EIOPA-BoS-20/600

Ghid privind guvernanța și securitatea în domeniul tehnologiei informației și comunicațiilor

EIOPA – Westhafen Tower, Westhafenplatz 1 – 60327 Frankfurt – Germany – Tel. + 49 69-951119-20;
Fax. + 49 69-951119-19; e-mail: info@eiopa.europa.eu site: www.eiopa.europa.eu

Cuprins

Context

1. În conformitate cu articolul 16 din Regulamentul (UE) nr. 1094/2010, EIOPA poate emite ghiduri și recomandări adresate autorităților competente și instituțiilor financiare cu scopul de a stabili practici de supraveghere consecvente, eficiente și eficace și de a asigura aplicarea comună, uniformă și consecventă a dreptului Uniunii.

2. Conform articolului 16 alineatul (3) din același regulament, autoritățile competente și instituțiile financiare trebuie să depună toate eforturile pentru a respecta aceste ghiduri și recomandări.

3. EIOPA a identificat necesitatea de a elabora un ghid specific privind guvernanța și securitatea în domeniul tehnologiei informației și comunicațiilor (TIC) în ceea ce privește articolele 41 și 44 din Directiva 2009/138/CE în contextul analizei efectuate ca răspuns la Planul de acțiune al Comisiei Europene privind FinTech (COM (2018) 0109 final), la Planul de convergență al EIOPA în materie de supraveghere 2018-2019[1] și în urma interacțiunilor cu alte câteva părți interesate[2].

4. După cum s-a raportat în avizul comun al autorităților europene de supraveghere adresat Comisiei Europene, Ghidul EIOPA privind sistemul de guvernanță *„nu reflectă în mod corespunzător importanța abordării gestionării riscurilor TIC (inclusiv a riscurilor cibernetice)”*. Nu există niciun ghid cu privire la elementele esențiale care sunt recunoscute în general ca făcând parte din guvernanța și securitatea în domeniul TIC corespunzătoare”.

5. Analiza situației (legislative) actuale din UE în ceea ce privește avizul comun de mai sus a arătat că majoritatea statelor membre ale UE au definit norme naționale pentru guvernanța și securitatea în domeniul TIC. Deși cerințele sunt similare, cadrul de reglementare este încă fragmentat. În plus, un sondaj privind practicile actuale de supraveghere a scos la iveală o diversitate de practici – de la „nicio supraveghere specifică” la „o supraveghere strictă” (inclusiv „inspecții din exterior” și „inspecții la fața locului”).

6. În plus, complexitatea TIC este în creștere, iar frecvența incidentelor legate de TIC (inclusiv a incidentelor cibernetice) este și ea în creștere, ca și impactul negativ al unor astfel de incidente asupra funcționării operaționale a întreprinderilor. Din acest motiv, gestionarea riscurilor TIC și de securitate este fundamentală pentru ca o întreprindere să-și atingă obiectivele strategice, corporative, operaționale și de reputație.

7. În plus, în sectorul asigurărilor, care cuprinde atât modele de afaceri tradiționale, cât și modele inovatoare, există o dependență din ce în ce mai mare de TIC în furnizarea de servicii de asigurare și în funcționarea operațională normală a întreprinderilor, de exemplu, digitalizarea sectorului asigurărilor (InsurTech, IoT etc.), precum și interconectarea prin canale de telecomunicații (internet, conexiuni mobile și fără fir și rețele de arie largă). Acest lucru face ca întreprinderile să fie vulnerabile la incidente de securitate, inclusiv la atacuri cibernetice. Prin urmare, este important să se asigure că întreprinderile sunt pregătite în mod corespunzător să-și gestioneze riscurile TIC și de securitate.

[1] https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

[2] Raportul publicat de EIOPA ca răspuns la Planul de acțiune al Comisiei Europene privind FinTech poate fi obținut aici.

8. În plus, recunoscând necesitatea întreprinderilor de a fi pregătite pentru riscuri cibernetice[3] și de a dispune de un cadru solid de securitate cibernetică, prezentul ghid acoperă, de asemenea, securitatea cibernetică ca parte a măsurilor de securitate a informațiilor ale întreprinderii. Deși prezentul ghid recunoaște că securitatea cibernetică ar trebui să fie abordată în cadrul gestionării generale a riscurilor TIC și de securitate a unei întreprinderi, este important să se sublinieze faptul că atacurile cibernetice au unele caracteristici specifice, care ar trebui să fie luate în considerare pentru a se asigura că măsurile de securitate a informațiilor atenuează în mod adecvat riscul cibernetic:

   a) atacurile cibernetice sunt adesea mai dificil de gestionat (și anume, de identificat, de neutralizat, de detectat, de respins și de surmontat pe deplin) decât majoritatea celorlalte surse de risc TIC și de securitate, iar amploarea daunelor este, de asemenea, dificil de determinat;

   b) unele atacuri cibernetice pot face ca gestionarea comună a riscurilor și mecanismele de asigurare a continuității activității, precum și procedurile de recuperare în caz de dezastru să devină ineficace, deoarece acestea ar putea propaga programe malware în sistemele de rezervă, pentru a le face indisponibile sau pentru a corupe datele de rezervă;

   c) furnizorii de servicii, brokerii, agenții (de administrare) și intermediarii pot deveni canale de propagare a atacurilor cibernetice. Amenințările tacite contagioase pot utiliza interconectivitatea prin legături de telecomunicații terțe pentru a penetra sistemul TIC al întreprinderii. Prin urmare, o întreprindere interconectată care are o relevanță individuală redusă poate deveni vulnerabilă și o sursă de propagare a riscurilor și poate avea un impact sistemic. Respectând principiul celei mai slabe verigi, securitatea cibernetică nu ar trebui să reprezinte doar o preocupare pentru principalii participanți la piață sau pentru furnizorii de servicii critice.

9. Obiectivul prezentului ghid este:

   a) să ofere clarificări și transparență participanților la piață cu privire la informațiile minime solicitate și la capacitățile de securitate cibernetică, și anume linia de bază în materie de securitate;

   b) să evite un eventual arbitraj de reglementare;

   c) să promoveze convergența în materie de supraveghere în ceea ce privește așteptările și procesele aplicabile în legătură cu guvernanța și securitatea în domeniul TIC ca element esențial pentru gestionarea adecvată a riscurilor TIC și de securitate.

