă de timp suficientă și dacă funcționarea normală poate fi restaurată.

(3) În plus față de cerințele menționate la alineatul (2), contrapărțile centrale includ în testarea planurilor lor de continuitate a activității TIC menționate la alineatul (1):

- (a) membrii compensatori;
- (b) furnizorii externi;

- (c) instituțiile relevante din infrastructura financiară cu care contrapărțile centrale au identificat interdependențe în politicile lor de continuitate a activității.
- (4) În plus față de cerințele menționate la alineatul (2), depozitarii centrali de titluri de valoare includ în testarea planurilor lor de continuitate a activității TIC menționate la alineatul (1), după caz:
 - (a) utilizatorii depozitarilor centrali de titluri de valoare;
 - (b) furnizorii de utilități critice și de servicii critice;
 - (c) alți depozitari centrali de titluri de valoare;
 - (d) alte infrastructuri ale pieței;
 - (e) orice alte instituții cu care depozitarii centrali de titluri de valoare au identificat interdependențe în politica lor de continuitate a activității.
- (5) Entitățile financiare documentează rezultatele testării menționate la alineatul (1). Orice deficiențe identificate ca urmare a testării respective sunt analizate, abordate și raportate organului de conducere.

Articolul 26

Planurile de răspuns și de recuperare în domeniul TIC

- (1) La elaborarea planurilor de răspuns și de recuperare în domeniul TIC menționate la articolul 11 alineatul (3) din Regulamentul (UE) 2022/2554, entitățile financiare iau în considerare rezultatele analizei impactului asupra activității (AIA) a entității financiare. Aceste planuri de răspuns și de recuperare în domeniul TIC:
 - (a) precizează condițiile care determină activarea sau dezactivarea lor, precum și orice excepții de la această activare sau dezactivare;
 - (b) descriu acțiunile care trebuie întreprinse pentru a asigura disponibilitatea, integritatea, continuitatea și recuperarea cel puțin a sistemelor și serviciilor TIC care sprijină funcțiile critice sau importante ale entității financiare;
 - (c) sunt concepute în așa fel încât să îndeplinească obiectivele de recuperare ale operațiunilor entităților financiare;
 - (d) sunt documentate și puse la dispoziția personalului implicat în executarea planurilor de răspuns și de recuperare în domeniul TIC și sunt ușor accesibile în caz de urgență;
 - (e) prevăd opțiuni de recuperare atât pe termen scurt, cât și pe termen lung, inclusiv de recuperare parțială a sistemelor;
 - (f) stabilesc obiectivele planurilor de răspuns și de recuperare în domeniul TIC și condițiile pentru declararea executării cu succes a acestor planuri.

În sensul literei (d), entitățile financiare specifică în mod clar rolurile și responsabilitățile.

- (2) Planurile de răspuns și de recuperare în domeniul TIC menționate la alineatul (1) identifică scenariile relevante, inclusiv scenarii de perturbări grave ale activității și de probabilitate crescută de apariție a unei perturbări. Planurile respective elaborează scenarii bazate pe informațiile actuale privind amenințările și pe învățămintele desprinse din evenimentele anterioare de perturbare a activității. Entitățile financiare iau în considerare în mod corespunzător toate scenariile următoare:
 - (a) atacuri cibernetice și transferuri între infrastructura TIC primară și capacitățile redundante, copiile de rezervă și instalațiile redundante;
 - (b) scenarii în care calitatea furnizării unei funcții critice sau importante se deteriorează la un nivel inacceptabil sau o astfel de funcție nu este furnizată și impactul potențial al insolvenței sau al altor disfuncționalități ale oricărui furnizor terț de servicii TIC relevant;
 - (c) indisponibilitatea parțială sau totală a sediilor, inclusiv a birourilor, a sediilor comerciale și a centrelor de date;
 - (d) defecțiuni substanțiale ale activelor TIC sau ale infrastructurii de comunicații;

