GHID METODOLOGIC PENTRU PUNEREA ÎN APLICARE A CERINȚELOR DE SECURITATE CIBERNETICĂ

aprobate prin Hotărârea de Guvern Nr. 562/2025

Aprobat prin Ordinul directorului
Agenției pentru Securitate Cibernetică
Nr. 09 din 08.04.2026

Agenția pentru Securitate Cibernetică
cu suportul Băncii Mondiale

+373 681 11 115

www.asc.gov.md

Cuprins

Introducere

Prezentul cadru este un set de măsuri concrete şi oferă o abordare clară, pas cu pas, care ajută organizaţiile să:

- îşi protejeze datele;
- reducă semnificativ riscul celor mai frecvente atacuri cibernetic;
- îşi îmbunătăţească reziliența cibernetică.

Cerinţele, cunoscute şi sub denumirea de controale sau măsuri, sunt susţinute de informaţii relevante din Cadrul de securitate cibernetică NIST, ISO 27001/ISO 27002, IEC 62443 şi Controalele critice de securitate CIS (ETSI TR 103 305-1).

Cadrul este construit în jurul a şase domenii principale: **Guvernanţă, Identificare, Protecţie, Detecţie, Răspuns şi Recuperare**.

Aceste şase domenii susţin o comunicare clară în toate structurile organizaţiei, tehnice şi non-tehnice, facilitând înţelegerea şi gestionarea riscurilor cibernetice. Prin utilizarea unui limbaj comun, acestea contribuie la integrarea securităţii cibernetice în procesele decizionale şi în strategia generală de gestionare a riscurilor.

Guvernanţă: poziţionează securitatea cibernetică drept obiectiv strategic, nu doar ca o sarcină tehnică. Stabileşte aşteptări, politici, responsabilităţi şi autorităţi clare şi se asigură că acestea sunt comunicate şi revizuite în întreaga organizaţie.

Identificare: ajută la construirea unei înţelegeri clare a ceea ce contează cel mai mult pentru organizaţie, cum ar fi sistemele, oamenii, activele, datele, procesele şi instrumentele care susţin operaţiunile. Această funcţie ajută la recunoaşterea potenţialelor ameninţări cibernetice şi pune bazele pentru decizii informate cu privire la gestionarea riscurilor de securitate cibernetică.

Protecţie: implică punerea în aplicare a măsurilor de protecţie pentru a reduce riscul unui incident cibernetic sau pentru a limita impactul acestuia. Aceasta include măsuri tehnice, procese şi eforturi de sensibilizare.

Detecţie: sprijină capacitatea de a observa rapid evenimentele de securitate cibernetică. Detectarea timpurie ajută la reducerea daunelor şi permite un răspuns mai rapid.

Răspuns: acoperă acţiunile întreprinse atunci când are loc un incident de securitate cibernetică. Ajută la limitarea problemei, coordonarea comunicării şi reducerea perturbărilor.

Recuperare: se concentrează pe restabilirea serviciilor şi operaţiunilor afectate după un incident. Include, de asemenea, învăţarea din eveniment pentru a îmbunătăţi reziliența viitoare.

La punerea în aplicare a cerinţelor minime de securitate, operatorii de servicii esenţiale/importante trebuie să ţină seama de faptul că măsurile de securitate (controalele) trebuie să fie:

- eficiente în îmbunătăţirea nivelului de securitate cibernetică a unui furnizor de servicii în raport cu peisajul actual şi previzibil al ameninţărilor;
- direcţionate pentru a se asigura că eforturile financiare, umane şi tehnice sunt aplicate măsurilor care vor avea cel mai mare impact asupra îmbunătăţirii securităţii unui furnizor de servicii;
- potrivite pentru a aborda vulnerabilităţile intersectoriale şi completate cu măsuri de securitate specifice sectorului;
- proporţionale cu riscurile, cu accent pe protejarea sistemelor şi infrastructurilor care stau la baza serviciilor esenţiale;
- concrete şi uşor de înţeles, pentru a se asigura că măsurile sunt puse în aplicare pe deplin şi contribuie activ la consolidarea nivelului de securitate cibernetică;
- verificabile, astfel încât furnizorul de servicii să poată furniza auditorilor evidenţe ale punerii în aplicare efective a măsurilor de securitate.

Prezentul Ghid metodologic are caracter strict de recomandare şi nu generează obligaţii juridice, fiind elaborat exclusiv ca instrument de orientare şi sprijin pentru aplicarea în mod coerent a prevederilor Hotărârii Guvernului nr. 562/2025.

Acest document este furnizat numai în scop informativ şi de guvernanţă internă. Acesta nu constituie consultanţă juridică, interpretare normativă sau o evaluare definitivă a conformităţii. Deşi s-au depus toate eforturile pentru a asigura acurateţea şi exhaustivitatea corelării dintre cerinţele normative şi controalele metodologice, organizaţia nu oferă nicio garanţie, expresă sau implicită, cu privire la conţinutul său.

Utilizatorii acestui document sunt responsabili de validarea aplicabilităţii sale la obligaţiile lor specifice de reglementare, contextului operaţional şi mediului de risc. Cerinţele de reglementare pot evolua, iar fiecare departament sau funcţie are responsabilitatea de a asigura conformitatea continuă cu cele mai recente legi, standarde şi aşteptări de supraveghere.

1. Guvernanță

1.1 Politica privind securitatea rețelelor și a sistemelor informatice

ÎNDRUMĂRI

Stabiliți o politică privind securitatea rețelelor și a sistemelor informatice, care să acopere toate sistemele, activele și procedurile care intră în domeniul de aplicare al politicii.
Asigurați-vă că personalul relevant și părțile externe interesate relevante iau la cunoștință politica privind securitatea rețelelor și a sistemelor informatice, de obicei prin intermediul unui document semnat sau al unei confirmări digitale, după caz.
În funcție de context, părțile externe pot fi furnizori, prestatori de servicii, acționari, autorități, vizitatori, grupuri de interese externe sau forumuri.
Confirmarea poate fi inclusă și în alte contracte, cum ar fi contractele de muncă sau contractele de prestare de servicii.
Politica ar trebui comunicată personalului relevant și părților externe interesate într-o formă relevantă, accesibilă și ușor de înțeles pentru cititorul vizat.
Personalul relevant și părțile externe interesate relevante pot să nu fie informate cu privire la textul integral al politicii. În funcție de rolul lor, ar trebui comunicat și confirmat un extras sau un rezumat care să conțină numai informații relevante. În cazul în care politica este distribuită în afara entității, ar trebui să se acorde atenție pentru a nu se divulga informații confidențiale.
Asigurați-vă că personalul este conștient de responsabilitățile sale în ceea ce privește securitatea rețelelor și a sistemelor informatice.
Asigurați-vă că politica privind securitatea rețelelor și a sistemelor informatice este aprobată de organele de conducere.
Asigurați-vă că politicile specifice fiecărui subiect sunt aprobate de un nivel adecvat de conducere.
Asigurați-vă că politica include îndrumări detaliate privind procedurile de gestionare a excepțiilor de la politică.

EXEMPLE DE EVIDENȚE

- O politică de securitate documentată pentru rețea și sistemele informatice.
- Data aprobării oficiale de către conducere.
- Confirmări semnate de către personal și părți externe (dacă este cazul).
- Dovada înțelegerii rolurilor și responsabilităților conducerii în materie de securitate.

Ref: Cerințe aprobate prin HG 562/2025 pct. 1.1–1.11, pct. 2, pct. 3.1–3.5

1.2 Roluri, responsabilități și autorități

ÎNDRUMĂRI

Redactați fișele de post în așa fel încât să prezinte în mod clar drepturile și responsabilitățile.

Atribuiți roluri și responsabilități de securitate personalului și includeți aceste roluri în organigrama organizației.

Descrieți rolurile și atribuiți responsabilitățile corespunzătoare (de exemplu, managerul responsabil cu securitatea informațiilor).

Asigurați-vă că rolurile alocate sunt adecvate dimensiunii și nevoilor entității.

Desemnarea oficială a personalului competent în roluri de securitate. Asigurați-vă că persoanele desemnate sunt competente pe baza unei educații, formări sau experiențe adecvate.

Informați personalul cu privire la rolurile de securitate din cadrul entității și stabiliți momentul în care fiecare rol trebuie contactat.

Informați personalul cu privire la obligațiile sale în materie de securitate a rețelei și a sistemului informatic, în funcție de rolul său.

Informați părțile externe interesate relevante cu privire la obligațiile lor în materie de securitate a rețelelor și a sistemelor informatice.

Pentru cerințele contractuale ale furnizorilor direcți și ale prestatorilor de servicii luați în considerare părțile terțe, adică entitățile sau organizațiile externe care nu sunt direct implicate în operațiunile entității vizate, dar care pot afecta totuși securitatea rețelei și a informațiilor acesteia.

Cerința ca tot personalul și terții să aplice măsurile de securitate a rețelelor și a sistemelor informatice trebuie comunicată într-o formă relevantă, accesibilă și ușor de înțeles pentru cititorul vizat.

Politica de securitate a rețelei și a informațiilor, politicile și procedurile specifice ale entităților relevante nu trebuie neapărat comunicate în întregime.

Desemnați o persoană (de exemplu, responsabilul cu securitatea informațiilor sau managerul de securitate a informațiilor) responsabilă cu supravegherea aspectelor legate de securitatea rețelei și a informațiilor.

Asigurați-vă că acest rol este recunoscut și autorizat în mod corespunzător de către organele de conducere.

Luaţi în considerare separarea sarcinilor şi a domeniilor de responsabilitate in conflict de interes pentru a reduce posibilitățile de modificare neautorizată sau neintenţionată sau de utilizare abuzivă a activelor entității. Cel puţin, luaţi în considerare faptul că evaluatorul (auditorul) trebuie să fie diferit de personalul sau de linia ierarhică a domeniului evaluat.

Rezultatele evaluării riscurilor sau ale analizei impactului asupra activității (BIA) ar putea fi utilizate pentru a identifica potențialele sarcini și domenii de responsabilitate cu conflict de interes.

EXEMPLE DE EVIDENȚE

- Fișele de post pentru rolurile relevante.
- Lista rolurilor de securitate cu titularii rolurilor și datele de contact.
- Documente oficiale de numire pentru rolurile cheie de securitate.
- Responsabilitățile postului documentate în mod clar.
- Dovada competenței personalului desemnat.
- Materiale de informare care explică rolurile de securitate și procedurile de contact.
- Acorduri cu terți (SLA, contracte, DPA).
- Recunoașterea de către terți a obligațiilor de securitate (dacă nu sunt acoperite de contracte).
- Documentație actualizată privind structura rolurilor de securitate.
- Procesele verbale ale ședințelor de conducere.
- Evidențe ale deciziilor legate de securitatea cibernetică.

Ref: Cerințe aprobate prin HG 562/2025 pct. 4

1.3 Cadrul de gestionare a riscurilor

ÎNDRUMĂRI

Entitatea poate utiliza cadrul actual de gestionare a riscurilor sau poate adopta unul nou. Un cadru de gestionare a riscurilor este abordarea structurată utilizată de o entitate pentru a identifica, evalua, gestiona şi atenua riscurile sale de securitate cibernetică.
Creaţi un plan de tratare a riscurilor care să asocieze riscurile identificate cu activele şi măsurile de atenuare a riscurilor asociate. Planul trebuie să includă cel puţin:

- o descriere a riscului identificat şi a modului în care acesta poate afecta negativ obiectivele de securitate;
- o opţiune de tratare a riscurilor (de exemplu, evitarea riscurilor, atenuarea riscurilor, transferul sau partajarea riscurilor sau acceptarea riscurilor);
- activele asociate riscului;
- măsurile care atenuează riscul;
- o procedură de evaluare a eficacităţii punerii în aplicare a măsurii (măsurilor);
- calendarul de implementare;
- rolurile responsabile.

Luaţi în considerare riscurile reziduale provenite de la terţi, de exemplu, încălcări ale securităţii datelor, vulnerabilităţi neadresate, nerespectarea reglementărilor din partea terţilor şi dependenţa excesivă de un singur terţ.
Asiguraţi-vă că riscurile reziduale sunt acceptate de organele de conducere sau, după caz, de persoanele responsabile şi care au autoritatea de a gestiona riscurile, în conformitate cu nivelurile acceptabile de risc rezidual ale entităţii.
Asiguraţi-vă că organele de conducere sau, după caz, persoanele responsabile şi care au autoritatea de a gestiona riscurile aprobă rezultatele evaluării riscurilor şi planul de tratare a riscurilor.
Stabiliţi apetitul la risc al entităţii, adică nivelul de risc pe care entitatea este dispusă să şi-l asume din punct de vedere strategic pentru a-şi atinge obiectivele. Criteriile pot include (listă orientativă, neexhaustivă):

- obiectivele strategice ale întreprinderii;
- aşteptările părţilor interesate;
- cerinţele de reglementare;
- cultura organizaţională.

Definiţi nivelul de toleranţă la risc, care se referă la nivelul de risc pe care o entitate este dispusă să îl accepte în urmărirea obiectivelor sale pe termen lung.
Definiţi criteriile de acceptare a riscului

EXEMPLE DE EVIDENȚE

- Cadru documentat de gestionare a riscurilor.
- Înregistrări ale evaluărilor de risc anterioare.
- Planul de tratare a riscurilor.
- Aprobarea de către conducere a rezultatelor evaluării riscurilor.
- Aprobarea de către conducere a riscurilor reziduale.
- Evidențe că riscurile reziduale legate de terți sunt identificate și atenuate.

Ref: Cerințe aprobate prin HG 562/2025
pct. 5, pct. 6.1-6.10, pct. 7, pct. 8, pct. 91, pct. 92.1-92.6, pct. 93

1.4 Monitorizarea conformității

ÎNDRUMĂRI

Elaborați un format standardizat pentru raportarea către organele de conducere. Luați în considerare următoarele elemente:

- indicatori cheie,
- starea conformității, inclusiv excepțiile de la politici,
- riscurile identificate și
- acțiunile recomandate.

Rapoartele sunt generate și prezentate organelor de conducere cel puțin o dată pe an.

Stabiliți proceduri pentru monitorizarea conformității.

Analizați și evaluați rezultatele revizuirii conformității.

EXEMPLE DE EVIDENȚE

- Rapoarte recente privind verificarea conformității.
- Jurnale ale excepțiilor de la politică.
- Înregistrări ale cererilor și aprobărilor de excepții, împreună cu detalii privind controalele compensatorii implementate.
- Proceduri documentate pentru monitorizarea conformității.
- Analiza și evaluarea documentate ale rezultatelor, inclusiv starea actuală a gestionării riscurilor entității.
- Planuri detaliate de monitorizare a conformității, inclusiv obiective și planificare pe termen lung, la nivel înalt.

Ref: Cerințe aprobate prin HG 562/2025 pct. 9, pct. 10, pct. 11

1.5 Politica de gestionare a incidentelor

ÎNDRUMĂRI

Definiţi o politică clară pentru gestionarea incidentelor (atât pentru incidentele operaţionale, cât şi pentru cele de securitate).

Definiţi obiective clare pentru politica de gestionare a incidentelor.

Aliniaţi politica de gestionare a incidentelor la planul de continuitate a activităţii şi de recuperare în caz de dezastru.

Stabiliţi un sistem de clasificare a incidentelor, care se referă la schema utilizată de entitate pentru a identifica consecinţele şi prioritatea unui incident, împreună cu criteriile de clasificare a evenimentelor ca incidente.

Asiguraţi-vă că politica de gestionare a incidentelor se referă la diferite tipuri de incidente.

Comunicaţi incidentul părţilor interesate şi personalului relevant, în conformitate cu un plan de comunicare. Planul de comunicare ar trebui să ia în considerare mecanismul de raportare a evenimentelor.

Identificaţi rolurile şi responsabilităţile necesare care trebuie atribuite pentru gestionarea incidentelor. Entităţile pot utiliza cadre de competenţe deja stabilite, de exemplu ECSF, pentru a le ajuta să identifice competenţele şi cunoştinţele necesare.

EXEMPLE DE EVIDENȚE

- Politica de gestionare a incidentelor (documentată și comunicată).
- Legături către planurile de continuitate a activității și de recuperare în caz de dezastru.
- Înregistrări ale testelor/exercițiilor comune pentru răspunsul la incidente și BCP/DR.
- Interviuri cu personalul cheie de răspuns la incidente și continuitatea afacerii.
- Sistem de clasificare a incidentelor.
- Plan de comunicare pentru gestionarea incidentelor.
- Proceduri pentru notificarea autorităților, CSIRT, clienților și furnizorilor.
- Simulări și activități de sensibilizare pentru testarea gradului de pregătire.
- Programul de testare și revizuire a politicii de gestionare a incidentelor.
- Istoricul versiunilor procedurii (actualizări).

Ref: Cerințe aprobate prin HG 562/2025 pct. 16, pct. 17.1-17.4, pct. 18

1.6 Evaluarea și clasificarea evenimentelor

ÎNDRUMĂRI

Utilizaţi criterii pentru a evalua dacă un eveniment suspect este sau nu un incident.
Determinaţi natura şi gravitatea evenimentului pe baza unui sistem de clasificare
În politica de gestionare a incidentelor, includeţi activităţi de evaluare a evenimentelor suspecte pentru a determina natura și gravitatea acestora. Aceste activităţi ar trebui să includă paşi precum:

- colectarea informaţiilor şi evidenţelor relevante legate de eveniment.
- analizarea impactului potenţial asupra sistemelor, datelor şi operaţiunilor entităţii.
- determinarea gravităţii incidentului pe baza unor criterii predefinite.

Implementaţi manuale sau ghiduri pentru a orienta acţiunile de evaluare iniţială pentru tipurile comune de incidente, de exemplu ransomware, phishing, pierderea datelor sau a dispozitivelor sau incendii.
Clasificaţi evenimentele în funcţie de natura, gravitatea şi impactul potenţial al acestora. Clasificările obişnuite pot include:

- gravitate scăzută, medie, ridicată sau critică;
- tipuri de incidente (de exemplu, infectarea cu software de tip malware sau acces neautorizat);
- incidente ce pot afecta reglementarea sau conformitatea.

Prioritizaţi evenimentul în funcţie de criterii specifice, efectuând o analiză a cauzelor principale, şi determinaţi cazurile recurente ale unui incident.
Revizuiţi şi corelaţi jurnalele.
Evaluaţi evenimentele anterioare şi clasificarea acestora pentru a îmbunătăţi procesele, procedurile şi pragurile de risc si/sau impact.

EXEMPLE DE EVIDENȚE

- Criterii definite în vigoare.
- Proceduri sau linii directoare documentate referitoare la evaluarea evenimentelor, inclusiv pașii pentru colectarea informațiilor, analizarea impactului și determinarea gravității.
- Existența unor criterii sau linii directoare documentate pentru prioritizarea evenimentelor în funcție de gravitate și impact potențial.
- Existența unui proces de triere a alertelor sau rapoartelor primite cu privire la evenimente suspecte.
- Ghiduri pentru tipuri comune de incidente.
- Revizuiri periodice ale evaluării și clasificării evenimentelor anterioare pentru îmbunătățirea proceselor, procedurilor și pragurilor.

Ref: Cerințe aprobate prin HG 562/2025 pct. 28, pct. 29.1-29.5

1.7 Planul de continuitate a activității și de recuperare în caz de dezastru

ÎNDRUMĂRI

Luați în considerare standardele recunoscute în industrie atunci când elaborați planul de continuitate a activității și de recuperare în caz de dezastru.

Creați o listă a dezastrelor naturale (de exemplu, incendii, inundații) și a altor evenimente (de exemplu, erori umane) care ar putea afecta serviciile, împreună cu o listă a capacităților de recuperare în caz de dezastru (de exemplu, copii de rezervă, teste, obiective de recuperare etc.).

Păstrați jurnale de activare și executare a planului de continuitate a activității.

Stabiliți ordinea de recuperare pe baza unor criterii.

Efectuați planificarea capacității astfel încât să existe capacitatea necesară pentru procesarea informațiilor, telecomunicații și suportul de mediu după activarea planului de continuitate a activității.

Luați în considerare furnizorii de servicii de telecomunicații primari și alternativi pentru a menține în mod corespunzător planurile de recuperare în caz de dezastru (pentru serviciile furnizate).

Asigurați-vă că serviciile terților (de exemplu, site-ul de rezervă) vor fi disponibile în caz de dezastru, acolo unde este cazul.

Implementați măsuri avansate pentru capacitățile de recuperare în caz de dezastru, acolo unde este cazul.

Pe baza rezultatelor BIA și a evaluării riscurilor, entitatea ar trebui să stabilească obiective de recuperare adecvate.

Stabilirea obiectivului de furnizare a serviciilor (SDO) pentru a determina nivelul minim de performanță care trebuie atins de funcțiile de afaceri în timpul modului alternativ de procesare.

Întrerupere maximă acceptabilă (MAO) sau perioadă maximă tolerabilă de întrerupere (MTPD) pentru a determina timpul necesar pentru ca impactul potențial al nefurnizării unui produs/serviciu sau al neefectuării unei activități să devină inacceptabil sau semnificativ, în conformitate cu evaluarea riscurilor. De obicei, acestea sunt mai lungi decât RTO. MAO se concentrează pe disponibilitatea serviciilor, în timp ce RPO se concentrează pe pierderea de date.

RTO, RPO și SDO pot fi utilizate pentru a determina procedurile de backup și redundanță.

Documentați planul de recuperare în caz de dezastru.

Testați, revizuiți și, dacă este necesar, actualizați planurile de continuitate a activității și de recuperare în caz de dezastru cel puțin o dată pe an.

Definiţi recuperarea completă şi reconstituirea sistemului informatic la o stare cunoscută, ca parte a testării planului de recuperare în caz de dezastru.

Actualizaţi planurile de continuitate a activităţii şi de recuperare în caz de dezastru, precum şi măsurile conexe.

Revizuiţi şi, dacă este necesar, actualizaţi rolurile şi responsabilităţile.

Revizuirea planurilor de recuperare în caz de dezastru ale terţilor dependenţi pentru a se asigura că planurile îndeplinesc cerinţele de continuitate a activităţii entităţii.

Comunicaţi modificările aduse planurilor de continuitate a activităţii şi de recuperare în caz de dezastru personalului cheie implicat.

EXEMPLE DE EVIDENȚE

- Planul de continuitate a activității și planul de recuperare în caz de dezastru.
- Alinierea la standarde/bune practici.
- Lista dezastrelor relevante și a capacităților de recuperare disponibile (interne sau terțe).
- Măsuri de răspuns în caz de dezastru, inclusiv site-uri de failover și backup-uri la distanță.
- Structuri organizaționale actualizate, comunicate în mod clar.
- Inventarul serviciilor esențiale și planurile de urgență aferente.
- BIA documentată cu obiective de recuperare definite.
- Procese, proceduri și măsuri de continuitate pentru evenimente perturbatoare.
- Planuri/programe pentru teste viitoare.
- Înregistrări ale testelor, revizuirilor și actualizărilor anterioare.
- Jurnale de activare și execuție a planului, inclusiv decizii și timpi de recuperare.
- Comunicări privind modificările planului (e-mailuri, intranet, documente).
- Evidențe că lecțiile învățate din teste sunt incorporate în planurile actualizate.

Ref: Cerințe aprobate prin HG 562/2025
pct. 38, pct. 39.1-39.8, pct. 40, pct. 41

1.8 Gestionarea copiilor de rezervă şi a redundanţei

ÎNDRUMĂRI

Luaţi în considerare dacă să investiţi în propria redundanţă sau să angajaţi terţi, de exemplu furnizori de servicii cloud, pentru a asigura nivelul corespunzator de redundanţă, în conformitate cu BIA.

Timpii de recuperare nu trebuie să depăşească obiectivele de recuperare.

Dacă o entitate angajează terţi pentru a asigura un nivel adecvat de redundanţă, ar trebui să se decidă în mod clar dacă este responsabilitatea entităţii să intocmeasca planurile de backup sau dacă terţii au vreo implicare în acest proces.

Verificaţi integritatea copiilor de rezervă.

Definiţi resursele minime necesare pentru a asigura cel puţin o redundanţă parţială pentru:

- reţea şi sisteme informatice
- active
- personal
- platforme multiple de comunicare, de exemplu reţele sociale, aplicaţii de mesagerie şi e-mail; şi metode multiple de alimentare a unui site, fie prin intermediul mai multor furnizori de energie electrică, fie printr-o combinaţie de furnizori de energie electrică şi mecanisme de rezervă, cum ar fi generatoarele.

Deciziile privind alocarea şi ajustarea resurselor trebuie să fie ghidate de necesitatea de backup şi redundanţă.