[3] Pentru o definiție a riscului cibernetic, vă rugăm să consultați Lexiconul cibernetic al CSF, 12 noiembrie 2018, https://www.fsb.org/wp-content/uploads/12th-1.pdf

Ghid privind guvernanța și securitatea în domeniul tehnologiei informației și comunicațiilor

Introducere

1. În conformitate cu articolul 16 din Regulamentul (UE) nr. 1094/2010[4], EIOPA emite ghiduri care oferă recomandări autorităților de supraveghere cu privire la modul în care întreprinderile de asigurare și reasigurare (denumite colectiv „întreprinderi") ar trebui să aplice cerințele în materie de guvernanță prevăzute în Directiva 2009/138/CE[5] („Directiva Solvabilitate II ") și în Regulamentul delegat (UE) nr. 2015/35[6] al Comisiei („Regulamentul delegat") în contextul guvernanței și securității în domeniul tehnologiei informației și comunicațiilor („TIC"). În acest scop, prezentul ghid se bazează pe dispozițiile privind guvernanța prevăzute la articolele 41, 44, 46, 47, 132 și 246 din Directiva Solvabilitate II și la articolele 258-260, 266, 268-271 și 274 din Regulamentul delegat. În plus, prezentul ghid se bazează, de asemenea, pe îndrumările din Ghidul EIOPA privind sistemul de guvernanță (EIOPA-BoS-14/253)[7] și din Ghidul EIOPA privind externalizarea către furnizorii de servicii cloud (EIOPA-BoS-19/270)[8].
2. Ghidul se aplică atât întreprinderilor individuale, cât și, *mutatis mutandis*, la nivelul grupului[9].
3. Autoritățile competente ar trebui să țină seama de principiul proporționalității[10], atunci când respectă sau supraveghează respectarea acestui ghid, care ar trebui să garanteze că mecanismele de guvernanță, inclusiv cele legate de guvernanța și securitatea în domeniul TIC, sunt proporționale cu natura, amploarea și complexitatea riscurilor corespunzătoare cu care se confruntă sau se pot confrunta întreprinderile respective.
4. Prezentul ghid ar trebui citit în paralel cu Directiva Solvabilitate II, Regulamentul delegat, Ghidul EIOPA privind sistemul de guvernanță și cu Ghidul EIOPA privind externalizarea către furnizorii de servicii cloud și fără a aduce atingere acestora. Prezentul ghid este menit să fie neutru din punct de vedere tehnologic și metodologic.

Definiții

5. Termenii care nu sunt definiți în prezentul ghid au sensul definit în Directiva Solvabilitate II.
6. În sensul prezentului ghid, se aplică următoarele definiții:

[4] 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).

[5] Directiva 2009/138/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 privind accesul la activitate și desfășurarea activității de asigurare și de reasigurare (Solvabilitate II) (JO L 335, 17.12.2009, p. 1).

[6] Regulamentul delegat (UE) 2015/35 al Comisiei din 10 octombrie 2014 de completare a Directivei 2009/138/CE a Parlamentului European și a Consiliului privind accesul la activitate și desfășurarea activității de asigurare și de reasigurare (Solvabilitate II) (JO L 12, 17.1.2015, p. 1).

[7] https://www.eiopa.europa.eu/content/guidelines-system-governance_en?source=search

[8] https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-outsourcing-cloud-service-providers_en?source=search

[9] Articolul 212 alineatul (1) din Directiva 2009/138/CE.

[10] Articolul 29 alineatul (3) din Directiva 2009/138/CE.

Proprietar de active	Persoana sau entitatea responsabilă și autorizată pentru un activ informațional sau TIC.
Disponibilitate	Proprietatea informațiilor de a putea fi accesate și utilizate la cerere (în termen) de către o entitate autorizată.
Confidențialitate	Proprietatea informațiilor de a nu fi puse la dispoziția persoanelor, entităților, proceselor sau sistemelor neautorizate sau de a nu fi divulgate acestora.
Atac cibernetic	Orice tip de piraterie informatică care duce la o tentativă ofensivă sau răuvoitoare de a distruge, expune, modifica, dezactiva, fura sau obține acces neautorizat la un activ informațional care vizează sistemele TIC sau de a le utiliza în mod neautorizat.
Securitate cibernetică	Păstrarea confidențialității, integrității și disponibilității informațiilor și/sau a sistemelor informatice prin mediul cibernetic.
Activ TIC	Un activ de natură software sau hardware care se găsește în mediul de afaceri.
Proiecte TIC	Orice proiect sau parte a acestuia în care sunt modificate, înlocuite sau implementate sisteme și servicii TIC.
Risc TIC și de securitate	Ca subcomponentă a riscului operațional; riscul înregistrării de pierderi din cauza încălcării confidențialității, pierderii integrității sistemelor și a datelor, caracterului necorespunzător sau indisponibilității sistemelor și datelor sau incapacității de a schimba tehnologia informației (TI) într-o perioadă de timp și la costuri rezonabile, atunci când cerințele de mediu sau de afaceri se schimbă (agilitate). Aceasta include riscuri de securitate care rezultă fie din procese interne inadecvate sau care nu și-au îndeplinit funcția în mod corespunzător, fie din evenimente externe, inclusiv din atacuri cibernetice sau din securitatea fizică inadecvată.
Securitatea informațiilor	Păstrarea confidențialității, a integrității și a disponibilității informațiilor și/sau a sistemelor informatice. În plus, pot fi implicate și alte proprietăți, cum ar fi autenticitatea, răspunderea, nerepudierea și fiabilitatea.

Servicii TIC	Serviciile furnizate de sisteme TIC și furnizori de servicii unuia sau mai multor utilizatori interni sau externi.
Sisteme TIC	Setul de aplicații, servicii, active TI, active TIC sau alte componente de prelucrare a informațiilor, inclusiv mediul de operare.
Activ informațional	O colecție de informații, corporale sau necorporale, care se cuvine să fie protejate.
Integritate	Proprietatea de a fi corect și complet.
Incident operațional sau de securitate	Un eveniment unic sau o serie de evenimente corelate neplanificate, care au sau vor avea probabil un impact negativ asupra integrității, disponibilității și confidențialității sistemelor și serviciilor TIC.
Furnizor de servicii	O entitate terță care realizează un proces, un serviciu sau o activitate ori părți din acestea, în baza unui angajament de externalizare.
Test de penetrare bazat pe amenințări	O încercare controlată de a compromite reziliența cibernetică a unei entități prin simularea tacticilor, tehnicilor și procedurilor actorilor răuvoitori din viața reală. Aceasta se bazează pe informații specifice privind amenințările și se concentrează asupra angajaților, proceselor și tehnologiei unei entități, cu un nivel minim de cunoștințe practice și impact asupra operațiunilor.
Vulnerabilitate	Un punct slab, o susceptibilitate sau un defect al unui activ sau al unui dispozitiv de comandă care poate fi exploatat de una sau mai multe amenințări.

7. Prezentul ghid se aplică începând de la 1 iulie 2021.

Recomandarea 1 – Proporționalitate

8. Întreprinderile ar trebui să aplice prezentul ghid în mod proporțional cu natura, amploarea și complexitatea riscurilor inerente activității lor.