- (e) indisponibilitatea unui număr critic de membri ai personalului sau a membrilor personalului responsabili cu garantarea continuității operațiunilor;
 - (f) impactul schimbărilor climatice și al evenimentelor legate de degradarea mediului, al dezastrelor naturale, al pandemiilor și al atacurilor fizice, inclusiv al intruziunilor și al atacurilor teroriste;
 - (g) atacuri din interior;
 - (h) instabilitatea politică și socială, inclusiv, după caz, în jurisdicția furnizorului terț de servicii TIC și în locul în care sunt stocate și prelucrate datele;
 - (i) întreruperi pe scară largă ale alimentării cu energie electrică.
- (3) În eventualitatea în care măsurile primare de recuperare s-ar putea să nu fie fezabile pe termen scurt din cauza costurilor, a riscurilor, a logisticii sau a unor circumstanțe neprevăzute, planurile de răspuns și de recuperare în domeniul TIC menționate la alineatul (1) iau în considerare opțiuni alternative.
- (4) Ca parte a planurilor de răspuns și de recuperare în domeniul TIC menționate la alineatul (1), entitățile financiare iau în considerare și pun în aplicare măsuri de continuitate pentru a atenua deficiențele furnizorilor terți de servicii TIC care sprijină funcții critice sau importante ale entității financiare.

CAPITOLUL V

Reportul privind revizuirea cadrului de gestionare a riscurilor TIC

Articolul 27

Formatul și conținutul raportului privind revizuirea cadrului de gestionare a riscurilor TIC

- (1) Entitățile financiare transmit raportul privind revizuirea cadrului de gestionare a riscurilor TIC menționat la articolul 6 alineatul (5) din Regulamentul (UE) 2022/2554 într-un format electronic cu funcție de căutare.
- (2) Entitățile financiare includ toate informațiile următoare în raportul menționat la alineatul (1):
- (a) o secțiune introductivă care:
 - (i) identifică în mod clar entitatea financiară care face obiectul raportului și descrie structura grupului acesteia, după caz;
 - (ii) descrie contextul raportului în ceea ce privește natura, amploarea și complexitatea serviciilor, activităților și operațiunilor entității financiare, organizarea, funcțiile critice identificate, strategia, proiectele sau activitățile majore în curs, relațiile și dependența acesteia de serviciile și sistemele TIC interne și contractate sau implicațiile pe care le-ar avea o pierdere totală sau o degradare gravă a acestor sisteme asupra funcțiilor critice sau importante și asupra eficienței pieței;
 - (iii) sintetizează modificările majore aduse cadrului de gestionare a riscurilor TIC de la raportul anterior prezentat;
 - (iv) furnizează conducerii executive un rezumat al profilului de risc TIC actual și pe termen scurt, al peisajului amenințărilor, al eficacității evaluate a controalelor sale și al posturii de securitate a entității financiare;
 - (b) data aprobării raportului de către organul de conducere al entității financiare;
 - (c) o descriere a motivului revizuirii cadrului de gestionare a riscurilor TIC în conformitate cu articolul 6 alineatul (5) din Regulamentul (UE) 2022/2554;
 - (d) data de început și data de sfârșit a perioadei de revizuire;
 - (e) indicarea funcției responsabile cu revizuirea;
 - (f) o descriere a modificărilor și îmbunătățirilor majore aduse cadrului de gestionare a riscurilor TIC de la revizuirea anterioară;