Adaptaţi frecvenţa verificării copiilor de rezervă la importanţa datelor pe baza evaluării riscurilor.Asiguraţi-vă că problemele şi lecţiile învăţate din exerciţii sunt abordate de persoanele responsabile şi că procesele şi sistemele relevante sunt actualizate în consecinţă.

Implicaţi furnizorii şi alte părţi terţe, cum ar fi partenerii de afaceri sau clienţii, în teste.

EXEMPLE DE EVIDENȚE

- Planuri de backup și jurnale de backup regulate.
- Backup-uri stocate separat, protejate, criptate și cu copii off-site.
- Configurații ale software-ului de backup care indică stocarea multimedia și utilizarea sumelor de control/hash.
- Proceduri clare de restaurare pentru toate sistemele și serviciile.
- Setări de stocare în cloud (dacă se utilizează) care confirmă recepția corectă a copiilor de rezervă.
- Teste regulate de restaurare, inclusiv recuperări complete la nivel de sistem și de fișiere.
- Simulări și activități de conștientizare pentru a verifica gradul de pregătire.
- Jurnale și rapoarte privind starea backup-ului, procesele și rezultatele testelor.
- Program de testare a copiilor de rezervă (scenarii, frecvență, roluri, șabloane).
- Rapoarte din testele anterioare, inclusiv timpii de recuperare și lecțiile învățate.
- Probleme abordate, cu planuri actualizate, revizuiri și jurnale de modificări.
- Contribuții ale furnizorilor/terților pentru îmbunătățirea scenariilor de testare.

Ref: Cerințe aprobate prin HG 562/2025 pct. 42, pct. 43.1-43.6, pct. 44, pct. 45.1-45.4, pct. 46, pct. 47

1.9 Politica de securitate a lanţului de aprovizionare

ÎNDRUMĂRI

Luaţi în considerare standardele recunoscute în industrie sau bunele practici atunci când elaboraţi politica privind lanţul de aprovizionare.

Rolul unui furnizor sau prestator de servicii poate fi unul sau mai multe dintre următoarele:

- Furnizor de TIC (inclusiv furnizor de software şi hardware)
- Producător
- furnizor de servicii gestionate
- furnizor de servicii de securitate gestionate
- furnizor de servicii de cloud computing.

În cazul software-ului liber şi open source (FOSS), comunităţile şi proiectele care dezvoltă, întreţin şi distribuie software în mod deschis nu pot fi considerate furnizori direcţi sau furnizori de servicii în cazul în care nu există o relaţie contractuală între entitatea relevantă şi proiectul open source, dincolo de aderarea la o licenţă standardizată de drepturi de autor, sau în cazul în care relaţia contractuală este cu un administrator de software open source.

Asiguraţi-vă că, în toate contractele noi şi reînnoite relevante, cerinţele de securitate sunt implementate corespunzator.

Efectuaţi o analiză de risc înainte de a încheia orice acord cu furnizorii şi prestatorii de servicii în legătură cu securitatea informaţiilor.

Revizuiţi politica privind lanţul de aprovizionare cel puţin o dată pe an.

Creaţi şi menţineţi un proces de monitorizare a furnizorilor şi prestatorilor de servicii pe durata ciclului de viaţă.

Stabiliţi o revizuire periodică (de exemplu, ca parte a unei întâlniri periodice cu furnizorii) şi urmăriţi abaterile de la SLA-urile convenite.

Definiţi şi atribuiţi responsabilităţi privind întreţinerea, exploatarea şi proprietatea activelor.

Asiguraţi-vă că monitorizarea include reevaluarea periodică a conformităţii furnizorilor şi prestatorilor de servicii şi monitorizaţi notele de lansare ale furnizorilor şi prestatorilor de servicii.

Asigurați-vă periodic de conformitatea configurației produsului cu recomandările furnizorului, cu o frecvență crescută pe măsură ce produsele îmbătrânesc.

Țineți evidența incidentelor de securitate legate de sau cauzate de furnizori și prestatori de servicii, deoarece acestea pot declanșa o revizuire neprogramată a furnizorilor și prestatorilor de servicii.

EXEMPLE DE EVIDENȚE

- Politica de securitate a lanțului de aprovizionare, aliniată la standarde și bune practici.
- Comunicarea către furnizori a obligațiilor lor în materie de securitate.
- Contracte care includ cerințe de securitate, inclusiv pentru furnizorii noi.
- Compararea contractelor cu ofertele pentru a verifica securitatea achizițiilor.
- Rezultatele analizei riscurilor furnizorilor.
- Planuri de revizuire a politicii și înregistrări ale revizuirilor anterioare.
- Lista incidentelor de securitate legate de furnizori sau prestatori de servicii.
- Evidențe ale actualizărilor politicilor după schimbări sau incidente majore.
- Înregistrări privind evaluarea furnizorilor.
- Monitorizarea nivelurilor de servicii conform SLA.
- Înregistrări privind răspunsul la incidente care implică probleme TIC legate de furnizori.
- Contracte aliniate la politica de securitate, inclusiv roluri, responsabilități și obligații de raportare a incidentelor.
- Documentația privind procesul de ieșire a furnizorului (tranziția serviciilor, gestionarea datelor, eliminarea accesului).
- Lista incidentelor de securitate legate de terți.

Ref: Cerințe aprobate prin HG 562/2025 pct. 53, 54.1-54.4, pct. 55.1-55.8, pct. 56, pct. 57, pct. 58.1-58.4, pct. 59.1-59.2

1.10 Ciclul de viaţă al dezvoltării securizate

ÎNDRUMĂRI

Luaţi în considerare politicile şi normele entităţii (dacă sunt disponibile) şi standardele recunoscute în industrie atunci când elaboraţi regulile pentru dezvoltarea sigură a sistemelor de reţea şi informaţionale.

Toate entităţile ar trebui să implementeze un proces de ciclu de viaţă al dezvoltării software-ului securizat (SSDLC). Cu toate acestea, entităţile mai mici pot utiliza un proces mai puţin exigent, cum ar fi implementarea practicilor de securitate prin proiectare şi a proceselor de testare a securităţii.

În funcţie de tipul cerinţei, regulile pentru dezvoltarea securizată a software-ului şi a sistemelor ar trebui să includă metode adecvate de testare a software-ului (de exemplu, testare black-box, testare ad-hoc, testare statică versus dinamică a securităţii aplicaţiilor).

Testaţi securitatea prin proiectare în diferite etape ale dezvoltării sigure a SSDLC înainte de punerea în funcţiune, utilizând instrumente independente şi o platformă de testare self-service pe tot parcursul SSDLC.

Atunci când se utilizează date reale de producţie - sau variaţii derivate ale acestora - pentru testare, asiguraţi-vă că aceste date sunt sanitizate sau anonimizate în mod corespunzător.

Atunci când utilizează componente de software liber şi open source, entităţile ar trebui să ţină seama de natura voluntară a proiectelor open source. Acolo unde este posibil, entităţile ar trebui să sprijine proiectele open source de care depind în adoptarea de sisteme sigure şi principii de codificare sigură (cum ar fi introducerea proceselor SSDLC adaptate modului de lucru al proiectului).

Aliniaţi regulile de dezvoltare securizată la politica şi procedurile de testare a securităţii şi la achiziţia securizată de servicii, sisteme sau procese de produse TIC.

Asigurati comunicarea regulilor interne de dezvoltare personalului relevant din cadrul departamentului de dezvoltare externalizat.

Organizaţi întâlniri periodice între unităţile organizaţionale în toate fazele ciclului de viaţă al dezvoltării.

Revizuiţi regulile pentru dezvoltarea securizată a reţelelor şi a sistemelor informatice cel puţin o dată la doi ani.

EXEMPLE DE EVIDENȚE

- Reguli de dezvoltare sigură, aliniate la politici, standarde și bune practici.
- Evidențe ale adoptării acestor reguli.
- Rezultatele testelor din medii de dezvoltare sigure, inclusiv protecția datelor de testare.
- Metode de testare a software-ului alese, cu justificarea acestora.
- Rezultate actualizate ale testelor SSDLC, aprobate atunci când este necesar.
- Metode de testare aplicate în fiecare etapă SSDLC.
- Verificarea consecvenței între regulile de dezvoltare securizată, politica de testare a securității și procesele de achiziție securizate.
- Comunicarea regulilor de dezvoltare către echipele interne și externalizate.
- Înregistrări ale întâlnirilor interdepartamentale privind dezvoltarea sistemelor/software-ului.
- Programele de revizuire a regulilor de dezvoltare securizată.
- Evidențe ale revizuirii dezvoltării patch-urilor și a configurațiilor sigure din proiectare.
- Procesele verbale ale ședințelor, concluziile revizuirii și acțiunile de îmbunătățire.
- Istoric versiuni/jurnale de modificări care prezintă actualizările și motivele acestora.
- Rapoarte de audit intern și extern privind procesele de dezvoltare securizată.
- Solicitări de modificare legate de regulile de dezvoltare securizată.
- Jurnale care urmăresc implementarea modificărilor pe parcursul procesului de dezvoltare.

Ref: Cerințe aprobate prin HG 562/2025
pct. 63, 64,1-64.6, 65, 66

1.11 Gestionarea modificărilor, remediere și întreținere

ÎNDRUMĂRI

Luați în considerare standardele recunoscute la nivel național și în industrie atunci când elaborați procedurile de gestionare a modificărilor.

Luați în considerare următoarele elemente pentru proceduri:

- solicitarea de modificare
- evaluarea riscurilor
- criterii de clasificare și prioritizare a schimbărilor
- cerințe pentru efectuarea revenirii la starea anterioară;
- documentarea modificărilor și aprobarea modificărilor.

Procedurile de gestionare a modificărilor pot permite fluxuri de lucru diferite, în funcție de importanța sistemului, de amploarea modificării și de urgență (de exemplu, punerea în aplicare a unui „flux de lucru pentru intervenții de urgență").

Pentru fiecare modificare, înregistrați etapele procedurii urmate.

Revizuiți și aprobați modificările în conformitate cu procedurile de gestionare a modificărilor, înainte de a le implementa.

Implementați și testați procedurile de gestionare a modificărilor pentru a vă asigura că modificările aduse rețelelor și sistemelor informatice sunt întotdeauna efectuate într-un mod predefinit.

Dacă este cazul, înființați un comitet consultativ pentru modificări (CAB) care să supravegheze și să aprobe modificările. CAB ar trebui să evalueze cererile de modificare pe baza riscului, impactului, cerințelor de resurse și alinierea la obiectivele de afaceri.

Luați în considerare efectuarea unei verificări obligatorii a integrității înainte de instalarea și implementarea unui nou software.

Asigurați-vă, acolo unde este cazul, că modificările sunt efectuate într-un mod autentificat, autorizat și care nu poate fi contestat.

Testați și validați modificările înainte de a le implementa în sistemele operaționale, acolo unde este cazul. Acolo unde este cazul, se poate efectua o analiză a impactului asupra securității într-un mediu de testare separat înainte de implementarea într-un mediu operațional.

Luați toate măsurile de precauție necesare înainte de a efectua modificări (de exemplu, faceți copii de rezervă ale imaginilor).

Planificați, efectuați, documentați și revizuiți înregistrările privind întreținerea și reparațiile componentelor sistemului în conformitate cu specificațiile furnizorului și/sau cerințele entității.

Asigurați-vă că modificările sunt permise numai cu instrumente aprobate și că executarea acestora este documentată.

Limitați utilizarea instrumentelor de întreținere numai la personalul autorizat.

Revizuiți procedurile de gestionare a modificărilor cel puțin o dată la doi ani.

Asigurați-vă că procedurile de gestionare acoperă modificările planificate și neplanificate, precum și faza de dezvoltare, dacă este cazul.

Asigurați-vă că procesul nu este ocolit.

EXEMPLE DE EVIDENȚE

- Proceduri documentate de gestionare a schimbărilor, aliniate la standarde.
- Înregistrări pentru fiecare modificare, inclusiv pașii și rezultatele.
- Procedura de întreținere a sistemului care acoperă scopul, domeniul de aplicare, rolurile, responsabilitățile și angajamentul conducerii.
- Jurnale ale revizuirilor periodice ale procedurilor de modificare, reparare și întreținere.
- Jurnale ale instalărilor de software.
- Evidențe ale MFA pentru inițierea schimbării/reparației/întreținerii (acolo unde este cazul).
- Planuri de testare și rezultate care demonstrează eficacitatea proceselor de modificare și întreținere.
- Evidențe din instrumentele de gestionare a modificărilor care impun utilizarea resurselor aprobate și a documentației obligatorii.
- ACL-uri care confirmă că accesul la instrumente este în conformitate cu politica de control al accesului.
- Programele de revizuire și procedurile actualizate cu comentarii/jurnale de modificare.
- Înregistrări de aprobare și monitorizare pentru activitățile de întreținere (la fața locului sau de la distanță).
- Jurnale ale tuturor modificărilor procedurilor, inclusiv detalii și aprobări.
- Jurnale de audit și înregistrări de conformitate (interne/externe).
- Jurnale de incidente care arată actualizările procedurilor după evenimente semnificative.

Ref: Cerințe aprobate prin HG 562/2025
pct. 70, pct. 71, pct. 72, pct. 73

1.12 Gestionarea și divulgarea vulnerabilităților

ÎNDRUMĂRI

Adoptați un cadru pentru evaluarea gravității vulnerabilităților pe baza unor modele (de exemplu, CVSS, sistemul de evaluare a predicției exploatării (EPSS) sau cadrul de evaluare a vulnerabilităților SANS) și completat cu indicatori de mediu și de amenințare, după caz.

Cel puțin, abordați fără întârziere vulnerabilitățile clasificate la niveluri superioare (de exemplu, „critice" și „ridicate" în CVSS) sau echivalente (de exemplu cele conform HG 824/2025 privind divulgarea coordonată a vulnerabilităților). În măsura posibilului, nu este recomandabil să acceptați riscul unor astfel de vulnerabilități și să nu le tratati.

Partajați informațiile obținute din scanările tehnice de vulnerabilitate cu personalul desemnat din întreaga entitate și cu autoritățile pentru a contribui la eliminarea vulnerabilităților similare din alte sisteme informatice.

Dezvăluiți vulnerabilitățile încă necunoscute către CSIRT-urile desemnate, în conformitate cu politicile naționale de dezvăluire coordonată a vulnerabilităților (CVD), acolo unde este cazul.

Identificați punctul unic de contact și canalele de comunicare cu furnizorii și prestatorii de servicii cu privire la problemele legate de securitatea rețelelor și a informațiilor.

Asigurați documentarea completă a vulnerabilităților identificate, a evaluărilor de risc asociate și a oricăror planuri de atenuare elaborate.

Definiți și stabiliți rolurile și responsabilitățile asociate gestionării vulnerabilităților.

Planurile de atenuare ar trebui să includă termene clare, responsabilități atribuite și proceduri de urmărire.

Toate planurile de atenuare, împreună cu motivele deciziilor de ne remediere, ar trebui revizuite și validate de către organismul de conducere responsabil cu supravegherea riscurilor.

Verificați informațiile din canalele de monitorizare a vulnerabilităților tehnice cel puțin de două ori pe an.

Luaţi în considerare inventarierea surselor de încredere disponibile de a raporta vulnerabilităţi tehnice în componentele identificate şi distribuiţi actualizări (de exemplu site-uri web ale editorilor de software, site-ul web ASC).

EXEMPLE DE EVIDENȚE

- Cadrul de evaluare a riscurilor pentru evaluarea gravității și impactului vulnerabilităților.
- Jurnale pentru vulnerabilități critice care arată că acestea au fost remediate.
- Licențe/abonamente pentru instrumente de scanare a vulnerabilităților.
- Configurații ale scanerului care confirmă acoperirea completă a infrastructurii și definiții actualizate.
- Jurnale de scanare care arată programele, rezultatele și acțiunile ulterioare.
- Rapoarte tehnice privind vulnerabilitățile.
- Jurnale SIEM și EDR/XDR care indică vulnerabilitățile detectate și alertele.
- Rapoarte de evaluare/testare de penetrare efectuate de terți și evidențe că problemele critice identificate au fost remediate.
- Înregistrări ale vulnerabilităților dezvăluite conform politicii naționale CVD.
- Interviuri cu persoana de contact desemnată pentru comunicarea cu furnizorii/rsponsabilii cu securitatea.
- Termene de remediere, personal responsabil și înregistrări de verificare.
- Planuri și programe de atenuare anterioare.
- Înregistrări ale vulnerabilităților neadresate, cu justificări.
- Lista canalelor de monitorizare (furnizori, consultanți).
- Înregistrări de revizuire și planuri de revizuire viitoare pentru canalele de monitorizare.
- Abonamente la servicii de alertă privind vulnerabilitățile (CERT, consultanți, furnizori etc.).
- Jurnale ale revizuirilor periodice ale canalelor de monitorizare.
- Înregistrări ale alertelor primite și ale măsurilor luate.
- Jurnale ale activităților de monitorizare, inclusiv datele și sursele verificate.

Ref: Cerințe aprobate prin HG 562/2025
pct. 87, 88.1-88.5, 89, 90

1.13 Politici și proceduri pentru evaluarea eficacității măsurilor de gestionare a riscurilor de securitate cibernetică

ÎNDRUMĂRI

Luați în considerare standardele recunoscute în industrie atunci când elaborați politica și procedurile de evaluare a implementării eficiente a măsurilor.

Implementați o politică de evaluare a eficacității implementării măsurilor care să fie proporțională cu nivelul de risc al entității, în conformitate cu evaluarea riscurilor.

Atunci când selectați măsuri pentru evaluarea eficacității implementării, luați în considerare costul implementării acestora.

Luați în considerare una sau mai multe dintre următoarele metode indicative pentru evaluarea eficacității implementării unei măsuri, în conformitate cu planul de tratare a riscurilor:

- autoevaluare
- compararea cu o listă de verificare a măsurii sau cu un standard
- evaluarea vulnerabilității
- testarea penetrării (de exemplu, internă, externă, echipă roșie/albastră)
- revizuirea codului de securitate
- audit (de exemplu, intern, extern, conformitate)
- monitorizarea performanței.

Serviciul de evaluare poate fi furnizat de o entitate externă sau de angajați special autorizați ai entității

Definiți indicatorii cheie de performanță (KPI) pentru a măsura eficacitatea măsurilor, inclusiv unul sau mai multe exemple notabile, cum ar fi (listă orientativă, neexhaustivă)

Dacă este posibil, utilizați aceiași KPI pentru fiecare evaluare și utilizați șabloane și liste de verificare standardizate pentru a asigura coerența și exhaustivitatea.

Revizuiți politica și procedurile de evaluare a eficacității măsurilor cel puțin o dată la doi ani, ținând seama de:

- modificările aduse sistemelor informatice;
- modificările aduse mediului de operare;
- tendințele legate de amenințări și vulnerabilități

Actualizaţi politica şi procedurile pe baza rezultatelor testelor de securitate şi a revizuirii independente a politicii privind securitatea reţelei şi a sistemelor informatice.

EXEMPLE DE EVIDENȚE

- Politici și proceduri documentate pentru evaluarea eficacității, aliniate la standarde.
- Evidențe ale raportării managementului cu privire la rezultatele implementării și monitorizării.
- Obiective și indicatori de performanță documentați pentru măsurarea eficacității.
- Înregistrări ale analizelor și evaluărilor din verificarile anterioare.
- Jurnale ale evaluărilor anterioare și planuri pentru cele viitoare.
- Roluri și responsabilități documentate.
- Înregistrări din revizuirile anterioare ale politicilor și programele de revizuire viitoare.
- Planul de tratare a riscurilor care reflectă rezultatele evaluării.
- Procesele verbale ale ședințelor în care se discută rezultatele testelor, eficacitatea politicilor și îmbunătățirile.
- Evidențe ale actualizărilor aduse politicilor și procedurilor pe baza revizuirilor eficacității.

Ref: Cerințe aprobate prin HG 562/2025 pct. 91, pct. 92.1-92.6, pct. 93

1.14 Sensibilizarea și practicile de bază în materie de igienă cibernetică

ÎNDRUMĂRI

Implementarea programelor de sensibilizare în materie de securitate cibernetică:

- utilizaţi diverse formate, cum ar fi ateliere, seminarii web şi module de e-learning;
- utilizaţi mai multe canale de comunicare (e-mailuri, buletine informative şi intranet) pentru a informa angajaţii cu privire la actualizările în materie de securitate cibernetică, riscuri şi practici de igienă cibernetică pentru utilizatori.

Includeţi practici de igienă cibernetică pentru utilizatorii relevanţi:

- politica privind birourile şi ecranele curate;
- utilizarea mijloacelor şi metodelor relevante de autentificare puternică, parole multifactoriale etc.;
- raportarea evenimentelor;
- utilizarea sigură a e-mailului şi navigarea pe internet;
- protecţie împotriva phishingului şi ingineriei sociale;
- utilizarea în condiţii de siguranţă a dispozitivelor mobile;
- utilizarea în condiţii de siguranţă a vehiculelor conectate ale entităţii;
- practici de conectare sigură;
- actualizări software;
- configurarea sigură a dispozitivelor;
- segmentarea reţelei;
- practici sigure de telemuncă.

Includeţi următoarele în program:

- Instruiţi personalul cu privire la politica de securitate a reţelelor şi a sistemelor informatice.
- Instruiţi personalul să recunoască atacurile de inginerie socială, cum ar fi phishing, pre-texting şi tailgating.
- Instruiţi personalul să fie conştient de cauzele expunerii accidentale a datelor. Exemple de subiecte includ livrarea eronată a datelor sensibile, pierderea unui dispozitiv portabil al utilizatorului final, furnizarea de acces neautorizat la un vehicul conectat al unei entităţi şi la datele stocate pe acesta şi publicarea datelor către un public neintenţionat.
- Instruirea personalului cu privire la pericolele conectării şi transmiterii de date prin reţele nesigure pentru activităţile entităţii. Dacă entitatea are angajaţi care lucrează de la distanţă, instruirea ar trebui să includă îndrumări pentru a se asigura că toţi utilizatorii îşi configurează în mod sigur infrastructura reţelei de acasă.
- Instruiţi personalul pentru a înţelege software-ul rău intenţionat şi neautorizat, importanţa detectării software-ului rău intenţionat şi riscurile şi consecinţele utilizării software-ului neautorizat.
- Oferiţi angajaţilor puncte de contact şi resurse pentru sfaturi suplimentare.

- Pentru a implementa programul de sensibilizare, consultaţi sursele disponibile, cum ar fi cele ale organizațiilor naționale sau internaționale de securitate cibernetică, AR-in-a-Box al ENISA şi Cybersecurity Skills Academy.
- Oferiţi periodic programe de sensibilizare în materie de securitate cibernetică.
- Luaţi în considerare indicatori de performanţă comuni pentru a măsura eficacitatea programului de sensibilizare.
- Revizuiţi şi actualizaţi programul de sensibilizare cel puţin o dată pe an.

EXEMPLE DE EVIDENȚE

- Program de sensibilizare documentat, cu obiective, conținut, frecvență și calendar.
- Materiale de sensibilizare (broșuri, e-mailuri, prezentări, module online).
- Înregistrări ale participării, cum ar fi jurnale, liste de prezență, certificate sau confirmări.
- Rezultate ale testelor sau evaluărilor care măsoară nivelul de înțelegere al angajaților.
- Feedback-ul angajaților cu privire la eficacitatea programului.
- Înregistrări ale programului revizuite și actualizate, care arată actualizări periodice.

Ref: Cerințe aprobate prin HG 562/2025
pct. 94, pct. 95.1-95.3, pct. 96

1.15 Instruire în materie de securitate

ÎNDRUMĂRI

Evaluaţi care roluri din cadrul entităţii necesită competenţe şi expertiză relevante în materie de securitate.

Oferiţi instruire care se concentrează pe competenţele specifice de securitate necesare pentru rolurile identificate.

Luaţi în considerare diverse metode de instruire, cum ar fi cursuri online, ateliere, laboratoare practice, simulări, certificări sau participarea la conferinţe sau seminarii web pe tema securităţii, precum şi menţinerea certificărilor.

Examinaţi dacă noua poziţie sau rolul unui angajat necesită instruire specifică în domeniul securităţii reţelelor şi informaţiilor.

Oferiţi periodic cursuri de formare în domeniul securităţii cibernetice.

Revizuiţi şi actualizaţi programul de formare cel puţin o dată pe an.

EXEMPLE DE EVIDENȚE

- Program de formare documentat care prezintă obiectivele în funcție de rol, conținut și frecvență.
- Înregistrări ale participării (jurnale, liste de prezență, certificate, confirmări).
- Materiale de instruire (fișe, prezentări, module online).
- Actualizări periodice care arată că programul este revizuit și îmbunătățit în timp.
- Feedback-ul angajaților pentru a evalua eficacitatea și a identifica îmbunătățirile.

