CONSILIUL DE SUPRAVEGHERE
PUBLICĂ A AUDITULUI

POLITICI
de securitate a informației

Aprobare:
Decizia Comitetului de supraveghere a auditului nr. 31 din 25.06.2026

web: www.cspa.md | email: cspa@cspa.md

Cuprins

1. Dispoziții generale

1.1. Declarația CSPA

Securitatea informațiilor în cadrul Consiliului de supraveghere publică a auditului (CSPA) reprezintă ansamblul măsurilor organizatorice, tehnice și procedurale implementate pentru a asigura confidențialitatea, integritatea și disponibilitatea informațiilor, precum și autenticitatea și trasabilitatea acestora.

Aceasta vizează protejarea tuturor resurselor informaţionale ale CSPA (date, sisteme, infrastructură IT, procese operaţionale), împotriva accesului neautorizat, pierderii, modificării sau divulgării necorespunzătoare, în conformitate cu cadrul intern de control și cerințele legale aplicabile, inclusiv statutul CSPA ca entitate critică desemnată de Agenția pentru Securitate Cibernetică (ASC).

CSPA stabileşte şi menţine obiective de securitate a informaţiilor aliniate rolului său de autoritate publică autonomă şi de administrator al Registrului public al auditorilor și al Registrului public al entităților de audit, după cum urmează:

- Asigurarea confidențialității informațiilor, prin protejarea datelor cu caracter personal ale auditorilor și entităților de audit, a deciziilor Consiliului, a corespondenței confidențiale și a altor informații sensibile pe care CSPA le gestionează, inclusiv limitarea accesului pe baza principiului "necesității de a cunoaște".
- Asigurarea integrității informațiilor, prin menținerea exactității și completitudinii Registrului public al auditorilor și al entităților de audit, a proceselor decizionale și a arhivelor, prevenind modificarea neautorizată a datelor. Înregistrările operaționale și deciziile Consiliului se păstrează pentru perioadele prevăzute de lege.
- Asigurarea disponibilității informațiilor, prin menținerea continuității operaționale și asigurarea accesului la Registrele publice, în conformitate cu cerințele legale de transparență.
- Asigurarea securității tehnice și operaționale a sistemelor, prin controlul strict al accesului la sistemele informatice care conțin Registrele publice, aplicarea principiilor de securitate cibernetică, inclusiv prin segmentarea rețelei, autentificare multifactorială și monitorizarea activităților, în conformitate cu HG 562/2025.
- Asigurarea conformității legale și de reglementare, prin respectarea Legii nr.271/2017 privind auditul situațiilor financiare, Legii nr.195/2024 privind protecția datelor cu caracter personal, Legii nr.48/2023 privind securitatea cibernetică și a Hotărârii Guvernului nr.562/2025, precum și a standardelor internaționale relevante. În calitate de entitate critică desemnată de ASC, CSPA își asumă angajamentul de a respecta și implementa integral cerințele tehnice și metodologice stabilite în Regulamentul aprobat prin HG 562/2025, inclusiv aplicarea măsurilor de securitate a rețelelor și sistemelor informatice, gestionarea riscurilor, evaluarea periodică a conformității și gestionarea incidentelor cibernetice cu impact semnificativ.

Activitățile de securitate a informațiilor în cadrul CSPA sunt ghidate de următoarele principii fundamentale:

- Abordare bazată pe risc – securitatea este dimensionată în funcție de impactul și probabilitatea riscurilor identificate;
- Responsabilitate și trasabilitate – toate acțiunile asupra sistemelor și datelor sunt atribuibile și monitorizate;
- Necesitatea de a cunoaște (need-to-know) și controlul accesului minim;
- Apărare în profunzime prin implementarea de controale în mai multe niveluri conexe;
- Separarea atribuțiilor pentru prevenirea conflictelor de interese și fraudelor;
- Continuitate și reziliență operațională, inclusiv prin mecanisme de backup și recuperare;
- Îmbunătățire continuă, bazată pe monitorizare, evaluări periodice și lecții învățate.

Conducerea CSPA își asumă responsabilitatea deplină pentru implementarea și eficacitatea securității informațiilor și se angajează să:

- asigure resursele necesare (umane, tehnice și financiare) și adecvate;
- promoveze o cultură organizațională orientată spre securitate;

- monitorizeze permanent performanța controalelor de securitate;
- sprijine procesele de control intern și extern;
- asigure îmbunătățirea continuă a domeniului securității informatice, inclusiv prin integrarea rezultatelor testelor, incidentelor și evaluărilor de risc.

CSPA stabilește clar rolurile și responsabilitățile privind securitatea informațiilor, după cum urmează:

- Comitetul de supraveghere – aprobă apoliticile de securitate elaborate de catre Consiliu;
- Organul executiv (Directorul CSPA) – asigură implementarea operațională a politicilor, aplicarea acestora]n cadrul activit[,ii Consiliului și alocarea resurselor;
- Responsabilul cu securitatea informației (Manager TIC) – coordonează și asigură implementarea Politicilor de securitate informațională;
- Funcţia de management al riscului – asigură procesul și participă la evaluarea riscurilor și monitorizează expunerile (aceste atribuții pot fi îndeplinite de Managerul TIC sau delegate);
- Toți angajații și terții – respectă politicile și regulamentul de securitate.

1.2. Introducere

Prezenta Politică stabilește cadrul de guvernanță pentru reziliența digitală a CSPA, în conformitate cu Legea nr.48/2023 privind securitatea cibernetică și HG nr.562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoare critice. Documentul răspunde necesității de a proteja datele cu caracter personal și celelalte informații sensibile gestionate de CSPA, inclusiv Registrul public al auditorilor și Registrul public al entităților de audit, contribuind totodată la consolidarea rezilienței cibernetice naționale.