Recomandarea 2 – TIC în cadrul sistemului de guvernanță

9. Organul administrativ, de conducere sau de control ar trebui să se asigure că sistemul de guvernanță al întreprinderilor, în special sistemul de gestionare a riscurilor și de control intern, gestionează în mod adecvat riscurile TIC și de securitate ale întreprinderilor.

10. Organul administrativ, de conducere sau de control ar trebui să se asigure că numărul și competențele membrilor personalului întreprinderilor sunt corespunzătoare pentru a veni permanent în sprijinul nevoilor lor operaționale TIC și a proceselor lor de gestionare a riscurilor TIC și de securitate, precum și pentru a asigura punerea în aplicare a strategiei lor TIC. În plus, personalul ar trebui să beneficieze în mod regulat de o formare adecvată cu privire la riscurile TIC și de securitate, inclusiv la securitatea informațiilor, astfel cum se prevede în recomandarea 13.

11. Organul administrativ, de conducere sau de control ar trebui să se asigure că resursele alocate sunt adecvate pentru a îndeplini cerințele de mai sus.

Recomandarea 3 – Strategia TIC

12. Organul administrativ, de conducere sau de control are responsabilitatea generală de a stabili și de a aproba strategia scrisă a întreprinderilor în domeniul TIC, ca parte a strategiei lor globale de afaceri și în conformitate cu aceasta, precum și de a supraveghea comunicarea și punerea sa în aplicare.

13. Strategia TIC ar trebui să definească cel puțin:

    a) modul în care ar trebui să evolueze domeniul TIC al întreprinderilor pentru a sprijini și a pune în mod eficient în aplicare strategia lor de afaceri, inclusiv evoluția structurii organizaționale, a modelelor de afaceri, a sistemului TIC și a dependențelor cheie de furnizorii de servicii;

    b) evoluția arhitecturii TIC, inclusiv a dependențelor de furnizorii de servicii; și

    c) obiective clare de securitate a informațiilor, punând accent pe sisteme și servicii TIC, pe procese și personal.

14. Întreprinderile ar trebui să se asigure că strategia TIC este pusă în aplicare, adoptată și comunicată în timp util tuturor angajaților și, după caz, furnizorilor de servicii relevanți.

15. De asemenea, întreprinderile ar trebui să instituie un proces de monitorizare și măsurare a eficacității punerii în aplicare a strategiei lor TIC. Acest proces ar trebui revizuit și actualizat în mod regulat.

Recomandarea 4 – Riscurile TIC și de securitate în cadrul sistemului de gestionare a riscurilor

16. Organul administrativ, de conducere sau de control are responsabilitatea generală de a institui un sistem eficace de gestionare a riscurilor TIC și de securitate în cadrul sistemului general de gestionare a riscurilor al întreprinderii. Aceasta include determinarea toleranței la risc pentru riscurile respective, în conformitate cu strategia de risc a întreprinderii, și un raport periodic scris privind rezultatul procesului de gestionare a riscurilor adresat organului administrativ, de conducere sau de control.

17. În cadrul sistemului lor general de gestionare a riscurilor, întreprinderile ar trebui să ia în considerare, în legătură cu riscurile TIC și de securitate (definind în același timp cerințele de protecție TIC descrise mai jos), cel puțin următoarele elemente:

    a) întreprinderile ar trebui să realizeze și să actualizeze periodic o cartografiere a proceselor și activităților lor economice, a funcțiilor aferente activității, a rolurilor și a activelor (de exemplu, activele informaționale și activele TIC), pentru a identifica importanța acestora și interdependențele lor cu riscurile TIC și de securitate;

b) întreprinderile ar trebui să identifice și să evalueze toate riscurile TIC și de securitate relevante la care sunt expuse și să clasifice procesele și activitățile economice, funcțiile aferente activității, rolurile și activele identificate (de exemplu, activele informaționale și activele TIC) din punctul de vedere al nivelului critic. De asemenea, întreprinderile ar trebui să evalueze cerințele de protecție în ceea ce privește, cel puțin, confidențialitatea, integritatea și disponibilitatea acestor procese și activități economice, funcții aferente activității, roluri și active (de exemplu, active informaționale și active TIC). Ar trebui identificați proprietarii de active, care sunt responsabili pentru clasificarea activelor;

c) metodele utilizate pentru determinarea nivelului critic, precum și a nivelului de protecție necesar, în special în ceea ce privește obiectivele de protecție a integrității, disponibilității și confidențialității, ar trebui să asigure faptul că cerințele de protecție rezultate sunt coerente și complete;

d) măsurarea riscurilor TIC și de securitate ar trebui realizată pe baza criteriilor TIC și de securitate definite, luând în considerare nivelul critic al proceselor și activităților lor economice, al funcțiilor aferente activității, al rolurilor și al activelor (de exemplu, activele informaționale și activele TIC), amploarea vulnerabilităților cunoscute și a incidentelor anterioare care au afectat întreprinderea;

e) evaluarea riscurilor TIC și de securitate ar trebui efectuată și documentată în mod regulat. De asemenea, această evaluare ar trebui realizată înainte de orice schimbare majoră a infrastructurii, a proceselor sau a procedurilor care afectează procesele și activitățile economice, funcțiile aferente activității, rolurile și activele (de exemplu, activele informaționale și activele TIC);

f) pe baza evaluării riscurilor, întreprinderile ar trebui, cel puțin, să definească și să pună în aplicare măsuri de gestionare a riscurilor TIC și de securitate identificate și să protejeze activele informaționale în conformitate cu clasificarea acestora. Aceasta ar trebui să includă definirea măsurilor de gestionare a riscurilor reziduale.

18. Rezultatele procesului de gestionare a riscurilor TIC și de securitate ar trebui să fie aprobate de organul administrativ, de conducere sau de control și incluse în procesul de gestionare a riscurilor operaționale în cadrul gestionării generale a riscurilor de către întreprinderi.

Recomandarea 5 – Auditul

19. Guvernanța, sistemele și procesele întreprinderilor aferente riscurilor lor TIC și de securitate ar trebui auditate periodic, în conformitate cu planul de audit al întreprinderilor[11], de către auditori cu suficiente cunoștințe, competențe și expertiză în domeniul riscurilor TIC și de securitate, pentru a oferi organului administrativ, de conducere sau de control asigurări independente cu privire la eficacitatea acestora. Frecvența și obiectul acestor audituri ar trebui să fie proporționale cu riscurile TIC și de securitate relevante.

[11] Articolul 271 din Regulamentul delegat.