Ref: Cerințe aprobate prin HG 562/2025
pct. 97, pct. 98, pct. 99.1-99.3, pct. 100, pct. 101

1.16 Proceduri de încetare sau modificare a contractului de muncă

ÎNDRUMĂRI

Includeţi clauze specifice în contractele de muncă care să descrie responsabilităţile şi îndatoririle continue ale angajaţilor în materie de securitate după încetarea contractului de muncă sau schimbarea rolului lor.

Asiguraţi-vă că aceste clauze acoperă protecţia informaţiilor confidenţiale, returnarea bunurilor companiei şi restricţiile privind accesul la reţeaua şi sistemele informatice ale entităţii.

Revocaţi accesul la reţea şi la sistemele informatice în timp util, la încetarea contractului de muncă sau la schimbarea funcţiei.

Identificaţi şi documentaţi toate bunurile care trebuie returnate la încetarea sau schimbarea contractului de muncă.

După o schimbare a locului de muncă, informaţi personalul cu privire la procedurile în vigoare.

EXEMPLE DE EVIDENȚE

- Documente, cum ar fi termenii și condițiile de angajare, contractele sau acordurile, care prezintă responsabilitățile și îndatoririle care rămân valabile după încetarea contractului de muncă sau a contractului.
- Înregistrări care confirmă returnarea în timp util a activelor entității.
- Înregistrări care confirmă revocarea la timp a drepturilor de acces.
- Copii ale notificărilor scrise adresate angajatului cu privire la încetarea sau schimbarea statutului de angajat.

Ref: Cerințe aprobate prin HG 562/2025 pct. 111, pct. 112

1.17 Politica de control al accesului

ÎNDRUMĂRI

Implementaţi şi menţineţi restricţii logice şi fizice de acces la reţea şi la sistemul informatic pe baza politicilor de control al accesului care ţin seama de bunele practici din industrie.

Asiguraţi-vă că aceste politici sunt documentate, comunicate tuturor părţilor interesate relevante şi includ orientări clare privind utilizarea adecvată a privilegiilor de acces.

Revizuiţi politicile cel puţin o dată pe an.
Luaţi în considerare cele două principii generale utilizate cel mai frecvent în contextul controlului accesului:

- necesitatea de a cunoaşte: unei entităţi i se acordă acces numai la informaţiile de care are nevoie pentru a-şi îndeplini sarcinile şi în conformitate cu clasificarea activelor;
- necesitatea utilizării: unei entităţi i se acordă acces la infrastructura tehnologiei informaţiei numai în cazul în care există o necesitate clară.

Luaţi în considerare următoarele aspecte atunci când specificaţi regulile de control al accesului:

- stabilirea de reguli bazate pe premisa privilegiului minim („totul este în general interzis, cu excepţia cazului în care este permis în mod expres”) în locul regulii mai slabe („totul este în general permis, cu excepţia cazului în care este interzis în mod expres”);
- modificările permisiunilor utilizatorilor iniţiate automat de reţea şi de sistemul informatic şi cele iniţiate de un administrator de sistem;
- momentul în care trebuie definită şi revizuită periodic aprobarea.

Luaţi în considerare modalităţi de implementare a controlului accesului, cum ar fi controlul accesului obligatoriu (MAC), controlul accesului discreţionar (DAC), controlul accesului bazat pe roluri (RBAC) şi controlul accesului bazat pe atribute (ABAC), în funcţie de nevoile organizaţiei.

Luaţi în considerare faptul că regulile de control al accesului pot conţine şi elemente dinamice (de exemplu, o funcţie care evaluează accesele anterioare sau valori specifice ale mediului).

EXEMPLE DE EVIDENȚE

- Politica de control al accesului care prezintă cerințele, procedurile și responsabilitățile.
- Rapoarte privind incidentele legate de accesul neautorizat și măsurile luate.
- Înregistrări ale revizuirilor și actualizărilor politicii.
- Rapoarte de audit intern/extern care evaluează eficacitatea controlului accesului.
- Revizuiri ale accesului care demonstrează conformitatea cu principiul „necesității de a cunoaște”/„necesității de a utiliza”.
- Înregistrări privind gestionarea modificărilor care documentează modificările aduse drepturilor de acces.
- Configurații ale sistemului de control al accesului.

Ref: Cerințe aprobate prin HG 562/2025
pct. 115, pct. 116.1-116.3, pct. 117

1.18 Clasificarea activelor

ÎNDRUMĂRI

Creaţi şi documentaţi nivelurile de clasificare pentru active, inclusiv convenţiile de clasificare.

Definiţi criteriile pentru revizuirea clasificării în timp.

Revizuiţi clasificarea cel puţin o dată pe an, luând în considerare:

- modificările legislative;
- modificările valorii, sensibilităţii şi importanţei activelor pe parcursul ciclului lor de viaţă.

Asiguraţi-vă că proprietarii activelor sunt responsabili pentru clasificarea acestora.

Comunicaţi personalului clasificarea activelor şi cerinţele de protecţie asociate.

EXEMPLE DE EVIDENȚE

- Niveluri de clasificare documentate pentru active;
- Documentație care prezintă programul revizuirilor;
- Înregistrări ale celei mai recente revizuiri și jurnale care detaliază modificările efectuate în timpul ultimei revizuiri, inclusiv reclasificări și adăugarea/eliminarea de active;
- Personalul cunoaște nivelurile de clasificare și cerințele de protecție pentru fiecare nivel.

Ref: Cerințe aprobate prin HG 562/2025 pct. 136, pct. 137.1-137.3, pct. 138, pct. 139, pct. 140.1-140.3, pct. 141

1.19 Politica privind suporturile de stocare amovibile

ÎNDRUMĂRI

Definiți, documentați și implementați o politică privind gestionarea suporturilor amovibile.

Comunicați politica angajaților și terților care manipulează suporturi de stocare amovibile pentru a vă asigura că aceștia sunt la curent cu politica.

Aliniați politica la clasificarea activelor și includeți cel puțin următoarele:

- definiții și domeniul de aplicare al suporturilor de stocare amovibile;
- cerințe de autorizare;
- linii directoare de utilizare;
- măsuri de control și protecție a suporturilor amovibile în timpul depozitării și transportului;
- tehnici de protejare a informațiilor pe suporturile de stocare amovibile;
- proceduri de răspuns la incidente pentru suporturile pierdute sau compromise.

Configurați rețeaua și sistemele informatice pentru a dezactiva funcția de rulare automată pentru toate mediile amovibile, pentru a preveni executarea automată a software-ului potențial rău intenționat.

Dacă conectarea suporturilor amovibile nu este interzisă din motive organizaționale, suporturile amovibile trebuie scanate pentru a detecta coduri rău intenționate, după caz, cu ajutorul unui software actualizat împotriva codurilor rău intenționate, înainte de a fi conectate la rețeaua și sistemele informatice ale entității și/sau în timp real.

Criptați datele sensibile stocate pe suporturi amovibile utilizând algoritmi criptografici puternici pentru a le proteja împotriva accesului neautorizat

Utilizați criptarea pentru a proteja datele stocate pe dispozitive de stocare portabile, asigurându-vă că utilizatorii neautorizați nu pot accesa datele în cazul pierderii sau furtului dispozitivului.

Implementați măsuri de securitate fizică, acolo unde este cazul, cum ar fi locuri de stocare sigure și jurnale de urmărire pentru dispozitivele de stocare portabile.

Monitorizați și auditați periodic utilizarea suporturilor amovibile pentru a asigura conformitatea cu politica.

EXEMPLE DE EVIDENȚE

- Politica documentată privind suporturile amovibile.
- Materiale de îndrumare pentru angajați și terți.
- Înregistrări de instruire sau confirmare care atestă că utilizatorii înțeleg politica.
- Materiale de sensibilizare (postere, e-mailuri, mementouri pe intranet).
- Configurații de protecție a terminalelor legate de suporturile amovibile.
- Jurnale de audit care urmăresc utilizarea suporturilor (inserare, scoatere, transferuri de date).
- Rapoarte de incidente care implică suporturi amovibile.
- Politică actualizată privind suporturile amovibile, care reflectă practicile curente.

Ref: Cerințe aprobate prin HG 562/2025 pct. 142, pct. 143.1-143.4, pct. 144

1.20 Utilităţi de sprijin

ÎNDRUMĂRI

Luaţi în considerare utilităţile necesare, acolo unde este relevant, care asigură funcţionarea continuă a reţelelor şi a sistemelor informatice, cum ar fi (listă orientativă, neexhaustivă):

- alimentarea cu energie electrică – energie electrică pentru menţinerea funcţionării sistemelor;
- apă pentru răcire şi alte necesităţi operaţionale;
- gaz pentru încălzire sau generarea de energie de rezervă;
- HVAC pentru menţinerea condiţiilor optime de funcţionare;
- telecomunicaţii – conectivitate la internet şi la reţea.

Includeţi în evaluarea riscurilor potenţialele defecţiuni şi întreruperi ale utilităţilor de sprijin.

Luaţi în considerare disponibilitatea utilităţilor auxiliare în planul de continuitate a activităţii

Luaţi în considerare disponibilitatea utilităţilor auxiliare atunci când implementaţi gestionarea capacitatilor de rezervă.

Luaţi în considerare implementarea de măsuri pentru protecţia utilităţilor auxiliare:

- răcire activă/pasivă;
- repornire automată după întreruperea alimentării cu energie electrică;
- alimentare de rezervă cu baterii;
- generatoare diesel;
- combustibil de rezervă;
- alimentare neîntreruptibilă, generatoare de rezervă;
- SLA pentru livrarea unei cantităţi suficiente de combustibil;
- companii de livrare;
- răcire redundantă;
- piese de schimb pentru componentele reţelelor şi sistemelor informatice;
- sisteme de alimentare de rezervă.

Efectuaţi teste de rutină ale măsurilor de protecţie.

Organizaţi revizuiri periodice pentru a evalua eficacitatea măsurilor de protecţie actuale.

Includeţi o simulare de pană totală de curent în verificarea procedurii de testare a generatoarelor de curent.

Sensibilizaţi angajaţii cu privire la dependenţa de utilităţile auxiliare.

Instruiți personalul cu privire la modul de a răspunde eficient la defecţiuni şi întreruperi ale utilităţilor auxiliare.

Instalaţi sisteme de monitorizare pentru a detecta defecţiunile sau întreruperile utilităţilor.

EXEMPLE DE EVIDENȚE

- Lista utilităților auxiliare cu rezultatele asociate ale evaluării riscurilor.
- Măsuri de protecție împotriva defecțiunilor și întreruperilor utilităților.
- Descrierea tipurilor de utilități relevante pentru operațiuni.
- Măsuri de protecție actualizate, inclusiv note de revizuire sau jurnale de modificări.
- Evidențe privind implementarea și testarea periodică a acestor măsuri de protecție.
- Comunicări interne care subliniază importanța și impactul utilităților auxiliare.
- Jurnale ale defecțiunilor sau întreruperilor utilităților detectate.

Ref: Cerințe aprobate prin HG 562/2025 pct. 150, pct. 151.1-151.6, pct. 152

2. Identificare

2.1 Gestionarea drepturilor de acces

ÎNDUMĂRĂRI

Asigurați-vă că fiecare utilizator are acces numai la informațiile necesare pentru rolul său („necesitatea de a ști").

Limitați permisiunile utilizatorilor la minimul necesar pentru îndeplinirea sarcinilor lor („privilegiu minim"). Revizuiți și ajustați periodic drepturile de acces, după cum este necesar.

Stabiliți care sarcini și domenii de responsabilitate trebuie separate. Stabiliți și urmați un proces de solicitare și aprobare a accesului, de preferință automatizat. Procesul ar trebui să:

- să acopere acordarea drepturilor de acces la active la angajarea unui nou utilizator sau la schimbarea rolului unui utilizator;
- să obțină autorizarea de la proprietarul activului; poate fi adecvată și aprobarea separată a drepturilor de acces de către organele de conducere;
- să se asigure că drepturile de acces sunt activate (de exemplu, de către furnizorii de servicii) numai după finalizarea cu succes a procedurilor de autorizare;
- să ia în considerare cerințele de afaceri și politica de control al accesului a entității;
- să ia în considerare separarea sarcinilor, inclusiv separarea rolurilor de aprobare și implementare a drepturilor de acces și separarea rolurilor conflictuale;
- verificarea faptului că nivelul de acces acordat este în conformitate cu politica de control al accesului și este în concordanță cu alte cerințe de securitate a informațiilor, cum ar fi separarea sarcinilor;
- se va lua în considerare acordarea de drepturi de acces temporare pentru o perioadă determinată și revocarea acestora la data expirării, în special pentru personalul temporar sau accesul temporar solicitat de personal.

Stabiliți și urmați un proces, de preferință automatizat, pentru revocarea accesului la active. Procesul ar trebui:

- să dezactiveze în timp util conturile la încetarea contractului, revocarea drepturilor sau schimbarea rolului unui utilizator, după caz; dezactivarea conturilor, în loc de ștergerea acestora, poate fi necesară pentru păstrarea pistelor de audit;
- sa modifice drepturile de acces ale utilizatorilor care și-au schimbat rolurile sau locurile de muncă;
- a elimina sau ajusta drepturile de acces, ceea ce se poate face prin eliminarea, revocarea sau înlocuirea cheilor, a informațiilor de autentificare, a cardurilor de identificare sau a abonamentelor.
- acolo unde este posibil, să permită diferitelor componente sau servicii să partajeze informații (semnale) despre revocarea accesului în timp util.

Limitați accesul terților în funcție de necesitate și durată. Utilizați conturi de acces temporare cu date de expirare și revizuiți periodic drepturile de acces ale terților.

Asigurați-vă că terții își recunosc responsabilitățile și obligațiile în materie de acces.

Păstrați o evidență centrală detaliată și actualizată (registru sau bază de date) a tuturor drepturilor de acces acordate, inclusiv numele de utilizator, rolurile, permisiunile și datele modificărilor de acces.

Stabiliți și mențineți un inventar al sistemelor de autentificare și autorizare, inclusiv al celor găzduite la fața locului sau la un furnizor de servicii la distanță.

Implementați înregistrarea tuturor activităților de gestionare a drepturilor de acces. Jurnalele trebuie să includă detalii despre cine a acordat sau modificat accesul, când și ce modificări au fost făcute.
Reduceți la minimum utilizarea conturilor generice și partajate și asigurați-vă că utilizatorii pot fi întotdeauna identificați pentru acțiunile lor în cadrul sistemelor TIC.
Revizuiți periodic drepturile de acces fizic și logic, ținând seama de:

- drepturile de acces ale utilizatorilor după încetarea sau schimbarea locului de muncă;
- autorizațiile pentru drepturile de acces privilegiate.

Revizuiți și actualizați periodic inventarul sistemelor de autentificare și autorizare.

Efectuați revizuiri ale controlului accesului la active pentru a verifica dacă toate privilegiile sunt autorizate în mod periodic, cel puțin o dată pe an.

Centralizați controlul accesului pentru toate activele printr-un serviciu de director sau un furnizor de autentificare unică (SSO), acolo unde este posibil.

Implementați o matrice de separare a sarcinilor și asigurați-vă că aceasta este actualizată în mod dinamic prin automatizarea modului în care sunt gestionate modificările ca răspuns la atribuirea rolurilor sau modificările sarcinilor (de exemplu, integrarea cu sistemele de control al accesului, IAM sau de planificare a resurselor întreprinderii (ERP)).

EXEMPLE DE EVIDENȚE

- Roluri de utilizator și drepturi de acces definite.
- Registru centralizat al drepturilor de acces cu utilizatori, roluri, niveluri de acces și date de modificare.
- Documentație aprobată privind cererile de acces pentru acordări, modificări și retrageri, inclusiv gestionarea securizată a copiilor de rezervă arhivate.
- Revizuiri periodice ale accesului care confirmă privilegiul minim (necesitatea de a cunoaște / necesitatea de a utiliza).
- Jurnale de sistem care arată acțiunile de gestionare a drepturilor de acces (creare, modificare, ștergere).
- Jurnale de audit cu marcaje temporale, ID-uri de utilizator și acțiuni.
- Înregistrări ale incidentelor legate de probleme privind drepturile de acces și acțiuni corective.
- Evidențe ale IAM sau ale altor sisteme care aplică controale de acces.
- Rapoarte de audit interne/externe care verifică conformitatea cu politica de control al accesului.
- Rezultatele inspecțiilor fizice ale sistemelor de control al accesului (dacă este cazul).
- Înregistrări ale revizuirilor și actualizărilor periodice ale proceselor de drepturi de acces.
- Evidențe privind utilizarea unui director centralizat sau a SSO, susținute de jurnale și documentație.
- Matrice de separare a sarcinilor.

Ref: Cerințe aprobate prin HG 562/2025 pct. 118, pct. 119.1-119.6, pct. 120

2.2 Conturi privilegiate și conturi de administrare a sistemului

ÎNDRUMĂRI

Alocaţi drepturi de acces privilegiate utilizatorilor, doar atunci când este necesar şi, de la caz la caz, în conformitate cu controlul accesului.

Identificaţi utilizatorii care au nevoie de acces privilegiat la o reţea şi la un sistem informatic (de exemplu, sisteme de operare, sisteme de gestionare a bazelor de date şi aplicaţii). Aceasta ar trebui să includă orice acces fizic privilegiat , de exemplu la coduri criptografice, chei sau dispozitive.

Menţineţi un proces de autorizare şi o evidenţă a tuturor drepturilor de acces privilegiate alocate, în conformitate cu procesul de acordare şi revocare a drepturilor de acces.

Introduceţi cerinţe de autentificare mai stricte pentru drepturile de acces privilegiat, cum ar fi reautentificarea sau autentificarea suplimentară înainte de utilizarea drepturilor de acces privilegiat.

Definiţi şi implementaţi cerinţe de expirare pentru drepturile de acces privilegiat, acolo unde este cazul.

În absenţa unui sistem care să permită atribuirea cu certitudine a tuturor utilizărilor unei persoane, stabiliţi reguli specifice pentru a evita utilizarea ID-urilor generice de utilizator administrativ (de exemplu, „root") şi gestionaţi şi protejaţi informaţiile de autentificare ale acestor identităţi.

Acordaţi acces privilegiat temporar numai pentru perioada necesară implementării modificărilor sau activităţilor aprobate (de exemplu, pentru activităţi de întreţinere), în loc să acordaţi drepturi de acces privilegiat permanente.

Luaţi în considerare frecvenţa operaţiunilor de administrare a sistemului: sarcini zilnice (de exemplu, copii de rezervă şi rutarea e-mailurilor) versus sarcini săptămânale sau lunare (de exemplu, verificarea memoriei şi a spaţiului pe disc).

Înregistraţi toate accesele privilegiate în scopuri de audit.

Atribuiţi identităţi separate cu drepturi de acces privilegiate utilizatorilor individuali, în loc să partajaţi sau să conectaţi identităţi. Grupaţi identităţile pentru o gestionare mai uşoară, dacă este necesar.

Utilizaţi identităţi cu drepturi de acces privilegiate exclusiv pentru sarcini administrative, nu pentru sarcini generale zilnice, cum ar fi verificarea e-mailurilor sau accesarea internetului. Acolo unde este posibil, ar trebui atribuite identităţi privilegiate separate pentru sarcini administrative.

Asigurați-vă că utilizatorii sunt conștienți de drepturile lor de acces privilegiat sau când se află în modul de acces privilegiat, de exemplu utilizând identități specifice de utilizator, setări ale interfeței utilizatorului sau echipamente.

Verificați dacă sarcinile, rolurile, responsabilitățile și competențele administratorilor de sistem îi califică în continuare pentru a lucra cu drepturi de acces privilegiate.

EXEMPLE DE EVIDENȚE

- Politica de acces privilegiat care definește regulile de utilizare și condițiile de acces.
- Lista utilizatorilor privilegiați și a sistemelor la care aceștia pot avea acces.
- Înregistrări de aprobare pentru acordarea accesului privilegiat.
- Jurnale de revizuire și revocare a accesului.
- Matrice de acces bazată pe roluri, care indică privilegiile necesare pentru fiecare rol.
- Controale și măsuri de monitorizare pentru acordarea, utilizarea și revocarea accesului privilegiat.
- Înregistrări privind atribuirea accesului legate de rolurile și responsabilitățile postului.
- Definiții clare ale rolurilor cu drepturile de acces corespunzătoare.
- Jurnale de audit și monitorizare care înregistrează activitatea de acces privilegiat și încercările neautorizate.
- Jurnale de gestionare a modificărilor care documentează actualizările accesului privilegiat (modificări de roluri, încetări).
- Rapoarte de audit intern/extern care verifică conformitatea cu politica și reglementările.

Ref: Cerințe aprobate prin HG 562/2025 pct. 121, pct. 122.1-122.4, pct. 123

2.3 Sisteme de administrare

ÎNDRUMĂRI

Accesul la sistemele de administrare trebuie controlat strict, în conformitate cu politica de control al accesului. Numai personalul autorizat ar trebui să aibă acces, iar toate activităţile trebuie înregistrate şi revizuite periodic.

Trebuie să existe măsuri pentru detectarea accesului neautorizat şi pentru asigurarea responsabilităţii prin intermediul pistelor de audit şi al evaluărilor periodice de securitate.

Jurnalele de acces din sistemele de administrare trebuie integrate în soluţia centralizată de gestionare a jurnalelor sau SIEM a entităţii. Alertele automate trebuie configurate pentru a detecta şi notifica orice încercări de acces suspecte sau neautorizate, asigurând un răspuns prompt şi respectarea continuă a politicilor de securitate.

Perioada de păstrare a jurnalelor trebuie să fie clar definită pe baza nevoilor organizaţiei, a cerinţelor legale şi a obiectivelor de securitate a reţelei şi a informaţiilor.

Jurnalele trebuie să înregistreze evenimentele relevante necesare pentru monitorizarea securităţii, detectarea incidentelor şi analiza criminalistică, cum ar fi încercările de acces, acţiunile administrative şi modificările sistemului.

Implementaţi controale stricte de acces pentru a vă asigura că sistemele administrative sunt utilizate exclusiv în scopul prevăzut. De exemplu, permiteţi accesul la sistemele de administrare a sistemelor numai personalului autorizat cu roluri specifice (de exemplu, administratori de sistem şi personal IT).

Izolaţi fizic sau logic sistemele administrative de alte servere de aplicaţii, de exemplu utilizaţi segmentarea reţelei pentru a crea zone separate pentru sistemele de administrare a sistemelor şi alte sisteme, cum ar fi serverele de aplicaţii. Dacă este cazul, inspectaţi fizic rack-urile serverelor pentru a vă asigura că sunt separate.

Solicitaţi mecanisme de autentificare puternice, cum ar fi MFA, pentru accesarea sistemelor de administrare a sistemului.

Criptaţi canalele de comunicare (de exemplu, protocolul Secure Shell, protocolul Secure Hypertext Transfer Protocol) pentru a proteja datele în tranzit către şi dinspre sistemele de administrare a sistemului.

Criptaţi fişierele de configurare sensibile şi datele de autentificare stocate pe sistemele de administrare a sistemului.

Luaţi în considerare utilizarea unei soluţii centralizate de gestionare a accesului privilegiat (PAM).

Luaţi în considerare utilizarea unui broker de securitate pentru accesul la cloud (CASB) pentru a îmbunătăţi vizibilitatea, controlul şi securitatea utilizării serviciilor cloud.

Auditaţi periodic jurnalele de sistem pentru a monitoriza modelele de utilizare şi a identifica orice activităţi neautorizate.

Instruiţi personalul în utilizarea corectă a sistemelor de administrare a sistemelor.

EXEMPLE DE EVIDENȚE

- Jurnale de acces care arată cine a accesat sistemele de administrare și când.
- Rapoarte de audit intern/extern care evaluează conformitatea cu politicile de acces administrativ.
- Documentație privind segmentarea rețelei care arată separarea sistemelor de administrare.
- Metode de autentificare documentate pentru securizarea accesului administrativ.
- Detalii privind criptarea datelor transmise către/din sistemele de administrare.
- Înregistrări privind răspunsul la incidente pentru utilizarea abuzivă sau accesul neautorizat al administratorilor.
- Înregistrări privind instruirea

Ref: Cerințe aprobate prin HG 562/2025 pct. 124, pct. 125.1-125.3

2.4 Identificare

ÎNDRUMĂRI

Stabiliţi şi menţineţi un inventar al tuturor identităţilor gestionate în cadrul entităţii.