Prin prezenta politică, CSPA își confirmă statutul de furnizor esenţial de servicii în sectorul critic, astfel cum a fost desemnat de către ASC în temeiul Legii nr. 48/2023 și al HG nr. 860/2024 cu privire la identificarea furnizorilor de servicii critice.

CSPA își asumă în mod expres angajamentul de a respecta și de a implementa integral cerințele tehnice și metodologice stabilite în Regulamentul cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice, aprobat prin Hotărârea Guvernului nr. 562/2025.

Angajamentul de conformare vizează în special:

- aplicarea măsurilor de securitate a rețelelor și sistemelor informatice;
- gestionarea riscurilor și evaluarea periodică a conformității;
- gestionarea incidentelor cibernetice cu impact semnificativ.

Prezenta politică de securitate a informației și toate procedurile conexe sunt elaborate, menținute și îmbunătățite continuu, în concordanță cu aceste obligații legale, reflectând angajamentul ferm al CSPA de a proteja infrastructura critică și de a contribui la consolidarea rezilienței cibernetice naționale.

1.3. Scopul și obiectivul Politicilor

Scopul prezentelor Politici este de a stabili cadrul general pentru asigurarea securității informației deținute de CSPA și protejarea resurselor informaționale aflate în gestiunea CSPA, de a minimiza riscurile TIC și a asigura continuitatea serviciilor de administrare a Registrelor publice.

Obiectivul politicii de securitate a informației este de a stabili contextul organizațional general privind securitatea informației și securității cibernetice cît și conformitatea cu cerințele HG 562/2025, în calitate de entitate critică, inclusiv gestionarea riscurilor, evaluarea periodică a conformității, raportarea incidentelor cibernetice și protejarea sistemelor informatice.

1.4. Noțiuni și abrevieri

În domeniul securității informației, în cadrul CSPA vor fi utilizate următoarele noțiuni și acronime:

Securitatea informației	păstrarea confidențialității, integrității și disponibilității informației în orice formă a sa (electronică, pe suport hârtie, etc.) și protejarea resurselor implicate la gestiunea acesteia.

Confidențialitate	proprietatea informației de a fi disponibilă doar persoanelor, entităților sau proceselor autorizate să dețină acces la ea.
Risc de securitate	probabilitatea ca un anumit eveniment se va realiza și va avea impact advers asupra confidențialității, integrității sau disponibilității informației sau a resurselor informaționale.
Integritate	proprietatea informației de a fi completă și neschimbată, proprietatea de a nu fi modificată sau alterată în mod neautorizat
Disponibilitate	proprietatea informației de a fi accesibilă și utilizabilă la cererea unei entități autorizate.
Incident de securitate a informației	un eveniment sau o serie de evenimente de securitate a informației care au o probabilitate semnificativă de a compromite activitățile CSPA și de a aduce amenințări securității informației.
Incident cibernetic	eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețelele și sistemele informatice sau accesibile prin intermediul acestora.
Sistem informațional (SI)	totalitatea sistemelor de gestiune a informației din cadrul CSPA, împreună cu resursele organizaționale asociate.
Autentificare multifactorială / MFA	un mecanism de securitate care presupune verificarea identității unui utilizator prin utilizarea a cel puțin două sau mai multe metode (factori) diferite de autentificare, înainte de a permite accesul la un sistem, aplicație sau resursă IT.
Registrul public al auditorilor	registrul gestionat de CSPA care cuprinde datele auditorilor autorizați, clasificat ca informație cu nivel ridicat de sensibilitate.
Registrul public al entităților de audit	registrul gestionat de CSPA care cuprinde datele entităților de audit autorizate, clasificat ca informație cu nivel ridicat de sensibilitate.

1.5. Domeniul de aplicare

Prezentele Politici de securitate se aplică:

a) salariaților, stagiarilor și colaboratorilor CSPA, indiferent de funcția deținută sau de locul de desfășurare a activității;

b) tuturor părților terțe, inclusiv, dar fără a se limita la: furnizorii de produse și servicii TIC, participanții care accesează resursele informaționale ale CSPA sau interacționează cu sistemele CSPA, prestatorii de servicii (mentenanță, consultanță) care desfășoară activități în incinta CSPA sau care au acces la sistemele informaționale ale CSPA

Toate părțile terțe menționate sunt obligate să respecte prezentele Politici și procedurile conexe, în măsura în care le sunt aplicabile, inclusiv notificarea imediată a incidentelor de securitate.

În conformitate cu prevederile art.22 alin.(4) din Legea nr.234/2016, serviciile TIC esențiale nu sunt externalizabile fără autorizarea prealabilă și cu menținerea integrală a responsabilității, controlului și gestionării riscurilor de către CSPA. Având în vedere dimensiunea redusă a CSPA, externalizarea unor servicii TIC poate fi luată în considerare în condițiile legii, cu menținerea responsabilității CSPA și monitorizarea strictă a conformității

1.6. Aprobarea și actualizarea Politicilor

Politicile se aprobă de Comitetul de supraveghere al CSPA și se aduc la cunoștința angajaților CSPA și părților externe interesate. Politicile intră în vigoare la data aprobării lor.

Politicile de securitate a informației vor fi revizuite anual ca rezultat al lecțiilor învățate, sau schimbării cerințelor și reglementărilor aferente aplicabile CSPA, precum și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor ori ale riscurilor.

