

Normă privind governanța și securitatea
sistemelor de tehnologia informațiilor și a comunicațiilor
- proiect -

În temeiul prevederilor art. 2 alin. (1) lit. b), art. 3 alin. (1) lit. b) și art. 6 alin. (2) din Ordonanța de urgență a Guvernului nr. 93/2012 privind înființarea, organizarea și funcționarea Autorității de Supraveghere Financiară, aprobată cu modificări și completări prin Legea nr. 113/2013, cu modificările și completările ulterioare,

în conformitate cu prevederile art. 179 alin. (4) din Legea nr. 237/2015 privind autorizarea și supravegherea activității de asigurare și reasigurare, cu modificările și completările ulterioare,

în urma deliberărilor Consiliului Autorității de Supraveghere Financiară în cadrul ședinței din data de _____,

Autoritatea de Supraveghere Financiară emite prezenta normă:

Articolul 1. Domeniul de aplicare și semnificații

(1) Prezenta normă reglementează governanța și securitatea sistemelor de tehnologia informațiilor și a comunicațiilor utilizate de către societățile de asigurare și de reasigurare.

(2) Prevederile prezentei norme se aplică, cu respectarea principiului proporționalității, societăților și în mod corespunzător grupurilor prevăzute la art. 1 alin. (2) pct. 20 și 56 de Legea nr. 237/2015 privind autorizarea și supravegherea activității de asigurare și reasigurare, cu modificările și completările ulterioare.

(3) Actele normative menționate în prezenta normă au următoarele semnificații:

1. Legea nr. 237/2015 - Legea nr. 237/2015 privind desfășurarea activității de asigurare și reasigurare, cu completările și modificările ulterioare;
2. Norma nr. 4/2018 - Norma A.S.F. nr. 4/2018 privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entitățile autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către Autoritatea de Supraveghere Financiară. cu completările și modificările ulterioare;
3. Norma nr. 33/2020 - Norma A.S.F. nr. 33/2020 privind externalizarea către furnizorii de servicii de tip cloud.

(4) Termenii și expresiile din prezenta normă au semnificațiile prevăzute în Legea nr. 237/2015, Norma nr. 4/2018 și Norma nr. 33/2020, precum și următoarele semnificații:

1. activ TIC - echipament software sau hardware utilizat în mediul de afaceri;
2. atac cibernetic - intervenție sau încercare de intervenție neautorizată asupra unui sistem TIC ce are drept scop distrugerea, modificarea, expunerea sau procurarea de seturi de informații, accesul neautorizat la seturi de informații sau utilizarea neautorizată a acestora;

3. confidențialitate - capacitatea informațiilor de a putea fi comunicate sau disponibile doar pentru persoane, entități și sisteme cărora le sunt destinate;
4. disponibilitate - capacitatea unor elemente de a fi disponibile pentru utilizare în timp util de către entități sau persoane care au drept de acces;
5. element TIC - proces, funcție și activitate operațională, critică sau semnificativă, activ TIC, bază de date;
6. furnizor de servicii TIC - terță parte care dezvoltă procese TIC, furnizează servicii TIC și desfășoară activități TIC, integral sau parțial, în temeiul unui contract de externalizare;
7. incident - un eveniment sau o serie de evenimente conexe și neașteptate cu impact negativ asupra integralității, disponibilității și confidențialității sistemelor și serviciilor TIC;
8. integralitate - capacitatea anumitor elemente de a fi complete și de a avea un grad ridicat de corectitudine;
9. proiect TIC - proiect conform căruia sistemele și serviciile TIC sunt modificate, înlocuite sau implementate, integral sau parțial;
10. proprietar de active TIC - persoană sau entitate care are răspundere pentru și atribuții de a dispune de activele TIC;
11. risc TIC - tip de risc operațional care generează pierderi din cauza neadecvării sistemelor TIC sau a utilizării defectuoase a acestora;
12. securitate cibernetică - ansamblu de măsuri și proceduri menite să asigure protejarea informațiilor și a sistemelor TIC dintr-un mediu cibernetic în ceea ce privește confidențialitatea, integralitatea, disponibilitatea, autenticitatea, relevanța și validitatea acestora;
13. serviciu TIC - servicii furnizate utilizatorilor interni și externi prin intermediul sistemelor TIC;
14. set de informații - grupare de informații electronice care necesită protecție;
15. sistem TIC - set de aplicații, active TIC, date informatice și alte structuri de utilizare a informațiilor, inclusiv mediul operațional;
16. vulnerabilitate - totalitatea punctelor slabe ale activelor TIC sau ale mecanismelor de protecție a acestora care pot fi vizate în cazul unui atac cibernetic.

