Autoritatea de Supraveghere Financiară - ASF - Normă nr. 25/2021 din 30 august 2021

Norma nr. 25/2021 privind guvernanţa şi securitatea sistemelor de tehnologia informaţiilor şi a comunicaţiilor utilizate de către societăţile de asigurare şi de reasigurare

În vigoare de la 13 septembrie 2021

Publicat în Monitorul Oficial, Partea I nr. 877 din 13 septembrie 2021. Formă aplicabilă la 20 decembrie 2023.

În temeiul prevederilor art. 2 alin. (1) lit. b), art. 3 alin. (1) lit. b) şi art. 6 alin. (2) din Ordonanţa de urgenţă a Guvernului nr. 93/2012 privind înfiinţarea, organizarea şi funcţionarea Autorităţii de Supraveghere Financiară, aprobată cu modificări şi completări prin Legea nr. 113/2013, cu modificările şi completările ulterioare,

în baza prevederilor art. 173 alin. (1) lit. t) şi ale art. 179 alin. (4) din Legea nr. 237/2015 privind autorizarea şi supravegherea activităţii de asigurare şi reasigurare, cu modificările şi completările ulterioare,

în urma deliberărilor Consiliului Autorităţii de Supraveghere Financiară în cadrul şedinţei din data de 25.08.2021,

Autoritatea de Supraveghere Financiară emite prezenta normă.

ARTICOLUL 1

Domeniul de aplicare şi semnificaţii

(1) Prezenta normă reglementează guvernanţa şi securitatea sistemelor de tehnologia informaţiilor şi a comunicaţiilor utilizate de către societăţile de asigurare şi de reasigurare.

(2) Prevederile prezentei norme se aplică, cu respectarea principiului proporţionalităţii, societăţilor şi în mod corespunzător grupurilor prevăzute la art. 1 alin. (2) pct. 20 şi 56 din Legea nr. 237/2015 privind autorizarea şi supravegherea activităţii de asigurare şi reasigurare, cu modificările şi completările ulterioare; în cazul societăţilor, prevederile prezentei norme se aplică atât societăţilor aflate sub incidenţa regimului de supraveghere Solvabilitate II, cât şi celor aflate sub incidenţa regimului naţional de supraveghere.

(3) Actele normative menţionate în prezenta normă au următoarele semnificaţii:

1. Legea nr. 237/2015 - Legea nr. 237/2015 privind autorizarea şi supravegherea activităţii de asigurare şi reasigurare, cu modificările şi completările ulterioare;

2. Norma nr. 4/2018 - Norma Autorităţii de Supraveghere Financiară nr. 4/2018 privind gestionarea riscurilor operaţionale generate de sistemele informatice utilizate de entităţile autorizate/avizate/înregistrate, reglementate şi/sau supravegheate de către Autoritatea de Supraveghere Financiară, cu modificările ulterioare;

3. Norma nr. 33/2020 - Norma Autorităţii de Supraveghere Financiară nr. 33/2020 privind externalizarea către furnizorii de servicii de tip cloud.

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

1. activ TIC - echipament software sau hardware utilizat în mediul de afaceri;

2. atac cibernetic - intervenţie sau încercare de intervenţie neautorizată asupra unui sistem TIC ce are drept scop distrugerea, modificarea, expunerea sau procurarea de seturi de date, accesul neautorizat la seturi de date sau utilizarea neautorizată a acestora;

3. confidenţialitate - capacitatea datelor de a putea fi comunicate doar persoanelor, entităţilor şi sistemelor cărora le sunt destinate;

4. disponibilitate - capacitatea unor elemente de a fi disponibile pentru utilizare în timp util de către entităţi sau persoane care au drept de acces;

5. element TIC - proces, funcţie şi activitate operaţională, critică sau semnificativă, activ TIC, bază de date;

6. furnizor de servicii TIC - terţă parte care dezvoltă procese TIC, furnizează servicii TIC şi desfăşoară activităţi TIC, integral sau parţial, în temeiul unui contract de externalizare;

7. incident - un eveniment sau o serie de evenimente conexe şi neaşteptate cu impact negativ asupra integrităţii, disponibilităţii şi confidenţialităţii sistemelor şi serviciilor TIC;