Recomandarea 6 – Măsurile și politica în domeniul securității informațiilor

20. Întreprinderile ar trebui să instituie o politică în domeniul securității informațiilor, aprobată de organul administrativ, de conducere sau de control, care ar trebui să definească principiile de nivel înalt și normele de protejare a confidențialității, integrității și disponibilității informațiilor întreprinderilor pentru a sprijini punerea în aplicare a strategiei TIC.

21. Politica ar trebui să conțină o descriere a rolurilor și responsabilităților principale de gestionare a securității informațiilor și ar trebui să stabilească cerințele referitoare la securitatea informațiilor pentru personal, procese și tehnologie, recunoscând faptul că personalul de la toate nivelurile are responsabilități în asigurarea securității informațiilor întreprinderilor.

22. Politica ar trebui comunicată în cadrul întreprinderii și ar trebui să se aplice tuturor membrilor personalului. De asemenea, acolo unde este cazul și este relevant, politica în domeniul securității informațiilor sau părți ale acesteia ar trebui comunicate și aplicate furnizorilor de servicii.

23. Pe baza politicii, întreprinderile ar trebui să instituie și să pună în aplicare mai multe proceduri specifice de securitate a informațiilor și măsuri de securitate a informațiilor, *printre altele*, pentru diminuarea riscurilor TIC și de securitate la care sunt expuse. Aceste proceduri și măsuri de securitate a informațiilor ar trebui să cuprindă toate procesele descrise în prezentul ghid, după caz.

Recomandarea 7 – Funcția de securitate a informațiilor

24. Întreprinderile ar trebui să stabilească, în cadrul sistemului lor de guvernanță și în conformitate cu principiul proporționalității, o funcție de securitate a informațiilor, responsabilitățile fiind atribuite unei persoane desemnate. Întreprinderile ar trebui să asigure independența și obiectivitatea funcției de securitate a informațiilor, separând-o în mod corespunzător de procesele de dezvoltare și exploatare TIC. Funcția ar trebui să fie subordonată organului administrativ, de conducere sau de control.

25. Sarcinile funcției de securitate a informațiilor sunt, de regulă, următoarele:

    a) să sprijine organul administrativ, de conducere sau de control atunci când definește și menține politica în domeniul securității informațiilor pentru întreprinderi și să controleze punerea în aplicare a acesteia;

    b) să raporteze și să consilieze periodic și ad-hoc organul administrativ, de conducere sau de control cu privire la situația securității informațiilor și la evoluția acesteia;

    c) să monitorizeze și să revizuiască punerea în aplicare a măsurilor de securitate a informațiilor;

    d) să se asigure că cerințele de securitate a informațiilor sunt respectate atunci când sunt utilizați furnizori de servicii;

    e) să se asigure că toți angajații și furnizorii de servicii care accesează informații și sisteme sunt informați în mod adecvat cu privire la politica în domeniul securității informațiilor, de exemplu prin sesiuni de formare și conștientizare cu privire la securitatea informațiilor;

f) să coordoneze examinarea operațională sau a incidentelor de securitate și să le raporteze pe cele relevante organului administrativ, de conducere sau de control.

Recomandarea 8 – Securitatea logică

26. Întreprinderile ar trebui să definească, să documenteze și să pună în aplicare proceduri de control al accesului logic sau de securitate logică (gestionarea identității și a accesului), în conformitate cu cerințele de protecție, astfel cum sunt definite la recomandarea 4. Aceste proceduri ar trebui puse în aplicare, impuse, monitorizate și revizuite periodic și ar trebui să includă și controale pentru monitorizarea anomaliilor. Aceste proceduri ar trebui să pună în aplicare cel puțin următoarele elemente, unde termenul „utilizator” include și utilizatori tehnici:

a) Nevoia de a ști, privilegiul minim și separarea sarcinilor: întreprinderile ar trebui să gestioneze drepturile de acces, inclusiv accesul de la distanță la activele informaționale și la sistemele lor de asistență, pe baza „nevoii de a ști”. Utilizatorilor ar trebui să li se acorde drepturile minime de acces strict necesare pentru executarea sarcinilor lor (principiul „privilegiului minim”), adică pentru protejarea accesului nejustificat la date sau pentru a împiedica alocarea unor combinații de drepturi de acces care pot fi utilizate pentru a eluda controalele (principiul „separării sarcinilor”);

b) Răspunderea utilizatorului: întreprinderile ar trebui să limiteze pe cât posibil utilizarea de conturi de utilizator generice și partajate și ar trebui să se asigure că utilizatorii pot fi în orice moment identificați și că se poate efectua trasabilitatea lor până la persoana fizică responsabilă sau până la sarcina autorizată pentru acțiunile întreprinse în sistemele TIC;

c) Drepturile de acces privilegiat: întreprinderile ar trebui să pună în aplicare controale solide ale accesului privilegiat la sistem prin limitarea strictă și supravegherea îndeaproape a conturilor cu drepturi sporite de acces la sistem (de exemplu, a conturilor de administrator);

d) Accesul de la distanță: pentru a asigura comunicarea în condiții de siguranță și reducerea riscurilor, accesul administrativ de la distanță la sistemele TIC critice ar trebui acordat numai pe baza principiului necesității de a cunoaște și atunci când se utilizează soluții de autentificare puternice;

e) Înregistrarea activităților utilizatorilor: activitățile utilizatorilor ar trebui înregistrate și monitorizate în mod proporțional, incluzând, cel puțin, activitățile utilizatorilor privilegiați. Jurnalele de acces ar trebui securizate pentru a împiedica modificarea sau ștergerea neautorizată și ar trebui păstrate o perioadă de timp proporțională cu nivelul critic al funcțiilor aferente activității, al proceselor de asistență și al activelor informaționale identificate, fără a aduce atingere cerințelor de păstrare a datelor, prevăzute în legislația națională și a UE. Întreprinderile ar trebui să utilizeze aceste informații pentru facilitarea identificării și investigării activităților anormale detectate în cadrul prestării de servicii;

f) Gestionarea accesului: drepturile de acces ar trebui acordate, retrase și modificate în timp util, în conformitate cu procedurile de aprobare predefinite, în cazul în care este implicat proprietarul activelor informaționale aplicabile. În cazul în care accesul nu mai este necesar, drepturile de acces ar trebui revocate imediat;

g) Evaluarea accesului: drepturile de acces ar trebui revizuite periodic pentru a se asigura că utilizatorii nu dețin privilegii excesive și că drepturile de acces sunt retrase atunci când nu mai sunt necesare;

h) Acordarea, modificarea, revocarea drepturilor de acces ar trebui documentate într-un mod care să faciliteze înțelegerea și analiza; și

i) Metodele de autentificare: întreprinderile ar trebui să aplice metode de autentificare suficient de solide care să asigure respectarea adecvată și eficientă a politicilor și procedurilor de control al accesului. Metodele de autentificare ar trebui să fie proporționale cu nivelul critic al sistemelor TIC, al informațiilor sau al procesului care este accesat. Acestea ar trebui să conțină cel puțin parole complexe sau metode de autentificare mai sigure (cum ar fi autentificarea cu doi factori), în funcție de riscul la care se expun.