(5) Categoria de riscuri TIC poate include:

- a) nerespectarea regulilor de confidențialitate;
- b) deficiențe ale integralității sistemelor TIC și ale informațiilor;
- c) inadecvarea sau indisponibilitatea sistemelor TIC și a informațiilor;
- d) incapacitatea de a modifica sistemele TIC în timp util și cu costuri rezonabile, atunci când mediul de afaceri se modifică;
- e) derularea cu deficiențe a unor procese interne;
- f) securitate fizică deficientă;
- g) evenimente externe, inclusiv atacuri cibernetic.

Articolul 2. Responsabilitatea conducerii

(1) Conducerea stabilește și aprobă, în cadrul strategiei generale de afaceri, strategia TIC și în cadrul politicii generale privind continuitatea activității, politica privind continuitatea activității TIC; de asemenea, conducerea aprobă politica privind securitatea cibernetică și raportul de management al riscului TIC.

(2) Conducerea este responsabilă pentru:

a) asigurarea comunicării în timp util către personalul relevant și furnizorii de servicii TIC a strategiei TIC și a politicii privind continuitatea activității TIC;

b) asigurarea supervizării aplicării în practică a strategiei TIC și a politicii privind continuitatea activității TIC;

c) managementul efectiv și adecvat al riscului TIC în cadrul sistemului de guvernare;

d) alocarea de resurse suficiente și adecvate pentru asigurarea guvernării și securității sistemelor TIC.

(3) Conducerea asigură aplicarea unor programe de instruire periodică cu scopul ca personalul să dețină în permanență pregătirea necesară pentru aplicarea strategiei TIC și pentru desfășurarea eficientă a operațiunilor TIC și a proceselor de management al riscului TIC.

Articolul 3. Prevederi generale referitoare la sistemul de guvernare

(1) Strategia TIC a societăților, stabilită și aprobată de conducerea acestora conform art. 2 alin. (1), are în vedere cel puțin următoarele:

a) modalitatea în care sistemele TIC sunt optimizate;

b) evoluția configurării sistemelor TIC, inclusiv în ceea ce privește dependențele principale de furnizorii de servicii TIC;

c) obiectivele principale privind securitatea cibernetică;

d) criteriile privind achiziționarea sau dezvoltarea internă a sistemelor TIC.

(2) Societățile optimizează sistemele TIC conform alin. (1) lit. a):

a) pentru a asigura implementarea strategiei de afaceri;

b) pentru ca acestea să fie elemente de bază în cadrul modelului de afaceri adoptat;

c) pentru ca acestea să fie adecvate în cazul modificării structurii organizatorice;

d) pentru a ține cont de dependențele principale de furnizorii de servicii TIC.

(3) Societățile instituie politici pentru a monitoriza și evalua eficiența aplicării strategiei TIC și activitățile care au impact asupra securității cibernetică, pe care le revizuiesc periodic, actualizându-le dacă este cazul, și elaborează proceduri în aplicarea acestora.

(4) În vederea asigurării funcționării eficiente a sistemelor TIC, societățile dezvoltă și aplică programe de pregătire periodică și programe pentru conștientizarea riscurilor TIC și a minimizării acestora, pentru toți angajații și pentru conducere.

(5) Scopul programelor prevăzute la alin. (4) este acela de a asigura desfășurarea activității și exercitarea atribuțiilor astfel încât să se reducă erorile umane, fraudă, utilizarea defectuoasă a sistemelor TIC și pierderile cauzate de acestea.