8. proiect TIC - proiect conform căruia sistemele şi serviciile TIC sunt modificate, înlocuite sau implementate, integral sau parţial;

9. proprietar de active TIC - persoană sau entitate care are răspundere pentru şi atribuţii de a dispune de activele TIC;

10. risc TIC - tip de risc operaţional care generează pierderi din cauza neadecvării sistemelor TIC sau a utilizării defectuoase a acestora;

11. securitate cibernetică - ansamblu de măsuri şi proceduri menite să asigure protejarea datelor şi a sistemelor TIC dintr-un mediu cibernetic în ceea ce priveşte confidenţialitatea, integritatea şi disponibilitatea acestora;

12. serviciu TIC - servicii furnizate utilizatorilor interni şi externi prin intermediul sistemelor TIC;

13. set de date - grupare de date electronice care necesită protecţie;

14. sistem TIC - set de aplicaţii, active TIC, date informatice şi alte structuri de utilizare a datelor, inclusiv mediul operaţional;

15. vulnerabilitate - totalitatea punctelor slabe ale activelor TIC sau ale mecanismelor de protecţie a acestora care pot fi vizate în cazul unui atac cibernetic.

(5) Categoria de riscuri TIC poate include:

a) nerespectarea regulilor de confidenţialitate;
b) deficienţe ale integrităţii sistemelor TIC şi ale datelor;
c) inadecvarea sau indisponibilitatea sistemelor TIC şi a datelor;
d) incapacitatea de a modifica sistemele TIC în timp util şi cu costuri rezonabile, atunci când mediul de afaceri se modifică;
e) derularea cu deficienţe a unor procese interne;
f) securitate fizică deficientă;
g) evenimente externe, inclusiv atacuri cibernetice.

ARTICOLUL 2

Responsabilitatea conducerii

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

(2) Conducerea este responsabilă pentru:
a) asigurarea comunicării în timp util către personalul relevant şi furnizorii de servicii TIC a strategiei TIC şi a politicii privind continuitatea activităţii TIC;
b) asigurarea supervizării aplicării în practică a strategiei TIC şi a politicii privind continuitatea activităţii TIC;
c) managementul efectiv şi adecvat al riscului TIC în cadrul sistemului de guvernanţă;
d) alocarea de resurse suficiente şi adecvate pentru asigurarea guvernanţei şi securităţii sistemelor TIC.

(3) Conducerea asigură aplicarea unor programe de instruire periodică cu scopul ca personalul să deţină în permanenţă pregătirea necesară pentru aplicarea strategiei TIC şi pentru desfăşurarea eficientă a operaţiunilor TIC şi a proceselor de management al riscului TIC.

ARTICOLUL 3

Prevederi generale referitoare la sistemul de guvernanţă

(1) Strategia TIC a societăţilor, stabilită şi aprobată de conducerea acestora conform art. 2 alin. (1), are în vedere cel puţin următoarele:
a) modalitatea în care sistemele TIC sunt optimizate;
b) evoluţia configurării sistemelor TIC, inclusiv în ceea ce priveşte dependenţele principale de furnizorii de servicii TIC;
c) obiectivele principale privind securitatea cibernetică;
d) criteriile privind achiziţionarea sau dezvoltarea internă a sistemelor TIC.

(2) Societăţile 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 ţine cont de dependenţele principale de furnizorii de servicii TIC.

(3) Societăţile instituie politici pentru a monitoriza şi evalua eficienţa aplicării strategiei TIC şi activităţile care au impact asupra securităţii cibernetice, pe care le revizuiesc periodic, actualizându-le dacă este cazul, şi elaborează proceduri în aplicarea acestora.

(4) În vederea asigurării funcţionării eficiente a sistemelor TIC, societăţile dezvoltă şi aplică programe de pregătire periodică şi programe pentru conştientizarea riscurilor TIC şi a minimizării acestora, pentru toţi angajaţii şi pentru conducere.

(5) Scopul programelor prevăzute la alin. (4) este acela de a asigura desfăşurarea activităţii şi exercitarea atribuţiilor astfel încât să se reducă erorile umane, frauda, utilizarea defectuoasă a sistemelor TIC şi pierderile cauzate de acestea.