Inventarul trebuie să includă atât identităţile utilizatorilor, cât şi identităţile privilegiate sau ale administratorilor de sistem. Inventarul trebuie să conţină, cel puţin, numele persoanei, numele de utilizator, datele de începere/încetare şi nivelul de privilegii pentru fiecare identitate.

Inventarul trebuie să includă, de asemenea, toate identităţile de serviciu şi să conţină cel puţin următoarele informaţii: proprietarul departamentului, data revizuirii, scopul şi nivelul de privilegii pentru fiecare identitate de serviciu.

Luaţi în considerare faptul că acordarea sau revocarea accesului la active este, de obicei, o procedură în mai mulţi paşi:

- confirmarea cerinţelor necesare pentru stabilirea unei identităţi;
- verificarea identităţii unei entităţi înainte de a-i aloca o identitate logică;
- stabilirea unei identităţi;
- configurarea şi activarea identităţii, care include şi configurarea şi setarea iniţială a serviciilor de autentificare conexe;
- acordarea sau revocarea drepturilor de acces specifice identităţii, pe baza deciziilor corespunzătoare de autorizare sau de acordare a drepturilor

Asiguraţi-vă că identităţile atribuite sistemelor de reţea şi informaţionale (utilizatori non-umani) sunt supuse unei aprobări separate în mod corespunzător şi unei supravegheri independente continue.

Aplicaţi înregistrarea în jurnal la gestionarea identităţilor, în cooperare cu securitatea resurselor umane, acolo unde este posibil.

Identităţile partajate trebuie evitate, cu excepţia cazurilor în care sunt strict necesare din motive bine întemeiate sau operaţionale. În astfel de cazuri, utilizarea lor trebuie justificată în mod formal, aprobată în mod explicit şi documentată corespunzător. Exemple de controale tehnice, procedurale şi de guvernanţă pentru îmbunătăţirea protecţiei acestora includ (listă orientativă, neexhaustivă):

- Aplicarea MFA;
- Aplicarea conceptului de privilegiu minim;
- Acces limitat în timp sau just-in-time;
- Verificarea credenţialelor partajate prin intermediul unui instrument care înregistrează cine a accesat identitatea şi când. Dacă verificarea nu este posibilă, luaţi în considerare utilizarea înregistrării sesiunilor privilegiate sau a auditului accesului bazat pe proxy;
- Tehnici de atribuire a sesiunilor pentru a lega utilizarea identităţii partajate de utilizatorii individuali;

- Înregistrare;
- Depozitarea credenţialelor cu rotaţie automată;
- Interzicerea stocării credenţialelor partajate în fişiere personale, e-mailuri sau platforme de mesagerie;
- Segmentarea reţelei, astfel încât utilizarea conturilor partajate să fie limitată la segmente de reţea izolate sau medii virtuale; şi
- Instruire obligatorie privind utilizarea acceptabilă şi responsabilitatea.

Aceste identităţi trebuie înregistrate în mod clar în cadrul de gestionare a riscurilor de securitate cibernetică, cu controale adecvate pentru a atenua riscurile asociate, inclusiv măsuri îmbunătăţite de monitorizare şi responsabilitate.

Verificaţi dacă toate identităţile active sunt revizuite. Acest lucru se poate face în mod periodic, cel puţin trimestrial sau mai frecvent. Cu toate acestea, pentru entităţile de dimensiuni foarte mici, acest lucru se poate face anual.

Dezactivaţi sau eliminaţi, în timp util, identităţile care nu mai sunt necesare, de exemplu ştergeţi sau dezactivaţi orice identităţi inactive după o perioadă predefinită de zile de inactivitate, acolo unde este posibil.

Centralizaţi gestionarea identităţilor printr-un serviciu de director sau de identitate.

Dacă este cazul, definiţi diferite niveluri de identificare necesare în funcţie de rol, utilizare sau necesitate.

EXEMPLE DE EVIDENȚE

- Politica sau procedurile documentate de gestionare a identității.
- Rapoarte de audit intern/extern care confirmă conformitatea cu politica și reglementările.
- Înregistrări de identitate (profiluri unice de utilizator legate de persoane fizice prin intermediul datelor HR).
- Jurnale de revizuiri și aprobări ale identității pentru utilizatorii sistemului.
- Jurnale sau rapoarte de gestionare a identității care arată activitatea operațională.
- Evidențe ale sistemelor IAM care aplică controale de identitate și acces.
- Înregistrări de aprobare pentru excepții de la regulile de gestionare a identității.
- Înregistrări ale verificărilor și actualizărilor periodice ale identității.
- Înregistrări ale modificărilor identității (schimbări de rol, încetări, inactivitate).
- Evidențe ale sistemelor centralizate IAM/SSO, susținute de documentație și jurnale.

Ref: Cerințe aprobate prin HG 562/2025 pct. 126, pct. 127.1-127.4, pct. 128, pct. 129

2.5 Autentificare

ÎNDRUMĂRI

Tehnologiile de autentificare sunt metode utilizate pentru a verifica identitatea utilizatorilor, dispozitivelor sau sistemelor înainte de a acorda acces la resurse. Iată câteva tehnologii comune de autentificare (listă orientativă, neexhaustivă):

- autentificare bazată pe parolă,
- chei de acces,
- autentificare cu doi factori,
- MFA,
- autentificare biometrică,
- autentificare bazată pe token, cum ar fi codul de acces unic (OTP),
- carduri inteligente,
- chei de securitate Fast Identity Online 2,
- autentificare bazată pe certificate,
- SSO,
- OpenID Connect.

Utilizaţi credenţiale de autentificare unice pentru toate activele entităţii. Implementarea celor mai bune practici include, cel puţin, o parolă de 8 caractere pentru conturile care utilizează MFA şi o parolă de 14 caractere pentru conturile care nu utilizează MFA.

Luaţi în considerare faptul că procesul de alocare şi gestionare a informaţiilor de autentificare trebuie să asigure că:

- parolele sau codurile PIN generate automat în timpul proceselor de înscriere ca informaţii de autentificare secrete temporare să fie imposibil de ghicit şi unice pentru fiecare utilizator; şi ca utilizatorii să fie obligaţi să le schimbe după prima utilizare;
- sunt stabilite proceduri pentru verificarea identităţii unui utilizator înainte de furnizarea de informaţii de autentificare noi, de înlocuire sau temporare;
- informaţiile de autentificare, inclusiv informaţiile de autentificare temporare, sunt transmise utilizatorilor într-un mod securizat (de exemplu, printr-un canal autentificat şi protejat) şi se evită utilizarea mesajelor electronice neprotejate (text clar);
- utilizatorii confirmă primirea informaţiilor de autentificare;
- informaţiile de autentificare implicite, predefinite sau furnizate de furnizori, sunt modificate imediat după instalarea sistemelor sau a software-ului;
- se păstrează înregistrări ale evenimentelor semnificative privind alocarea şi gestionarea informaţiilor de autentificare şi se garantează confidenţialitatea acestora, iar metoda de păstrare a înregistrărilor este aprobată (de exemplu, utilizarea unui instrument aprobat de stocare a parolelor).

Atunci când parolele sunt utilizate ca informaţii de autentificare, sistemul de gestionare a parolelor ar trebui:

- să permită utilizatorilor să îşi selecteze şi să îşi schimbe propriile parole şi să includă o procedură de confirmare pentru a remedia erorile de introducere;
- să impună utilizarea parolelor puternice;
- să oblige utilizatorii să îşi schimbe parolele la prima conectare, dacă este cazul;

- să impună schimbarea parolelor atunci când este necesar, de exemplu după un incident de securitate sau la încetarea sau schimbarea locului de muncă, atunci când un utilizator cunoaște parolele pentru identități care rămân active (de exemplu, identități partajate);
- să împiedice utilizarea parolelor utilizate în mod obișnuit și a combinațiilor compromise de nume de utilizator și parole din sistemele piratate;
- să nu afișeze parolele pe ecran atunci când sunt introduse; și
- stocați și transmiteți parolele într-o formă protejată.

Se recomandă utilizarea MFA rezistentă la phishing. Mai jos este o listă a soluțiilor disponibile în prezent, ordonate de la cea mai puternică la cea mai slabă.

- „Puternic":
  - Rezistentă la phishing:
    - fără secrete partajate, nu este vulnerabilă la atacuri de tip „man-in-the-middle";
    - cheie privată criptografică protejată care poate fi înregistrată în siguranță la:
      - un domeniu, în conformitate cu standardele Fast Identity Online (FIDO) și W3C WebAuthn
      - un furnizor de încredere, în conformitate cu infrastructura cheii publice și standardele X.509 ale Uniunii Internaționale a Telecomunicațiilor.
- MFA „mediu", de exemplu:
  - notificări push, potrivire de numere sau bazată pe aplicații.
- MFA „de ultimă instanță", de exemplu:
  - mesaj text sau e-mail OTP.

Efectuați criptarea și hash-ul parolelor în conformitate cu tehnicile criptografice aprobate pentru parole.

Generați o alertă atunci când este detectată o potențială încercare sau o încălcare reușită a controalelor de conectare.

Ajustați metodele de autentificare în funcție de riscul asociat evaluat. De exemplu, solicitați autentificare suplimentară pentru tranzacții cu risc ridicat sau acces la active cu un grad mai ridicat de criticitate.

Utilizați metode de autentificare mai stricte pentru activele cu un grad de importanță mai ridicat.

Asigurați-vă că fiecare utilizator are date de autentificare unice. Evitați conturile partajate și implementați politici stricte pentru gestionarea datelor de autentificare.

Efectuați audituri periodice ale procedurilor și tehnologiilor de autentificare pentru a vă asigura că acestea rămân actualizate, acolo unde este cazul, și eficiente împotriva amenințărilor emergente.

Rămâneți la curent cu progresele în tehnologia de autentificare și integrați noi metode pe măsură ce acestea devin disponibile.

Recomandați tuturor utilizatorilor care au acces la informații de autentificare sau le utilizează să respecte următoarele:

- Informațiile secrete de autentificare, cum ar fi parolele, sunt păstrate confidențiale. Informațiile personale folosite ca secrete de autentificare nu trebuie partajate cu nimeni.

Informațiile secrete de autentificare utilizate în contextul identităţilor legate de mai mulţi utilizatori sau legate de entităţi non-personale sunt partajate exclusiv cu persoanele autorizate.

- Informațiile de autentificare afectate sau compromise sunt modificate imediat după notificarea sau orice altă indicaţie a unei compromiteri.
- Atunci când parolele sunt utilizate ca informaţii de autentificare, se selectează parole puternice, în conformitate cu recomandările privind cele mai bune practici. De exemplu, parolele nu se bazează pe nimic ce poate fi uşor ghicit sau obţinut de către alte persoane utilizând informaţii legate de persoana respectivă (de exemplu, nume, numere de telefon şi date de naştere); parolele nu se bazează pe cuvinte din dicţionar sau combinaţii ale acestora; utilizaţi fraze de acces uşor de reţinut şi încercaţi să includeţi caractere alfanumerice şi speciale; parolele trebuie să aibă o lungime minimă.
- Nu se utilizează aceleaşi acreditări pentru diferite reţele şi sisteme informatice.
- Obligaţia de a respecta aceste reguli este inclusă şi în termenii şi condiţiile de angajare.

EXEMPLE DE EVIDENȚE

- Politica de control al accesului care definește procedurile și tehnologiile de autentificare securizate.
- Jurnale ale sistemului de autentificare care arată încercările reușite și eșuate.
- Evidențe ale sistemelor IAM sau similare care impun autentificarea și controlul accesului.
- Rapoarte de audit intern/extern care verifică implementarea și conformitatea autentificării sigure.
- Documentație privind protocoalele de autentificare și autorizare, inclusiv evidențe de testare care confirmă implementarea securizată.
- Jurnale sau rapoarte legate de autentificare care indică activitatea operațională.
- Rapoarte de audit de conformitate care confirmă că gestionarea identității și autentificării este în conformitate cu politicile și reglementările.
- Înregistrări ale revizuirilor și actualizărilor periodice ale identității.
- Înregistrări ale modificărilor identității (schimbări de rol, încetări).
- Rapoarte de audit din revizuirile periodice ale tehnologiilor și procedurilor de autentificare.
- Jurnale care arată implementarea noilor metode de autentificare pe măsură ce acestea sunt introduse.
- Documentație de instruire pentru angajați privind practicile de autentificare sigură.
- Materiale de sensibilizare care subliniază importanța autentificării sigure.

Ref: Cerințe aprobate prin HG 562/2025 pct. 130, pct. 131.1-131.6, pct. 132, pct. 133

2.6 Autentificare multifactorială

ÎNDRUMĂRI

Selectaţi metode MFA adecvate şi mecanisme de autentificare continuă în funcţie de nevoile de securitate ale entităţii şi de clasificarea activului. De asemenea, este o bună practică să se ţină seama de confortul utilizatorului atunci când se selectează şi se implementează o soluţie:

- OTP bazat pe mesaje de testare: simplu, dar mai puţin sigur din cauza riscurilor precum schimbarea cartelei SIM;
- aplicaţii de autentificare: generează OTP-uri bazate pe timp;
- notificări push: trimit o cerere de aprobare către dispozitivul utilizatorului;
- tokenuri hardware: de exemplu, dispozitive fizice care generează OTP-uri, carduri inteligente;
- chei de acces;
- chei de securitate Fast Identity Online 2;
- biometrie: amprente digitale, recunoaştere facială etc.

Luaţi în considerare autentificarea continuă pentru a evita ameninţări specifice, cum ar fi deturnarea sesiunilor, furtul de credenţiale şi ameninţările interne.

Determinaţi ce reţele şi sisteme informatice necesită utilizarea protecţiei MFA pe baza clasificării activului care urmează să fie accesat. Ori de câte ori este posibil, utilizaţi MFA rezistentă la phishing.

Analizaţi rolurile utilizatorilor şi nivelul de acces necesar pentru fiecare rol pentru a determina metodele MFA adecvate.

Luaţi în considerare MFA, în special atunci când accesaţi sisteme de la distanţă, accesaţi sisteme de administrare a sistemelor, accesaţi informaţii sensibile etc.

Aplicaţi MFA pe sistemele conectate la internet, cum ar fi e-mailul, desktopul la distanţă şi VPN-urile.

Definiţi când şi cum este necesară MFA (de exemplu, la fiecare conectare, o dată pe sesiune sau pentru acţiuni cu risc ridicat).

Integraţi MFA cu soluţii SSO pentru un acces fără probleme. Ori de câte ori este posibil, utilizaţi MFA rezistent la phishing.

Implementaţi metode de rezervă sigure pentru utilizatorii care pierd accesul la metodele MFA.

Informaţi utilizatorii cu privire la importanţa MFA şi la modul de utilizare a acesteia.

Monitorizaţi regulat jurnalele MFA pentru a detecta activităţi suspecte.

Menţineţi actualizate sistemul MFA şi dispozitivele asociate.

Combinați MFA cu alte tehnici pentru a solicita factori suplimentari în circumstanțe specifice, pe baza unor reguli și modele predefinite, cum ar fi accesul dintr-o locație neobișnuită, de pe un dispozitiv neobișnuit sau la o oră neobișnuită.

Evaluați și alegeți un furnizor MFA care se potrivește cerințelor entității:

- ușurința integrării: asigurați-vă că soluția MFA se integrează bine cu sistemele existente;
- experiența utilizatorului: urmăriți un echilibru între securitate și confortul utilizatorului;
- scalabilitate: alegeți o soluție care poate crește odată cu entitatea;
- asistență și fiabilitate: asigurați-vă că furnizorul oferă asistență robustă și fiabilitate ridicată.

Testați soluția MFA cu un grup restrâns de utilizatori.

Asigurați-vă că implementarea MFA respectă cerințele legale (de exemplu, GDPR).

EXEMPLE DE EVIDENȚE

- Jurnale de acces MFA care arată utilizarea în rețea și în sistemele informatice.
- Configurații ale soluției de autentificare care demonstrează implementarea MFA.
- Politica de control al accesului care definește metodele MFA, inclusiv orice opțiuni rezistente la phishing.
- Documentație privind clasificarea activelor care arată ce sisteme necesită MFA.
- Rezultatele evaluării riscurilor care justifică cerințele MFA.
- Lista rolurilor utilizatorilor cu drepturi de acces și analiza care determină metodele MFA adecvate.
- Fișiere de configurare și jurnale care confirmă că MFA este activată pe anumite sisteme.
- Setări ale sistemului de autentificare care reflectă cerințele MFA definite.
- Jurnale de aplicare care arată cerințele MFA aplicate.
- Documentație/capturi de ecran care arată integrarea MFA cu SSO.
- Înregistrări de instruire (prezență, materiale) privind utilizarea și importanța MFA.
- Rapoarte periodice ale sistemului MFA care arată monitorizarea și detectarea activităților suspecte.
- Evidențe de configurare a factorilor de autentificare suplimentari aplicați prin reguli predefinite.

Ref: Cerințe aprobate prin HG 562/2025 pct. 134, pct. 135

3. Protecție

3.1 Revizuirea independentă a securității informațiilor și a rețelei

ÎNDRUMĂRI

Asigurați-vă că revizuirea independentă este efectuată de o persoană sau persoane cu competențele adecvate (listă orientativă, neexhaustivă):

- cunoștințe tehnice în domeniul securității cibernetice, de exemplu standardele de securitate cibernetică (ISO/IEC 27001, cadrul de securitate cibernetică al Institutului Național de Standarde și Tehnologie (NIST) etc.),
- cunoștințe despre industrie
- competențe în evaluarea riscurilor,
- cunoștințe în materie de conformitate și reglementare, de exemplu Legea nr. 48/2023 privind securitatea cibernetică, Directiva NIS2, GDPR,
- bună înțelegere a bunelor practici în materie de audit și
- bună înțelegere a situațiilor în care certificarea tehnică și conformitatea sunt necesare și trebuie documentate în raportul de conformitate, pentru a se asigura că standardele globale sunt implementate corect.

Stabilirea unui proces de revizuire independentă a securității informațiilor și a rețelelor, incluzând (listă orientativă și neexhaustivă):

- domeniul de aplicare și scopul revizuirilor independente (de exemplu, conformitate, evaluarea riscurilor, respectarea politicilor);
- metodologia revizuirilor (de exemplu, listă de verificare standardizată, bazată pe standarde, ad hoc, modul în care abordează procesele care vor fi testate în timp real pentru conformitate (de exemplu, serviciul cloud) sau cele care vor fi evaluate periodic);
- rolul comitetului de revizuire;
- frecvența evaluărilor independente;
- cine ar trebui să efectueze revizuirile independente (intern sau extern); și
- modele pentru rapoartele de revizuire independentă.

Menținerea independenței în conformitate cu regulamentul;

Dacă este cazul, luați în considerare măsuri alternative la separarea liniilor ierarhice (listă orientativă și neexhaustivă):

- revizuirea rotației personalului;
- înființarea unui comitet de revizuire cu membri din diferite departamente;
- furnizor extern de servicii de revizuire.

Analizați și evaluați rezultatele revizuirii independente.

Raportați rezultatele către organele de conducere.
Utilizați un format standardizat de raportare către organele de conducere. Luați în considerare următoarele elemente (listă orientativă, neexhaustivă):

- rezumatul executiv, inclusiv domeniul de aplicare și principalele concluzii,
- o metodologie,
- constatări detaliate, inclusiv lacunele identificate și problemele de neconformitate,
- recomandări și

- concluzii.

Rapoartele sunt generate şi prezentate organelor de conducere cel puțin o dată pe an.

Luarea de măsuri corective sau justificarea, acceptarea şi documentarea riscurilor reziduale.

Rezultatele evaluărilor independente ar trebui să se reflecte în mod sistematic în rezultatele evaluării riscurilor şi în planurile de tratare a riscurilor. Mai precis, atunci când un risc este identificat sau reevaluat printr-o evaluare independentă, evaluarea riscului corespunzător ar trebui actualizată în consecinţă. Acest lucru garantează că profilul de risc rămâne precis şi că orice riscuri emergente sau în evoluţie sunt identificate şi abordate în mod adecvat în cadrul general de gestionare a riscurilor.

Revizuirile independente ar trebui să aibă loc cel puțin o dată pe an, ţinând seama de:

- incidente semnificative, dacă există;
- modificările mediului de operare;
- modificările aduse peisajului ameninţărilor şi cerinţelor legale şi de reglementare în materie de securitate cibernetică; şi
- modificările aduse politicii privind securitatea reţelelor şi a sistemelor informatice şi/sau politicilor specifice anumitor teme.

Asiguraţi-vă că procesul de revizuire independentă este aprobat de organele de conducere.

Asiguraţi-vă că rezultatele revizuirii sunt aprobate de organele de conducere.

EXEMPLE DE EVIDENȚE

- Rezultatele documentate ale revizuirii/auditului independent.
- Evidențe ale competenței evaluatorului (experiență, calificări, certificări).
- Proces documentat pentru revizuiri independente de securitate.
- Declarații privind conflictele de interese.
- Contracte cu furnizori externi de revizuire.
- Planuri de revizuire independentă care detaliază domeniul de aplicare și activitățile.
- Înregistrări ale analizelor și evaluărilor, inclusiv documentația privind riscurile reziduale.
- Procesele verbale ale evaluărilor anterioare.
- Înregistrări privind măsurile corective, inclusiv documentația și aprobările bugetare.
- Ultimele rezultate ale monitorizării conformității și ale auditului.
- Înregistrări actualizate în registrul de riscuri care reflectă rezultatele revizuirilor.
- Rapoarte de revizuire independente cu constatări, recomandări și măsuri luate.
- Rezumatele revizuirilor anterioare, inclusiv domeniul de aplicare și frecvența.
- Înregistrări ale incidentelor semnificative și documentația de revizuire aferentă.
- Planuri sau programe anuale de revizuire.
- Proceduri documentate aprobate de conducere.
- Aprobarea de către conducere a riscurilor reziduale.

Ref: Cerințe aprobate prin HG 562/2025 pct. 12, pct. 13, pct. 14, pct. 15

3.2 Registrul furnizorilor și prestatorilor de servicii

ÎNDRUMĂRI

Menţineţi registrul actualizat pentru a vă asigura că toate informaţiile sunt actuale şi exacte, adică adăugaţi, actualizaţi şi eliminaţi furnizorii şi prestatorii de servicii din registru în cazul unor modificări.

Efectuaţi revizuiri ale registrului, cel puţin o dată pe an sau atunci când apar modificări semnificative, pentru a vă asigura că toate informaţiile sunt actuale şi exacte.

În plus faţă de elementele menţionate în regulament, luaţi în considerare datele de începere şi de încheiere a contractului şi regiunea fiecărui furnizor direct şi prestator de servicii.

Clasificaţi furnizorii direcţi şi prestatorii de servicii. Clasificarea poate include una sau mai multe caracteristici (listă orientativă, neexhaustivă):

- sensibilitatea activelor achiziţionate,
- volumul activelor achiziţionate,
- cerinţele de disponibilitate,
- reglementările aplicabile,
- riscul inerent şi riscul atenuat.

Actualizaţi şi revizuiţi clasificările anual sau atunci când apar modificări semnificative. Exemple de categorii pot fi:

- critice – cele cu un impact semnificativ asupra operaţiunilor entităţii;
- strategice – parteneri de mare valoare care contribuie la activele informaţionale, de exemplu furnizori de servicii cloud, furnizori de servicii de analiză a datelor, dezvoltatori de software şi furnizori de servicii de telecomunicaţii;
- de rutină – cele cu impact minim asupra entităţii.

EXEMPLE DE EVIDENȚE

- Registrul furnizorilor direcți și al furnizorilor de servicii.
- Evidențe ale actualizării registrului în urma modificărilor furnizorilor sau prestatorilor de servicii.
- Planuri sau programe de revizuire pentru menținerea registrului.
- Lista contractelor sau a acordurilor privind nivelul serviciilor (SLA) aliniate la politica de securitate a lanțului de aprovizionare.
- Evidențe privind clasificarea furnizorilor pe baza criteriilor definite.
- Descriere clară a grupării și gestionării furnizorilor în funcție de importanță și nivel de risc.
- Evidențe privind evaluarea riscurilor care arată măsuri adaptate pentru fiecare categorie de furnizori, cu controale îmbunătățite pentru furnizorii critici.

Ref: Cerințe aprobate prin HG 562/2025 pct. 53, 54.1-54.4, pct. 55.1-55.8, pct. 56, pct. 57, pct. 58.1-58.4, pct. 59.1-59.2

3.3 Securitatea în achiziționarea de servicii sau produse TIC

ÎNDRUMĂRI

Integrați securitatea cibernetică ca o componentă permanentă a procesului de achiziție, dedicând o secțiune specifică abordării acesteia. Aceasta include orice proces de achiziție pentru selectarea furnizorilor de servicii.