27. Accesul electronic prin depunerea de cereri de acces la date și sisteme TIC ar trebui să fie limitat la minimul necesar pentru prestarea serviciului relevant.

Recomandarea 9 – Securitatea fizică

28. Întreprinderile ar trebui să definească, să documenteze și să pună în aplicare măsuri de securitate fizică (de exemplu, măsuri de protecție împotriva căderilor de tensiune, incendiilor, inundațiilor și accesului fizic neautorizat) pentru a-și proteja sediile, centrele de date și zonele sensibile împotriva accesului neautorizat și pericolelor pentru mediu.

29. Accesul fizic la sistemele TIC ar trebui acordat numai persoanelor autorizate. Autorizarea ar trebui atribuită în conformitate cu sarcinile și responsabilitățile persoanei în cauză și limitată la persoanele care sunt instruite și monitorizate în mod corespunzător. Accesul fizic ar trebui revizuit periodic pentru a se asigura că drepturile de acces sunt revocate imediat ce nu mai sunt necesare.

30. Măsurile adecvate de protecție împotriva pericolelor pentru mediu ar trebui să fie proporționale cu importanța clădirilor și nivelul critic al operațiunilor sau al sistemelor TIC din aceste clădiri.

Recomandarea 10 – Securitatea operațiunilor TIC

31. Întreprinderile ar trebui să pună în aplicare proceduri pentru a asigura confidențialitatea, integritatea și disponibilitatea sistemelor și serviciilor TIC, în vederea reducerii la minimum a impactului aspectelor de securitate asupra prestării de servicii TIC. Aceste proceduri ar trebui să cuprindă următoarele măsuri:

a) identificarea posibilelor vulnerabilități, care ar trebui evaluate și remediate prin asigurarea actualizării sistemelor TIC, inclusiv a programelor software furnizate de întreprinderi utilizatorilor lor interni și externi, prin instalarea de patch-uri de securitate critice, inclusiv de actualizări la definițiile programelor antivirus, sau prin punerea în aplicare de controale compensatoare;

b) implementarea de configurații securizate de referință pentru toate componentele critice, precum sisteme de operare, baze de date, routere sau comutatoare;

c) implementarea segmentării rețelei, de sisteme de prevenire a pierderii datelor și criptarea traficului din rețea (în conformitate cu clasificarea activelor informaționale);

d) implementarea protecției punctelor finale, inclusiv a serverelor, a stațiilor de lucru și a dispozitivelor mobile. Întreprinderile ar trebui să evalueze dacă un

punct final îndeplinește standardele de securitate definite de acestea, înainte de a i se acorda acces la rețeaua corporației;

e) asigurarea existenței unor mecanisme de verificare a integrității sistemelor TIC;

f) criptarea datelor în stare de repaus și în tranzit (în conformitate cu clasificarea activelor informaționale).

Recomandarea 11 – Monitorizarea securității

32. Întreprinderile ar trebui să stabilească și să pună în aplicare proceduri și procese de monitorizare continuă a activităților care afectează securitatea informațiilor întreprinderilor. Politica ar trebui să acopere cel puțin următoarele aspecte:

    a) factorii interni și externi, inclusiv funcțiile administrative privind TIC și cele aferente activității;

    b) tranzacțiile efectuate de furnizorii de servicii, de alte entități și de utilizatorii interni; și

    c) eventualele amenințările interne și externe.

33. Pe baza monitorizării, întreprinderile ar trebui să implementeze mecanisme corespunzătoare și eficiente de detectare, de raportare și de reacție la activități anormale și amenințări, cum ar fi intruziuni fizice sau logice, încălcări ale confidențialității, integrității și disponibilității activelor informaționale, coduri dăunătoare și vulnerabilități cunoscute în mod public ale programelor software și hardware.

34. Rapoartele de monitorizare a securității ar trebui să ajute întreprinderile să înțeleagă natura incidentelor operaționale sau de securitate, să identifice tendințele și să sprijine investigațiile interne ale întreprinderilor pentru a le permite să ia deciziile corespunzătoare.

Recomandarea 12 – Revizuirea, evaluarea și testarea securității informațiilor

35. Întreprinderile ar trebui să efectueze o varietate de diferite revizuiri, evaluări și testări ale securității informațiilor pentru a asigura identificarea eficientă a vulnerabilităților din sistemele și serviciile lor TIC. De exemplu, întreprinderile pot efectua analiza lacunelor pe baza standardelor de securitate a informațiilor, revizuiri ale conformității, audituri interne și externe ale sistemelor informatice sau revizuiri ale securității fizice.

36. Întreprinderile ar trebui să instituie și să pună în aplicare un cadru de testare a securității informațiilor, care să valideze robustețea și eficacitatea măsurilor lor de securitate a informațiilor și să se asigure că acest cadru ține seama de amenințările și vulnerabilitățile identificate prin procesul de monitorizare a amenințărilor și de evaluare a riscurilor TIC și de securitate.

37. Testarea ar trebui efectuată în condiții de siguranță și securitate de către verificatori independenți, care au suficiente cunoștințe, competențe și expertiză în testarea măsurilor de securitate a informațiilor.

38. Întreprinderile ar trebui să efectueze teste în mod regulat. Domeniul de aplicare, frecvența și metoda de testare (cum ar fi testele de penetrare, inclusiv testele de penetrare bazate pe amenințări) ar trebui să fie proporționale cu nivelul de risc

identificat. Testarea sistemelor TIC critice și scanările vulnerabilităților ar trebui efectuate anual.

39. Întreprinderile ar trebui să se asigure că se efectuează teste ale măsurilor de securitate în caz de modificări la nivelul infrastructurii, al proceselor sau al procedurilor și în caz de modificări ca urmare a unor incidente operaționale sau de securitate majore sau a lansării de aplicații critice, noi sau modificate substanțial. Întreprinderile ar trebui să monitorizeze și să evalueze rezultatele testelor de securitate și să-și actualizeze măsurile de securitate în mod corespunzător și fără întârzieri nejustificate, în cazul sistemelor TIC critice.

Recomandarea 13 – Formarea și conștientizarea cu privire la securitatea informațiilor

40. Întreprinderile ar trebui să instituie programe de formare în domeniul securității informațiilor pentru toți membrii personalului, inclusiv pentru organul administrativ, de conducere sau de control, pentru a se asigura că aceștia sunt instruiți pentru a-și îndeplini sarcinile și responsabilitățile, în vederea reducerii erorii umane, a furtului, a fraudei, a utilizării abuzive sau a pierderii. Întreprinderile ar trebui să se asigure că programul de formare prevede formarea tuturor membrilor personalului în mod regulat.