1.7. Administrarea Politicilor

Responsabil de administrarea și actualizarea Politicii este Managerul TIC al CSPA. În activitatea sa, Managerul TIC este susținut de Consiliul de supraveghere și de Directorul CSPA, precum și de fiecare angajat al CSPA, în dependență de rolurile și atribuțiile funcționale ale acestora. Managerul TIC va monitoriza noile tendințe și abordări aplicate în domeniul securității informației și va propune modificări în vederea consolidării securității informaționale a CSPA.

1.8. Principiile politicii de securitate a informației

În scopul atingerii obiectivelor politicii de securitate în cadrul tuturor proceselor de activitate ale CSPA și aferent tuturor resurselor informaționale, se vor aplica următoarele principii:

Responsabilitatea

responsabilitatea pentru asigurarea securității informației trebuie să fie clar stabilită. Aplicarea acestui principiu semnifică și faptul că pentru toate acțiunile semnificative legate de informații și resursele , poate fi identificată în mod clar persoana responsabilă. Externalizarea serviciilor către terțe părți nu exonerează CSPA de obligațiile sale în domeniul securității informației.

Conștientizarea

toate părțile implicate trebuie să aibă acces, în limită suficientă și necesară, la principiile, standardele și normele de securitate a informației aplicabile sau disponibile, și să conștientizeze amenințările de securitate aferente domeniilor de responsabilitate proprii.

Multilateralitatea

standardele, normele, procedurile și măsurile aplicate în scopul asigurării securității informației trebuie să adreseze multilateral viziunile și necesitățile tuturor părților implicate, fiind în final corelate la obiectivele și necesitățile CSPA.

Proporționalitatea

măsurile de securitate aplicate trebuie să fie proporționale nivelului riscurilor de compromitere a securității informației.

Integrarea

standardele, normele și procedurile aferente securității informației trebuie să fie corelate la politică, integrate și coordonate reciproc. Măsurile aplicate în scopul asigurării securității informației trebuie să fie considerate în cadrul unui sistem integrat de măsuri de protecție, astfel încât în ansamblu, să asigure nivelul de securitate necesar, într-o manieră optimă.

Promptitudinea

toți cei responsabili trebuie să reacționeze în timp util și într-o manieră coordonată pentru a preveni sau a răspunde la amenințările și incidentele de securitate a informației.

Evaluarea

riscurile de compromitere a securității informației trebuie să fie periodic evaluate, în scopul asigurării corespunderii măsurilor de securitate necesităților CSPA și fundamentării deciziilor de tratare a riscurilor.

Raportarea

orice eveniment, vulnerabilitate sau incident care poate afecta securitatea activelor informaționale ale organizației trebuie să fie documentat, comunicat și escaladat corespunzător către părțile responsabile, într-un mod prompt și eficient.

1.9. Roluri și responsabilități

Membrii Comitetului de supraveghere, organul executiv și salariaţii CSPA sunt obligaţi să asigure securitatea informaţiei aflate în posesia sa şi la care au acces. Pentru realizarea obiectivului politicii de securitate în cadrul CSPA se stabilesc următoarele roluri și responsabilități:

Comitetul de supraveghere a auditului al CSPA

- aprobă Politicile de securitate a informațiilor și modificările acestora;
- aprobă Regulamentul privind securitatea informației;
- acceptă riscurile reziduale în urma evaluărilor de risc, în conformitate cu criteriile stabilite;
- este informat anual cu privire la starea securității informaționale și la rezultatele auditului independent.

Directorul CSPA

- coordonează modificările la Politici și le prezintă pentru aprobare către Comitetul de supraveghere a auditului al CSPA;
- asigură implementarea operațională a politicilor și alocarea resurselor.

Managerul TIC

- asigură elaborarea și actualizarea prezentelor Politici;
- monitorizează cerințele legislației, inclusiv noile acte normative în domeniul securității cibernetice și aplică aceste cerințe în cadrul CSPA;
- asigură elaborarea și actualizarea Regulamentului privind securitatea informației;
- coordonează implementarea politicii și standardelor de securitate, asigură înțelegerea prevederilor acestora;
- monitorizează respectarea prevederilor politicii și standardelor de securitate a informației;
- identifică deficiențele în cadrul proceselor existente și asigură înlăturarea acestora;
- organizează și implementează cerințele de securitate aferente datelor cu caracter personal, în calitate de operator de date;
- acordă și revizuiește la necesitate drepturile de acces la informație și resurse informaționale;
- acordă suport pentru desfășurarea independentă a auditului securității informației;
- raportează către ASC incidentele cibernetice cu impact semnificativ, în termenele legale;
- în calitate de entitate critică, asigură conformitatea cu cerințele HG 562/2025, inclusiv aplicarea măsurilor de securitate a rețelelor și sistemelor informatice, gestionarea riscurilor și evaluarea periodică a conformității.

Posesorul informației / resursei informaționale (pentru Registrele publice, deciziile Consiliului, arhive etc.)

- stabilește nivelul de clasificare a resurselor informaționale;
- determină cerinţele de securitate sub aspectul confidenţialităţii, integrităţii, autenticităţii şi disponibilităţii;
- participă la procesul de evaluare a riscurilor pentru resursele pe care le deține;
- aprobă măsurile de tratare a riscurilor propuse și acceptă riscurile reziduale;
- informează imediat Managerul TIC despre orice incident de securitate care afectează resursa informațională din gestiune.

Utilizatorul SI (toți angajații CSPA)

- respectă în mod necondiţionat prezenta politică de securitate și normele aferente;
- cunoaşte şi aplică regulile privind clasificarea informaţiei, controlul accesului, gestionarea parolelor, utilizarea echipamentelor TIC;
- nu divulgă parolele proprii de acces, nu le scrie pe suporturi nesigure și nu le partajează cu alte persoane;
- nu lasă stațiile de lucru nesupravegheate fără a bloca sesiunea activă;
- asigură confidențialitatea, integritatea și disponibilitatea informației la care are acces;
- participă la sesiuni de instruire și conștientizare în domeniul securității informației;
- informează imediat Managerul TIC în cazul depistării incidentelor ce ţin de securitatea informaţională;

- semnează la angajare declarația de confidențialitate.