(6) Societăţile stabilesc în sistemul de guvernanţă metodologia de dezvoltare şi de aplicare a proiectelor TIC, având în vedere cerinţele de securitate cibernetică, astfel încât:

a) să asigure implementarea corectă a strategiei TIC;

b) să minimizeze riscurile generate de interdependenţele dintre proiectele TIC;

c) să minimizeze dependenţa portofoliilor de proiecte TIC de anumite resurse sau de anumiţi specialişti.

(7) În procedurile prevăzute la alin. (3), societăţile stabilesc cerinţe referitoare la:

a) aprobarea sistemelor şi serviciilor TIC, dezvoltate intern sau achiziţionate;

b) măsurile de securitate cibernetică asociate sistemelor şi serviciilor TIC;

c) asigurarea independenţei structurii de dezvoltare a sistemelor TIC, a structurii de testare a acestora şi a structurilor nonoperaţionale faţă de activităţile operaţionale.

(8) În cadrul politicii generale privind externalizarea, societăţile stabilesc criteriile şi condiţiile în funcţie de care selectează furnizorii de servicii TIC şi condiţiile în funcţie de care este necesară schimbarea acestora.

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

a) nivelul de calitate garantat pentru serviciile furnizate;

b) obiectivele de securitate cibernetică şi obiectivele privind monitorizarea acesteia;

c) măsurile prin care se asigură securitatea cibernetică;

d) specificaţii tehnice privind durata de viaţă a datelor, dreptul de acces la date şi auditarea acestora;

e) locaţia centrelor de date;

f) modalităţile de criptare;

g) planurile de asigurare a continuităţii activităţii şi planurile pentru situaţii de urgenţă;

h) procedurile privind managementul incidentelor;

i) stabilirea clară a canalelor de raportare;

j) condiţiile de reziliere a contractelor.

(10) Societăţile 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 societăţi prevede auditarea periodică a politicii de management al riscului TIC, inclusiv a procedurilor şi sistemelor instituite în vederea aplicării acesteia, de către persoane care au suficiente cunoştinţe şi expertiză în domeniu, frecvenţa auditului fiind stabilită în funcţie 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, societăţile determină nivelul toleranţei la risc, în concordanţă cu strategia generală de risc adoptată.

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

a) cartarea periodică a elementelor TIC pentru a stabili interdependenţa dintre acestea şi riscurile TIC;

b) identificarea şi evaluarea riscurilor TIC pe baza unor criterii stabilite în funcţie de nivelul de semnificaţie al elementelor TIC, vulnerabilităţile cunoscute şi incidentele anterioare;

c) clasificarea elementelor TIC expuse la riscurile TIC în funcţie de pragul de semnificaţie stabilit şi de nivelul de protecţie a acestora din punctul de vedere al confidenţialităţii, integrităţii şi disponibilităţii;

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

e) metodele utilizate pentru determinarea pragului de semnificaţie şi a nivelului de protecţie prevăzute la lit. c) pentru a se asigura o abordare unitară şi consecventă;

f) evaluarea şi documentarea periodic a riscurilor TIC;

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

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

i) stabilirea metodelor şi a măsurilor pentru protejarea activelor TIC în funcţie de clasificarea acestora;

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

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

ARTICOLUL 5

Managementul operaţiunilor TIC

(1) În conformitate cu strategia TIC stabilită şi aprobată de conducere, societăţile elaborează politici privind managementul operaţiunilor TIC având în vedere cel puţin:

a) derularea operaţiunilor TIC;

b) capacitatea activelor TIC de a face faţă disfuncţionalităţilor;

c) înregistrarea de incidente.

(2) Societăţile menţin şi actualizează un registru al activelor TIC astfel încât să fie posibilă identificarea promptă a fiecărui element în ceea ce priveşte proprietarul, localizarea şi clasificarea acestuia din punctul de vedere al securităţii cibernetice.

(3) Societăţile monitorizează cel puţin:

a) capacitatea activelor TIC de a contribui la desfăşurarea eficientă a activităţii, pe toată durata de viaţă a acestora;

b) respectarea cerinţelor de management al riscului;

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

d) documentarea actualizării şi optimizării activelor TIC.

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

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

b) modalităţile de conectare şi monitorizare a operaţiunilor TIC pentru asigurarea detectării, analizării şi corectării erorilor.