Documentați procesul de achiziție sigură a serviciilor, sistemelor sau produselor TIC și descrieți procedurile relevante care susțin procesul.

Luați în considerare standardele recunoscute în industrie atunci când elaborați procesul

Cerințele de securitate trebuie să includă cel puțin mijloacele de detectare, monitorizare și protecție împotriva modificărilor neautorizate ale software-ului și informațiilor.

Asigurați-vă că contractele de asistență acoperă ciclul de viață al sistemului și cerințele de gestionare a uzurii morale, inclusiv data până la care sistemul trebuie să fie asistat și includeți alerte continue.

Preferați furnizorii care oferă informații clare privind sfârșitul ciclului de viață și care intenționează să furnizeze remedieri separate pentru problemele critice de securitate.

Asigurați-vă că ofertele solicită furnizorilor sau prestatorilor de servicii să ofere soluții testate pentru problemele de securitate în tehnologiile vechi sau noi, în mod gratuit și imediat ce se constată o problemă de securitate relevantă.

Luați în considerare și următoarele informații care descriu funcțiile de securitate cibernetică implementate, cum ar fi (listă orientativă, neexhaustivă):

- riscurile potențiale care ar putea apărea în urma achiziționării serviciului, sistemului sau produsului TIC specific. Acest lucru ar putea implica testarea penetrării pentru a identifica amenințările, vulnerabilitățile și impactul potențial asupra operațiunilor entității;
- instrumentele de securitate potențiale care trebuie deja să fie implementate, de exemplu un firewall, un sistem de detectare a intruziunilor, un SIEM sau un EDR/XDR;
- un mecanism specific de securitate care ar putea fi necesar, cum ar fi un algoritm specific de criptare sau un mecanism particular de control al accesului (de exemplu, MFA);
- standardele de securitate cibernetică pentru serviciul, sistemul sau produsul TIC pe care entitatea trebuie să le respecte;
- după caz, nivelul de asigurare necesar al produsului, sistemului sau serviciului TIC și existența unui certificat relevant în conformitate cu Schema europeană de securitate cibernetică pentru produsele TIC bazată pe criterii comune (EUCC).

Luați în considerare evaluarea securității unui serviciu, sistem sau produs TIC înainte de achiziție

Revizuiți cel puțin o dată pe an procesele pentru achiziționarea în condiții de siguranță a serviciilor, sistemelor sau produselor TIC, precum și procedurile bazate pe acestea.

Revizuiți jurnalele sau înregistrările tuturor modificărilor aduse proceselor de achiziție sigură a serviciilor, sistemelor sau produselor TIC și procedurilor bazate pe acestea, inclusiv detaliile modificărilor, aprobările și datele de punere în aplicare.

Aliniați ofertele și contractele la politica de securitate a lanțului de aprovizionare a entității

Pentru serviciile, sistemele sau produsele TIC care nu sunt furnizate de un furnizor (de exemplu, proiecte open source), entitățile ar trebui să împărtășească cu acestea rezultatele relevante ale evaluărilor interne.

Aplicarea achiziționării sigure a sistemelor sau proceselor de produse TIC și a procedurilor relevante atât pentru produsele software, cât și pentru cele hardware, indiferent dacă acestea au fost dezvoltate intern sau achiziționate.

Monitorizați continuu furnizorii sau prestatorii de servicii.

În plus, luați în considerare următoarele aspecte atunci când formulați oferte având în vedere securitatea cibernetică (listă orientativă, neexhaustivă):

- asigurați alerte continue, patch-uri și propuneri de atenuare în cazul în care sunt descoperite vulnerabilități în sistem sau produs;
- clarificați răspunderea furnizorului sau a prestatorului de servicii în cazul unor atacuri cibernetice sau incidente relevante pentru serviciul, sistemul sau produsul respectiv; și
- luați în considerare securitatea cibernetică în timpul implementării proiectului și înainte de predare, inclusiv (listă orientativă, neexhaustivă):
    - revizuiri ale proiectului;
    - testele de acceptare;
    - teste de punere în funcțiune;
    - teste de acceptare la fața locului; și
    - documentație.

Asigurați-vă că furnizorii de servicii de decomisionare iau în considerare aspecte precum dezactivarea conturilor de utilizator și de serviciu, întreruperea fluxurilor de date și asigurarea eliminării în condiții de siguranță a datelor entității din sistemele furnizorilor sau ale prestatorilor de servicii.

Software-ul gratuit și open-source este adesea obținut gratuit de la comunități și proiecte care dezvoltă, întreține și distribuie software, spre deosebire de achiziționarea de la furnizori sau prestatori de servicii. Atunci când utilizează un astfel de software fără a-l achiziționa, entitățile relevante nu pot impune obligații de conformitate care să depășească respectarea termenilor licenței software-ului open-source.

EXEMPLE DE EVIDENȚE

- Modele de licitație care includ cerințe de securitate cibernetică pentru servicii, sisteme sau produse TIC.
- Proces de achiziție documentat, aliniat la standardele și bunele practici relevante.
- Licitații anterioare sau în curs de desfășurare care demonstrează considerente de securitate cibernetică.
- Comparații între contract și licitație care confirmă alinierea la politica de securitate a lanțului de aprovizionare.
- Înregistrări ale testelor de securitate efectuate înainte de achiziționarea sistemelor sau produselor TIC.
- Certificate sau rapoarte de testare emise de organisme acreditate de evaluare a conformității.
- Planuri sau programe de revizuire pentru procesele de achiziție sigure și procedurile conexe.
- Procese-verbale de revizuire și înregistrări ale modificărilor care arată actualizările proceselor de achiziție și îmbunătățirile de securitate.
- Rezultatele auditului care confirmă conformitatea cu procesele interne de achiziție securizată și cu reglementările externe.
- Documentație privind gestionarea modificărilor pentru actualizările procedurilor de achiziție, inclusiv aprobările.
- Înregistrări privind răspunsul la incidente care arată modul în care incidentele semnificative influențează actualizările proceselor de achiziție.
- Evidențe că proiectele interne acordă prioritate securității la achiziționarea de servicii, sisteme sau produse TIC.

Ref: Cerințe aprobate prin HG 562/2025 pct. 60, pct. 61.1-61.6, pct. 62

3.4 Gestionarea configurației

ÎNDRUMĂRI

Stabiliți procese documentate bazate pe cele mai bune practici și standarde de securitate a informațiilor

Mențineți și documentați setările de configurare detaliate pentru următoarele proceduri operaționale (listă orientativă, neexhaustivă):

- prelucrarea și gestionarea informațiilor,
- copii de rezervă,
- cerințe de programare, inclusiv interdependențe cu alte sisteme,
- gestionarea erorilor sau a altor condiții excepționale,
- proceduri de repornire și recuperare a sistemului,
- mecanisme și setări criptografice și
- informații privind pista de audit și jurnalul de sistem.

Luați în considerare următorii parametri legați de securitate pentru setările de configurare (listă orientativă, neexhaustivă):

- setări de registru,
- setări de permisiuni pentru conturi, fișiere și directoare și
- setări pentru funcții, porturi, protocoale, servicii și conexiuni la distanță.

Utilizați mecanisme automatizate pentru a gestiona, aplica și verifica în mod centralizat setările de configurare pentru software și hardware, inclusiv dispozitivele mobile și vehiculele conectate ale entității.

Dacă este cazul, implementați o bază de date de gestionare a configurației pentru a cataloga și clasifica toate elementele de configurație (CI), inclusiv atributele lor de securitate (de exemplu, nivelul patch-urilor, regulile firewall-ului și starea criptării).

Asigurați-vă că toate configurațiile de rețea, software și sistem respectă standardele de securitate și operaționale stabilite pentru funcții, porturi, protocoale și servicii.

Monitorizați și controlați modificările aduse setărilor de configurare în conformitate cu politica entității privind securitatea rețelelor și a sistemelor informatice, precum și cu politicile și procedurile specifice.

Identificați software-ul neautorizat să ruleze pe sistemele informatice.

După caz, revizuiți și actualizați periodic configurațiile software.

După caz, identificați programele software autorizate să ruleze pe sistemul informatic.

Aplicaţi o politică de refuzare generală, cu permisiuni acordate prin excepţie, pentru a permite rularea software-ului autorizat.

Stabiliţi proceduri pentru utilizarea serviciilor de reţea pentru a restricţiona accesul numai la serviciile sau aplicaţiile necesare.

Gestionaţi o configuraţie de bază sigură pentru mediile de dezvoltare şi testare separat de configuraţia de bază operaţională, acolo unde este cazul.

Identificaţi, documentaţi şi aprobaţi orice abateri de la setările de configurare stabilite pe baza excepţiilor definite privind cerinţele operaţionale.

Luaţi în considerare ghidurile de consolidare/cele mai bune practici şi principiile generale de securitate cibernetică (de exemplu, funcţionalitate minimă şi privilegii minime) ca bază pentru derivarea configuraţiilor de securitate definite.

Stabiliţi, documentaţi şi menţineţi setările de configurare respectând politica de control al accesului.

Dacă este cazul, testaţi configuraţia înainte de implementare.

Utilizaţi măsuri de securitate pentru a detecta şi a răspunde la modificările neautorizate ale setărilor de configurare definite.

Stabiliţi un plan de gestionare a configuraţiei care să conţină:

- roluri, responsabilităţi, procese şi proceduri de gestionare a configuraţiei;
- un proces de identificare a CI-urilor pe parcursul ciclului de viaţă al dezvoltării sistemului; şi
- un proces pentru gestionarea configuraţiei CI pe tot parcursul ciclului lor de viaţă.

Protejaţi planul de gestionare a configuraţiei împotriva divulgării şi modificării neautorizate.

Implementaţi controale îmbunătăţite, inclusiv scanarea periodică a vulnerabilităţilor, consolidarea strictă a configuraţiei, izolarea acolo unde este posibil şi monitorizarea continuă pentru a compensa produsele care nu beneficiază de actualizări oficiale după încetarea suportului furnizorului.

Revizuiţi şi, dacă este cazul, actualizaţi configuraţiile cel puţin o dată pe lună pentru a vă asigura că patch-urile au fost aplicate, că backup-ul a fost executat conform planului şi că monitorizarea este în vigoare pentru a identifica şi alerta fără întârziere erorile fatale ale serverului/dispozitivului/discului.

Elaboraţi, păstraţi şi revizuiţi periodic jurnalele de modificări referitoare la configuraţia de securitate a sistemelor informatice.

Revizuiți și actualizați configurațiile după modificări majore (de exemplu, actualizări de software) și incidente anterioare.

Acolo unde este posibil, obțineți fișiere de configurare de bază pentru sistemele și dispozitivele cheie, pentru a le compara cu configurațiile actuale.

EXEMPLE DE EVIDENȚE

- Proces documentat de configurare a sistemului, aliniat la standarde și bune practici.
- Tabele de configurare pentru hardware, software, servicii și rețele.
- Configurații de bază sigure (producție, dezvoltare și testare), inclusiv funcții esențiale, caracteristici restricționate, setări de securitate implicite și porturi/protocoale/servicii permise.
- Excepții aprobate de la configurațiile de bază cu controale compensatorii.
- Plan de gestionare a configurației, inclusiv comparații cu listele de control al accesului.
- Mecanisme de securitate, cum ar fi controale de acces logice/fizice, criptare și înregistrarea auditului.
- Plan actualizat de gestionare a configurației, note de revizuire și jurnale de modificări.
- Rezultate documentate ale revizuirii și instantanee ale configurației înainte/după modificări.
- Jurnale de audit care urmăresc modificările de configurare și activitățile de revizuire.
- Alerte de monitorizare pentru modificări neașteptate sau neconforme ale configurației.
- Procesele verbale ale ședințelor care documentează discuțiile și deciziile privind configurația.
- Notificări/memento-uri despre revizuirile de configurare viitoare.
- Înregistrări din instrumentele de gestionare a configurației care confirmă datele de configurare exacte și actualizate.
- Înregistrări privind răspunsul la incidente, care arată modul în care incidentele legate de configurație influențează actualizările.

Ref: Cerințe aprobate prin HG 562/2025 pct. 67, pct. 68.1-68.2, pct. 69

3.5 Gestionarea patch-urilor de securitate

ÎNDRUMĂRI

Luaţi în considerare standardele bine cunoscute atunci când elaboraţi procedurile de gestionare a patch-urilor de securitate

Acţiunile pot varia în funcţie de reţea şi de sistemul informatic (de exemplu, aplicarea obligatorie a patch-urilor pentru toate sistemele expuse sau dispozitivele conectate la internet, cum ar fi firewall-urile sau routerele, şi aplicarea limitată a patch-urilor numai în circumstanţe specifice, de exemplu în sisteme izolate sau vechi, în care aplicarea regulată a patch-urilor poate fi imposibilă sau indisponibilă).

Stabiliţi un proces, în combinaţie cu inventarul activelor, pentru a fi informat atunci când este publicat un nou patch de securitate şi programaţi implementarea patch-urilor în consecinţă.

Aplicarea patch-urilor ar trebui să fie o activitate standard în cadrul întreţinerii normale şi al planificării întreruperilor serviciilor. Cu toate acestea, unele defecţiuni pot necesita aplicarea imediată a patch-urilor, în funcţie de gravitatea lor.

Prioritizaţi şi aplicaţi patch-urile în funcţie de risc. Evaluaţi gravitatea vulnerabilităţii, expunerea sistemului afectat şi probabilitatea de exploatare.

Implementaţi tehnologii de gestionare a vulnerabilităţilor pentru a identifica software-ul neactualizat şi configurat incorect.

Definiţi sursele relevante de informaţii de securitate, luând în considerare activele dvs., şi monitorizaţi-le continuu pentru anunţuri de patch-uri, remedierea cu sau fără patch-uri şi ameninţări generale.

Verificaţi sursele de patch-uri prin (listă orientativă, neexhaustivă):

- certificate digitale pentru verificarea furnizorului;
- semnături digitale ale patch-urilor
- jurnalele de modificări furnizate de furnizor; şi
- feedback-ul din partea comunităţii cu privire la fiabilitatea furnizorului.

Luaţi în considerare o strategie pentru aplicarea patch-urilor după aprobare sau testare, urmând procedura de gestionare a modificărilor (listă orientativă, neexhaustivă):

- Blue/green permite aplicarea patch-urilor mai întâi într-un mediu izolat identic cu mediul de producţie, iar apoi în mediul de producţie. Acest lucru asigură zero timp de nefuncţionare şi o opţiune de revenire imediată.
- Implementarea progresivă permite actualizarea treptată a unor părţi ale mediului de producţie, câte un set de servere sau instanţe pe rând, în loc să se implementeze un patch dintr-o singură dată. Este ideală pentru medii mari şi distribuite.
- Comutatoarele de funcţii permit implementarea de noi funcţii sau patch-uri în producţie, dar le menţin dezactivate până când sunt gata de utilizare. Acestea sunt potrivite pentru controlul noilor funcţii sau patch-uri atunci când sunt activate, facilitând testarea şi lansarea.
- Implementarea în umbră permite implementarea directă a codului sau a patch-urilor noi în producţie, dar urmăreşte traficul live prin oglindirea cererilor utilizatorilor atât în sistemul

actual, cât şi în cel nou, pentru a observa cum se comportă noua versiune fără a afecta experienţa utilizatorului. Este ideală pentru testarea noilor funcţii în producţie fără a afecta utilizatorii.
- Implementările de remedieri rapide sunt utilizate pentru patch-uri critice care trebuie aplicate imediat pentru a rezolva probleme grave.

Acolo unde este cazul şi pentru a reduce riscurile legate de actualizări semnificative în dependenţe importante, luaţi în considerare efectuarea unui test utilizând *versiuni candidate* ale acestor componente, pentru a obţine o indicaţie timpurie a incompatibilităţilor sau a modificărilor majore, astfel încât acestea să poată fi remediate. Dacă oricare dintre aceste componente este un software open source, oferiţi feedback cu privire la orice probleme constatate în timpul acestui test.

Depuneţi eforturi proporţionale cu dimensiunea şi importanţa entităţii pentru a vă asigura că patch-urile de securitate nu introduc vulnerabilităţi sau instabilităţi suplimentare. Exemple de informaţii care susţin o astfel de decizie pot include (listă orientativă, neexhaustivă):

- documentaţia furnizorului privind patch-ul:
  - ce vulnerabilităţi sau erori specifice sunt abordate,
  - dacă patch-ul remediază o problemă de securitate, îmbunătăţeşte performanţa, adaugă funcţii sau rezolvă probleme de stabilitate,
  - cerinţele de sistem sau orice configuraţii specifice necesare sau modificări ale setărilor sistemului,
  - instrucţiuni de instalare privind modul de aplicare a patch-ului şi dacă acesta necesită o repornire sau o configurare suplimentară;
- gradul de gravitate - patch-urile care remediază vulnerabilităţi critice sunt mai susceptibile de a fi aplicate; şi
- bloguri, forumuri şi liste de discuţii dedicate securităţii, pentru a identifica eventualele probleme cunoscute sau incompatibilităţi introduse de patch.

Dacă aplicarea patch-ului nu este fezabilă, luaţi în considerare măsuri alternative, cum ar fi întărirea strictă a configuraţiei, sisteme de detectare a intruziunilor, scanarea regulată a vulnerabilităţilor, segmentarea sau izolarea reţelei, acolo unde este posibil, controlul accesului şi monitorizarea.

Procedurile de gestionare a patch-urilor trebuie să indice domeniul de aplicare, rolurile şi responsabilităţile.

Efectuaţi actualizări ale sistemului de operare şi ale aplicaţiilor pe activele întreprinderii prin gestionarea automată a patch-urilor.

Utilizaţi instrumente adecvate de gestionare a patch-urilor pentru a îndeplini cerinţele prevăzute de regulament.

Deoarece patch-urile pot cauza uneori probleme, se recomandă să faceţi o copie de rezervă a sistemului înainte de a le aplica.

Aveţi un plan de revenire la starea anterioară pentru a vă asigura că sistemul revine la o stare anterioară sigură dacă aplicarea patch-urilor nu funcţionează sau dacă remedierea problemei nu este posibilă.

Eliminaţi hardware-ul şi software-ul neacceptate din reţea într-un timp rezonabil şi acceptat, în conformitate cu evaluarea riscurilor entităţii.

Includeți cerințele privind patch-urile și actualizările în politica privind lanțul de aprovizionare și în contracte, în criteriile de evaluare și selecție a ofertelor pentru noi servicii, sisteme sau produse TIC, luând în considerare, printre alte aspecte, durata de viață a sistemului.

EXEMPLE DE EVIDENȚE

- Proceduri documentate de gestionare a patch-urilor care acoperă identificarea, evaluarea, testarea, implementarea și verificarea.
- Jurnale de implementare a patch-urilor cu marcaje temporale, personalul responsabil și sistemele afectate.
- Inventarul actualizat al activelor, care reflectă patch-urile recent anunțate și calendarul planificat.
- Evidențe ale testării înainte de implementare (planuri de testare, rezultate, probleme rezolvate).
- Documentație privind cererile de modificare, inclusiv aprobări și evaluări de impact.
- Piste de audit care urmăresc activitățile legate de patch-uri, de la identificare până la implementare.
- Verificări pentru cele mai recente patch-uri și acțiuni aprobate pentru aplicarea acestora.
- Înregistrări revizuite și aprobate ale modificărilor pentru activitățile de aplicare a patch-urilor.
- Evidențe de verificare a furnizorului (certificate digitale, semnături).
- Rapoarte de audit interne/externe care evaluează eficacitatea gestionării patch-urilor.
- Evidențe privind prioritizarea patch-urilor, în special pentru patch-urile critice.
- Documentație privind riscurile reziduale pentru patch-urile amânate sau neaplicate.
- Rapoarte de incidente legate de vulnerabilități necorectate.
- Jurnale de modificări ale sistemului, inclusiv patch-uri aplicate, reveniri la versiuni anterioare și probleme întâmpinate.
- Decizii documentate de a nu aplica patch-uri, cu controale compensatorii.
- Plan actualizat de tratare a riscurilor.
- Documentația ședințelor de revizuire a proceselor de gestionare a patch-urilor (ordine de zi, prezență, procese verbale, acțiuni).
- Evidențe ale atribuirii rolurilor și responsabilităților în gestionarea patch-urilor.
- Instrumente de gestionare a patch-urilor cu jurnale de configurare și utilizare.
- Plan de revenire la starea anterioară.
- Documentație privind achizițiile (contracte, oferte, criterii de evaluare) care prezintă cerințele de gestionare a patch-urilor și considerente privind ciclul de viață.

Ref: Cerințe aprobate prin HG 562/2025 pct. 77.1-77.4, pct. 78

3.6 Securitatea rețelei

ÎNDRUMĂRI

Luați în considerare standardele cunoscute atunci când implementați măsuri pentru securitatea rețelei.

Implementați principiile de securitate prin proiectare, integrând securitatea la fiecare nivel al proiectării rețelei, inclusiv la nivel fizic, de legătură de date, de rețea, de transport și de aplicații.

Implementați configurații sigure pentru rețelele fără fir.

Dacă este cazul, luați în considerare conceptul zero-trust de acces la rețea.

Identificați măsurile tehnice pentru tranziția la cele mai recente protocoale de comunicare la nivel de rețea (de exemplu, tranziția la Protocolul Internet versiunea 6).

Definiți rolurile, responsabilitățile și calendarul pentru tranziția la protocoalele de comunicare de ultimă generație la nivel de rețea.

Aprobarea, înregistrarea și efectuarea întreținerii la distanță a rețelelor și a sistemelor informatice într-un mod care să împiedice accesul neautorizat.

Luați în considerare următoarele aspecte pentru comunicările prin e-mail (listă orientativă, neexhaustivă):

- standarde precum Start transport layer security (STARTTLS), autentificarea bazată pe DNS a entităților numite (DANE), autentificarea, raportarea și conformitatea mesajelor bazate pe domeniu (DMARC), DomainKeys identified mail (DKIM) și cadrul de politici al expeditorului
- filtrarea internă a spamului/înșelătoriilor/virușilor și
- rescrierea URL-urilor, scanarea URL-urilor și detonarea URL-urilor într-un sandbox.

Luați în considerare bunele practici de securitate DNS (listă orientativă, neexhaustivă):

- implementarea extensiilor de securitate DNS (DNS SEC)

Deși frecvența revizuirilor măsurilor de securitate a rețelei depinde de evaluarea riscurilor entității, ca regulă generală, entitatea ar putea (listă orientativă, neexhaustivă):

- sa efectueze monitorizarea continuă a rețelelor pentru amenințări în timp real;
- să efectueze săptămânal scanări pentru a detecta noi vulnerabilități;
- sa efectueze revizuirea și, eventual, actualizarea lunară a regulilor firewall-ului și a altor instrumente; și
- sa evalueze anual întreaga rețea.

Revizuiți jurnalele sau înregistrările tuturor modificărilor aduse regulilor de securitate a rețelei, inclusiv detaliile modificărilor, aprobările și datele de implementare.

Asigurați-vă că aceste revizuiri sunt efectuate în mod regulat și documentate în mod cuprinzător.

Comunicați personalului modul corect de utilizare a dispozitivelor mobile, inclusiv a vehiculelor conectate ale entității și a altor accese la distanță.

Dacă este cazul, aplicați soluții capabile să colecteze, să analizeze și să detecteze toate anomaliile, exfiltrările, intruziunile și cele mai sofisticate amenințări.

EXEMPLE DE EVIDENȚE

- Măsuri documentate de securitate a rețelei, aliniate la standarde și bune practici.
- Diagrame actuale ale rețelei, inclusiv conexiuni out-of-band (OOB).
- Configurații și seturi de reguli pentru firewall care demonstrează aplicarea politicilor de control al traficului.
- Fișiere de configurare a routerelor și comutatoarelor, inclusiv setări VLAN și ACL.
- Configurații sigure ale rețelei wireless (de exemplu, WPA3, 802.1X/EAP, actualizări de firmware).
- ACL-uri documentate care reglementează fluxul de trafic între dispozitivele de rețea.
- Politici pentru utilizarea sigură a dispozitivelor mobile și a accesului la distanță, inclusiv vehicule conectate și telemuncă.
- Controale ale conturilor privilegiate, cu jurnale și politici de sprijin.
- Lista dispozitivelor de rețea care nu pot fi actualizate sau care nu sunt acceptate.
- Jurnale de acces care arată personalul autorizat care efectuează modificări și revizuiri ale regulilor de rețea.
- Planuri pentru trecerea la protocoale moderne la nivel de rețea.
- Programele de revizuire și rapoartele din revizuirile anterioare ale securității rețelei.
- Jurnale ale firewall-ului/routerului/dispozitivelor de rețea care indică încercările de acces și modificările de configurare.
- Rapoarte SIEM și EDR/XDR care agregă și analizează evenimentele de securitate.
- Jurnale VPN și de acces la distanță, inclusiv conexiuni OOB și anomalii.
- Evidențe ale existenței soluțiilor NAC sau echivalente, cu jurnale și setări de configurare.
- Înregistrări ale revizuirilor periodice ale regulilor de rețea, inclusiv date și rezultate.
- Comunicări către personal privind utilizarea corectă a dispozitivelor mobile și a accesului la distanță.
- Existența și configurarea soluțiilor IDS/IPS.