1.10. Implementarea Politicilor

În scopul atingerii obiectivelor stabilite și implementării prevederilor Politicilor, se vor întreprinde următoarele măsuri:

Toate părțile implicate vor întreprinde consecvent măsurile necesare conform responsabilităților individuale stabilite prin prezenta politică.

Vor fi stabilite și menținute în stare actuală standardele de securitate a informației în cadrul CSPA. Respectarea standardelor este obligatorie în cadrul tuturor activităților CSPA. Excepțiile trebuie constatate și justificate în conformitate cu principiile de asigurare a securității informației din prezenta politică.

Riscurile de securitate vor fi sistematic evaluate în cadrul tuturor activităților și aferent tuturor resurselor informaționale importante ale CSPA. Planurile de tratare a riscurilor și măsurile de securitate vor fi implementate și documentate.

CSPA va efectua anual evaluarea riscurilor aferente rețelelor și sistemelor informatice. Rezultatele evaluării, incidentele semnificative și stadiul implementării măsurilor de securitate vor fi raportate periodic Comitetului de supraveghere. Măsurile de securitate implementate vor fi evaluate periodic în vederea asigurării eficacității acestora și îmbunătățirii continue a securității informației.

2. Managementul resurselor informaționale

2.1. Responsabilitatea pentru resurse

Resursele informaționale ale CSPA sunt clar identificate și sunt supuse procesului de inventariere prin intermediul Registrului de evidență a resurselor informaționale, care este actualizat în mod continuu.

Pentru toate resursele informaționale este desemnat un posesor (persoană sau subdiviziune). În cazul în care o resursă informațională este utilizată de mai multe subdiviziuni, drepturile și responsabilitățile ale posesorilor sunt definite reieșind din importanța resursei informaționale în cadrul activității subdiviziunii și necesitatea subdiviziunii de a controla resursa.

La necesitate, sunt stabilite și implementate reguli de utilizare a resurselor informaționale, iar respectarea acestora este monitorizată. Posesorul resursei informaționale poartă responsabilitate primară pentru asigurarea securității ei.

Toate activele informaționale sunt inventariate și monitorizate în mod sistematic.

2.2. Clasificarea informației

Un clasificator al informației este definit în conformitate cu necesitățile CSPA, având următoarele niveluri minime de clasificare:

Nivel de clasificare	Descriere	Exemple
Public	Informație care poate fi divulgată fără restricții, în conformitate cu legea.	Buletine informative publice, rapoarte anuale publicate.
Intern	Informație destinată uzului intern al CSPA, a cărei divulgare neautorizată poate cauza prejudicii minore.	Proceduri interne, circulare, e-mailuri interne nesensibile.

Nivel de clasificare	Descriere	Exemple
Confidențial	Informație a cărei divulgare neautorizată poate afecta interesele CSPA sau ale persoanelor vizate.	Decizii ale Consiliului în faza de proiect, corespondență confidențială, drafturi de rapoarte.
Strict confidențial	Informație cu grad ridicat de sensibilitate, a cărei divulgare neautorizată poate avea consecințe grave.	Datele nepublice din cadrul Registrului public al auditorilor și al Registrului public al entităților de audit, date cu caracter personal cu acces restricționat,, parole de acces la sisteme critice.

Responsabilitatea primară privind clasificarea informației revine posesorului informației. Informația clasificată are atașat un marcator ce indică categoria din care face parte informația.

3. Securitatea resurselor umane

3.1. Asigurarea securității la angajare

Responsabilitățile de securitate informațională pentru noii salariați sunt comunicate la etapa de angajare. Angajații potențiali sunt verificați în mod adecvat, conform procedurilor de verificare definite.

În scopul asigurării confidențialității informațiilor, la angajarea personalului sau în momentul în care angajatul urmează să dispună de acces la informații confidențiale, CSPA va aplica față de salariatul în cauză sau de membrul organului de conducere clauze de confidențialitate incluse într-un acord separat sau în contractul individual de muncă. Clauzele vor prevedea obligația angajatului/stagiarului privind păstrarea confidențialității informațiilor la care a obținut acces sau pe care le-a aflat, inclusiv pentru perioada de după încetarea activității în CSPA sau în perioada suspendării activității.
Excepție de la clauza respectivă este personalul tehnic desemnat aleatoriu de către compania locator, care asigură buna funcționare a oficiului CSPA.

3.2. Instruirea

Salariații CSPA beneficiază de instruire privind securitatea informației la un nivel adecvat pentru funcția și responsabilitățile deținute. Sunt planificate programe anuale de instruire privind prevenirea atacurilor de tip phishing, ingineria socială, igienă cibernetică.

3.3. Asigurarea securității în activitatea angajaților și terților

Cerințele de securitate a informației sunt respectate necondiționat de toți angajații/stagiarii CSPA, precum și de reprezentanții terțelor părți, în cazul în care acestea sunt autorizate să acceseze resursele informaționale ale CSPA.

La prima accesare a sistemului informațional al CSPA, utilizatorii SI sunt obligați să-și schimbe parolele setate inițial de Managerul TIC. Angajații/stagiarii și reprezentanții terțelor părți cunosc și respectă cerințele de securitate stabilite de politicile și standardele CSPA.