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

a) monitorizarea capacităţii activelor TIC de a asigura prevenirea, detectarea şi contracararea disfuncţionalităţilor în timp util şi eficient;

b) capacitatea sistemelor TIC de a stoca datele în siguranţă şi de a asigura recuperarea acestora în mod eficient;

c) frecvenţa stocărilor de siguranţă în concordanţă cu nivelul de semnificaţie al datelor şi sistemelor TIC.

(6) Societăţile se asigură că stocările de siguranţă sunt realizate în locaţii care nu interferează cu locaţia principală astfel încât să se evite expunerea la aceleaşi riscuri a tuturor locaţiilor.

(7) Societăţile determină nivelul de semnificaţie al datelor şi sistemelor TIC în funcţie de rezultatele evaluării riscurilor, astfel încât să se asigure respectarea standardelor de recuperare a datelor.

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

a) criteriile adecvate şi pragurile de semnificaţie pentru încadrarea evenimentelor drept incidente;

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

c) minimizarea efectelor incidentelor şi reluarea eficientă şi în timp util a activităţii după înregistrarea acestora;

d) mecanisme pentru identificarea cauzelor care stau la baza producerii incidentelor şi măsurile pentru prevenirea producerii din nou a aceloraşi incidente;

e) mecanisme pentru asigurarea monitorizării şi gestionării incidentelor;

f) alocarea clară a responsabilităţii pentru managementul incidentelor;

g) managementul incidentelor astfel încât să se asigure reluarea şi continuarea activităţilor critice atunci când se înregistrează disfuncţionalităţi;

h) canalele de comunicare şi raportare a incidentelor în cadrul structurii organizatorice în funcţie de pragurile de semnificaţie stabilite;

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

j) mecanismele de comunicare şi colaborare cu factorii externi adecvaţi în caz de producere a unor incidente cu scopul de a minimiza efectele acestora şi de a restabili nivelul normal de funcţionare.

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

(10) Societăţile instituie politici privind modificările aduse sistemelor TIC şi elaborează proceduri în aplicarea acestora, având în vedere cel puţin:

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

b) identificarea modificărilor realizate în situaţii de urgenţă şi comunicarea acestora în timp util proprietarilor de active TIC pentru analize ulterioare;

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

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

(11) Societăţile instituie proceduri referitoare la durata de viaţă a activelor TIC pentru managementul riscului de degradare şi de scădere a eficienţei acestora din punctul de vedere al evoluţiei tehnologice, inclusiv la modalitatea de distrugere a activelor respective.

ARTICOLUL 6

Prevederi generale referitoare la securitatea cibernetică

(1) În vederea implementării strategiei TIC stabilite şi aprobate de conducere conform art. 2 alin. (1), societăţile instituie politici privind securitatea cibernetică în care stabilesc principii şi reguli pentru a se asigura respectarea confidenţialităţii, integrităţii şi disponibilităţii activelor TIC.

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

a) alocarea clară a atribuţiilor şi răspunderii pentru managementul securităţii cibernetice;

b) criteriile avute în vedere la derularea proceselor şi achiziţionarea echipamentelor tehnologice;

c) cerinţele specifice pentru tot personalul în funcţie de nivelul ierarhic.

(3) Societăţile 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) Societăţile desemnează persoanele cărora le alocă atribuţiile funcţiei de securitate cibernetică care este independentă de funcţiile operaţionale şi de cele de dezvoltare a sistemelor TIC, pentru a putea asigura în mod obiectiv securitatea cibernetică.

(5) Prin excepţie de la prevederile alin. (4), societăţile pot aloca atribuţiile funcţiei de securitate cibernetică unor persoane care deţin funcţii operaţionale, cu respectarea principiului documentării, numai dacă sunt îndeplinite cumulativ următoarele condiţii:

a) cumularea funcţiilor este necesară date fiind natura, amploarea şi complexitatea riscurilor inerente activităţii;

b) nu apar conflicte de interese pentru persoanele care exercită funcţia de securitate cibernetică;

c) costurile pentru menţinerea în funcţia de securitate cibernetică a unor persoane care nu exercită alte funcţii ar genera pentru societăţi costuri disproporţionate în raport cu totalul cheltuielilor administrative.