Ref: Cerințe aprobate prin HG 562/2025 pct. 79, pct. 80.1-80.12, pct. 81

3.7 Segmentarea rețelei

ÎNDRUMĂRI

Luați în considerare standardele bine cunoscute atunci când segmentați rețelele.

Integrați segmentarea derivată din evaluarea riscurilor în diagrama rețelei.

Asigurați-vă că segmentele sunt în conformitate cu rezultatele evaluării riscurilor.

Aplicați un set gradat de măsuri în diferite domenii logice ale rețelei pentru a segrega și mai mult mediile de securitate ale rețelei, inclusiv:

- sisteme accesibile publicului;
- rețele interne;
- active cu grad ridicat de criticitate.

Implementați subrețele pentru componentele sistemului accesibile publicului care sunt separate fizic și/sau logic de rețelele interne ale organizației.

Determinați gradul de separare fizică a componentelor sistemului de componentele distincte fizic:

- în rafturi separate în aceeași încăpere,
- în camere separate pentru componentele cu grad ridicat de criticitate și separare geografică mai semnificativă a componentelor cu grad ridicat de criticitate.

Implementați adrese de rețea separate (adică subrețele diferite) pentru a vă conecta la sisteme din domenii de securitate diferite.

Monitorizați și controlați comunicațiile la limita externă a sistemului, precum și la limitele interne cheie din cadrul sistemului, inclusiv încălcările segmentării.

Dacă este cazul, izolați instrumentele, mecanismele și componentele de suport pentru securitatea informațiilor de alte componente interne ale sistemului informațional, dacă este cazul, prin implementarea de subrețele separate fizic, cu interfețe gestionate către alte componente ale sistemului.

Rutați toate accesele privilegiate în rețea printr-o interfață dedicată și gestionată în scopul controlului accesului și al auditului.

Implementaţi o interfaţă gestionată pentru fiecare serviciu de telecomunicaţii extern.

Revizuiţi şi, dacă este necesar, actualizaţi procesul pentru regulile de segmentare a reţelei cel puţin o dată pe an.

EXEMPLE DE EVIDENȚE

- Reguli documentate de segmentare a rețelei, aliniate la standarde și bune practici.
- Rezultatele evaluării riscurilor care susțin deciziile de segmentare.
- Note din interviurile cu personalul care explică motivele segmentării.
- Diagrame actualizate ale rețelei care arată zonele (DMZ, internă, pentru oaspeți etc.) și conexiunile OOB.
- Verificarea faptului că diagramele corespund funcțiilor de afaceri și profilurilor de risc.
- Criterii documentate pentru crearea și menținerea zonelor de rețea.
- Configurații VLAN pe comutatoare/routere aliniate cu zonele de securitate și funcțiile de afaceri.
- Măsuri de securitate specifice zonei (IDS/IPS, monitorizare etc.).
- Configurații ale dispozitivelor (routere, switch-uri, firewall-uri) care impun segmentarea.
- ACL-uri care reflectă cerințele de separare a sarcinilor.
- Configurații firewall care acceptă regulile de segmentare.
- Rapoarte de testare a penetrării și scanare a vulnerabilităților care evaluează eficacitatea segmentării.
- Programele de revizuire a regulilor de segmentare.
- Jurnale/înregistrări care confirmă efectuarea revizuirilor periodice.
- Documentație privind gestionarea modificărilor pentru actualizările de segmentare legate de riscuri și nevoi ale organizației.
- Documentație privind răspunsul la incidente, care arată revizuirea segmentării după incidente majore.
- Analiza post-incident care evaluează eficacitatea segmentării și ajustările.
- Rapoarte de audit intern/extern care acoperă controalele de segmentare.
- Evidențe ale revizuirilor periodice și determinate de evenimente ale segmentării.
- Procesele verbale ale ședințelor IT/securitate privind segmentarea.
- Rezultatele testelor de penetrare și ale evaluării vulnerabilităților care evaluează în mod specific controalele de segmentare.
- Evidențe ale testelor efectuate după schimbări majore sau incidente.

Ref: Cerințe aprobate prin HG 562/2025 pct. 82, pct. 83.1-83.8, pct. 84

3.8 Protecție împotriva software-ului rău intenționat și neautorizat

ÎNDRUMĂRI

Utilizaţi mecanisme de detectare şi protecţie împotriva software-ului rău intenţionat şi neautorizat la punctele de intrare şi ieşire ale sistemului şi la staţiile de lucru, serverele şi dispozitivele mobile din reţea pentru a detecta şi elimina codurile rău intenţionate transportate prin poştă electronică, ataşamente de poştă electronică , accese web sau medii amovibile sau inserate prin exploatarea vulnerabilităţilor sistemului.

Configuraţi mecanismele de protecţie împotriva codurilor rău intenţionate astfel încât:

- să fie active în permanenţă;
- să efectueze scanări periodice ale sistemului în mod regulat şi scanări în timp real ale fişierelor din surse externe pe măsură ce fişierele sunt descărcate, deschise sau executate;
- să genereze notificări atunci când este detectat un software suspectat a fi rău intenţionat şi neautorizat;
- să dezinfecteze şi să pună în carantină fişierele infectate;
- să restaureze setările sistemului şi asiguraţi-vă că setările critice nu pot fi dezactivate sau restricţionate.

Aplicaţi lista albă a aplicaţiilor şi monitorizaţi activităţile neautorizate şi comportamentul sistemului, acolo unde este cazul.

Asiguraţi-vă că mecanismele de protecţie împotriva programelor rău intenţionate şi neautorizate sunt gestionate centralizat, acolo unde este cazul.

Asiguraţi-vă că există mecanisme care împiedică utilizatorii să eludeze capacităţile de protecţie împotriva software-ului rău intenţionat şi neautorizat.

Asiguraţi-vă că mecanismele de protecţie împotriva spamului sunt utilizate la punctele de intrare în sistem, cum ar fi staţiile de lucru, serverele sau dispozitivele mobile de calcul din reţea.

Actualizaţi mecanismele de protecţie împotriva codurilor rău intenţionate (inclusiv definiţiile semnăturilor) ori de câte ori sunt disponibile noi versiuni, în conformitate cu regulile de configurare şi procedurile de gestionare a patch-urilor ale entităţii.

Abordaţi problemele legate de falsele pozitive în timpul detectării şi eradicării codurilor rău intenţionate şi impactul potenţial asupra disponibilităţii sistemului.

Aliniați regulile de monitorizare și înregistrare a software-ului de detectare și reparare rău intenționat și neautorizat cu instrumentele și procedurile de monitorizare și înregistrare ale entității și cu politica de control al accesului și de gestionare a activelor ale entității.

EXEMPLE DE EVIDENȚE

- Sisteme de protecție a terminalelor (EPP, EDR) implementate în rețea.
- Sisteme actualizate de detectare a programelor malware.
- Instrumente de monitorizare a software-ului neautorizat, întreținute complet.
- Configurații firewall, IDS/IPS și gateway web securizat care impun controale asupra malware-ului și software-ului neautorizat.
- Soluții de listare albă a aplicațiilor, cu reguli și configurații actuale.
- Documentație privind instrumentele de securitate gestionate centralizat.
- Înregistrări de actualizare care arată aplicarea regulată a patch-urilor pentru mecanismele de detectare și protecție.
- Înregistrări ale scanărilor periodice.
- Monitorizarea și înregistrarea sistemelor pentru a detecta executarea de coduri rău intenționate sau neautorizate.
- Jurnale de detectare a amenințărilor (amenințări blocate sau detectate).
- Jurnale cuprinzătoare care acoperă activitatea utilizatorilor, excepțiile și incidentele de securitate.
- Mecanisme documentate de protecție împotriva spamului.
- Evaluarea riscurilor care definește nivelurile necesare de monitorizare a jurnalelor.

Ref: Cerințe aprobate prin HG 562/2025 pct. 85, pct. 86

3.9 Criptografie

ÎNDRUMĂRI

Asigurați-vă că politica și procedurile cuprinzătoare legate de criptografie sunt în conformitate cu reglementările relevante și standardele de ultimă generație

Asigurați-vă că politica și procedurile acoperă mecanismele criptografice, cum ar fi semnăturile digitale și hash-urile, pentru a:

- proteja confidențialitatea și integritatea datelor în tranzit și în repaus;
- a detecta modificările neautorizate ale datelor stocate marcate ca fiind critice
- asigura eliminarea în condiții de siguranță a datelor după utilizarea lor legală.

Configurați un mecanism (manual sau automat) pentru selectarea, stabilirea și gestionarea (inclusiv actualizarea) cheilor criptografice.

Aplicați criptarea în transferul de informații sensibile (de exemplu, generarea și gestionarea cheilor).

Luați în considerare criptarea suporturilor electronice care conțin informații confidențiale/sensibile.

Asigurați confidențialitatea și integritatea datelor cu mecanisme criptografice, de exemplu (listă orientativă, neexhaustivă):

- partajarea informațiilor;
- scanarea traficului de rețea;
- utilizarea stocării sigure online (de exemplu, criptarea cloud pe partea clientului) și offline;
- eliminarea datelor sensibile de pe suporturile de stocare.

Mențineți disponibilitatea informațiilor în cazul pierderii cheilor criptografice, de exemplu prin depozitarea cheilor de criptare.

Produceți, controlați și distribuiți chei criptografice simetrice și asimetrice utilizând tehnologia și procesele de gestionare a cheilor.

Luați în considerare mecanisme automate de gestionare a cheilor criptografice pentru a:

- genera chei pentru diferite sisteme criptografice și diferite aplicații;
- genera și a obține certificate de chei publice;
- distribui cheile utilizatorilor vizați
- gestiona cheile compromise.

Păstrați jurnale ale activităților de gestionare a cheilor criptografice pentru a asigura responsabilitatea, trasabilitatea și sprijinul pentru activitățile de răspuns la incidente și de audit. Cel puțin, înregistrarea ar trebui să includă generarea sau reînnoirea cheilor, transmiterea cheilor și distrugerea sau revocarea cheilor.

Dacă este cazul, ar trebui înregistrate şi activităţile de recuperare, arhivare şi stocare a cheilor, în special în medii în care este necesară manipularea manuală sau protecţia cheilor cu grad ridicat de siguranţă.

Asiguraţi protecţia cheilor criptografice împotriva modificării şi pierderii.

Asiguraţi protecţia cheilor secrete şi private împotriva utilizării şi divulgării neautorizate.

Asiguraţi autenticitatea cheilor publice.

Protejaţi fizic echipamentele utilizate pentru generarea, stocarea şi arhivarea cheilor.

Limitaţi utilizarea proceselor criptografice ad hoc.

Luaţi în considerare, acolo unde este cazul, o abordare bazată pe agilitate criptografică. Caracteristicile principale ale acestei abordări sunt:

- flexibilitatea în selectarea algoritmilor;
- design modular al arhitecturii, prin care componentele criptografice pot fi modificate sau actualizate independent, fără a afecta întregul sistem;
- actualizări şi patch-uri regulate;
- respectarea cadrelor legislative şi a guvernanţei utilizării criptografiei în cadrul reţelelor şi sistemelor informatice ale entităţii;
- asigurarea compatibilităţii cu tehnologiile viitoare prin luarea în considerare a algoritmilor criptografici cuantici.

Luaţi în considerare evaluarea metodelor de criptare alese pentru a verifica dacă acestea respectă standardele industriale pentru metode sigure.

Asiguraţi-vă că politica de criptografie este în conformitate cu standardele relevante din industrie şi cu progresele înregistrate în acest domeniu.

Revizuiţi politica şi procedurile de criptografie cel puţin o dată pe an.

Menţineţi o procedură care să specifice modul în care se efectuează revizuirea politicii şi a procedurilor de criptografie, inclusiv personalul responsabil şi intervalele de revizuire.

Asigurați-vă că modificările aduse măsurilor criptografice sunt testate înainte de a fi aplicate.

Asigurați-vă că modificările aduse măsurilor criptografice sunt comunicate angajaților.

EXEMPLE DE EVIDENȚE

- Politica și procedurile de criptografie, aliniate la reglementări și standarde de ultimă generație.
- Linii directoare documentate privind criptarea, inclusiv algoritmi aprobați, lungimi ale cheilor și protocoale.
- Măsuri de protecție pentru cheile private/secrete.
- Evidențe ale mecanismelor criptografice care asigură confidențialitatea și integritatea datelor stocate și în tranzit.
- Mecanisme de gestionare a cheilor (manuale sau automate), inclusiv stabilirea, rotația și stocarea acestora.
- Evidențe ale implementării criptării în toate sistemele (baze de date, fișiere, comunicații).
- Mecanisme de control al accesului pentru cheile criptografice și datele criptate.
- Jurnale care arată accesul restricționat și monitorizarea acțiunilor legate de chei.
- Evaluări ale măsurilor criptografice pentru protecția confidențialității datelor.
- Evidențe ale generării sigure a cheilor.
- Rapoarte de audit intern/extern care evaluează controalele criptografice.
- Documentație care arată adoptarea celor mai bune practici criptografice, inclusiv modul în care sunt identificate și aplicate actualizările.
- Jurnale de modificări pentru politicile și procedurile criptografice.
- Planuri de testare și rezultate care demonstrează eficacitatea măsurilor criptografice actualizate.
- Notificări/memento-uri privind revizuirile viitoare ale politicilor de criptografie.
- Înregistrări de comunicare care informează personalul despre actualizările politicilor.
- Evidențe privind menținerea la curent cu evoluțiile în domeniul criptografiei.

Ref: Cerințe aprobate prin HG 562/2025 pct. 102, 103.1-103.12, 104

3.10 Securitatea resurselor umane

ÎNDRUMĂRI

Definiţi roluri şi responsabilităţi clare în materie de securitate pentru angajaţi, în conformitate cu politicile de securitate ale entităţii şi cu rolul funcţional al fiecărui angajat. Definiţi responsabilităţile relevante în materie de securitate pentru furnizorii direcţi şi prestatorii de servicii, în cadrul obligaţiilor contractuale, asigurându-vă că acestea sunt adecvate naturii serviciilor furnizate şi în conformitate cu cerinţele generale de securitate ale entităţii.

Stabiliţi programe de integrare şi formare continuă care să includă atât sensibilizarea la securitate, cât şi formarea în domeniul securităţii cibernetice specifică rolului, adaptată la diferite expuneri la riscuri.

Implementaţi evaluări periodice pentru a evalua înţelegerea responsabilităţilor de securitate, susţinute de formare obligatorie de perfecţionare, după cum este necesar.

Asiguraţi-vă că responsabilităţile de securitate sunt documentate în mod oficial şi integrate în fişele de post, acordurile contractuale şi procesele de evaluare a performanţei. Încorporaţi responsabilităţile relevante de securitate în acordurile contractuale sau în acordurile privind nivelul serviciilor (SLA) pentru furnizorii direcţi şi prestatorii de servicii, cu un limbaj clar în ceea ce priveşte aşteptările şi cerinţele de conformitate.

Promovaţi o cultură a responsabilităţii prin solicitarea recunoaşterii oficiale a obligaţiilor de securitate şi prin corelarea conformităţii cu stimulente şi măsuri disciplinare, acolo unde este cazul.

Dezvoltaţi şi menţineţi un registru centralizat al înregistrărilor de formare, confirmărilor, certificărilor şi clauzelor contractuale pentru a demonstra conformitatea şi a facilita auditurile.

Solicitaţi furnizorilor şi prestatorilor de servicii să desemneze persoane de contact responsabile pentru securitatea cibernetică şi încurajaţi sau impuneţi participarea la briefinguri de securitate relevante sau la programe de formare oferite de entitate.

Implementaţi periodic acţiuni de sensibilizare cu privire la practicile de igienă cibernetică pentru utilizatori, adaptate diferitelor roluri şi responsabilităţi. Ori de câte ori este cazul, solicitaţi angajaţilor furnizorilor direcţi şi furnizorilor de servicii să urmeze acţiuni similare de sensibilizare cu privire la igiena cibernetică prin clauze contractuale.

Comunicaţi tuturor angajaţilor, furnizorilor şi prestatorilor de servicii practici clare şi concise de igienă cibernetică pentru utilizatori. Solicitaţi confirmarea primirii şi înţelegerii.

Luaţi în considerare organizarea de cursuri de formare specializate pentru utilizatorii cu acces administrativ sau privilegiat, concentrându-vă pe responsabilităţile specifice ale acestora.

Stabiliţi indicatori de performanţă legaţi de responsabilităţile de securitate şi includeţi-i în evaluările de management.

Organizaţi şedinţe informative periodice pentru membrii organelor de conducere cu privire la importanţa securităţii reţelelor şi a sistemelor informatice, responsabilităţile lor specifice şi impactul potenţial al incidentelor.

Efectuaţi verificări amănunţite ale Referinţe lor, acolo unde este cazul, pentru a verifica experienţa anterioară şi performanţele candidatului în roluri similare.

Luaţi în considerare proceduri de verificare, inclusiv verificări ale antecedentelor, pentru a vă asigura potrivirea candidatului pentru rolul respectiv.

Validaţi orice certificări relevante revendicate de candidat, pentru a vă asigura că acestea sunt actuale şi legitime.

Utilizaţi teste scrise sau evaluări practice pentru a evalua cunoştinţele şi abilităţile candidatului în ceea ce priveşte securitatea reţelelor şi a sistemelor informatice.

Utilizaţi comisii de interviu, acolo unde este cazul, care să includă şi experţi în securitate, pentru a evalua competenţele tehnice şi comportamentale ale candidatului.

Stabiliţi un program formal pentru revizuirea sarcinilor personalului şi a angajamentelor de resurse. Acest lucru ar trebui să aibă loc cel puţin o dată pe an.

EXEMPLE DE EVIDENȚE

- Corelarea rolurilor cu competențele, specificând care angajați au nevoie de competențe specifice în materie de securitate.
- Evidențe privind formarea angajaților, furnizorilor și prestatorilor de servicii (materiale, prezență, feedback).
- Confirmări semnate care atestă înțelegerea și acceptarea responsabilităților de securitate.
- Rapoarte de audit care evaluează cât de bine înțelege și aplică personalul responsabilitățile de securitate.
- Înregistrări ale evaluării performanțelor care includ responsabilitățile de securitate, acolo unde este relevant.
- Contracte cu furnizorii/prestatorii de servicii care includ clauze privind responsabilitățile în materie de securitate sau justificări documentate în cazul în care acestea lipsesc.
- Certificări/atestări de securitate cibernetică de la organisme recunoscute pentru personalul cu roluri critice în materie de securitate.
- Materiale de sensibilizare (videoclipuri, diapozitive, buletine informative, postere, conținut intranet).
- Înregistrări care confirmă că utilizatorii privilegiați/administrativi înțeleg și respectă obligațiile lor de securitate.
- Contracte de muncă, politici, coduri de conduită care demonstrează că utilizatorii au fost informați cu privire la așteptările în materie de igienă cibernetică.
- Registrele sesiunilor de formare (prezență, programe).
- Evidențe că furnizorii/prestatorii de servicii beneficiază de formare în materie de securitate adecvată rolului lor.
- Mecanisme de angajare care asigură personal calificat (verificarea referințelor, validarea certificărilor, teste).
- Utilizarea cadrelor/standardelor de securitate cibernetică și a modelelor de maturitate.
- Atribuirea actualizată a rolurilor angajaților.
- Înregistrări ale proceselor de revizuire, inclusiv criterii, constatări și modificări rezultate.

Ref: Cerințe aprobate prin HG 562/2025
pct. 105, pct. 106.1-106.4, pct. 107, pct. 111, pct. 112

3.11 Verificarea antecedentelor

ÎNDRUMĂRI

Identificaţi rolurile, responsabilităţile şi autorităţile care necesită verificarea antecedentelor

Efectuaţi verificarea antecedentelor angajaţilor şi, dacă este cazul, ale furnizorilor direcţi şi ale prestatorilor de servicii.

Dacă este cazul, definiţi criteriile pentru rolurile, responsabilităţile şi autorităţile care vor fi exercitate numai de persoane care au fost supuse verificării antecedentelor. O listă orientativă, neexhaustivă, este următoarea:

- directori şi membri ai conducerii superioare,
- roluri cu acces la informaţii sensibile,
- roluri cu responsabilităţi financiare,
- funcţii care implică achiziţii şi gestionarea furnizorilor,
- roluri care acordă acces la active fizice sau sunt responsabile de securitatea fizică.

Definiţi criteriile şi limitările pentru verificarea antecedentelor (de exemplu, cine este eligibil să verifice persoanele şi cum, când şi de ce se efectuează verificările).

Pentru verificarea antecedentelor, luaţi în considerare verificarea cazierului judiciar al persoanei în cauză în ceea ce priveşte infracţiunile care ar fi relevante pentru o anumită funcţie.

Asiguraţi-vă că verificările cazierului judiciar sunt în conformitate cu cerinţele legale şi de reglementare (de exemplu, legislaţia naţională (a muncii) şi GDPR).

Colectaţi şi gestionaţi informaţiile despre candidaţii la un loc de muncă, ţinând seama de toate legile, reglementările şi normele etice aplicabile, inclusiv protecţia datelor cu caracter personal. Acest lucru poate include colectarea de Referinţe profesionale.

Luaţi în considerare cerinţele de verificare din acordurile contractuale dintre entitate şi furnizorii direcţi şi prestatorii de servicii în cazul personalului contractat de un furnizor extern.

Repetaţi periodic verificarea pentru a confirma adecvarea continuă a personalului, în funcţie de importanţa rolului, responsabilităţilor şi autorităţilor unei persoane.

Entităţile ar trebui să aibă dreptul să se bazeze pe verificările antecedentelor contractorilor angajaţi de o agenţie de recrutare terţă parte cu care entitatea vizată are contracte pentru prestarea de servicii.

Dacă este necesar, revizuiţi şi actualizaţi procedura de verificare a antecedentelor cel puţin o dată pe an.

EXEMPLE DE EVIDENȚE

- Procesul documentat de verificare a antecedentelor.
- Rezultatele verificării pentru angajați și, după caz, pentru furnizori și prestatori de servicii.
- Analiză bazată pe roluri, care identifică pozițiile care necesită verificări ale antecedentelor.
- Îndrumări pentru angajați cu privire la momentul și modul de efectuare a verificării antecedentelor.
- Înregistrări ale verificărilor de Referințe efectuate pentru angajați și terțe părți relevante.
- Formulare de consimțământ semnate de angajați sau candidați care autorizează verificarea.
- Documentația privind măsurile de urmărire luate atunci când se constată discrepanțe sau probleme.
- Contracte sau acorduri cu furnizori terți de servicii de verificare, care confirmă conformitatea cu cerințele legale și de politică.
- Înregistrări ale verificărilor de securitate în curs pentru rolurile care necesită verificări continue.
- Comentarii de revizuire sau jurnale de modificări care documentează actualizările procedurii de verificare a antecedentelor.

Ref: Cerințe aprobate prin HG 562/2025 pct. 108, pct. 109.1-109.2, pct. 110

3.12 Procesul disciplinar

ÎNDRUMĂRI

Asigurați-vă că procesul responsabilizează angajații pentru încălcarea politicilor de securitate a rețelei și a sistemului informatic.

Implicați resursele umane în implementarea procesului disciplinar, asigurându-vă că acesta este în conformitate cu cerințele legale și de reglementare (de exemplu, legislația națională a muncii și GDPR).

Comunicați și sensibilizați angajații cu privire la proces.

Protejați identitatea persoanelor supuse măsurilor disciplinare, acolo unde este posibil, în conformitate cu cerințele aplicabile.

Revizuiți și actualizați periodic procesul disciplinar la intervale planificate și imediat când apar modificări legale sau modificări operaționale sau de risc semnificative.