(6) Societățile stabilesc în sistemul de guvernanță metodologia de dezvoltare și de aplicare a proiectelor TIC, având în vedere cerințele de securitate cibernetică, astfel încât:

- a) să asigure implementarea corectă a strategiei TIC;
- b) să minimizeze riscurile generate de interdependențele dintre proiectele TIC;
- c) să minimizeze dependența portofoliilor de proiecte TIC de anumite resurse sau de anumiți specialiști.

(7) În procedurile prevăzute la alin. (3), societățile stabilesc cerințe referitoare la:

- a) aprobarea sistemelor și serviciilor TIC, dezvoltate intern sau achiziționate;
- b) măsurile de securitate cibernetică asociate sistemelor și serviciilor TIC;
- c) asigurarea independenței structurii de dezvoltare a sistemelor TIC, a structurii de testare a acestora și a structurilor non-operaționale față de activitățile operaționale.

(8) În cadrul politicii generale privind externalizarea, societățile stabilesc criteriile și condițiile în funcție de care selectează furnizorii de servicii TIC și condițiile în funcție de care este necesară schimbarea acestora.

(9) Fără a aduce atingere Normei nr. 33/2020, în cazul externalizării sistemelor TIC, a serviciilor TIC și a funcțiilor critice, contractele încheiate de societăți cu furnizorii de servicii TIC includ clauze referitoare cel puțin la:

- a) nivelul de calitate garantat pentru serviciile furnizate;
- b) obiectivele de securitate cibernetică și obiectivele privind monitorizarea acestora;
- c) măsurile prin care se asigură securitatea cibernetică;
- d) specificații tehnice privind durata de viață a informațiilor, dreptul de acces la informații și auditarea acestora;
- e) locația centrelor de informații;
- f) modalitățile de criptare;
- g) planurile de asigurare a continuității activității și planurile pentru situații de urgență;
- h) procedurile privind managementul incidentelor;
- i) stabilirea clară a canalelor de raportare;
- j) condițiile de reziliere a contractelor.

(10) Societățile asigură monitorizarea respectării de către furnizorii de servicii TIC a clauzelor specificate în contractele de furnizare de servicii.

(11) Planul general de audit elaborat de societăți prevede auditarea periodică a politicii de management al riscului TIC, inclusiv a procedurilor și sistemelor instituite în vederea aplicării acesteia, de către persoane care au suficiente cunoștințe și expertiză în domeniu, frecvența auditului fiind stabilită în funcție de riscurile relevante.

(12) Prevederile alin. (11) se aplică coroborat cu prevederile Normei nr. 4/2018.

Articolul 4. Procesul de management al riscului TIC

(1) În cadrul procesului de management al riscului TIC, societățile determină nivelul toleranței la risc, în concordanță cu strategia generală de risc adoptată.

(2) Procesul de management al riscului TIC derulat de societăți are în vedere cel puțin următoarele:

a) cartarea periodică a elementelor TIC pentru a stabili interdependența dintre acestea și riscurile TIC;

b) identificarea și evaluarea riscurilor TIC pe baza unor criterii stabilite în funcție de nivelul de semnificație al elementelor TIC, vulnerabilitățile cunoscute și incidentele anterioare;

c) clasificarea elementelor TIC expuse la riscurile TIC în funcție de pragul de semnificație stabilit și de nivelul de protecție a acestora din punct de vedere al confidențialității, integralității și disponibilității;

d) identificarea proprietarilor de active TIC pentru a se realiza clasificarea prevăzută la lit. c);

e) metodele utilizate pentru determinarea pragului de semnificație și a nivelului de protecție prevăzute la lit. c) pentru a se asigura o abordare unitară și consecventă;

f) evaluarea și documentarea periodic a riscurilor TIC;

g) evaluarea și documentarea riscurilor TIC înainte de realizarea unor modificări semnificative ale infrastructurii și ale procedurilor care au impact asupra elementelor TIC;

h) stabilirea metodelor și a măsurilor pentru gestionarea, monitorizarea și raportarea riscurilor identificate;

i) stabilirea metodelor și a măsurilor pentru protejarea activelor TIC în funcție de clasificarea acestora;

j) stabilirea metodelor și a măsurilor pentru gestionarea, monitorizarea și raportarea riscurilor reziduale.

(3) Raportul periodic de management al riscului prezentat conducerii include și rezultatele procesului de management al riscului TIC.