- (g) un rezumat al concluziilor revizuirii, precum și o analiză și o evaluare detaliate ale gravității punctelor slabe, deficiențelor și lacunelor identificate în cadrul de gestionare a riscurilor TIC în cursul perioadei de revizuire;
- (h) o descriere a măsurilor de remediere a punctelor slabe, deficiențelor și lacunelor identificate, inclusiv a tuturor elementelor următoare:
 - (i) un rezumat al măsurilor luate pentru remedierea punctelor slabe, deficiențelor și lacunelor identificate;
 - (ii) o dată preconizată pentru punerea în aplicare a măsurilor și datele legate de controlul intern al punerii în aplicare, inclusiv informații privind stadiul punerii în aplicare a măsurilor respective la data redactării raportului, explicând, după caz, dacă există riscul ca termenele să nu fie respectate;
 - (iii) instrumentele care urmează să fie utilizate și identificarea funcției responsabile cu punerea în aplicare a măsurilor, precizând dacă instrumentele și funcțiile sunt interne sau externe;
 - (iv) o descriere a impactului modificărilor măsurilor avute în vedere asupra resurselor bugetare, umane și materiale ale entității financiare, inclusiv asupra resurselor dedicate punerii în aplicare a oricăror măsuri corective;
 - (v) informații privind procesul de informare a autorității competente, după caz;
 - (vi) în cazul în care punctele slabe, deficiențele sau lacunele identificate nu fac obiectul unor măsuri corective, o explicație detaliată a criteriilor utilizate pentru analizarea impactului respectivelor puncte slabe, deficiențe sau lacune și pentru evaluarea riscului TIC rezidual aferent, precum și a criteriilor utilizate pentru acceptarea riscului rezidual aferent;
- (i) informații privind evoluțiile viitoare planificate ale cadrului de gestionare a riscurilor TIC;
- (j) concluziile revizuirii cadrului de gestionare a riscurilor TIC;
- (k) informații privind revizuirile anterioare, inclusiv:
 - (i) o listă a revizuirilor anterioare realizate până în momentul respectiv;
 - (ii) dacă este cazul, stadiul punerii în aplicare a măsurilor corective identificate în ultimul raport;
 - (iii) în cazul în care măsurile corective propuse în revizuirile anterioare s-au dovedit inefficiente sau au creat provocări neprevăzute, o descriere a modului în care măsurile corective respective ar putea fi îmbunătățite sau a provocărilor neprevăzute respective;
- (l) sursele de informații utilizate la pregătirea raportului, inclusiv toate elementele următoare:
 - (i) pentru entitățile financiare, altele decât microîntreprinderile, astfel cum sunt menționate la articolul 6 alineatul (6) din Regulamentul (UE) 2022/2554, rezultatele auditurilor interne;
 - (ii) rezultatele evaluărilor de conformitate;
 - (iii) rezultatele testării rezilienței operaționale digitale și, după caz, rezultatele testelor avansate, pe baza testelor de penetrare bazate pe amenințări (TLPT), ale instrumentelor, sistemelor și proceselor TIC;
 - (iv) sursele externe.

În sensul literei (c), în cazul în care revizuirea a fost inițiată în urma unor instrucțiuni în materie de supraveghere sau a unor concluzii derivate din testarea rezilienței operaționale digitale sau din procesele de audit relevante, raportul conține trimeri explicite la astfel de instrucțiuni sau concluzii, permițând identificarea motivului inițierii revizuirii. În cazul în care revizuirea a fost inițiată în urma incidentelor legate de TIC, raportul conține lista tuturor incidentelor legate de TIC cu o analiză a cauzei principale a incidentelor respective.

În sensul literei (f), descrierea conține o analiză a impactului modificărilor asupra strategiei de reziliență operațională digitală a entității financiare, asupra cadrului de control intern în domeniul TIC al entității financiare și asupra guvernancei gestionării riscurilor TIC ale entității financiare.

TITLUL III

CADRUL SIMPLIFICAT DE GESTIONARE A RISCURILOR TIC PENTRU ENTITĂȚILE FINANCIARE MENȚIONATE LA articolul 16 alineatul (1) DIN REGULAMENTUL (UE) 2022/2554

CAPITOLUL I

Cadrul simplificat de gestionare a riscurilor TIC

Articolul 28

Guvernanța și organizarea

(1) Entitățile financiare menționate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554 dispun de un cadru intern de guvernanță și control care asigură gestionarea eficace și prudentă a riscurilor TIC pentru a atinge un nivel ridicat de reziliență operațională digitală.

(2) Ca parte a cadrului lor simplificat de gestionare a riscurilor TIC, entitățile financiare menționate la alineatul (1) se asigură că organul lor de conducere:

- (a) poartă responsabilitatea generală de a se asigura că respectivul cadru simplificat de gestionare a riscurilor TIC permite realizarea strategiei de afaceri a entității financiare în conformitate cu apetitul la risc al entității financiare respective și se asigură că riscurile TIC sunt luate în considerare în acest context;
- (b) stabilește roluri și responsabilități clare pentru toate sarcinile legate de TIC;
- (c) stabilește obiective în materie de securitate a informațiilor și cerințe TIC;
- (d) aprobă, supraveghează și revizuieste periodic:
 - (i) clasificarea activelor informaționale ale entității financiare, astfel cum se menționează la articolul 30 alineatul (1) din prezentul regulament, lista principalelor riscuri identificate, precum și analiza impactului asupra activității și politicile conexe;
 - (ii) planurile de continuitate a activității ale entității financiare și măsurile de răspuns și de recuperare menționate la articolul 16 alineatul (1) litera (f) din Regulamentul (UE) 2022/2554;
- (e) alocă și revizuieste cel puțin o dată pe an bugetul necesar pentru a răspunde nevoilor de reziliență operațională digitală ale entității financiare în ceea ce privește toate tipurile de resurse, inclusiv programe de conștientizare cu privire la securitatea TIC și cursuri de formare în domeniul rezilienței operaționale digitale relevante, precum și competențe TIC pentru toți membrii personalului;
- (f) specifică și pune în aplicare politicile și măsurile incluse în capitolele I, II și III din prezentul titlu pentru identificarea, evaluarea și gestionarea riscurilor TIC la care este expusă entitatea financiară;
- (g) identifică și pune în aplicare procedurile, protocoalele TIC și instrumentele necesare pentru a proteja toate activele informaționale și activele TIC;
- (h) se asigură că personalul entității financiare menține în permanență un nivel suficient de cunoștințe și competențe pentru a înțelege și a evalua riscurile TIC și impactul acestora asupra operațiunilor entității financiare, proporțional cu riscul TIC gestionat;
- (i) stabilește mecanisme de raportare, inclusiv frecvența, formatul și conținutul raportării către organul de conducere cu privire la securitatea informațiilor și reziliența operațională digitală.