Parolele utilizatorilor trebuie să respecte cerințele minime de complexitate: lungime minimă de 8 caractere (sau 12 caractere dacă MFA nu este disponibil), includerea a cel puțin trei categorii de caractere (litere mari, litere mici, cifre, caractere speciale). Pentru conturile privilegiate sau cele care au acces la date sensibile (Registre publice), se recomandă parole de minimum 14-16 caractere.

3.4. Încetarea activității sau schimbarea locului de muncă

La încetarea activității sau transferul în altă funcție a utilizatorilor, drepturile de acces sunt revocate, iar resursele încredințate sunt înapoiate. Pentru utilizatorii care au deținut acces privilegiat, conturile sunt blocate, iar parolele de acces privilegiat se modifică.

4. Securitatea fizică și a mediului de lucru

4.1. Zone de securitate

Având în vedere dimensiunea redusă a CSPA, se identifică următoarele zone de securitate:

- Arhiva cu documente ce conține Registrele publice, deciziile Consiliului, documentele de personal și alte informații confidențiale, amplasată într-un spațiu securizat, cu acces restricționat doar persoanelor autorizate de conducerea CSPA.
- Zona operațională (biroul comun), unde se află serverele, echipamentele de rețea și stațiile de lucru.

Zonele de securitate sunt dotate cu mijloace adecvate de control al accesului și protejate de riscuri naturale și externe (incendii, inundații etc.).

4.2. Controlul accesului fizic

Personalul CSPA dispune de chei electronice de acces în clădirea cu oficii și cheie mecanică de acces în birou. Biroul CSPA este delimitat în zone de acces. Accesul la zona operațională și la arhivă se efectuează doar cu autorizare prealabilă. Vizitatorii nu au acces în zonele de securitate decât în prezența unui angajat CSPA. Personalul de servicii (curățenie, tehnic) va avea acces doar în prezența angajaților CSPA.

4.3. Echipamente de supraveghere

CSPA dispune de echipamente de supraveghere asigură securitatea încăperilor și care va include:

sistem de pază a accesului în încăperile CSPA;

sistem de alarmă anti-incendiară;

4.4. Securitatea echipamentelor TI

Echipamentele TI din dotarea CSPA sunt menținute și utilizate adecvat. Se interzice utilizarea echipamentului TI personal pentru gestionarea informației confidențiale care aparține CSPA, cu excepția cazurilor autorizate de Managerul TIC și cu implementarea măsurilor de securitate suplimentare (criptare, MFA). La casare, mediile de stocare sunt șterse ireversibil.

5. Gestiunea comunicațiilor și operațiunilor

5.1. Proceduri și responsabilități operaționale

Gestionarea resurselor informaționale este executată de persoane autorizate. Mediile de dezvoltare, testare și producere sunt separate pentru a reduce riscul de acces nesancționat.

5.2. Gestiunea serviciilor terților părți

Având în vedere dimensiunea redusă a CSPA, serviciile TIC (găzduire, mentenanță, suport) pot fi externalizate, dar cu păstrarea responsabilității CSPA asupra securității datelor. În cadrul acordurilor cu terțe părți sunt prevăzute măsuri adecvate de securitate, inclusiv obligația de notificare a incidentelor.

5.3. Planificarea și acceptanța sistemelor TI

Sistemele noi și modificările semnificative sunt analizate din punct de vedere al conformării cu cerințele de securitate înainte de implementare, în conformitate cu cerințele Stivei tehnologice guvernamentale și Cadrului de acceptanță.

5.4. Protecția contra softului cu potențial dăunător

Mijloace de prevenire, detectare și restabilire sunt implementate la nivelul componentelor vulnerabile. Aplicațiile antivirus rulează permanent, sunt actualizate în mod regulat și nu pot fi stopate neautorizat. Instalarea patch-urilor de securitate critice se va realiza în termen de 7 zile de la disponibilitate, iar a celor ordinare în termen de 30 zile, după testarea prealabilă.

Stațiile de lucru mobile sau cele de rezervă vor primi actualizări de securitate cel puțin o dată la 6 luni.

5.5. Copii de rezervă

Pentru informația critică (Registrele publice, deciziile Consiliului, bazele de date) sunt efectuate regulat copii de rezervă, păstrate în condiții de securitate, respectând principiul "3-2-1" (3 copii, 2 medii diferite, 1 copie off-site). Copiile de rezervă sunt testate periodic prin restaurare.

5.6. Securitatea rețelelor de comunicații electronice

Rețeaua internă este gestionată și controlată corespunzător. Pentru accesarea rețelei CSPA din exterior (lucru de la distanță) se va utiliza conexiune securizată cu autentificare.

5.7. Gestionarea suporturilor de informație

Utilizarea suporturilor mobile de informație este autorizată doar în baza necesităților de serviciu. Suporturile care circulă în afara biroului sunt criptate. Retragerea din utilizare asigură confidențialitatea datelor stocate.

5.8. Schimbul de informație

Schimbul de informație cu terțe părți (entități de audit, autorități, petenți) se realizează prin canale securizate, utilizând criptarea în cazul informațiilor confidențiale. Integrarea cu platformele guvernamentale partajate (MConnect, MPass, MSign, MLog) se face în conformitate cu Stiva tehnologică guvernamentală.

5.9. Monitorizare

Sunt asigurate jurnale de audit care înregistrează activitățile utilizatorilor, evenimentele de securitate și tentativele de acces eșuat. Jurnalele sunt păstrate pentru o perioadă de cel puțin 12 luni (sau perioada mai lungă cerută de reglementările aplicabile, de ex. 10 ani pentru înregistrările operaționale), protejate împotriva accesului neautorizat și modificărilor. Ceasurile sistemelor sunt sincronizate cu o sursă de timp precisă (NTP).