Articolul 5. Managementul operațiunilor TIC

(1) În conformitate cu strategia TIC stabilită și aprobată de conducere, societățile elaborează proceduri privind managementul operațiunilor TIC având în vedere cel puțin:

a) derularea operațiunilor TIC;

b) capacitatea activelor TIC de a face față disfuncționalităților;

c) înregistrarea de incidente.

(2) Societățile mențin și actualizează un registru al activelor TIC astfel încât să fie posibilă identificarea promptă a fiecărui element în ceea ce privește proprietarul, localizarea și clasificarea acestuia din punctul de vedere al securității cibernetice.

(3) Societățile monitorizează cel puțin:

a) capacitatea activelor TIC de a contribui la desfășurarea eficientă a activității, pe toată durata de viață a acestora;

b) respectarea cerințelor de management al riscului;

c) asigurarea faptului că activele TIC sunt susținute de furnizorii terți sau de personalul propriu răspunzător de dezvoltarea acestora;

d) documentarea actualizării și optimizării activelor TIC.

(4) În aplicarea politicilor prevăzute la alin. (1) lit. a) societățile elaborează proceduri având în vedere cel puțin:

a) modalitățile în care sistemele și serviciile TIC, în special cele critice, sunt derulate, monitorizate și controlate;

b) modalitățile de conectare și monitorizare a operațiunilor TIC pentru asigurarea detectării, analizării și corectării erorilor.

(5) În aplicarea politicilor prevăzute la alin. (1) lit. b) societățile elaborează proceduri având în vedere cel puțin:

a) monitorizarea capacității activelor TIC de a asigura prevenirea, detectarea și contracararea disfuncționalităților în timp util și eficient;

b) capacitatea sistemelor TIC de a stoca informațiile în siguranță și de a asigura recuperarea acestora în mod eficient;

c) frecvența stocărilor de siguranță în concordanță cu nivelul de semnificație al informațiilor și sistemelor TIC.

(6) Societățile se asigură că stocările de siguranță sunt realizate în locații care nu interferează cu locația principală astfel încât să se evite expunerea la aceleași riscuri a tuturor locațiilor.

(7) Societățile determină nivelul de semnificație al informațiilor și sistemelor TIC în funcție de rezultatele evaluării riscurilor, astfel încât să se asigure respectarea standardelor de recuperare a informațiilor.

(8) În aplicarea politicilor prevăzute la alin. (1) lit. c), societățile elaborează proceduri având în vedere cel puțin:

a) criteriile adecvate și pragurile de semnificație pentru încadrarea evenimentelor drept incidente;

b) mecanisme de avertizare timpurie pentru detectarea în timp util a incidentelor;

c) minimizarea efectelor incidentelor și reluarea eficientă și în timp util a activității după înregistrarea acestora;

d) mecanisme pentru identificarea cauzelor care stau la baza producerii incidentelor și măsurile pentru prevenirea producerii din nou a aceluiași incident;

e) mecanisme pentru asigurarea monitorizării și gestionării incidentelor;

f) alocarea clară a responsabilității pentru managementul incidentelor;

g) managementul incidentelor astfel încât să se asigure reluarea și continuarea activităților critice atunci când se înregistrează disfuncționalități;

h) canalele de comunicare și raportare a incidentelor în cadrul structurii organizatorice în funcție de pragurile de semnificație stabilite;

i) modul de gestionare a sesizărilor externe privind aspecte de securitate cibernetică;

j) mecanismele de comunicare și colaborare cu factorii externi adecvați în caz de producere a unor incidente cu scopul de a minimiza efectele acestora și de a restabili nivelul normal de funcționare.

(9) Societățile asigură informarea în timp real a conducerii cu privire la înregistrarea unor incidente semnificative, la impactul acestora și la măsurile aplicate pentru controlarea impactului respectiv.

(10) Societățile instituie politici privind modificările aduse sistemelor TIC și elaborează proceduri în aplicarea acestora, având în vedere cel puțin:

a) înregistrarea, evaluarea, testarea, aprobarea, autorizarea și implementarea modificărilor în mod controlat;

b) identificarea modificărilor realizate în situații de urgență și comunicarea acestora în timp util proprietarilor de active TIC pentru analize ulterioare;

c) determinarea impactului modificărilor asupra măsurilor de securitate cibernetică a mediului operațional existent;

d) adoptarea de măsuri pentru minimizarea riscurilor induse de modificări.