EXEMPLE DE EVIDENȚE

- Proces disciplinar documentat care descrie tipurile de încălcări și acțiunile necesare.
- Evidențe ale comunicării politicii către toți angajații (e-mailuri, procese verbale ale ședințelor, materiale de instruire).
- Înregistrări ale încălcărilor politicii și ale măsurilor disciplinare corespunzătoare, care demonstrează aplicarea consecventă a acesteia.
- Evidențe justificative pentru încălcări, cum ar fi interviuri, declarații ale martorilor, e-mailuri, înregistrări digitale, jurnale de sistem sau înregistrări telefonice.
- Revizuirea și actualizarea înregistrărilor

Ref: Cerințe aprobate prin HG 562/2025 pct. 113, pct. 114

3.13 Gestionarea activelor

ÎNDRUMĂRI

Asiguraţi-vă că angajaţii, furnizorii direcţi, prestatorii de servicii şi orice alte părţi terţe care utilizează sau gestionează activele entităţii cunosc politica.

Luaţi în considerare dispozitivele mobile, cum ar fi smartphone-urile şi tabletele, şi stabiliţi o strategie pentru gestionarea dispozitivelor mobile, inclusiv Bring-Your-Own-Device (BYOD)

Identificaţi, documentaţi şi implementaţi o politică pentru gestionarea activelor pe tot parcursul ciclului lor de viaţă (achiziţie, utilizare, depozitare, transport şi eliminare).

Asiguraţi-vă că politica include cel puţin depozitarea în condiţii de siguranţă, transportul în condiţii de siguranţă şi ştergerea şi distrugerea irecuperabilă. De exemplu:

- creaţi manuale de utilizare şi materiale de instruire privind utilizarea corectă şi sigură a activelor;
- stabiliţi linii directoare pentru depozitarea sigură, ţinând cont de gestionarea copiilor de rezervă;
- definiţi protocoale pentru transferul sigur, inclusiv luaţi în considerare procesele de migrare sigură, atunci când transferaţi date către un serviciu cloud;
- prezentaţi metode de ştergere a datelor şi de distrugere fizică, asigurând ştergerea completă şi irecuperabilă.

Asiguraţi-vă că politica acoperă utilizarea corectă a tuturor activelor din domeniul de aplicare, atât la sediu, cât şi în afara sediului (de exemplu, dispozitive mobile, date în cloud, date tranzitorii sau informaţii sensibile).

Asiguraţi-vă că activele pot fi transferate în spaţii externe numai după aprobarea de către organismele de conducere autorizate, în conformitate cu politica.

Corelaţi politica de gestionare a activelor cu clasificarea activelor, furnizând detalii privind gestionarea pentru fiecare nivel de clasificare.

Revizuirea şi actualizarea politicii privind gestionarea activelor cel puţin o dată pe an

EXEMPLE DE EVIDENȚE

- Politica documentată privind gestionarea activelor, aliniată la practicile actuale și actualizată periodic.
- Declarații semnate de angajați, furnizori, prestatori de servicii și terți, prin care aceștia confirmă că înțeleg și acceptă politica.
- Liste de acces ale utilizatorilor, formulare de solicitare de acces și înregistrări de aprobare legate de gestionarea activelor.
- Rapoarte de incidente care implică pierderea, furtul, deteriorarea sau utilizarea necorespunzătoare a activelor.
- Politica actualizată privind gestionarea activelor, cu istoricul versiunilor.
  Înregistrări ale revizuirilor și jurnale de modificări care arată evaluarea periodică și actualizările procedurilor de gestionare a activelor.

Ref: Cerințe aprobate prin HG 562/2025 pct. 139, pct. 140.1-140.3, pct. 141

3.14 Inventarul activelor

ÎNDRUMĂRI

Asiguraţi-vă că toate activele, inclusiv hardware, software, date şi servicii, sunt enumerate în inventar.

Verificaţi periodic acurateţea înregistrărilor din inventar.

Actualizaţi prompt inventarul pentru a reflecta orice modificări, cum ar fi active noi, active scoase din uz sau modificări ale stării activelor.
Utilizaţi convenţii de denumire şi metode de categorizare standardizate pentru a menţine coerenţa în cadrul inventarului.

Asiguraţi-vă că intrările din inventar conţin datele din îndrumările descrise (eşantionare).
Implementaţi reguli de validare în cadrul inventarului pentru a vă asigura că datele introduse sunt complete şi consecvente.
Luaţi în considerare adăugarea unuia sau mai multora dintre următoarele elemente la inventar:

- ID-ul unic al activului,
- tipul de activ, de exemplu software, inclusiv maşini virtuale (versiune), hardware (sistem de operare/firmware), servicii, utilităţi de asistenţă, facilităţi, sisteme de încălzire, ventilaţie şi aer condiţionat
- (HVAC), personal şi înregistrări fizice,
- proprietarul activului şi informaţii de contact,
- unitatea operaţională responsabilă de activ, fie numele departamentului intern, fie numele furnizorului extern,
- descrierea activului,
- locaţia activului,
- data ultimei actualizări/patch-uri a activului,
- clasificarea activului în conformitate cu evaluarea riscurilor,
- tipul de informaţii şi clasificarea acestora procesate în activ,
- sfârşitul ciclului de viaţă al activului, dacă este cazul,
- relaţia cu alte active
- cerinţe de înregistrare.

Efectuaţi revizuiri periodice pentru a verifica acurateţea şi exhaustivitatea inventarului. Păstraţi istoricul modificărilor.

EXEMPLE DE EVIDENȚE

- Documentație pentru inventarul activelor
- Inventarul actualizat al activelor
- Înregistrări ale revizuirilor sau istoricul modificărilor.
- Înregistrări ale indicatorilor cheie urmăriți, cum ar fi numărul de active, tipurile de active, conformitatea cu politicile de inventariere și actualizarea la timp a informațiilor.
- Configurația instrumentului de inventariere a activelor, dacă există
- Inventarul actualizat al activelor, inclusiv istoricul modificărilor.
- Rapoarte periodice generate cu privire la starea inventarului, modificări și constatări ale auditului.

Ref: Cerințe aprobate prin HG 562/2025 pct. 139, pct. 140.1-140.3, pct. 141, pct. 145, pct. 146.1-146.2, pct. 147, pct. 148, pct. 149

3.15 Depozitarea, returnarea sau ștergerea activelor la încetarea contractului de muncă

ÎNDRUMĂRI

Definiţi proceduri pentru a vă asigura că activele sunt depozitate, returnate sau șterse irevocabil la încetarea raporturilor de muncă sau a relaţiilor contractuale.

Asiguraţi-vă că procedurile identifică în mod clar toate activele care trebuie returnate, în conformitate cu inventarul activelor, care poate include (listă orientativă, neexhaustivă):

- dispozitive finale ale utilizatorilor, de exemplu computere, tablete şi telefoane etc. şi/sau dispozitive de stocare portabile, inclusiv vehicule, care pot stoca date local pe vehicul şi/sau partaja date extern prin intermediul telematicii. Identificaţi unde utilizatorul procesează, transferă sau stochează datele entităţii pentru a determina domeniul de aplicare al dispozitivelor finale ale utilizatorilor;
- echipamente specializate;
- hardware de autentificare (de exemplu, carduri de acces, chei mecanice, jetoane fizice şi carduri inteligente);
- copii fizice ale informațiilor.

EXEMPLE DE EVIDENȚE

- Proceduri documentate pentru returnarea la timp a bunurilor la încetarea raporturilor de muncă.
- Jurnale sau înregistrări care indică faptul că datele privind bunurile returnate au fost șterse în conformitate cu procedurile.
- Formulare completate cu lista de verificare la ieșire, care includ etapele de returnare a bunurilor și ștergerea datelor, semnate de angajatul care părăsește compania și de superiorii relevanți.

Ref: Cerințe aprobate prin HG 562/2025 pct. 139, pct. 140.1-140.3, pct. 141

3.16 Protecție împotriva amenințărilor fizice și de mediu

ÎNDRUMĂRI

Luați în considerare riscurile asociate amenințărilor fizice și de mediu actuale și previzionate la adresa rețelei și a sistemelor informatice, acolo unde este relevant.

Includeți în evaluare locațiile (fizice) ale facilităților entității.

Pe baza rezultatelor evaluării riscurilor, determinați activele care trebuie protejate împotriva amenințărilor fizice și de mediu.

Implementați măsuri împotriva amenințărilor fizice și de mediu. Parametrii care trebuie luați în considerare sunt (listă orientativă, neexhaustivă):

- scopul și domeniul de aplicare;
- rețeaua și sistemele informatice vizate;
- descrierea instalațiilor;
- roluri și responsabilități;
- angajamentul conducerii;
- coordonarea între unitățile organizaționale;
- respectarea legislației naționale și a legislației UE, inclusiv protecția datelor cu caracter personal.

Luați în considerare potențialele amenințări fizice și de mediu relevante pentru context, locație și mediul operațional. Lista următoare oferă exemple (indicative și neexhaustive) pentru a sprijini planificarea bazată pe riscuri:

- incendii, inundații sau evenimente naturale (de exemplu, cutremure, furtuni),
- tulburări publice sau acces neautorizat, furt sau vandalism,
- incidente cu materiale periculoase (de exemplu, scurgeri de substanțe chimice),
- schimbări de mediu pe termen lung (de exemplu, tendințe climatice, calitatea aerului).

Luați în considerare măsuri împotriva amenințărilor fizice și de mediu, cum ar fi (listă orientativă, neexhaustivă):

- măsuri de control al accesului fizic (de exemplu, acte de identitate, ecusoane, registre; sistem de gestionare a vizitatorilor și bariere fizice);
- sisteme de supraveghere (de exemplu, CCTV, puncte de intrare, ieșiri, mecanisme de blocare și personal de securitate);
- controlul climatizării (de exemplu, controlul temperaturii și umidității și sisteme HVAC);
- măsuri de prevenire și intervenție în caz de incendiu (de exemplu, alarme de incendiu, detectoare de fum, sisteme de sprinklere și stingătoare de incendiu);

Luați în considerare măsuri sporite (maxime) care să fie activate în cazul unor niveluri de amenințare ridicate sau în scenarii specifice. Exemple de astfel de măsuri includ (listă orientativă, neexhaustivă):

- Personal de securitate suplimentar, controale avansate de acces biometric şi proceduri de blocare.
- Sisteme de monitorizare îmbunătăţite, surse de alimentare redundante şi senzori de mediu avansaţi

Planificaţi şi efectuaţi teste periodice, cum ar fi exerciţii trimestriale de incendiu şi evaluări anuale ale măsurilor de securitate fizică.

Efectuaţi atât teste anunţate, cât şi teste neanunţate.

EXEMPLE DE EVIDENȚE

- Raport de evaluare a riscurilor care acoperă locațiile fizice (centre de date, birouri, camere de servere), amenințările de mediu și cartografierea activelor critice în funcție de locații.
- Documentație privind măsurile de protecție fizică și de mediu și punerea lor în aplicare.
- Rapoarte care definesc pragurile minime și maxime de control pentru riscurile de mediu și fizice.
- Jurnale de monitorizare a mediului (temperatură, umiditate, alerte de intruziune).
- Înregistrări ale incidentelor pentru abateri de la praguri, inclusiv acțiunile întreprinse și notificările trimise.
- Rapoarte de testare care detaliază obiectivele, procedurile, rezultatele și problemele identificate.
- Procesele-verbale ale ședințelor de revizuire care documentează discuțiile, concluziile și deciziile privind măsurile de protecție.

Ref: Cerințe aprobate prin HG 562/2025 pct. 153, 154.1-154.3, pct. 155

3.17 Controlul perimetrului şi al accesului fizic

ÎNDRUMĂRI

Implementaţi controlul accesului fizic la perimetru, acolo unde este relevant, ţinând cont de măsurile de protecţie împotriva ameninţărilor fizice şi de mediu.

Asiguraţi-vă că controlul accesului fizic este integrat cu controlul accesului logic şi al reţelei, în conformitate cu procedurile de securitate a resurselor umane, pentru a sprijini detectarea activităţilor suspecte şi pentru a spori securitatea generală a organizaţiei.

În evaluarea riscurilor, luaţi în considerare riscurile asociate accesului fizic neautorizat, deteriorării şi interferenţei cu reţeaua şi sistemele informatice.

Pe baza rezultatelor evaluării riscurilor, determinaţi activele cu grad ridicat de criticitate şi impactul compromiterii acestora. Acest lucru va ajuta la identificarea perimetrului pentru astfel de active.

Preveniţi accesul fizic neautorizat la facilităţi şi stabiliţi măsuri adecvate.

Măsurile de control al accesului fizic concepute pentru a proteja entitatea în ansamblu vor proteja şi activele individuale.

Luaţi în considerare introducerea unor măsuri suplimentare specifice de control al accesului pentru anumite active sau instalaţii.

Luaţi în considerare măsuri de securitate fizică (listă orientativă, neexhaustivă):

- controale fizice ale accesului, cum ar fi carduri de acces, scanere biometrice, încuietori şi personal de securitate pentru a restricţiona accesul în zonele cu grad ridicat de criticitate,
- controlul electronic al intrării, cu o pistă de audit,
- segmentarea spaţiilor sau crearea de zone în funcţie de nivelurile de autorizare şi conţinutul acestora,
- camere CCTV şi sisteme de monitorizare pentru observarea continuă a zonelor sensibile, garduri, bariere şi patrule de securitate pentru securizarea perimetrelor fizice,
- paznici şi/sau alarme pentru monitorizarea tuturor punctelor de acces fizic la instalaţia în care se află sistemul informatic, 24 de ore pe zi, şapte zile pe săptămână.
- Elaborarea şi aplicarea procedurilor de acordare, revizuire şi revocare a drepturilor de acces fizic.
- Identificarea unui funcţionar desemnat în cadrul entităţii pentru a revizui şi aproba lista personalului cu acces fizic autorizat.
- Menţinerea unei liste a personalului cu acces autorizat la facilităţi şi a nivelurilor de autorizare ale acestora.
- Revizuirea listelor de acces fizic.
- Utilizarea testelor de intruziune care includ, acolo unde este cazul, încercări neanunţate de a ocoli sau eluda măsurile asociate punctelor de acces fizic la instalaţie.

La limita fizică a instalației sau a rețelei și a sistemului informatic, efectuați verificări de securitate pentru a detecta exfiltrarea neautorizată de informații sau îndepărtarea componentelor sistemului informatic.

EXEMPLE DE EVIDENȚE

- Politica de securitate fizică documentată, inclusiv descrieri ale instalațiilor și sistemelor din domeniul de aplicare.
- Rezultatele evaluării riscurilor care identifică amenințările fizice și controalele necesare.
- Evidențe ale măsurilor de securitate fizică implementate (de exemplu, controale de acces, bariere, supraveghere).
- Proceduri pentru acordarea, revizuirea și revocarea drepturilor de acces fizic.
- Înregistrări ale simulărilor și activităților de sensibilizare care testează pregătirea personalului și procedurile de control al accesului.
- Programele și rezultatele testelor și verificărilor de securitate fizică.
- Lista actualizată a personalului cu acces fizic autorizat.

Ref: Cerințe aprobate prin HG 562/2025 pct. 156, pct. 157.1-157.4, pct. 158

4. Detecție

4.1 Monitorizare și înregistrare

ÎNDRUMĂRI

Identificați unul sau mai multe obiective de monitorizare și înregistrare (listă orientativă, neexhaustivă):

- detectarea amenințărilor,
- asigurarea conformității,
- asistență în cazul incidentelor,
- optimizarea performanței,
- detectarea anomaliilor,
- monitorizarea rapoartelor privind vulnerabilitățile noi emise pentru orice componente software gratuite și open source utilizate de entitate,
- prevenirea pierderii de date,
- asistență în investigații criminalistice și
- monitorizarea stării rețelei.

Procedurile trebuie să descrie (listă orientativă, neexhaustivă):

- obiectivele,
- date pentru colectare și instrumente relevante,
- descrierea algoritmilor de date și
- mecanismelor de notificare a personalului relevant.

Selectați instrumente care servesc obiectivelor de monitorizare și înregistrare în conformitate cu criterii specifice (listă orientativă, neexhaustivă):

- ușurința utilizării,
- integrarea cu rețeaua și sistemul de informații existente, inclusiv operațiunile transfrontaliere și considerentele asociate în materie de reglementare, securitate și performanță,
- minimizarea intervenției manuale,
- capacitatea de a colecta date din diverse surse, de exemplu rețele, sisteme și aplicații,
- funcții de securitate oferite, de exemplu criptare și control al accesului și
- costuri și licențiere.

Pentru a minimiza falsele pozitive și falsele negative, în măsura în care este posibil, luați în considerare una sau mai multe dintre următoarele (listă orientativă, neexhaustivă):

- stabilirea modelelor de trafic de rețea;
- utilizați algoritmi de analiză și învățare automată;
- actualizați continuu instrumentele de monitorizare automată pentru a vă adapta la noile amenințări și schimbări din mediu; și
- reglați parametrii și pragurile pe baza celor mai recente date și feedback.

Dacă este cazul, asigurați-vă că toate riscurile potențiale sunt acoperite în mod corespunzător de cazurile de utilizare relevante, de exemplu cazul de utilizare pentru accesul la date critice, cazul de utilizare pentru exfiltrarea datelor sau cazul de utilizare pentru infectarea cu ransomware, astfel încât nicio amenințare critică să nu rămână nedetectată.

În ceea ce privește configurația critică, luați în considerare setările și parametrii care sunt esențiali pentru funcționarea, securitatea și performanța corespunzătoare a rețelei și a sistemului informatic al entității. Aceste configurații sunt esențiale, deoarece orice modificare sau configurare incorectă ar putea avea un impact semnificativ, inclusiv întreruperi ale sistemului, vulnerabilități de securitate sau performanță redusă a rețelei și a sistemului informatic al entității.

Consultați rezultatele evaluării riscurilor pentru a determina ce trafic de rețea trebuie înregistrat. De exemplu, dacă anumite active sunt identificate ca fiind cu risc ridicat (de exemplu, din cauza faptului că sunt potențial vulnerabile sau cruciale pentru operațiunile organizației), traficul lor de intrare și de ieșire ar trebui înregistrat pentru monitorizare și analiză.

Luați în considerare utilizarea detectării anomaliilor sau a pragurilor de alarmă adaptive pentru a completa regulile statice tradiționale.

Asigurați-vă că procedurile sunt concepute pentru a detecta în timp util atacurile bazate pe rețea, pe baza modelelor anormale de trafic de intrare și ieșire și/sau a atacurilor de tip „denial of service" (DoS).

Asigurați-vă că pragurile de alarmă, acolo unde este cazul, au fost stabilite în conformitate cu rezultatele evaluării riscurilor. Urmează o listă orientativă și neexhaustivă de exemple cu praguri:

- traficul de rețea relevant de ieșire și de intrare: vârfuri de volum de trafic care depășesc 50% din traficul normal într-o perioadă de 10 minute pe un port specific;
- accesul la sisteme și aplicații: trei sau mai multe blocări de cont în decurs de 15 minute;
- acces privilegiat: două sau mai multe cazuri de escaladare a privilegiilor (de exemplu, de la utilizator normal la administrator) în decurs de 24 de ore
- antivirus: malware detectat pe mai multe terminale într-un interval scurt de timp;
- utilizarea resurselor sistemului: instalarea de software neautorizat într-un interval scurt de timp.

Asigurați-vă că perioada de păstrare a jurnalelor este definită în conformitate cu nevoile afacerii, rezultatele evaluării riscurilor și cerințele/obligațiile legale.

Perioada de păstrare a jurnalelor de rezervă nu trebuie să fie mai scurtă decât perioada de revizuire a jurnalelor.

Perioada de păstrare trebuie să fie în conformitate cu prevederile regulamentului.

Ștergeți datele la expirarea perioadei de păstrare.

Luați în considerare mecanisme de protejare a jurnalelor împotriva accesului sau modificărilor neautorizate (listă orientativă, neexhaustivă):

- criptare,
- controlul accesului,
- hashare și
- înregistrarea tuturor accesărilor și modificărilor aduse fișierelor jurnal.

Controlul accesului trebuie să fie în conformitate cu prevederile regulamentului.

Luați în considerare următoarele aspecte pentru sincronizarea orei:

- Utilizați servere NTP (Network Time Protocol) sau PTP (Precision Time Protocol) pentru o sincronizare precisă și fiabilă a timpului

- Utilizaţi NTP autentificat pentru a împiedica entităţile rău intenţionate să manipuleze sincronizarea orei
- Configuraţi un server central de timp în cadrul entităţii Acest server trebuie să se sincronizeze cu o sursă de timp externă fiabilă şi apoi să distribuie ora către toate celelalte sisteme din reţea
- Utilizaţi mai multe surse de timp pentru a evita un singur punct de eşec
- Planificaţi modul în care este gestionată sincronizarea orei între sistemele locale (de exemplu, serverele din centrul de date al companiei), serviciile cloud şi platformele software-as-a-service (SaaS), în special dacă organizaţia utilizează un mediu hibrid (o combinaţie de sisteme locale şi bazate pe cloud).

Activele înregistrate trebuie marcate ca atare în inventarul activelor, în conformitate cu prevederile regulamentului.

Implementaţi măsuri pentru a proteja datele de jurnal împotriva pierderii, inclusiv, dar fără a se limita la, stocarea redundantă în mai multe locaţii (de exemplu, cloud, servere secundare), păstrarea evenimentelor de jurnal procesate în sisteme structurate şi conservarea informaţiilor de securitate derivate (de exemplu, alerte, metrici) în conformitate cu prevederile regulamentului. Aceste abordări complementare asigură atât integritatea datelor, cât şi continuitatea operaţională în monitorizarea securităţii şi răspunsul la incidente.

Implementaţi instrumente separate pentru a monitoriza capacitatea şi disponibilitatea sistemelor principale de monitorizare şi înregistrare ale entităţii.

Determinaţi frecvenţa revizuirilor pe baza rezultatelor evaluării riscurilor legate de importanţa activelor, asigurându-vă că revizuirile sunt efectuate cel puţin o dată pe an.

Includeţi testarea procedurilor de monitorizare şi înregistrare în testarea securităţii.

Revizuiţi un eşantion aleatoriu de jurnale pentru a verifica dacă toate activele care ar trebui să facă obiectul jurnalului sunt efectiv luate în considerare.

În plus faţă de elementele menţionate în regulament, ultima conectare pentru fiecare cont trebuie înregistrată.

Documentaţi procedurile de monitorizare şi înregistrare.
Evaluaţi frecvenţa activităţilor de monitorizare pentru a vă asigura că acestea sunt suficiente pentru a sprijini deciziile de securitate bazate pe riscuri pentru protejarea adecvată a reţelei şi a sistemelor informatice ale entităţii.
Asiguraţi-vă că datele cu caracter personal incluse în jurnale nu sunt prelucrate în mod inutil. Atunci când este necesar, se implementează un nivel suplimentar de protecţie după efectuarea unei evaluări a impactului asupra protecţiei datelor.

Stabiliţi liniile de bază ale jurnalelor în conformitate cu nevoile şi capacităţile întreprinderii (listă orientativă, neexhaustivă):

- structurate sau semi-structurate, dacă este posibil, în loc de format nestructurat;
- format de date consecvent, în conformitate cu instrumentele selectate şi standardele cunoscute, de exemplu JavaScript Object Notation şi extensible markup language (XML);
- nivelul jurnalului în conformitate cu nivelul de clasificare al activului înregistrat – entitatea ar trebui să atribuie un nivel de jurnal mai ridicat, de exemplu „eroare”/„fatal”, activelor cu grad ridicat de clasificare, în timp ce nivelurile de jurnal mai scăzute, de exemplu „info”/„debug”, ar trebui utilizate pentru activele cu un grad de clasificare mai scăzut; şi
- standardul pentru marcajele de timp, de exemplu ISO-8601, RFC 3339 sau RFC 9557.

Fiecare intrare de jurnal ar trebui să conţină metadatele necesare, cum ar fi (listă orientativă, neexhaustivă):

- nivelul de jurnal;
- marca temporală;
- identificatorul sursei, de exemplu aplicaţia sau dispozitivul relevant pentru intrare; şi
- un identificator unic pentru înregistrare.

Corelaţi datele din diferite surse, dacă este cazul.

Selectaţi instrumente care monitorizează şi protejează dispozitivele finale.

Selectaţi instrumente care pot colecta şi analiza traficul de reţea în timp real pentru a detecta anomalii, exfiltrarea datelor şi chiar cele mai avansate ameninţări, oferind în acelaşi timp opţiunea de remediere automată.