5.10. Informația publică

Publicarea informației pe site-ul CSPA se face în conformitate cu Legea privind transparența decizională și Regulamentul CSPA, asigurând integritatea informației publicate.

6. Controlul accesului la resursele informaționale

6.1 Gestionarea accesului utilizatorilor la SI

Accesul la resursele informaționale se acordă în strictă conformitate cu necesitățile de serviciu și principiul privilegiului minim. Toți utilizatorii dețin identificatori de acces unici. Parolele utilizatorilor sunt modificate periodic (cel puțin anual) și respectă cerințele minime de complexitate.

6.2 Controlul accesului la rețea

Accesul la rețea este bazat pe identificare și autentificare. Regulile de rutare a traficului sunt clar stabilite. Accesul de la distanță se face numai prin conexiuni securizate.

6.3 Controlul la sistemele de operare și mediile de virtualizare

Există proceduri care permit accesul la sistem doar utilizatorilor autorizați. Conturile privilegiate sunt utilizate exclusiv pentru administrare. Parolele de acces sunt modificate periodic (cel puțin anual) și respectă cerințele de complexitate.

6.4 Accesul la aplicații și informații

Fișierele curente de lucru se păstrează pe servere securizate sau în cloud guvernamental, nu pe stațiile de lucru locale. Pentru datele cu caracter personal, se aplică măsuri sporite de protecție, în conformitate cu Legea nr.195/2024.

6.5 Utilizarea echipamentului mobil și lucrul de la distanță

Echipamentele mobile (laptopuri) sunt criptate și protejate prin parolă puternică. Nu sunt lăsate nesupravegheate în locuri publice.
Accesările din exterior a resurselor informaționale sunt efectuate într-un mod securizat, prin autentificarea utilizatorilor SI. Locația fizică și mijloacele de accesare din care se efectuează accesarea la distanță a SI al CSPA asigură un nivel adecvat de securitate pentru echipamentele TI și informația accesată.

7. Achiziționarea, dezvoltarea și mentenanța sistemelor TI

7.1. Cerințele de securitate pentru TI

Cerințele de securitate sunt integrate în toate etapele ciclului de viață al sistemelor TI. În cadrul procesului de achiziție se aplică principiile "securitate prin proiectare" (security by design). Contractele și specificațiile tehnice pentru sistemele care prelucrează date din Registrele publice trebuie să includă cerințe de securitate explicite, inclusiv funcționalități de securitate, actualizări de securitate, testarea și validarea, suport post-implementare.

Toate sistemele informaționale noi trebuie să respecte Stiva Tehnologică Guvernamentală (STG) și Cadrul de acceptanță și guvernanță pentru sistemele informaționale de stat, în vederea asigurării interoperabilității, portabilității și sustenabilității pe termen lung.

7.2. Procesarea corectă a datelor în cadrul aplicațiilor

Aplicațiile asigură mecanisme de validare a datelor. Activitățile importante se înregistrează în jurnale de audit securizate

7.3. Securitatea fișierelor de sistem

Toate modificările aferente mediului de operare pentru sistemele de aplicații critice sunt strict controlate. Orice modificare în prealabil se testează și se autorizează de posesorul sistemului. Mediile de operare pentru sistemele de aplicații critice se izolează de alte medii, pentru a evita compromiterea securității lor în rezultatul compromiterii securității sistemelor mai puțin critice.

Accesul la codurile sursă ale aplicațiilor program este strict limitat. Fișierele de configurație ale sistemelor de aplicație se protejează corespunzător. Parolele existente în fișierele de configurație se criptează.

7.4. Securitatea în procesul de dezvoltare și suport

În cazul dezvoltării sau modificării sistemelor esențiale se vor aplica cerințe:

- dezvoltare securizată – se utilizează reguli de dezvoltare securizată (secure coding standards), care includ prevenirea vulnerabilităților comune, revizuirea codului și analiza statică/dinamică;
- separarea mediilor – mediile de dezvoltare, testare și producție sunt separate fizic sau logic, iar accesul între medii este controlat;
- testarea securității – înainte de punerea în producție, sistemele sunt supuse unor teste de securitate adecvate sistemului;
- date de testare - în cazul utilizării datelor reale pentru testare, acestea vor fi protejate conform nivelului de clasificare și, de preferință, sunt anonimizate. Utilizarea datelor cu caracter personal în testare se face cu aprobarea expresă și în condițiile legii.

Modificările aplicațiilor sunt guvernate de o procedură formală de gestionare a schimbărilor, care impun testarea și autorizarea prealabilă a oricăror intervenții în mediul de producție.

Accesul la mediul de producție și testare pentru persoanele ce participă la elaborarea sistemelor este limitat strict la persoanele autorizate.

Aplicațiile critice, în cazul modificărilor în componentele hard sau aferente mediului de operare, se testează pentru a se asigura că nu există impact negativ asupra funcționării acestora.

Elaborarea sistemelor de aplicații pentru CSPA de către terțe părți se efectuează în baza acordurilor formale între părți și CSPA, în baza unui proces documentat ce corespunde politicilor interne. Toate sistemele aplicative, dezvoltate intern sau achiziționate din exterior, sunt adecvat documentate.

8. Gestiunea incidentelor de securitate a informației

Un incident de securitate a informației este considerat cu impact semnificativ dacă îndeplinește cel puțin una dintre următoarele condiții:

- gravitatea consecințelor este determinată ca fiind cel puțin înaltă în raportul de evaluare a riscurilor;
- serviciul nu poate fi continuat după expirarea perioadei maxime admise (SLA);

- continuitatea serviciului altui furnizor esențial este perturbată;
- sunt cauzate prejudicii materiale sau nonmateriale considerabile.