(11) Societățile instituie proceduri referitoare la durata de viață a activelor TIC pentru managementul riscului de degradare și de scădere a eficienței acestora din punct de vedere al evoluției tehnologice, inclusiv la modalitatea de distrugere a activelor respective.

Articolul 6. Prevederi generale referitoare la securitatea cibernetică

(1) În vederea implementării strategiei TIC stabilite și aprobate de conducere conform art. 2 alin. (1), societățile instituie politici privind securitatea cibernetică în care stabilesc principii și reguli pentru a se asigura respectarea confidențialității, integralității și disponibilității activelor TIC.

(2) În politicile prevăzute la alin. (1), societățile au în vedere cel puțin:

a) alocarea clară a atribuțiilor și răspunderii pentru managementul securității cibernetică;

b) criteriile avute în vedere la derularea proceselor și achiziționarea echipamentelor tehnologice;

c) cerințele specifice pentru tot personalul în funcție de nivelul ierarhic.

(3) Societățile elaborează proceduri în vederea punerii în practică a politicilor prevăzute la alin. (1) având drept scop dezvoltarea de procese prin care să minimizeze riscurile TIC.

(4) Societățile desemnează persoanele cărora le alocă atribuțiile funcției de securitate cibernetică care este independentă de funcțiile operaționale și de cele de dezvoltare a sistemelor TIC pentru a putea asigura în mod obiectiv securitatea cibernetică.

(5) Funcția instituită conform alin. (4) are cel puțin următoarele atribuții:

a) consiliază conducerea în vederea stabilirii politicii privind securitatea cibernetică;

b) asigură cunoașterea de către toți furnizorii de servicii TIC și de către toți angajații care au acces la informații și la sistemele TIC a politicii privind securitatea cibernetică prin organizarea unor sesiuni de informare și de instruire;

c) supervizează aplicarea și respectarea procedurilor prevăzute la alin. (3) de către furnizorii de servicii TIC și de către toți angajații care au acces la informații și la sistemele TIC;

d) coordonează procesul de verificare a producerii incidentelor de securitate;

e) transmite un raport către conducere, periodic sau ad-hoc, referitor la stadiul elementelor menționate la lit. a) - d).

Articolul 7. Securitatea tehnică, fizică și a operațiunilor TIC

(1) În aplicarea politicilor menționate la art. 6 alin. (1), societățile elaborează proceduri referitoare la securitatea tehnică pentru a asigura managementul identității utilizatorilor care au acces la sistemele TIC și controlul asupra disfuncționalităților.

(2) În procedurile prevăzute la alin. (1), societățile abordează cel puțin următoarele elemente:

a) managementul dreptului de acces, inclusiv accesul de la distanță, la activele TIC și sistemele pe care acestea se bazează;

b) limitarea dreptului de acces al utilizatorilor, proporțional cu atribuțiile alocate acestora;

c) prevenirea accesului neautorizat;

d) limitarea utilizării conturilor generice sau partajate și asigurarea identificării în permanență a utilizatorilor autorizați și a proceselor autorizate;

e) mecanismele de control al accesului discreționar;

f) mecanismele privind accesul administrativ de la distanță la sistemele TIC critice și procesul de autentificare;

g) modalitățile de înregistrare și monitorizare a activității utilizatorilor, în special a celor cu drepturi discreționare, în funcție de nivelul de semnificație al activității respective;

h) perioada de arhivare a înregistrărilor menționate la lit. g), în funcție de nivelul de semnificație al activității, al proceselor și al activelor TIC;

i) modalitățile de prevenire a modificării sau eliminării neautorizate a înregistrărilor menționate la lit. g);

j) modalitățile de identificare și analizare, pe baza înregistrărilor menționate la lit. g), a acțiunilor anormale detectate în timpul furnizării de servicii;

k) condițiile în care se acordă sau se modifică dreptul de acces al proprietarilor de active TIC și condițiile de retragere promptă a dreptului respectiv;

l) condițiile pentru revizuirea periodică a dreptului de acces pentru ca acesta să fie acordat în funcție de nivelul de semnificație al activității utilizatorilor și măsurile adoptate ulterior revizuirii;

m) cerințele privind documentarea acordării, modificării și retragerii dreptului de acces;

n) metodele de autentificare a utilizatorilor, în conformitate cu politica privind controlul accesului și nivelul de semnificație al sistemelor TIC, informațiilor și proceselor la care există acces.