(3) Entitățile financiare menționate la alineatul (1) pot, în conformitate cu dreptul Uniunii și cu dreptul sectorial național, să externalizeze sarcinile de verificare a conformității cu cerințele de gestionare a riscurilor TIC către furnizori TIC intragrup sau furnizori terți de servicii TIC. În cazul unei astfel de externalizări, entitățile financiare rămân pe deplin responsabile de verificarea conformității cu cerințele de gestionare a riscurilor TIC.

(4) Entitățile financiare menționate la alineatul (1) asigură o separare adecvată și independența funcțiilor de control și de audit intern.

(5) Entitățile financiare menționate la alineatul (1) se asigură că asupra cadrului lor simplificat de gestionare a riscurilor TIC se realizează un audit intern efectuat de auditori, în conformitate cu planul de audit al entităților financiare. Auditorii dispun de suficiente cunoștințe, competențe și expertiză în domeniul riscurilor TIC și sunt independenți. Frecvența și obiectivul auditurilor TIC sunt proporționale cu riscurile TIC ale entității financiare.

(6) Pe baza rezultatului auditului menționat la alineatul (5), entitățile financiare menționate la alineatul (1) asigură verificarea și remedierea în timp util a constatărilor critice ale auditului TIC.

Articolul 29

Politica și măsurile de securitate a informațiilor

(1) Entitățile financiare menționate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554 elaborează, documentează și pun în aplicare o politică de securitate a informațiilor în contextul cadrului simplificat de gestionare a riscurilor TIC. Politica de securitate a informațiilor specifică principiile și normele de nivel înalt pentru protejarea confidențialității, integrității, disponibilității și autenticității datelor și a serviciilor pe care le furnizează entitățile financiare respective.

(2) Pe baza politicii lor de securitate a informațiilor menționate la alineatul (1), entitățile financiare menționate la alineatul (1) stabilesc și pun în aplicare măsuri de securitate TIC pentru a atenua expunerea lor la riscurile TIC, inclusiv măsuri de atenuare puse în aplicare de furnizorii terți de servicii TIC.

Măsurile de securitate TIC includ toate măsurile menționate la articolele 30-38.

Articolul 30

Clasificarea activelor informaționale și a activelor TIC

(1) Ca parte a cadrului simplificat de gestionare a riscurilor TIC menționat la articolul 16 alineatul (1) litera (a) din Regulamentul (UE) 2022/2554, entitățile financiare menționate la alineatul (1) de la articolul respectiv identifică, clasifică și documentează toate funcțiile critice sau importante, activele informaționale și activele TIC care le sprijină, precum și interdependențele acestora. Entitățile financiare revizuiesc identificarea și clasificarea respectivă atunci când este necesar.

(2) Entitățile financiare menționate la alineatul (1) identifică toate funcțiile critice sau importante sprijinite de furnizorii terți de servicii TIC.

Articolul 31

Gestionarea riscurilor TIC

(1) Entitățile financiare menționate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554 includ în cadrul lor simplificat de gestionare a riscurilor TIC toate elementele următoare:

- (a) stabilirea nivelurilor de toleranță la risc pentru riscurile TIC, în conformitate cu apetitul la risc al entității financiare;
- (b) identificarea și evaluarea riscurilor TIC la care este expusă entitatea financiară;
- (c) specificarea strategiilor de atenuare cel puțin pentru riscurile TIC care nu se încadrează în nivelurile de toleranță la risc ale entității financiare;
- (d) monitorizarea eficacității strategiilor de atenuare menționate la litera (c);
- (e) identificarea și evaluarea riscurilor TIC și de securitate a informațiilor care rezultă din orice modificare majoră a sistemului TIC sau a serviciilor, proceselor sau procedurilor TIC, precum și din rezultatele testelor de securitate TIC și după orice incident major legat de TIC.