41. Întreprinderile ar trebui să instituie și să pună în aplicare programe periodice de conștientizare în materie de securitate pentru instruirea personalului lor, inclusiv a organului administrativ, de conducere sau de control, cu privire la abordarea riscurilor legate de securitatea informațiilor.

Recomandarea 14 – Gestionarea operațiunilor TIC

42. Întreprinderile ar trebui să-și gestioneze operațiunile TIC pe baza strategiei TIC. Documentele ar trebui să definească modul în care întreprinderile operează, monitorizează și își verifică sistemele TIC și serviciile TIC, inclusiv documentarea proceselor, a procedurilor și a operațiunilor TIC critice.

43. Întreprinderile ar trebui să pună în aplicare proceduri de înregistrare și monitorizare în cazul operațiunilor TIC critice, pentru a permite depistarea, analiza și corectarea erorilor.

44. Întreprinderile ar trebui să mențină un inventar actualizat al activelor lor TIC. Inventarul activelor TIC ar trebui să fie suficient de detaliat pentru a permite identificarea imediată a unui activ TIC, a amplasamentului acestuia, a nivelului de securitate și a proprietarului.

45. Întreprinderile ar trebui să monitorizeze și să gestioneze ciclul de viață al activelor TIC, pentru a se asigura că acestea îndeplinesc și susțin în continuare cerințele de afaceri și de gestionare a riscurilor. Întreprinderile ar trebui să monitorizeze dacă distribuitorii lor sau programatorii interni oferă asistență pentru activele TIC și dacă sunt instalate toate patch-urile și actualizările pe bază de procese documentate. Riscurile care decurg din active TIC depășite sau pentru care nu se mai oferă asistență ar trebui evaluate și diminuate. Activele TIC scoase din uz ar trebui prelucrate și eliminate în condiții de siguranță.

46. Întreprinderile ar trebui să pună în aplicare procese de planificare și monitorizare a performanțelor și capacităților, pentru a împiedica, a detecta și a interveni prompt la probleme importante legate de performanța sistemelor TIC și de lipsa capacităților TIC.

47. Întreprinderile ar trebui să definească și să pună în aplicare proceduri pentru realizarea de copii de rezervă și de restaurare a datelor și a sistemelor TIC, pentru a se asigura că pot fi recuperate, conform cerințelor. Domeniul de aplicare și frecvența operațiunilor de realizare a copiilor de rezervă ar trebui stabilite în conformitate cu cerințele de redresare aferente activității și cu nivelul critic al datelor și al sistemelor TIC și ar trebui evaluate în funcție de riscuri. Testarea procedurilor de realizare a copiilor de rezervă și de restaurare ar trebui efectuată periodic.

48. Întreprinderile ar trebui să se asigure că copiile de rezervă ale datelor și ale sistemelor TIC sunt stocate într-unul sau mai multe locuri în afara amplasamentului principal, la o distanță sigură și suficient de mare față de amplasamentul principal, pentru a nu fi expuse acelorași riscuri.

Recomandarea 15 – Gestionarea problemelor și incidentelor TIC

49. Întreprinderile ar trebui să instituie și să pună în aplicare un proces de gestionare a problemelor și incidentelor, pentru a monitoriza și înregistra incidentele operaționale sau de securitate și pentru a permite întreprinderilor să continue sau să reia procesele și funcțiile critice aferente activității, atunci când se produc întreruperi.

50. Întreprinderile ar trebui să stabilească criterii și praguri adecvate pentru clasificarea unui eveniment drept incident operațional sau de securitate, precum și indicatori de avertizare timpurie care ar trebui să servească drept alertă pentru a permite detectarea timpurie a acestor incidente.

51. Pentru a minimiza impactul evenimentelor defavorabile și a permite redresarea la timp, întreprinderile ar trebui să instituie procese și structuri organizaționale corespunzătoare pentru a asigura monitorizarea, manevrarea și urmărirea integrate și consecvente ale incidentelor operaționale și de securitate și pentru a asigura identificarea și eliminarea principalelor cauze și adoptarea de acțiuni/măsuri corective, pentru a evita reproducerea unor astfel de incidente. Procesul de gestionare a problemelor și incidentelor ar trebui să stabilească:

    a) procedurile de identificare, urmărire, înregistrare, categorisire și clasificare a incidentelor potrivit unei reguli de prioritate definită de întreprindere și bazată pe nivelul critic al activității și pe contractele de servicii;

    b) rolurile și responsabilitățile pentru diferite scenarii de incidente (de exemplu, erori, defecțiuni, atacuri cibernetice);

    c) o procedură de gestionare a problemelor pentru a identifica, analiza și soluționa principala cauză a unuia sau mai multor incidente; întreprinderile ar trebui să analizeze incidentele operaționale sau de securitate care au fost identificate sau care au avut loc în cadrul și/sau în afara organizației, și ar trebui să ia în considerare lecțiile-cheie învățate din aceste analize și să actualizeze în consecință măsurile de securitate;

    d) planuri eficiente de comunicare internă, inclusiv proceduri de notificare și escaladare a incidentelor – care să acopere și reclamațiile clienților legate de securitate – pentru a garanta că:

        i. incidentele cu un posibil impact negativ ridicat asupra sistemelor și serviciilor TIC critice sunt raportate personalului de conducere de nivel superior relevant;

        ii. organul administrativ, de conducere sau de control este informat ad-hoc în caz de incidente semnificative, cel puțin cu privire la impactul,

măsurile luate și controalele suplimentare care urmează să fie definite ca urmare a incidentelor.

e) proceduri de intervenție în caz de incidente, pentru reducerea impactului acestora și pentru a garanta că serviciul devine operațional și sigur rapid;

f) planuri specifice de comunicare externă pentru procese și funcții critice aferente activității pentru:

   i. a colabora cu părțile interesate relevante, pentru a interveni în mod eficient în caz de incidente și a se redresa în urma acestora;

   ii. a oferi părților externe [de exemplu, clienților, altor participanți la piață, autorităților (de supraveghere) relevante, după caz și în conformitate cu regulamentul aplicabil] informații la timp, inclusiv rapoarte cu privire la incidente.

Recomandarea 16 – Gestionarea proiectelor TIC

52. Întreprinderile ar trebui să pună în aplicare o metodologie de proiect TIC (inclusiv considerente independente privind cerințele de securitate), cu un proces de guvernanță adecvat și o conducere pentru punerea în aplicare a proiectelor, pentru a sprijini în mod eficient punerea în aplicare a strategiei TIC prin intermediul proiectelor TIC.