(3) Societățile limitează accesul prin intermediul aplicațiilor la informații și la sistemele TIC la nivelul necesar pentru ca operațiunile să se desfășoare eficient.

(4) În aplicarea politicilor prevăzute la art. 6 alin. (1), societățile elaborează proceduri referitoare la securitatea fizică, având în vedere cel puțin:

a) condițiile în care se autorizează accesul fizic la sistemele TIC în funcție de nivelul de instruire a fiecărei persoane, atribuțiile și responsabilitățile acesteia;

b) modalitățile de monitorizare a personalului;

c) măsurile pentru prevenirea accesului neautorizat în sediu, în perimetrele sensibile și la centrele de stocare a informațiilor;

d) condițiile în care dreptul de acces fizic este retras și revizuirea acestora;

e) măsurile pentru prevenirea deteriorării sistemelor TIC din cauze externe, independente de factorul uman, proporționale cu importanța sediului și cu nivelul de semnificație al operațiunilor TIC derulate și al sistemelor TIC localizate în sediu;

f) documentarea elementelor prevăzute la lit. a) - e).

(5) Societățile instituie politici cu scopul de a minimiza impactul aspectelor legate de securitate asupra operațiunilor TIC.

(6) În aplicarea politicilor prevăzute la alin. (5), societățile elaborează proceduri, având în vedere cel puțin:

a) asigurarea confidențialității, integralității și disponibilității sistemelor TIC și serviciilor TIC;

b) identificarea vulnerabilităților și modalitățile de evaluare și remediere a acestora prin optimizarea sistemelor TIC, a programelor software puse la dispoziția utilizatorilor interni și externi și adecvarea programelor antivirus sau dezvoltarea unor mecanisme de control;

c) configurarea securizată a componentelor critice ale sistemelor TIC;

d) segmentarea rețelei, prevenirea scurgerii de informații și criptarea traficului din rețea în conformitate cu clasificarea seturilor de date;

e) evaluarea dispozitivelor finale de accesare a rețelei pentru stabilirea gradului în care acestea respectă standardele de securitate;

f) mecanismele de verificare a integrității sistemelor TIC;

g) criptarea informațiilor stocate sau tranzitate, în funcție de clasificarea activelor TIC.

Articolul 8. Planurile pentru asigurarea continuității activității

(1) Societățile instituie planuri pentru asigurarea continuității activității în care prevăd cel puțin:

a) obligația de identificare a riscurilor care pot afecta sistemele TIC și serviciile TIC;

b) măsuri pentru a proteja sau a restabili confidențialitatea, integralitatea și disponibilitatea elementelor TIC;

c) perioadele maxime de restabilire a funcționalității sistemelor TIC în situațiile în care se înregistrează incidente;

d) perioadele maxime în care informațiile pot fi pierdute în cazul în care se produc incidente la anumite niveluri ale serviciilor TIC;

e) realizarea unui număr suficient de teste și de scenarii de disfuncționalitate a sistemelor TIC;

f) realizarea de scenarii de invadare controlată a sistemelor TIC pentru verificarea rezilienței cibernetice a acestora, prin tehnici, tactici și proceduri cunoscute de efectuare a unui atac cibernetic, care are în vedere anumite zone de date, procese și tehnologii și anumiți angajați, fără ca aceștia să fie avertizați și fără ca această simulare să aibă efecte negative asupra operațiunilor în desfășurare;

g) realizarea de analize în urma testelor și scenariilor pentru determinarea nivelului de asigurare a securității cibernetice;

h) măsurile pentru comunicarea eficientă și în timp util atât intern, cât și cu factori externi în caz de urgență sau de funcționare defectuoasă a sistemelor TIC;

i) actualizarea periodică a planurilor în funcție de rezultatele testelor efectuate, de evenimentele înregistrate și de modificarea obiectivelor și a activității.