- (2) Entitățile financiare menționate la alineatul (1) efectuează și documentează periodic evaluarea riscurilor TIC, proporțional cu profilul de risc TIC al entităților financiare.
- (3) Entitățile financiare menționate la alineatul (1) monitorizează în permanență amenințările și vulnerabilitățile care sunt relevante pentru funcțiile lor critice sau importante, precum și activele informaționale și activele TIC și revizuiesc periodic scenariile de risc care afectează respectivele funcții critice sau importante.
- (4) Entitățile financiare menționate la alineatul (1) stabilesc praguri de alertă și criterii pentru declanșarea și inițierea proceselor de răspuns la incidentele legate de TIC.

Articolul 32

Securitatea fizică și de mediu

- (1) Entitățile financiare menționate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554 identifică și pun în aplicare măsuri de securitate fizică concepute pe baza peisajului amenințărilor și în conformitate cu clasificarea menționată la articolul 30 alineatul (1) din prezentul regulament, cu profilul general de risc al activelor TIC și cu activele informaționale accesibile.
- (2) Măsurile menționate la alineatul (1) protejează sediile entităților financiare și, după caz, centrele de date ale entităților financiare în care se află activele TIC și activele informaționale împotriva accesului neautorizat, a atacurilor și a accidentelor, precum și împotriva amenințărilor și pericolelor de mediu.
- (3) Protecția împotriva amenințărilor și pericolelor de mediu este proporțională cu importanța sediilor respective și, după caz, a centrelor de date și cu caracterul critic al operațiunilor sau al sistemelor TIC situate în acestea.

CAPITOLUL II

Elemente suplimentare ale sistemelor, protocoalelor și instrumentelor menite să reducă la minimum impactul riscurilor TIC

Articolul 33

Controlul accesului

Entitățile financiare menționate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554 elaborează, documentează și pun în aplicare proceduri pentru controlul accesului logic și fizic și asigură respectarea, monitorizarea și revizuirea periodică a procedurilor respective. Aceste proceduri conțin următoarele elemente de control al accesului logic și fizic:

- (a) drepturile de acces la activele informaționale, la activele TIC și la funcțiile sprijinite de acestea, precum și la locurile critice unde operează entitatea financiară sunt gestionate pe baza principiului necesității de a cunoaște, al necesității de a utiliza și al celor mai mici privilegii, inclusiv pentru accesul la distanță și accesul de urgență;
- (b) răspunderea utilizatorului, care asigură faptul că utilizatorii pot fi identificați atunci când efectuează acțiuni în sistemele TIC;
- (c) proceduri de gestionare a conturilor pentru acordarea, modificarea sau revocarea drepturilor de acces pentru conturile de utilizator și conturile generice, inclusiv pentru conturile de administrator generice;
- (d) metode de autentificare care sunt proporționale cu clasificarea menționată la articolul 30 alineatul (1) și cu profilul general de risc al activelor TIC și care se bazează pe cele mai avansate practici;
- (e) drepturile de acces sunt revizuite periodic și sunt retrase atunci când nu mai sunt necesare.

În sensul literei (c), entitatea financiară acordă acces privilegiat, acces de urgență și acces cu drepturi de administrator pe baza principiului necesității de a cunoaște sau ad-hoc pentru toate sistemele TIC și înregistrează evenimentele de acces respective în jurnale în conformitate cu articolul 34 primul paragraf litera (f).

În sensul literei (d), entitățile financiare utilizează metode de autentificare puternică bazate pe cele mai avansate practici pentru accesul de la distanță la rețeaua entităților financiare, pentru accesul privilegiat și pentru accesul la activele TIC care sprijină funcții critice sau importante care sunt disponibile publicului.