(6) Funcţia instituită conform alin. (4) are cel puţin următoarele atribuţii:

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

b) asigură cunoaşterea de către toţi furnizorii de servicii TIC şi de către toţi angajaţii care au acces la date şi la sistemele TIC a politicii privind securitatea cibernetică prin organizarea unor sesiuni de informare şi de instruire;

c) supervizează aplicarea şi respectarea procedurilor prevăzute la alin. (3) de către furnizorii de servicii TIC şi de către toţi angajaţii care au acces la date şi 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 menţionate la lit. a)-d).

ARTICOLUL 7

Securitatea activelor TIC, fizică şi a operaţiunilor TIC

(1) În aplicarea politicilor menţionate la art. 6 alin. (1), societăţile elaborează proceduri referitoare la securitatea activelor TIC pentru a asigura managementul identităţii utilizatorilor care au acces la sistemele TIC şi controlul asupra disfuncţionalităţilor.

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

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

b) limitarea dreptului de acces al utilizatorilor, proporţional cu atribuţiile alocate acestora;

c) prevenirea accesului neautorizat;

d) limitarea utilizării conturilor generice sau partajate şi asigurarea identificării în permanenţă a utilizatorilor autorizaţi şi a proceselor autorizate;

e) mecanismele de control al accesului discreţionar;

f) mecanismele privind accesul administrativ de la distanţă la sistemele TIC critice şi procesul de autentificare;

g) modalităţile de înregistrare şi monitorizare a activităţii utilizatorilor, în special a celor cu drepturi discreţionare, în funcţie de nivelul de semnificaţie al activităţii respective;

h) perioada de arhivare a înregistrărilor menţionate la lit. g), în funcţie de nivelul de semnificaţie al activităţii, al proceselor şi al activelor TIC;

i) modalităţile de prevenire a modificării sau eliminării neautorizate a înregistrărilor menţionate la lit. g);

j) modalităţile de identificare şi analizare, pe baza înregistrărilor menţionate la lit. g), a acţiunilor anormale detectate în timpul furnizării de servicii;

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

l) condiţiile pentru revizuirea periodică a dreptului de acces pentru ca acesta să fie acordat în funcţie de nivelul de semnificaţie al activităţii utilizatorilor şi măsurile adoptate ulterior revizuirii;

m) cerinţele privind documentarea acordării, modificării şi retragerii dreptului de acces;

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

(3) Societăţile limitează accesul prin intermediul aplicaţiilor la date şi la sistemele TIC la nivelul necesar pentru ca operaţiunile să se desfăşoare eficient.

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

a) condiţiile în care se autorizează accesul fizic la sistemele TIC în funcţie de nivelul de instruire al fiecărei persoane, atribuţiile şi responsabilităţile acesteia;

b) modalităţile de monitorizare a personalului;

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

d) condiţiile în care dreptul de acces fizic este retras şi revizuirea acestora;

e) măsurile pentru prevenirea deteriorării sistemelor TIC din cauze externe, independente de factorul uman, proporţionale cu importanţa sediului şi cu nivelul de semnificaţie al operaţiunilor TIC derulate şi al sistemelor TIC localizate în sediu;

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

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

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

a) asigurarea confidenţialităţii, integrităţii şi disponibilităţii sistemelor TIC şi serviciilor TIC;

b) identificarea vulnerabilităţilor şi modalităţile de evaluare şi remediere a acestora prin optimizarea sistemelor TIC, a programelor software puse la dispoziţia utilizatorilor interni şi externi şi adecvarea programelor antivirus sau dezvoltarea unor mecanisme de control;

c) configurarea securizată a componentelor critice ale sistemelor TIC;

d) implementarea segmentării reţelei, prevenirii scurgerii de date şi criptării traficului din reţea în conformitate cu clasificarea seturilor de date;

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

f) mecanismele de verificare a integrităţii sistemelor TIC;

g) criptarea datelor stocate sau tranzitate, în funcţie de clasificarea activelor TIC.