(2) În vederea elaborării planurilor pentru asigurarea continuității activității, societățile colaborează cu toți factorii externi și interni adecvați.

(3) În cadrul planurilor pentru asigurarea continuității activității, societățile prevăd realizarea unor analize de impact pe bază de scenarii pentru a evalua efectele cantitative și calitative ale unor disfuncționalități severe, având în vedere cel puțin:

- a) informațiile interne și externe;
- b) clasificarea elementelor TIC în funcție de nivelul de semnificație;
- c) interdependențele dintre elementele TIC.

(4) În funcție de analizele de impact realizate conform alin. (3), societățile configurează sistemele și serviciile TIC astfel încât să prevină disfuncționalitățile cauzate de evenimentele care afectează componentele cheie.

(5) Pe baza analizelor de impact realizate conform alin. (3), societățile elaborează planuri privind modalitatea de reacție și de recuperare a sistemelor TIC și serviciilor TIC astfel încât să se minimizeze efectele negative asupra activității, în care prevăd cel puțin:

- a) obiectivele procesului de recuperare;
- b) situațiile care determină activarea planurilor respective;
- c) alocarea în mod clar a responsabilităților și atribuțiilor;
- d) măsurile pentru asigurarea integralității, disponibilității și recuperării în principal a celor mai importante active TIC, activități și servicii TIC;
- e) măsurile pentru situațiile în care recuperarea nu este posibilă într-un termen scurt și factorii care pot afecta recuperarea;

f) măsurile pentru asigurarea continuității în cazul în care furnizorii de servicii TIC înregistrează disfuncționalități, având în vedere politica privind sistemul de guvernare și în special, politica privind externalizarea;

g) măsuri pentru situațiile în care sunt activate clauzele de reziliere a contractelor de externalizare;

h) condițiile care necesită actualizarea planurilor respective.

(6) Societățile actualizează planurile prevăzute la alin. (5) în funcție de incidentele înregistrate anterior, de rezultatele testelor efectuate, de noile riscuri identificate, de modificarea obiectivelor privind procesul de recuperare, de modificarea priorităților și de alte elemente pe care le consideră necesare.

(7) Planurile prevăzute la alin. (5) sunt documentate, sunt accesibile personalului adecvat și departamentelor suport în caz de urgență și au în vedere măsuri pe termen scurt și pe termen lung.

Articolul 9. Monitorizarea securității cibernetice și a planurilor pentru asigurarea continuității activității

(1) Societățile instituie politici cu scopul de a monitoriza activitățile care au impact asupra securității cibernetice, de a se înțelege natura incidentelor și de a se identifica tendințele; politicile respective sunt revizuite periodic.

(2) În aplicarea politicilor prevăzute la alin. (1), societățile elaborează proceduri pe care le revizuiesc periodic, având în vedere cel puțin următoarele elemente care pot afecta securitatea cibernetică:

- a) factorii interni și externi;
- b) activitățile furnizorilor de servicii TIC;
- c) posibilele amenințări din interior și din exterior;
- d) mecanismele pentru detectarea, raportarea și contracararea activităților anormale și a amenințărilor.

(3) Societățile elaborează periodic un raport în urma monitorizării securității cibernetice pe baza căruia adoptă decizii și instituie mecanisme de control.

(4) Societățile verifică și evaluează periodic securitatea cibernetică și efectuează teste pentru a identifica vulnerabilitățile sistemelor TIC și serviciilor TIC, cel puțin din punct de vedere al standardelor de securitate și al aplicării politicii interne, având în vedere recomandările auditului extern și ale funcției de audit intern.

(5) Societățile instituie un cadru pentru testarea securității cibernetice cu scopul de a valida adecvarea și eficiența măsurilor adoptate pentru asigurarea acesteia, având în vedere amenințările și vulnerabilitățile identificate în procesul de monitorizare a riscurilor TIC.

(6) Cadrul pentru testarea securității cibernetice prevăzut la alin. (5) prevede, în funcție de natura, amploarea și complexitatea riscurilor inerente activității desfășurate de societăți, cel puțin:

- a) elementele ce urmează a fi testate;
- b) frecvența realizării testelor;
- c) metodele de testare.