53. Întreprinderile ar trebui să monitorizeze și să atenueze în mod corespunzător riscurile ce decurg din portofoliul de proiecte TIC, ținând seama și de riscurile care pot rezulta din interdependențele dintre diferite proiecte și din dependențele mai multor proiecte de aceleași resurse și/sau competențe.

Recomandarea 17 – Achiziția și dezvoltarea de sisteme TIC

54. Întreprinderile ar trebui să elaboreze și să pună în aplicare un proces care să reglementeze achiziția, dezvoltarea și întreținerea sistemelor TIC pentru a asigura o protecție completă a confidențialității integrității și disponibilității datelor care urmează să fie prelucrate, precum și îndeplinirea cerințelor de protecție definite. Acest proces ar trebui conceput folosind o abordare bazată pe riscuri.

55. Întreprinderile ar trebui să se asigure că, înainte ca achizițiile de sisteme sau activitățile de dezvoltare să aibă loc, cerințele funcționale și nefuncționale (inclusiv cerințele de securitate a informațiilor) și obiectivele tehnice sunt clar definite.

56. Întreprinderile ar trebui să se asigure că sunt instituite măsuri pentru a preveni modificarea neintenționată sau manipularea intenționată a sistemelor TIC pe durata dezvoltării.

57. Întreprinderile ar trebui să dispună de o metodologie de testare și de aprobare a sistemelor TIC, a serviciilor TIC și a măsurilor de securitate a informațiilor.

58. Întreprinderile ar trebui să testeze în mod corespunzător sistemele TIC, serviciile TIC și măsurile de securitate a informațiilor, pentru a identifica eventualele puncte slabe, încălcări și incidente de securitate.

59. Întreprinderile ar trebui să asigure separarea mediilor de producție de mediile de dezvoltare, de testare și de alte medii care nu au legătură cu producția.

60. Întreprinderile ar trebui să pună în aplicare măsuri de protejare a integrității codului sursă (după caz) a sistemelor TIC. De asemenea, ar trebui să documenteze în mod amănunțit dezvoltarea, implementarea, operarea și/sau configurarea sistemelor TIC, pentru a reduce orice dependență inutilă de experții în domeniu.

61. Procesele de achiziție și dezvoltare a sistemelor TIC ale întreprinderilor ar trebui să se aplice și sistemelor TIC dezvoltate sau gestionate de utilizatorii finali ai funcției aferente activității din afara organizației TIC (de exemplu, în aplicațiile gestionate de întreprinderi sau în aplicațiile informatice ale utilizatorilor finali) folosind o abordare bazată pe riscuri. Întreprinderile ar trebui să țină o evidență a aplicațiilor care sprijină procesele sau funcțiile critice aferente activității.

Recomandarea 18 – Gestionarea modificărilor TIC

62. Întreprinderile ar trebui să instituie și să pună în aplicare un proces de gestionare a modificărilor TIC pentru a se asigura că toate modificările aduse sistemelor TIC sunt înregistrate, evaluate, testate, aprobate, autorizate și implementate în mod controlat. Modificările survenite în timpul unor modificări TIC urgente sau de urgență ar trebui să poată fi urmărite și notificate ex post proprietarului de active relevant pentru analiza ex post.

63. Întreprinderile ar trebui să stabilească dacă modificările aduse mediului operațional existent influențează măsurile de securitate existente sau dacă impun adoptarea de măsuri suplimentare pentru atenuarea riscurilor implicate. Aceste modificări ar trebui să fie în conformitate cu procesul formal de gestionare a modificărilor al întreprinderilor.

Recomandarea 19 – Gestionarea continuității activității

64. În cadrul politicii generale a întreprinderilor de continuitate a activității, organul administrativ, de conducere sau de control are responsabilitatea de a stabili și de a aproba politica întreprinderilor de continuitate a TIC. Politica de continuitate a TIC ar trebui să fie comunicată în mod corespunzător în cadrul întreprinderilor și ar trebui să se aplice tuturor membrilor personalului relevanți și, după caz, furnizorilor de servicii.

Recomandarea 20 – Analiza impactului asupra activității

65. Ca parte a unei bune gestionări a continuității activității, întreprinderile ar trebui să efectueze o analiză a impactului asupra activității pentru a evalua expunerea întreprinderilor la întreruperi grave ale activității și potențialul impact al acestora, cantitativ și calitativ, utilizând date interne și/sau externe și o analiză pe bază de scenarii. Analiza impactului asupra activității ar trebui să țină seama și de nivelul critic al proceselor și activităților economice, al funcțiilor aferente activității, al rolurilor și al activelor (de exemplu, activele informaționale și activele TIC) identificate și clasificate, precum și de interdependențele lor în conformitate cu recomandarea 4.

66. Întreprinderile ar trebui să se asigure că sistemele și serviciile lor TIC sunt concepute și sunt în concordanță cu analiza lor de impact asupra activității, de exemplu cu redundanța anumitor componente critice, pentru a preveni întreruperile cauzate de evenimente cu impact asupra componentelor respective.

Recomandarea 21 – Planificarea continuității activității

67. Planurile generale de asigurare a continuității activității (BCP) ale întreprinderilor ar trebui să țină seama de riscurile semnificative care ar putea afecta negativ sistemele și serviciile TIC. Planurile ar trebui să sprijine obiectivele de protejare și, dacă este necesar, de restabilire a confidențialității, integrității și disponibilității proceselor și activităților economice, ale funcțiilor aferente activității, ale rolurilor și ale activelor (de exemplu, activele informaționale și activele TIC) întreprinderilor. Întreprinderile

ar trebui să se coordoneze cu părțile interesate interne și externe relevante, după caz, pe durata elaborării acestor planuri.

68. Întreprinderile ar trebui să pună la dispoziție planuri de asigurare a continuității pentru a se asigura că pot reacționa în mod corespunzător la eventualele scenarii de intrare în dificultate conform unui obiectiv timp de recuperare (intervalul maxim în care un sistem sau un proces trebuie restabilit după un incident) și unui obiectiv punct de recuperare (perioada maximă în care se pot pierde date în cazul unui incident la un nivel predefinit al serviciilor).

69. Întreprinderile ar trebui să ia în considerare o serie de scenarii diferite în planurile lor de asigurare a continuității activității, inclusiv scenarii extreme, dar plauzibile, și scenarii de atac cibernetic, și să evalueze impactul potențial al unor astfel de scenarii. Pe baza acestor scenarii, întreprinderile ar trebui să descrie modul în care sunt asigurate continuitatea sistemelor și serviciilor TIC și securitatea informațiilor acestora.