ARTICOLUL 8

Planurile pentru asigurarea continuităţii activităţii

(1) Societăţile instituie planuri pentru asigurarea continuităţii activităţii în care prevăd cel puţin:

a) obligaţia de identificare a riscurilor care pot afecta sistemele TIC şi serviciile TIC;

b) măsuri pentru a proteja sau a restabili confidenţialitatea, integritatea şi disponibilitatea elementelor TIC;

c) perioadele maxime de restabilire a funcţionalităţii sistemelor TIC în situaţiile în care se înregistrează incidente;

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

e) realizarea unui număr suficient de teste şi de scenarii de disfuncţionalitate a sistemelor TIC;

f) realizarea de scenarii de atac cibernetic controlat asupra sistemelor TIC pentru verificarea rezilienţei cibernetice a acestora, prin tehnici, tactici şi proceduri cunoscute de efectuare a unui atac cibernetic, care are în vedere zone de date, procese, tehnologii şi angajaţi care nu sunt avertizaţi şi fără ca simularea respectivă să aibă efecte negative asupra operaţiunilor în desfăşurare;

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

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

i) actualizarea periodică a planurilor în funcţie de rezultatele testelor efectuate, de evenimentele înregistrate şi de modificarea obiectivelor şi a activităţii.

(2) În vederea elaborării planurilor pentru asigurarea continuităţii activităţii, societăţile colaborează cu toţi factorii externi şi interni adecvaţi.

(3) În cadrul planurilor pentru asigurarea continuităţii activităţii, societăţile prevăd realizarea unor analize de impact pe bază de scenarii pentru a evalua

efectele cantitative şi calitative ale unor disfuncţionalităţi severe, având în vedere cel puţin:

a) datele interne şi externe;

b) clasificarea elementelor TIC în funcţie de nivelul de semnificaţie;

c) interdependenţele dintre elementele TIC.

(4) În funcţie de analizele de impact realizate conform alin. (3), societăţile configurează sistemele şi serviciile TIC astfel încât să prevină disfuncţionalităţile cauzate de evenimentele care afectează componentele-cheie.

(5) Pe baza analizelor de impact realizate conform alin. (3), societăţile elaborează planuri privind modalitatea de reacţie şi de recuperare a sistemelor TIC şi serviciilor TIC astfel încât să se minimizeze efectele negative asupra activităţii, în care prevăd cel puţin:

a) obiectivele procesului de recuperare;

b) situaţiile care determină activarea planurilor respective;

c) alocarea în mod clar a responsabilităţilor şi atribuţiilor;

d) măsurile pentru asigurarea integrităţii, disponibilităţii şi recuperării în principal a celor mai importante active TIC, activităţi şi servicii TIC;

e) măsurile pentru situaţiile în care recuperarea nu este posibilă într-un termen scurt şi factorii care pot afecta recuperarea;

f) măsurile pentru asigurarea continuităţii în cazul în care furnizorii de servicii TIC înregistrează disfuncţionalităţi, având în vedere politica privind sistemul de guvernanţă şi, în special, politica privind externalizarea;

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

h) condiţiile care necesită actualizarea planurilor respective.

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

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

ARTICOLUL 9

Monitorizarea securităţii cibernetice şi a planurilor pentru asigurarea continuităţii activităţii

(1) Societăţile instituie politici cu scopul de a monitoriza activităţile care au impact asupra securităţii cibernetice, de a se înţelege natura incidentelor şi de a se identifica tendinţele; politicile respective sunt revizuite periodic.

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

a) factorii interni şi externi;

b) activităţile furnizorilor de servicii TIC;

c) posibilele ameninţări din interior şi din exterior;

d) mecanismele pentru detectarea, raportarea şi contracararea activităţilor anormale şi a ameninţărilor.

(3) Societăţile elaborează periodic un raport în urma monitorizării securităţii cibernetice pe baza căruia adoptă decizii şi instituie mecanisme de control.

(4) Societăţile verifică şi evaluează periodic securitatea cibernetică şi efectuează teste pentru a identifica vulnerabilităţile sistemelor TIC şi serviciilor TIC, cel puţin din punctul de vedere al standardelor de securitate şi al aplicării politicii interne, având în vedere recomandările auditului extern şi ale funcţiei de audit intern.

(5) Societăţile instituie un cadru pentru testarea securităţii cibernetice cu scopul de a valida adecvarea şi eficienţa măsurilor adoptate pentru asigurarea acesteia, având în vedere ameninţările şi vulnerabilităţile identificate în procesul de monitorizare a riscurilor TIC.

(6) Cadrul pentru testarea securităţii cibernetice prevăzut la alin. (5) prevede, în funcţie de natura, amploarea şi complexitatea riscurilor inerente activităţii desfăşurate de societăţi, cel puţin:

a) elementele ce urmează a fi testate;

b) frecvenţa realizării testelor;

c) metodele de testare.