Articolul 34

Securitatea operațiunilor TIC

Ca parte a sistemelor, protocoalelor și instrumentelor lor și pentru toate activele TIC, entitățile financiare menționate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554:

- (a) monitorizează și gestionează ciclul de viață al tuturor activelor TIC;
- (b) monitorizează dacă activele TIC sunt sprijinite de furnizori terți de servicii TIC ai entităților financiare, după caz;
- (c) identifică cerințele în materie de capacitate ale activelor TIC și măsurile de menținere și îmbunătățire a disponibilității și eficienței sistemelor TIC și de prevenire a deficitelor de capacitate TIC înainte ca acestea să se concretizeze;
- (d) efectuează scanarea automată a vulnerabilităților și evaluări ale activelor TIC, proporționale cu clasificarea acestora, astfel cum se menționează la articolul 30 alineatul (1), și cu profilul general de risc al activului TIC, și implementează corecții pentru a aborda vulnerabilitățile identificate;
- (e) gestionează riscurile legate de activele TIC care sunt învechite sau moștenite sau care nu mai beneficiază de asistență;
- (f) înregistrează în jurnale evenimentele legate de controlul accesului logic și fizic, operațiunile TIC, inclusiv activitățile de trafic de sistem și de rețea, precum și gestionarea modificărilor TIC;
- (g) identifică și pun în aplicare măsuri de monitorizare și analiză a informațiilor privind activitățile și comportamentele anormale pentru operațiunile TIC critice sau importante;
- (h) pun în aplicare măsuri de monitorizare a informațiilor relevante și actualizate cu privire la amenințările cibernetice;
- (i) pun în aplicare măsuri de identificare a posibilelor scurgeri de informații, a codurilor dăunătoare și a altor amenințări la adresa securității, precum și a vulnerabilităților cunoscute public ale software-ului și hardware-ului și verifică dacă există noi actualizări de securitate corespunzătoare.

În sensul literei (f), entitățile financiare aliniază nivelul de detaliu al jurnalelor la scopul acestora și la utilizarea activelor TIC care produc înregistrările în jurnalele respective.

Articolul 35

Securitatea datelor, a sistemului și a rețelelor

Entitățile financiare menționate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554 elaborează și pun în aplicare, ca parte a sistemelor, protocoalelor și instrumentelor lor, garanții care asigură securitatea rețelelor împotriva intruziunilor și a utilizării abuzive a datelor și care mențin disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor. În special, ținând seama de clasificarea menționată la articolul 30 alineatul (1) din prezentul regulament, entitățile financiare stabilesc toate elementele următoare:

- (a) identificarea și punerea în aplicare a măsurilor de protecție a datelor în uz, în tranzit și în repaus;
- (b) identificarea și punerea în aplicare a măsurilor de securitate privind utilizarea software-ului, a mediilor de stocare a datelor, a sistemelor și a dispozitivelor de punct final care asigură transferul și stocarea datelor entității financiare;
- (c) identificarea și punerea în aplicare a măsurilor de prevenire și detectare a conexiunilor neautorizate la rețeaua entității financiare, precum și de securizare a traficului de rețea între rețelele interne ale entității financiare și internet și alte conexiuni externe;
- (d) identificarea și punerea în aplicare a unor măsuri care asigură disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor în timpul transmisiilor în rețea;
- (e) un proces care asigură ștergerea în condiții de siguranță a datelor, aflate în sediile entității financiare sau stocate extern, pe care entitatea financiară nu mai are nevoie să le colecteze sau să le stocheze;
- (f) un proces de eliminare sau scoatere din uz în condiții de siguranță a dispozitivelor de stocare a datelor aflate în sediile entității financiare sau a dispozitivelor de stocare a datelor stocate în exterior, care conțin informații confidențiale;

- (g) identificarea și punerea în aplicare a unor măsuri care asigură că telemunca și utilizarea dispozitivelor de punct final private nu au un impact negativ asupra capacității entității financiare de a-și desfășura activitățile critice în mod adecvat, în timp util și în condiții de siguranță.

Articolul 36

Testarea securității TIC

- (1) Entitățile financiare menționate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554 stabilesc și pun în aplicare un plan de testare a securității TIC pentru a valida eficacitatea măsurilor lor de securitate TIC elaborate în conformitate cu articolele 33, 34 și 35 și cu articolele 37 și 38 din prezentul regulament. Entitățile financiare se asigură că planul respectiv ține seama de amenințările și vulnerabilitățile identificate ca parte a cadrului simplificat de gestionare a riscurilor TIC menționat la articolul 31 din prezentul regulament.
- (2) Entitățile financiare menționate la alineatul (1) revizuiesc, evaluează și testează măsurile de securitate TIC, ținând seama de profilul general de risc al activelor TIC ale entității financiare.
- (3) Entitățile financiare menționate la alineatul (1) monitorizează și evaluează rezultatele testelor de securitate și își actualizează măsurile de securitate în consecință, fără întârzieri nejustificate, în cazul sistemelor TIC care sprijină funcții critice sau importante.