În cazul producerii unui incident cibernetic cu impact semnificativ, Managerul TIC notifică ASC în termen de 24 de ore de la momentul luării la cunoștință. Notificarea inițială conține informațiile disponibile (natura incidentului, sistemele afectate, măsurile deja întreprinse).
În termen de 72 de ore de la momentul luării la cunoștință, se transmite o actualizare care include evaluarea inițială a gravității și impactului, indicatorii de compromitere (dacă sunt disponibili).
În termen de o lună de la soluționarea incidentului, se transmite un raport final cuprinzând cauzele producerii, durata, măsurile aplicate și impactul.
În cazul în care incidentul este în desfășurare la momentul transmiterii raportului final, se transmite un raport intermediar, iar raportul final se transmite în termen de o lună de la finalizarea gestionării.

În absența Managerului TIC, responsabilitatea notificării revine Directorului CSPA sau unei persoane desemnate prin procedura internă

Orice angajat care detectează un eveniment suspect sau un incident de securitate raportează imediat Managerului TIC.

Angajații sunt încurajați să raporteze și incidentele fără impact semnificativ, în scopul îmbunătățirii continue.
Managerul TIC activează procedura de răspuns la incidente, care include: limitarea (conținerea) incidentului, eradicarea cauzei, redresarea serviciilor.
Toate acțiunile sunt înregistrate în jurnalul de incident, iar dovezile sunt păstrate în condiții de securitate pentru eventuale investigații ulterioare.

După închiderea incidentului, se efectuează o analiză post-incident („lessons learned”) pentru a identifica cauza principală și a îmbunătăți măsurile de prevenire și detectare. Rezultatele sunt documentate și prezentate Consiliului de Supraveghere.

9. Continuitatea activității

9.1. Planificarea continuității activității sistemelor TI

CSPA asigură continuitatea proceselor de activitate cheie în situații de incident major. Se efectuează periodic o analiză a impactului asupra activității și se menține un plan de continuitate actualizat. Având în vedere dimensiunea redusă a CSPA, planul este proporțional cu resursele disponibile, dar acoperă cel puțin activitățile critice.

9.2. Restabilirea sistemelor TI

Sunt stabiliți indicatori pentru nivelul de continuitate (RTO, RPO, SDO). Procedurile de restabilire se testează cel puțin o dată pe an. CSPA identifică o locație alternativă de lucru sau o soluție de lucru de la distanță ca locație de rezervă în caz de indisponibilitate a biroului principal. Copiile de rezervă ale Registrelor publice și ale datelor critice sunt stocate într-o locație separată fizic de sediul CSPA.

CONSILIUL DE SUPRAVEGHERE
PUBLICĂ A AUDITULUI

PROCEDURĂ INTERNĂ
Managementul Riscurilor Cibernetice

Aprobare:
Decizia Comitetului de supraveghere a auditului nr. 31 din 25.06.2026

web: www.cspa.md | email: cspa@cspa.md

Cuprins

1. Dispoziții Generale

Prezenta procedură instituie cadrul normativ intern pentru managementul riscurilor de securitate a rețelelor și sistemelor informatice în cadrul Consiliul de supraveghere publică a auditului (CSPA). Obiectivul fundamental este asigurarea rezilienței operaționale în conformitate cu cerințele Hotărârii Guvernului nr. 562/2025.

Procedura transformă orientările din documentele normative aplicabile în norme interne cu forță juridică obligatorie. Toate departamentele și angajații CSPA au obligația de a implementa măsurile de control descrise.

1.1. Particularități arhitecturale CSPA

CSPA este o entitate critică desemnată de Agenția pentru Securitate Cibernetică (ASC), cu un efectiv redus și o infrastructură IT minimală, constând în:

- Stații de lucru și laptopuri administrative;
- Nextcloud, Zimbra pentru colaborare și stocare;
- Conexiune la internet prin rețea securizată (VPN pentru lucrul de la distanță);
- Echipamente de birou (imprimantă, switch, punct de acces WiFi, eventual NAS pentru copii de rezervă locale).

Riscurile cibernetice se concentrează pe confidențialitatea registrelor (date personale), integritatea acestora și disponibilitatea serviciilor administrative.

1.2. Domeniu de aplicare

- Toate sistemele informatice ale CSPA: stații de lucru, laptopuri, infrastructura de rețea locală, orice aplicație internă care prelucrează registrele publice.
- Toate activele informatice fizice din sediul CSPA.
- Toți angajații CSPA și colaboratorii externi cu acces la sistemele informatice ale CSPA.
- Furnizorii de servicii TIC (Microsoft, eventual furnizor de găzduire pentru registre, furnizor de suport IT).

1.3. Documente de referință

- Hotărârea Guvernului nr. 562/2025 privind securitatea rețelelor și sistemelor informatice.
- Regulamentul de Securitate Informațională CSPA.

1.4. Declanșarea procedurii și tipurile de evaluări

Aplicarea prezentei proceduri se declanșează în una dintre următoarele situații:

- evaluarea anuală planificată a riscurilor cibernetice pentru toate activele și serviciile CSPA;
- evaluarea inițială la introducerea unui activ nou, a unei aplicații noi, a unui serviciu externalizat nou sau a unei schimbări majore de arhitectură;
- reevaluarea extraordinară după producerea unui incident semnificativ, după un control/audit extern, după constatări ale BNM/ASC/CNPF sau după identificarea unei vulnerabilități critice;
- reevaluarea extraordinară după producerea unui incident semnificativ, după un control/audit extern, după constatări ale ASC sau după identificarea unei vulnerabilități critice;
- reevaluarea punctuală la solicitarea Organului executiv CSPA, a Comitetului de supraveghere CSPA sau a persoanei responsabile de conformitate.