Recomandarea 22 – Planuri de intervenție și de redresare

70. Pe baza analizei impactului asupra activității și a scenariilor plauzibile, întreprinderile ar trebui să elaboreze planuri de intervenție și de redresare. Aceste planuri ar trebui să precizeze condițiile în care poate fi declanșată activarea planurilor și măsurile care trebuie luate pentru a asigura integritatea, disponibilitatea, continuitatea și redresarea cel puțin a sistemelor TIC, a serviciilor TIC și a datelor critice ale întreprinderilor. Planurile de intervenție și de redresare ar trebui să vizeze atingerea obiectivelor de redresare a operațiunilor întreprinderilor.

71. Planurile de intervenție și de redresare ar trebui să țină seama de opțiunile de redresare pe termen scurt și, după caz, de cele pe termen lung. Planurile ar trebui, cel puțin:

    a) să pună accentul pe redresarea operațiunilor serviciilor TIC, ale funcțiilor aferente activității, ale proceselor de asistență, ale activelor informaționale importante și pe interdependențele lor, pentru a evita efectele negative asupra funcționării întreprinderii;

    b) să fie documentate și puse la dispoziția unităților operaționale și de asistență și să fie ușor accesibile în caz de urgență, incluzând o definire clară a rolurilor și a responsabilităților; și

    c) să fie în permanență actualizate în conformitate cu lecțiile învățate din incidente, teste, cu noile riscuri și amenințări identificate și cu prioritățile și obiectivele de redresare modificate.

72. Planurile ar trebui să aibă în vedere și opțiuni alternative, în cazul în care este posibil ca redresarea să nu fie fezabilă pe termen scurt, din cauza costurilor, riscurilor, logisticii sau a situațiilor neprevăzute.

73. În cadrul planurilor de intervenție și de redresare, întreprinderile ar trebui să aibă în vedere punerea în aplicare a unor măsuri de asigurare a continuității pentru a atenua neîndeplinirea obligațiilor de către furnizorii de servicii, care sunt de importanță vitală pentru continuitatea serviciilor TIC ale întreprinderilor (în conformitate cu dispozițiile Ghidului EIOPA privind sistemul de guvernanță și ale Ghidului privind externalizarea către furnizorii de servicii cloud).

Recomandarea 23 – Testarea planurilor

74. Întreprinderile ar trebui să-și testeze planurile de asigurare a continuității activității și să se asigure că funcționarea proceselor și activităților lor economice, a funcțiilor aferente activității, a rolurilor și a activelor (de exemplu, activele informaționale) și a activelor TIC critice și interdependențele acestora (inclusiv cele furnizate de furnizori de servicii) sunt testate cu regularitate, pe baza profilului de risc al întreprinderilor.

75. Planurile de asigurare a continuității activității ar trebui actualizate regulat, pe baza rezultatelor testelor, a informațiilor privind amenințările curente și a lecțiilor învățate din evenimente anterioare. Orice modificări relevante ale obiectivelor de redresare (inclusiv obiectivul timp de redresare și obiectivul punct de redresare) și/sau orice modificări ale proceselor și activităților economice, ale funcțiilor aferente activității, ale rolurilor și ale activelor (de exemplu, activele informaționale și activele TIC) ar trebui , de asemenea, incluse.

76. Testarea planurilor de asigurare a continuității activității ar trebui să demonstreze capacitatea acestora de a susține viabilitatea activităților până la restabilirea operațiunilor critice la un nivel predefinit al serviciilor sau de toleranță la impact.

77. Rezultatele testelor ar trebui documentate și toate deficiențele identificate în urma testelor ar trebui analizate, abordate și raportate organului administrativ, de conducere sau de control.

Recomandarea 24 – Comunicările în situații de criză

78. În cazul unei întreruperi sau al unei urgențe și pe parcursul punerii în aplicare a planurilor de asigurare a continuității activității, întreprinderile ar trebui să se asigure că au introdus măsuri eficiente de comunicare în situații de criză, astfel încât toate părțile interesate interne și externe relevante, inclusiv autoritățile de supraveghere relevante, atunci când reglementările naționale o cer, cât și furnizorii de servicii relevanți să fie informați în timp util și în mod corespunzător.

Recomandarea 25 – Externalizarea serviciilor și sistemelor TIC

79. Fără a aduce atingere Ghidului EIOPA privind externalizarea către furnizorii de servicii cloud, întreprinderile ar trebui să se asigure că, în cazul în care serviciile și sistemele TIC sunt externalizate, cerințele relevante pentru serviciul sau sistemul TIC sunt îndeplinite.

80. În cazul externalizării funcțiilor critice sau importante, întreprinderile ar trebui să se asigure că obligațiile contractuale ale furnizorului de servicii (de exemplu, contractele, acordurile privind nivelul serviciilor, dispozițiile de reziliere a contractelor relevante) includ cel puțin următoarele:

    a) obiective și măsuri corespunzătoare și proporționale de securitate a informațiilor, inclusiv cerințe precum cerințe minime de securitate a informațiilor, specificații privind ciclul de viață al datelor întreprinderilor, drepturi de audit și de acces, precum și orice cerințe privind amplasarea centrelor de date și cerințe de criptare a datelor, securitatea rețelei și procesele de monitorizare a securității;

    b) acorduri privind nivelul serviciilor, pentru a asigura continuitatea serviciilor și sistemelor TIC și obiectivele de performanță în condiții normale, precum și cele furnizate în planurile de urgență în cazul întreruperii serviciilor; și

c) proceduri de gestionare a incidentelor operaționale și de securitate, inclusiv escaladarea și raportarea.

81. Întreprinderile ar trebui să monitorizeze și să se asigure că furnizorii respectivi îndeplinesc obiectivele de securitate, măsurile și obiectivele de performanță ale întreprinderii.

Reguli de conformitate și raportare

82. Prezentul document cuprinde recomandări emise în temeiul articolului 16 din Regulamentul (UE) nr. 1094/2010. Conform articolul 16 alineatul (3) din același regulament, autoritățile competente și întreprinderile trebuie să depună toate eforturile pentru a respecta aceste ghiduri și recomandările.

83. Autoritățile competente care respectă sau intenționează să respecte prezentul ghid ar trebui să îl includă în mod corespunzător în cadrul de reglementare sau de supraveghere.

84. Autoritățile competente trebuie să transmită la EIOPA confirmarea respectării sau a intenției de a respecta prezentul ghid, prezentând motivele în cazul neconformității, în termen de două luni de la publicarea versiunilor traduse.

85. În lipsa unui răspuns până la împlinirea acestui termen, se va considera că autoritățile competente nu respectă cerințele de raportare și vor fi raportate ca atare.

Prevedere finală cu privire la revizuire

86. Prezentul ghid va fi supus unei revizuiri de către EIOPA.