Articolul 37

Achiziționarea, dezvoltarea și întreținerea sistemelor TIC

Entitățile financiare menționate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554 concep și pun în aplicare, după caz, o procedură care reglementează achiziționarea, dezvoltarea și întreținerea sistemelor TIC urmând o abordare bazată pe riscuri. Această procedură:

- (a) asigură că, înainte de orice achiziție sau dezvoltare a sistemelor TIC, cerințele funcționale și nefuncționale, inclusiv cerințele de securitate a informațiilor, sunt specificate și aprobate în mod clar de către funcția operațională în cauză;
- (b) asigură testarea și aprobarea sistemelor TIC înainte de prima lor utilizare și înainte de introducerea de modificări în mediul de producție;
- (c) identifică măsuri de atenuare a riscului de modificare neintenționată sau de manipulare intenționată a sistemelor TIC în timpul dezvoltării și implementării în mediul de producție.

Articolul 38

Gestionarea proiectelor și a modificărilor TIC

- (1) Entitățile financiare menționate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554 elaborează, documentează și pun în aplicare o politică de gestionare a proiectelor TIC și specifică rolurile și responsabilitățile pentru punerea în aplicare a acesteia. Procedura respectivă acoperă toate etapele proiectelor TIC, de la inițierea până la încheierea lor.
- (2) Entitățile financiare menționate la alineatul (1) elaborează, documentează și pun în aplicare o procedură de gestionare a modificărilor TIC pentru a se asigura că toate modificările aduse sistemelor TIC sunt înregistrate, testate, evaluate, aprobate, implementate și verificate într-un mod controlat și cu garanții adecvate pentru a menține reziliența operațională digitală a entității financiare.

CAPITOLUL III

Gestionarea continuității activității TIC

Articolul 39

Componentele planului de continuitate a activității TIC

- (1) Entitățile financiare menționate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554 își elaborează planurile de continuitate a activității TIC ținând seama de rezultatele analizei expunerilor lor la perturbări grave ale activității și de impactul potențial al unor astfel de perturbări și de scenariile la care ar putea fi expuse activele TIC care sprijină funcții critice sau importante, inclusiv scenariul unui atac cibernetic.
- (2) Planurile de continuitate a activității TIC menționate la alineatul (1):
- (a) sunt aprobate de organul de conducere al entității financiare;
 - (b) sunt documentate și ușor accesibile în caz de urgență sau de criză;
 - (c) alocă resurse suficiente pentru executarea acestora;
 - (d) stabilesc nivelurile de recuperare planificate și termenele pentru recuperarea și reluarea funcțiilor și principalele dependențe interne și externe, inclusiv de furnizorii terți de servicii TIC;
 - (e) identifică condițiile care pot declanșa activarea planurilor de continuitate a activității TIC și măsurile care trebuie luate pentru a asigura disponibilitatea, continuitatea și recuperarea activelor TIC ale entităților financiare care sprijină funcții critice sau importante;
 - (f) identifică măsurile de restaurare și recuperare pentru funcțiile operaționale critice sau importante, procesele de sprijin, activele informaționale și interdependențele acestora pentru a evita efectele negative asupra funcționării entităților financiare;
 - (g) identifică procedurile și măsurile pentru copiile de rezervă care specifică domeniul de aplicare al datelor care fac obiectul copiilor de rezervă, precum și frecvența minimă de efectuare a copiilor de rezervă, pe baza caracterului critic al funcției care utilizează datele respective;
 - (h) iau în considerare opțiuni alternative în cazul în care recuperarea s-ar putea să nu fie fezabilă pe termen scurt din cauza costurilor, a riscurilor, a logisticii sau a unor circumstanțe neprevăzute;
 - (i) specifică modalitățile de comunicare internă și externă, inclusiv planurile de escaladare;
 - (j) se actualizează în funcție de învățămintele desprinse din incidente, de teste, de noile riscuri și amenințări identificate, de obiectivele de recuperare modificate și de modificările majore ale organizării entității financiare și ale activelor TIC care sprijină funcții critice sau operaționale.