EXEMPLE DE EVIDENȚE

- Proceduri documentate și instrumente de înregistrare/monitorizare implementate.
- Setări de configurare a funcției de înregistrare aliniate la obiective, standarde și bune practici.
- Măsuri de protecție care asigură confidențialitatea, integritatea și disponibilitatea jurnalelor.
- Instrumente aprobate de colectare, monitorizare, stocare și analiză a jurnalelor, în conformitate cu practicile de ultimă generație.
- Sisteme SIEM pentru corelarea evenimentelor și detectarea anomaliilor.
- Instrumente EDR/XDR implementate pentru monitorizarea la nivel de terminal.
- Mecanisme de reducere a falselor pozitive/negative.
- Corelarea cazurilor de utilizare cu riscurile relevante pentru o monitorizare cuprinzătoare.
- Fișiere jurnal de eșantion, inclusiv jurnale DNS și DHCP (actuale și istorice).
- Rapoarte periodice de analiză a jurnalelor care evidențiază anomaliile.
- Praguri de alarmă și înregistrări ale alarmelor declanșate.
- Fluxuri de lucru pentru raportarea evenimentelor.
- Perioadă definită de păstrare a jurnalelor, conformă cu cerințele de reglementare și mai scurtă decât perioada de revizuire.
- Procese de gestionare a jurnalelor care asigură că datele expirate nu sunt păstrate.
- Mecanisme de control al accesului la jurnale, aliniate la cerințele de reglementare.
- Mecanisme de sincronizare a timpului pentru jurnale.
- Mecanisme redundante de stocare a jurnalelor.
- Jurnale de la instrumente de monitorizare care indică capacitatea și disponibilitatea sistemelor primare de înregistrare.
- Planuri sau programe de revizuire pentru înregistrare și monitorizare.
- Proceduri documentate care susțin gestionarea jurnalelor.
- Stabilirea valorilor de referință pentru jurnale.
- Jurnale eșantion care conțin metadatele necesare.

Ref: Cerințe aprobate prin HG 562/2025 pct. 19, pct. 21.1-21.12, pct. 22, pct. 23, pct. 24, pct. 25, pct. 28, pct. 29.1-29.5

4.2 Testarea securității

ÎNDUMĂRĂRI

Luați în considerare standardele recunoscute în industrie atunci când elaborați politica de testare.

Stabiliți și mențineți un program de testare adecvat dimensiunii, complexității și maturității entității.

Asigurați-vă că rețeaua și sistemele informatice sunt supuse unor teste continue, în special în medii care utilizează practici de integrare continuă/implementare continuă. Testele periodice trebuie efectuate la configurare, după actualizări sau modificări semnificative și după întreținere, pentru a menține o securitate și o performanță robuste.

Luați în considerare o serie de teste de securitate (de exemplu, evaluări de vulnerabilitate, teste de penetrare, revizuirea codului, hacking etic, programe de recompensare a descoperirii de bug-uri, simulări de atacuri cibernetice, red teaming, teste de conformitate cu protocolul sau exerciții de răspuns cibernetic) și selectați cel mai adecvat (sau mai multe) pentru a testa procedura, serviciul sau instrumentul specific în timp.

Testele la nivel de entitate ar trebui efectuate la intervale planificate sau atunci când apar incidente sau modificări semnificative.

Efectuați audituri interne și/sau externe în rețelele, sistemele și procesele entității într-o manieră ad-hoc.

Înregistrați evidențele în timpul testării. Necesitatea, domeniul de aplicare, frecvența, tipul și rezultatele trebuie documentate într-o manieră comprehensibilă pentru un expert terț.

Utilizați criterii pentru a evalua rezultatele testelor similare cu criteriile pentru efectuarea evaluărilor riscurilor de securitate cibernetică.

Evaluați, urmăriți și remediați constatările cu grad ridicat de criticitate în ceea ce privește confidențialitatea, integritatea, autenticitatea sau disponibilitatea serviciului furnizat.

Documentați evaluarea criticității și acțiunile de atenuare pentru fiecare constatare. Asigurați-vă că rezultatele evaluării riscurilor și planurile de tratare a riscurilor sunt actualizate în consecință.

Atunci când testarea relevă o problemă de securitate subiacentă într-o componentă gratuită și open source, aceste constatări trebuie comunicate proiectului open source relevant. Dacă se dezvoltă un patch pentru a remedia problema, codul relevant trebuie, de asemenea, comunicat proiectului open source relevant, într-o manieră adecvată pentru integrare.

Dacă este cazul, orice teste de securitate automatizate scrise de entități pentru componentele open source pe care le utilizează trebuie comunicate proiectelor open source relevante.

Revizuiți politica și procedurile de testare a securității cel puțin o dată la doi ani.

Pentru sistemele cu integrări externe (de exemplu, servicii cloud) care nu sunt controlate de organizaţie, asiguraţi-vă că toate punctele finale ale interfeţei de programare a aplicaţiilor externe sunt testate temeinic.

Determinaţi evenimentele de securitate auditate care sunt adecvate pentru a sprijini investigaţiile incidentelor de securitate.

Implementaţi instrumente pentru testarea automată, cum ar fi instrumente de analiză a codului sau scanere de vulnerabilităţi.

Asiguraţi-vă că politica este aprobată, comunicată şi acceptată de personalul relevant şi de terţe părţi.

Asiguraţi-vă că mediul (mediile) de dezvoltare şi testare este (sunt) separat(e) de mediul de producţie.

Revizuiţi politica şi procedurile de testare a securităţii atunci când au loc incidente semnificative sau modificări majore ale reţelei şi sistemului informatic.

EXEMPLE DE EVIDENȚE

- Proceduri și politici documentate privind testarea securității, aliniate la standarde și bune practici.
- Linii directoare și standarde pe care entitatea le respectă pentru efectuarea testelor de securitate.
- Roluri și responsabilități definite pentru personalul implicat în testare.
- Planuri sau programe de testare pentru testele de securitate periodice și ad-hoc.
- Rapoarte din testele anterioare, care acoperă evaluări de vulnerabilitate, teste de penetrare, revizuiri de cod și alte tipuri de teste.
- Rapoarte de audit intern și extern care evaluează practicile de testare.
- Politici și proceduri actualizate, inclusiv comentarii de revizuire și jurnale de modificări.
- Documentație completă privind testarea, inclusiv planuri de testare, cazuri de testare și șabloane de rapoarte.
- Elemente de politică care acoperă părțile de testare aprobate, nivelurile de confidențialitate, obiectivele testelor și gestionarea rezultatelor.
- Evidențe că personalul relevant înțelege procedurile și instrumentele de testare.
- Cerințe de audit documentate legate de testarea securității.
- Lista instrumentelor de testare, inclusiv scopul, întreținerea și practicile de actualizare.
- Licențe sau abonamente valabile pentru instrumente și servicii operaționale.
- Evidențe că instrumentele sunt utilizate în mod activ și configurate corespunzător.
- Înregistrări care arată actualizările politicilor și procedurilor de testare pe baza lecțiilor învățate și a amenințărilor emergente.

Ref: Cerințe aprobate prin HG 562/2025 pct. 74, pct. 75.1-75.4, pct. 76

5. Răspuns

5.1 Raportarea evenimentelor

ÎNDRUMĂRI

Definiţi ce constituie un eveniment suspect pe baza unor criterii (listă orientativă, neexhaustivă):

- dacă confidenţialitatea, integritatea sau disponibilitatea reţelei sau a sistemului informatic au fost afectate;
- persistenţa, adică dacă evenimentul este în curs de desfăşurare sau nu;
- impactul, de exemplu numărul de active (potenţial) afectate; şi
- încălcarea conformităţii cu un regulament sau cu politicile entităţii.

Elaboraţi orientări clare şi concise cu privire la informaţiile care trebuie incluse într-un raport. Aliniaţi aceste informaţii cu informaţiile care ar putea fi transmise CSIRT sau, după caz, autorităţii competente, dacă evenimentul este notificat în conformitate cu regulamentul. Ca bună practică, ar trebui raportate cel puţin următoarele informaţii (listă orientativă, neexhaustivă):

- data şi ora evenimentului,
- orice capturi de ecran, jurnale sau alte evidenţe relevante,
- informaţii de contact pentru urmărirea cazului, dacă este necesar.

Oferiţi mai multe canale de raportare, cum ar fi e-mailul, un formular web, o linie telefonică dedicată sau o aplicaţie mobilă. Asiguraţi-vă că aceste canale sunt uşor accesibile şi intuitive de utilizat.

Puneţi la dispoziţia personalului, furnizorilor şi clienţilor entităţii mijloace adecvate de raportare.

Luaţi în considerare raportarea anonimă pentru a încuraja persoanele să raporteze evenimentele de securitate fără teama de represalii.

Luaţi în considerare obligaţiile legale de a raporta un incident autorităţii competente în conformitate cu reglementările, inclusiv orice obligaţii privind momentul în care incidentul trebuie raportat.

Reamintiţi periodic părţilor interesate mecanismul de raportare prin buletine informative trimise prin e-mail, afişe şi alte canale de comunicare.

Organizaţi exerciţii sau simulări periodice pentru a testa eficacitatea mecanismului de raportare.

Păstraţi o evidenţă a tuturor evenimentelor raportate.

Asiguraţi-vă că respectaţi alte reglementări şi legi relevante privind confidenţialitatea datelor, confidenţialitatea şi raportarea incidentelor.

Solicitaţi consiliere juridică, dacă este necesar, pentru a înţelege implicaţiile juridice ale mecanismului de raportare.

Evaluaţi comunicările şi raportările anterioare privind evenimentele.

Revizuiţi şi actualizaţi mecanismul de raportare şi planurile de comunicare pe baza schimbărilor sau evenimentelor anterioare.

EXEMPLE DE EVIDENȚE

- Mecanism de raportare documentat care descrie modul în care trebuie raportate evenimentele de securitate.
- Modele pentru raportarea evenimentelor (formulare, formate structurate).
- Evidențe că personalul cunoaște mecanismul și înțelege pe cine trebuie să contacteze atunci când observă activități suspecte.
- Canale multiple de raportare (e-mail, telefon, formulare web, portaluri).
- Înregistrări ale rapoartelor de evenimente anterioare și comunicări conexe.
- Proceduri de comunicare documentate care acoperă:
    - motivele raportării (specifice organizației, juridice),
    - tipurile de evenimente vizate,
    - conținutul necesar al notificărilor,
    - canalele de raportare,
    - rolurile responsabile.
- Materiale de instruire și sensibilizare pentru angajați, furnizori și clienți.
- Simularea și activitățile de sensibilizare înregistrarea testării gradului de pregătire și adecvare a mecanismului de raportare.
- Înregistrări ale evenimentelor, inclusiv impactul, cauza, măsurile luate și lecțiile învățate.
- Rezumatele revizuirilor anterioare ale mecanismului de raportare.

Ref: Cerințe aprobate prin HG 562/2025 pct. 26, pct. 27

5.2 Răspunsul la incidente

ÎNDRUMĂRI

Înființați o echipă dedicată de răspuns la incidente, formată din angajați cu expertiza tehnică și autoritatea necesare pentru a răspunde în mod eficient la incidente, acolo unde este cazul.

Definiți rolurile și responsabilitățile în cadrul echipei de răspuns la incidente, cum ar fi coordonatorii de incidente, analiștii și persoanele de legătură pentru comunicare, după caz.

Luați în considerare standardele recunoscute în industrie atunci când elaborați procedurile de răspuns la incidente.

Implementați manuale sau ghiduri pentru a orienta acțiunile de răspuns la incidente pentru tipurile comune de incidente.

Creați proceduri de răspuns la incidente.

Asigurați-vă că gestionarea incidentelor de securitate cibernetică ține seama de prioritățile entității și de impactul incidentului.

- Recunoașteți și abordați potențialele conflicte între următoarele obiective în timpul gestionării incidentelor:
- activități de criminalistică – păstrarea și securizarea probelor în scopuri legale, de conformitate sau de investigare,
- activități de răspuns la incidente – atenuarea și eliminarea amenințărilor actuale pentru a preveni deteriorarea în continuare și
- continuitatea operațională – minimizarea întreruperilor serviciilor IT și menținerea operațiunilor critice.

În cazul în care aceste obiective intră în conflict, stabiliți un proces clar de luare a deciziilor care:

- acordă prioritate pe baza nivelurilor acceptate de toleranță la risc, a impactului asupra activității și a obligațiilor legale,
- implică coordonarea între echipele de securitate cibernetică, juridică/de conformitate și operațională și
- documentează motivele deciziilor de stabilire a priorităților pentru a asigura transparența și responsabilitatea.

Elaborați manuale de răspuns la incidente care să includă procesul decizional și căile de escaladare pentru gestionarea compromisurilor între păstrarea probelor, limitarea amenințărilor și continuitatea operațională.

Țineți la curent organele de conducere.

Asigurați-vă că planul de comunicare include proceduri privind modul de comunicare a incidentului către autoritățile relevante, CSIRT național și părțile interesate interne și externe, inclusiv, după caz, clienți, furnizori direcți, furnizori de servicii și, dacă se utilizează surse deschise, contacte pentru proiecte de software gratuit și cu sursă deschisă.

Includeți informații de contact pentru personalul cheie, părțile interesate externe și autoritățile relevante.

Înregistrați informațiile privind răspunsul la incidente, care conțin (listă orientativă, neexhaustivă):

- momentul detectării, izolării și eradicării; o momentul în care sistemele și-au revenit;
- indicatori de compromitere;
- cauza principală;
- acțiunile întreprinse în fiecare fază, și anume detectarea, izolarea și eradicarea;
- evaluarea amplorii și a nivelului de impact al incidentului;
- comunicările în timpul răspunsului la incident;
- lecțiile învățate și recomandările după incident;
- CSIRT sau autoritatea competentă a fost notificată cu privire la incident

Testați procedurile de răspuns la incidente ale entității cel puțin o dată pe an.

Testați diferite tipuri de incidente, de exemplu ransomware, phishing, încălcarea securității datelor și DoS.

Asigurați-vă că scenariile de testare implică angajați din diferite departamente, precum și părți interesate externe, de exemplu furnizori și prestatori de servicii.

Dacă este necesar, includeți organismele de conducere în teste, astfel încât acestea să înțeleagă rolul lor în timpul unui incident.

Efectuați analize post-test pentru a identifica eventualele lecții învățate.

Actualizați procedurile de răspuns la incidente pe baza lecțiilor învățate din test, dacă este cazul.

EXEMPLE DE EVIDENȚE

- Roluri definite de răspuns la incidente în cadrul echipei de răspuns.
- Standarde și bune practici documentate pe care entitatea le urmează pentru gestionarea incidentelor.
- Planuri de răspuns la incidente și manuale pentru tipuri comune de incidente.
- Proceduri detaliate de răspuns, inclusiv tipuri de incidente, obiective, responsabilități, căi de escaladare și implicarea organismului de conducere.
- Înregistrări care arată modul în care au fost rezolvate obiectivele conflictuale în timpul incidentelor anterioare.
- Proceduri pentru comunicarea incidentelor către autorități, CSIRT, clienți și furnizori.
- Jurnale de răspuns la incidente care documentează măsurile luate.
- Utilizarea sistemelor de sprijin, cum ar fi SIEM, EDR/XDR sau platforme de ticketing.
- Planuri sau programe pentru viitoarele teste de răspuns la incidente.
- Înregistrări din testele de răspuns la incidente anterioare, care acoperă diferite scenarii de incidente.

Ref: Cerințe aprobate prin HG 562/2025
pct. 16, pct. 17.1-17.4, pct. 18, pct. 30, pct. 31.1-31.3, pct. 32.1-32.2, pct. 33, pct. 34, pct. 35, pct. 36, pct. 37

5.3 Gestionarea crizelor

ÎNDRUMĂRI

Luaţi în considerare standardele recunoscute în industrie atunci când elaboraţi procesul de gestionare a crizelor.

Reţineţi că fiecare criză poate fi diferită şi că poate fi necesară o analiză suplimentară pe bază ad hoc.

Luaţi în considerare diversele aspecte (de exemplu, tehnice, operaţionale, de comunicare şi remediere) ale gestionării crizelor, inclusiv procesele, rolurile şi responsabilităţile.

Deoarece escaladarea unui incident la statutul de criză depinde de apetitul de risc al unei entităţi şi de capacităţile sale de gestionare a incidentelor, entitatea ar trebui să definească criteriile pentru declararea unei crize.

Acestea se pot referi la incidente care au un impact grav, depăşind un anumit prag de toleranţă. Aceste criterii pot include următoarele (listă orientativă şi neexhaustivă):

- incidentul prezintă un risc semnificativ pentru activele critice sau operaţiunile cu grad ridicat de criticitate, de exemplu incidente de gravitate ridicată (de exemplu, încălcări ale securităţii datelor care implică informaţii sensibile);
- incidentul perturbă în mod semnificativ operaţiunile organizaţiei, de exemplu, perioade de nefuncţionare prelungite, pierderea pe scară largă a serviciilor sau impact semnificativ asupra serviciului pentru clienţi;
- amploarea incidentului, adică dacă afectează mai multe sisteme, departamente sau locaţii geografice, indicând o ameninţare mai largă;
- impactul potenţial asupra reputaţiei entităţii – incidentele care ar putea duce la o expunere publică sau la pierderea încrederii clienţilor ar trebui escaladate;
- impactul potenţial al incidentului de securitate cibernetică asupra confidenţialităţii, integrităţii, autenticităţii şi disponibilităţii datelor;
- complexitatea şi motivaţiile actorilor implicaţi în ameninţare. Incidentele legate de ameninţări persistente avansate sau de criminalitatea cibernetică organizată pot necesita un răspuns la un nivel superior, care depăşeşte capacităţile entităţii;
- potenţialul de escaladare ulterioară (de exemplu, dacă vulnerabilităţile ar putea fi exploatate din nou sau dacă malware-ul se răspândeşte).

Pentru comunicarea în situaţii de criză, luaţi în considerare (listă orientativă, neexhaustivă):

- obligaţiile legale de comunicare, cum ar fi momentul comunicării, în special în ceea ce priveşte cerinţele de notificare;
- modul în care informaţiile vor fi diseminate către părţile interesate interne şi externe (angajaţi, clienţi, furnizori direcţi şi prestatori de servicii, servicii de urgenţă etc.) în timpul unei crize;
- modele de comunicare;

- canalele de comunicare care vor fi utilizate pentru fiecare tip de parte interesată, având în vedere că:
    - părţile interesate interne şi externe pot utiliza canale de comunicare diferite;
    - canalele normale de comunicare ar putea să nu fie sigure în situaţii de criză;
    - trebuie indicate şi canalele utilizate pentru notificarea şi comunicarea cu autorităţile competente;
- informaţii de contact actualizate pentru părţile interesate interne şi externe.

Implementaţi un proces de gestionare şi utilizare a informaţiilor primite de la CSIRT. Luaţi în considerare următoarele etape (listă orientativă, neexhaustivă):

- desemnaţi un punct de contact cu CSIRT;
- asiguraţi-vă că persoana de contact are cunoştinţe suficiente cu privire la incidente şi informaţii privind ameninţările.
- clasificaţi informaţiile primite în categorii precum incidente, vulnerabilităţi, ameninţări şi măsuri de atenuare.
- Atribuiţi niveluri de prioritate în funcţie de gravitate şi de impactul potenţial asupra entităţii, dacă informaţiile sunt relevante sau aplicabile
- solicitaţi persoanei de contact CSIRT să examineze informaţiile din punct de vedere al relevanţei şi urgenţei.
- validaţi informaţiile în raport cu jurnalele interne, fluxurile de informaţii privind ameninţările şi politicile de securitate existente.
- în cazul vulnerabilităţilor şi ameninţărilor, dacă este cazul, să colaboreze cu echipele relevante (IT, securitate, operaţiuni) pentru a elabora o strategie de atenuare;
- actualizaţi sau creaţi planuri de răspuns la incidente pe baza naturii ameninţărilor sau incidentelor raportate.
- dacă este cazul, să pună în aplicare măsurile de atenuare şi să comunice cu părţile interesate relevante.
- să împărtăşească voluntar informaţii şi feedback cu privire la incidente şi măsuri de atenuare cu CSIRT.

Testaţi anual procesul de gestionare a crizelor.

Testaţi procesul de gestionare a crizelor, de exemplu, printr-un exerciţiu sau o simulare, prin (listă orientativă, neexhaustivă):

- luând în considerare situaţiile de criză din trecut;
- compararea rezultatelor testelor cu obiectivele definite, de exemplu obiectivele de recuperare
- utilizarea rezultatelor comparaţiei pentru actualizarea şi îmbunătăţirea procedurii de gestionare a crizelor.

Revizuiţi şi actualizaţi, dacă este necesar, procesul de gestionare a crizelor după un test sau în urma unor incidente semnificative sau a unor modificări semnificative ale operaţiunilor sau riscurilor.

Revizuirea şi actualizarea politicii privind securitatea reţelelor şi a sistemelor informatice şi a măsurilor organizatorice de gestionare a crizelor după un test sau în urma unor incidente semnificative sau a unor modificări semnificative ale operaţiunilor sau riscurilor.

EXEMPLE DE EVIDENȚE

- Proces documentat de gestionare a crizelor, aliniat la standarde și bune practici.
- Lista echipei de gestionare a crizelor, inclusiv rolurile, datele de contact și supleanții.
- Înregistrări ale comunicărilor anterioare cu CSIRT și autoritățile competente (e-mailuri, procese-verbale, corespondență).
- Evidențe că persoana de contact desemnată are cunoștințe suficiente în materie de gestionare a incidentelor și de informații privind amenințările.
- Documentație care arată integrarea între planurile de gestionare a crizelor și planurile de răspuns la incidente, în special pentru incidentele legate de TIC.
- Rapoarte care identifică crize anterioare, probabilitatea reapariției acestora și impactul potențial asupra activității.
- Documentație privind testele de gestionare a crizelor, inclusiv scenarii, participanți și rezultate.
- Rapoarte post-acțiune care evidențiază punctele forte, punctele slabe și domeniile care necesită îmbunătățiri.
- Înregistrări interne/externe ale revizuirii și auditului planului de gestionare a crizelor, inclusiv concluzii și măsuri corective.

Ref: Cerințe aprobate prin HG 562/2025
pct. 48, pct. 49.1- 49.3, pct. 50, pct. 51, pct. 52

6. Recuperare

6.1 Revizuiri post-incident

ÎNDRUMĂRI

Efectuaţi o analiză a cauzelor fundamentale şi identificaţi cauza fundamentală a incidentului, acolo unde este posibil. Identificaţi factorii care au contribuit la incident şi domeniile care pot fi îmbunătăţite în procesele de detectare, răspuns şi recuperare în caz de incident.

Investigaţi incidentele semnificative şi redactaţi rapoarte finale privind incidentele, incluzând măsurile luate şi recomandările pentru a reduce apariţia în viitor a acestui tip de incidente.

Documentaţi lecţiile învăţate, însoţite de recomandări şi de proprietarii acestora, pe baza jurnalelor de răspuns la incidente.

Partajaţi orice constatări relevante din analiza post-incident cu părţile interesate afectate, de exemplu furnizori, prestatori de servicii, administratori de componente gratuite şi open source.

Analizaţi constatările revizuirii post-incident pentru a identifica lacunele şi punctele slabe din reţeaua entităţii şi din starea securităţii informaţiilor. Asiguraţi-vă că lacunele şi punctele slabe identificate sunt reflectate în evaluarea riscurilor şi în planul de tratare a riscurilor.

Evaluaţi dacă măsurile existente de tratare a riscurilor au fost eficiente în prevenirea sau atenuarea incidentului.

Documentaţi în mod cuprinzător constatările şi lecţiile învăţate din fiecare revizuire post-incident.

Luaţi în considerare dacă cerinţele de securitate a informaţiilor au fost îndeplinite pe parcursul gestionării unui incident de securitate cibernetică sau dacă este necesar să se ia măsuri pentru a le restabili (de exemplu, resetarea parolelor pentru accesul administrativ de urgenţă).

Efectuaţi o revizuire anuală sau o revizuire după incidente semnificative, pentru a determina dacă un incident a dus la o revizuire post-incident.

EXEMPLE DE EVIDENȚE

- Rezultatele analizei cauzelor principale pentru incidente semnificative.
- Rapoarte individuale de gestionare a incidentelor care documentează modul în care a fost gestionat fiecare incident major.
- Lecții învățate din incidentele anterioare, documentate.
- Rapoarte de revizuire post-incident care detaliază concluziile, lecțiile învățate și îmbunătățirile recomandate.
- Înregistrări ale măsurilor de analiză, rezolvare și atenuare, inclusiv comunicarea către personalul relevant.
- Evaluarea actualizată a riscurilor și planul de tratare a riscurilor care include constatările post-incident.
- Planuri sau programe pentru revizuiri ulterioare incidentelor.

Ref: Cerințe aprobate prin HG 562/2025 pct. 35, pct. 36, pct. 37

Anexe

Adiţional puteţi accesa anexele:

1. **Corelarea dintre prevederile Hotărârii Guvernului Nr. 562 din 2025 și recomandările Ghidului metodologic**

2. **Exemple de soluții tehnice open-source**