(7) Societățile stabilesc frecvența prevăzută la alin. (6) lit. b), având în vedere cel puțin:

- a) modificarea infrastructurii, a proceselor dezvoltate și a procedurilor;
- b) modificările cauzate de incidentele înregistrate;
- c) modificările semnificative ale aplicațiilor utilizate.

(8) Societățile se asigură că:

a) testarea securității cibernetice se realizează în condiții depline de siguranță de către persoane independente care au cunoștințe și experiență adecvată în domeniul testării;

b) testarea sistemelor TIC cu nivel ridicat de semnificație se realizează cel puțin anual;

c) rezultatele testelor sunt evaluate și aplicarea măsurilor adoptate în conformitate cu rezultatele respective este monitorizată;

d) măsurile de securitate sunt actualizate în timp util.

(9) Societățile asigură testarea periodică a planurilor de continuitate a activității prevăzute la art. 8, a elementelor TIC și a interdependențelor dintre acestea, inclusiv relațiile cu furnizorii de servicii TIC, cu scopul de a evalua capacitatea de susținere a activității până la redresarea operațiunilor critice la un anumit nivel al impactului și la un nivel predefinit al asigurării serviciilor.

(10) Societățile asigură faptul că rezultatele testelor realizate conform alin. (9) sunt documentate, iar deficiențele identificate sunt analizate și sunt raportate conducerii împreună cu recomandările necesare pentru remedierea acestora.

(11) Societățile testează periodic capacitatea de stocare de siguranță a sistemelor TIC și în funcție de rezultatele testelor revizuiesc procedurile privind siguranța stocării datelor și restaurarea acestora.

(12) Societățile stabilesc metodologia de testare a sistemelor TIC, a serviciilor TIC și a măsurilor de securitate cibernetică asociate în timpul dezvoltării interne a sistemelor TIC sau înainte de achiziționarea acestora, cu scopul de a identifica potențialele puncte slabe și incidente.

Articolul 10. Dezvoltarea internă a sistemelor TIC sau achiziționarea acestora

(1) Societățile instituie politici bazate pe risc referitoare la dezvoltarea internă a sistemelor TIC sau la achiziționarea acestora, care au drept scop menținerea sistemelor respective astfel încât să se respecte cerințele de securitate cibernetică privind confidențialitatea, integralitatea și disponibilitatea informațiilor.

(2) Societățile stabilesc în mod clar obiectivele tehnice, cerințele operaționale și neoperaționale, regulile de securitate cibernetică înainte de achiziționarea sau dezvoltarea internă a sistemelor TIC.

(3) Societățile stabilesc proceduri pentru prevenirea unor modificări neintenționate sau intenționate ale sistemelor TIC în timpul dezvoltării interne a acestora și se asigură că furnizorii de servicii TIC au instituite proceduri similare.

(4) Societățile stabilesc proceduri pentru asigurarea integrității codurilor sursă ale sistemelor TIC și pentru documentarea întregului proces de dezvoltare a sistemelor TIC astfel încât să reducă dependența de experți.

(5) Societățile includ în procedurile referitoare la achiziționarea sau dezvoltarea internă a sistemelor TIC măsuri pentru utilizatorii finali ai aplicațiilor; de asemenea, mențin un registru al aplicațiilor critice pentru activitate.

Articolul 11. Prevederi finale și intrarea în vigoare

(1) În cadrul sistemului de guvernare, societățile pun în aplicare toate procedurile și politicile elaborate conform prevederilor prezentei norme, în vederea asigurării guvernancei și securității sistemelor TIC.

(2) Nerespectarea prevederilor prezentei norme se sancționează de către A.S.F. conform prevederilor art. 163 din Legea nr. 237/2015.

(3) Prezenta normă se publică în Monitorul Oficial al României, Partea I, și intră în vigoare la data publicării acesteia.

(4) Până la data de 31 decembrie 2021, societățile revizuiesc sistemul de guvernare instituit, politicile, procedurile și contractele de externalizare pentru a efectua modificările necesare în vederea conformării cu prevederile prezentei norme.