(7) Societăţile stabilesc frecvenţa prevăzută la alin. (6) lit. b), având în vedere cel puţin:

a) modificarea infrastructurii, a proceselor dezvoltate şi a procedurilor;

b) modificările cauzate de incidentele înregistrate;

c) modificările semnificative ale aplicaţiilor utilizate.

(8) Societăţile se asigură că:

a) testarea securităţii cibernetice se realizează în condiţii depline de siguranţă de către persoane independente care au cunoştinţe şi experienţă adecvată în domeniul testării;

b) testarea sistemelor TIC cu nivel ridicat de semnificaţie, inclusiv sistemele importante prevăzute în Norma nr. 4/2018, se realizează cel puţin anual;

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

d) măsurile de securitate sunt actualizate fără întârziere în urma evaluării prevăzute la lit. c).

(9) Societăţile asigură testarea periodică a planurilor de continuitate a activităţii prevăzute la art. 8, a elementelor TIC şi a interdependenţelor dintre acestea, inclusiv relaţiile cu furnizorii de servicii TIC, cu scopul de a evalua capacitatea de susţinere a activităţii până la redresarea operaţiunilor critice la un anumit nivel al impactului şi la un nivel predefinit al asigurării serviciilor.

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

(11) Societăţile testează periodic capacitatea de stocare de siguranţă a sistemelor TIC şi în funcţie de rezultatele testelor revizuiesc procedurile privind siguranţa stocării datelor şi restaurarea acestora.

(12) Societăţile stabilesc metodologia de testare a sistemelor TIC, a serviciilor TIC şi a măsurilor de securitate cibernetică asociate în timpul dezvoltării interne a sistemelor TIC sau înainte de achiziţionarea acestora, cu scopul de a identifica potenţialele puncte slabe şi incidente.

ARTICOLUL 10

Dezvoltarea internă a sistemelor TIC sau achiziţionarea acestora

(1) Societăţile instituie politici bazate pe risc referitoare la dezvoltarea internă a sistemelor TIC sau la achiziţionarea acestora, care au drept scop menţinerea sistemelor respective astfel încât să se respecte cerinţele de securitate cibernetică privind confidenţialitatea, integritatea şi disponibilitatea datelor.

(2) Societăţile stabilesc în mod clar obiectivele tehnice, cerinţele operaţionale şi neoperaţionale, regulile de securitate cibernetică înainte de achiziţionarea sau dezvoltarea internă a sistemelor TIC.

(3) Societăţile stabilesc proceduri pentru prevenirea unor modificări neintenţionate sau intenţionate ale sistemelor TIC în timpul dezvoltării interne a acestora şi se asigură că furnizorii de servicii TIC au instituite proceduri similare.

(4) Societăţile stabilesc proceduri pentru asigurarea integrităţii codurilor-sursă ale sistemelor TIC şi pentru documentarea întregului proces de dezvoltare a sistemelor TIC astfel încât să reducă dependenţa de experţi.

(5) Societăţile includ în procedurile referitoare la achiziţionarea sau dezvoltarea internă a sistemelor TIC măsuri pentru utilizatorii finali ai aplicaţiilor; de asemenea, menţin un registru al aplicaţiilor critice pentru activitate.

ARTICOLUL 11

Prevederi finale şi intrarea în vigoare

(1) În cadrul sistemului de guvernanţă, societăţile pun în aplicare toate procedurile şi politicile elaborate conform prevederilor prezentei norme, în vederea asigurării guvernanţei şi securităţii sistemelor TIC.

(2) Nerespectarea prevederilor prezentei norme se sancţionează de către Autoritatea de Supraveghere Financiară conform prevederilor art. 163 din Legea nr. 237/2015, cu modificările şi completările ulterioare.

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

(4) Pentru a efectua modificările necesare în vederea conformării cu prevederile prezentei norme, societăţile revizuiesc sistemul de guvernanţă instituit, politicile şi procedurile până la data de 30 iunie 2022 şi revizuiesc contractele de externalizare până la data de 31 decembrie 2022.

Preşedintele Autorităţii de Supraveghere Financiară,
Nicu Marcu

Bucureşti, 30 august 2021.

Nr. 25.