În sensul literei (f), măsurile menționate la litera respectivă prevăd măsuri de atenuare a deficiențelor furnizorilor terți critici.

Articolul 40

Testarea planurilor de continuitate a activității

- (1) Entitățile financiare menționate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554 își testează planurile de asigurare a continuității activității menționate la articolul 39 din prezentul regulament, inclusiv scenariile menționate la articolul respectiv, cel puțin o dată pe an pentru procedurile legate de copiile de rezervă și de restaurare sau la fiecare modificare majoră a planului de continuitate a activității.
- (2) Testarea planurilor de continuitate a activității menționate la alineatul (1) demonstrează că entitățile financiare menționate la alineatul respectiv sunt în măsură să își mențină viabilitatea activităților până la restabilirea operațiunilor critice și identifică eventualele deficiențe ale planurilor respective.
- (3) Entitățile financiare menționate la alineatul (1) documentează rezultatele testării planurilor de continuitate a activității și orice deficiențe identificate ca urmare a testării respective sunt analizate, abordate și raportate organului de conducere.

CAPITOLUL IV

Reportul privind revizuirea cadrului simplificat de gestionare a riscurilor TIC

Articolul 41

Formatul și conținutul raportului privind revizuirea cadrului simplificat de gestionare a riscurilor TIC

- (1) Entitățile financiare menționate la articolul 16 alineatul (1) din Regulamentul (UE) 2022/2554 transmit raportul privind revizuirea cadrului de gestionare a riscurilor TIC menționat la alineatul (2) al articolului respectiv într-un format electronic cu funcție de căutare.
- (2) Raportul menționat la alineatul (1) include toate informațiile următoare:
- (a) o secțiune introductivă care conține:
- (i) o descriere a contextului raportului în ceea ce privește natura, amploarea și complexitatea serviciilor, activităților și operațiunilor entității financiare, organizarea entității financiare, funcțiile critice identificate, strategia, proiectele sau activitățile majore în curs, relațiile și dependența entității financiare de serviciile și sistemele TIC interne și externalizate sau implicațiile pe care le-ar avea o pierdere totală sau o degradare gravă a acestor sisteme asupra funcțiilor critice sau importante și a eficienței pieței;
 - (ii) un rezumat executiv al riscurilor TIC actuale și pe termen scurt identificate, al peisajului amenințărilor, al eficacității evaluate a controalelor sale și al posturii de securitate a entității financiare;
 - (iii) informații privind domeniul care face obiectul raportului;
 - (iv) un rezumat al modificărilor majore aduse cadrului de gestionare a riscurilor TIC de la raportul anterior;
 - (v) un rezumat și o descriere a impactului modificărilor majore aduse cadrului simplificat de gestionare a riscurilor TIC de la raportul anterior;
- (b) dacă este cazul, data aprobării raportului de către organul de conducere al entității financiare;
- (c) o descriere a motivelor revizuirii, inclusiv:
- (i) dacă revizuirea a fost inițiată în urma unor instrucțiuni în materie de supraveghere, dovezi ale unor astfel de instrucțiuni;
 - (ii) dacă revizuirea a fost inițiată în urma apariției unor incidente legate de TIC, lista tuturor incidentelor legate de TIC cu o analiză a cauzei principale a incidentelor respective;
- (d) data de început și data de sfârșit a perioadei de revizuire;
- (e) persoana responsabilă cu revizuirea;
- (f) un rezumat al constatărilor și o autoevaluare a gravității punctelor slabe, deficiențelor și lacunelor identificate în cadrul de gestionare a riscurilor TIC pentru perioada de revizuire, inclusiv o analiză detaliată a acestora;
- (g) măsurile de remediere identificate pentru a remedia punctele slabe, deficiențele și lacunele cadrului simplificat de gestionare a riscurilor TIC, precum și data preconizată pentru punerea în aplicare a măsurilor respective, inclusiv monitorizarea punctelor slabe, a deficiențelor și a lacunelor identificate în rapoartele anterioare, în cazul în care punctele slabe, deficiențele și lacunele respective nu au fost încă remediate;
- (h) concluziile generale privind revizuirea cadrului simplificat de gestionare a riscurilor TIC, inclusiv orice alte evoluții planificate.

TITLUL IV

DISPOZIȚII FINALE

Articolul 42

Intrarea în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 13 martie 2024.

Pentru Comisie
Președinta
Ursula VON DER LEYEN