Tipuri de evaluare utilizate: (i) evaluare completă anuală; (ii) evaluare punctuală pe activ/proces; (iii) reevaluare extraordinară după incident/control; (iv) reevaluare de confirmare după implementarea măsurilor.

1.5. Etapele procedurii de evaluare

Procesul de evaluare a riscurilor cibernetice se efectuează în mod obligatoriu în următoarele etape:

- Inițierea evaluării.

- Stabilirea echipei de evaluare (Managerul TIC și, după caz, un membru al Comitetului de supraveghere).
- Actualizarea inventarului activelor și colectarea datelor tehnice, operaționale, contractuale și de continuitate.
- Identificarea amenințărilor, vulnerabilităților, dependențelor și controalelor existente.
- Evaluarea riscului inerent, rezidual și țintă, inclusiv estimarea impactului financiar, operațional, juridic și reputațional.
- Validarea rezultatelor cu deținătorii de procese.
- Formarea planului de măsuri, estimarea resurselor necesare, stabilirea termenelor, responsabililor și dependențelor.
- Aprobarea rezultatelor de către Directorul CSPA sau Comitetului de supraveghere CSPA (pentru riscuri critice/înalte).
- Monitorizarea implementării măsurilor și reevaluarea riscurilor după implementare sau la apariția unor evenimente noi.

2. Roluri și Responsabilități

Guvernanța riscului cibernetic se bazează pe o structură clară, proporțională cu dimensiunea CSPA.

Rol / Funcție	Responsabilități principale
Comitetului de supraveghere CSPA	Aprobă politica de management al riscului și analiza anuală a riscurilor cibernetice. Aprobă apetitul la risc și pragurile de toleranță. Acceptă riscurile reziduale care depășesc pragul de toleranță (după justificare).
Directorul CSPA	Alocă resursele umane, tehnice și financiare necesare implementării controalelor. Supraveghează integrarea riscurilor cibernetice în profilul general de risc. Aprobă escaladarea imediată în cazul riscurilor critice.
Managerul TIC (poate fi o singură persoană, intern sau externalizat)	Coordonează evaluările tehnice, monitorizarea conformității și raportarea. Este punct unic de contact pentru ASC. Notifică ASC în cel mult 24 de ore de la constatarea unui incident semnificativ, conform HG 562/2025. Implementează măsurile tehnice (configurare securizare stații, MFA, backup, antivirus) și coordonează furnizorii externi (Microsoft, suport IT). Monitorizează starea controalelor tehnice (antivirus, monitorizare, jurnalizare).
Toți angajații	Respectă procedurile de securitate informațională. Raportează imediat incidentele sau anomaliile suspecte (ex. e-mail de phishing, funcționare neobișnuită). Participă obligatoriu la instruirile anuale de securitate.

2.1. Obligații de raportare și notificare

- Incidentele de securitate cibernetică cu impact semnificativ se notifică ASC în cel mult 24 de ore de la constatare, conform HG 562/2025 (notificare preliminară), cu actualizare la 72 de ore și raport final în termen de o lună.
- Orice incident care afectează confidențialitatea sau integritatea Registrelor publice (date cu caracter personal) se raportează imediat și către Autoritatea Națională de Protecție a Datelor (ANPD), conform Legii nr. 195/2024.

2.2. Colaborarea cu furnizorii externi

Pentru activele, serviciile și controalele operate de furnizori externi, evaluarea riscurilor se efectuează cu implicarea acestora acolo unde este posibil:

- Managerul TIC solicită furnizorilor informațiile necesare privind securitatea, controalele existente, RTO/RPO, incidentele relevante, rezultatele testelor de securitate;
- solicitările și răspunsurile se documentează și se păstrează ca anexă la dosarul evaluării;
- în cazul în care informația necesară nu este furnizată, Managerul TIC consemnează limitarea, aplică o ipoteză prudentă de risc și escaladează situația Directorului CSPA pentru acțiune contractuală.

3. Inventarul și Clasificarea Activelor Informatice

Inventarul activelor informatice constituie baza evaluării riscurilor. Fiecare activ este clasificat după importanță (CRITIC / RIDICAT / MEDIU / SCĂZUT), confidențialitate, integritate și disponibilitate (scala 1–5), cu indicarea parametrilor de continuitate RTO și RPO acolo unde este cazul.

Inventarul complet este menținut de Managerul TIC (de ex. în format tabelar electronic). Exemplu orientativ:

ID	Activ / Sistem	Gestionar	Importanță	Confidențialitate (1-5)	Disponibilitate (1-5)	RTO	RPO
REG-01	Registrul public al auditorilor (bază date)	CSPA / furnizor IT	CRITIC	5	5	4	24h
REG-02	Registrul public al entităților de audit	CSPA / furnizor IT	CRITIC	5	5	4	24h
SW-01	Microsoft 365 (Email, Teams, SharePoint, OneDrive)	Microsoft / CSPA	RIDICAT	4	4	4	N/A
HW-01	Stații de lucru	CSPA	MEDIU	3	3	3	N/A
HW-02	Laptopuri	CSPA	MEDIU	3	3	3	N/A
NW-01	Router / Switch / AP	CSPA	RIDICAT	2	4	4	4h
SEC-01	Soluție antivirus / EDR	CSPA	RIDICAT	2	4	4	N/A

3.1. Obligații privind inventarul

- Revizuire anuală – clasificarea activelor și metricile de continuitate se revizuiesc obligatoriu cel puțin o dată pe an.
- Actualizare la schimbare – orice modificare majoră (achiziție, retragere, schimbare de configurație) necesită actualizarea inventarului în termen de 10 zile lucrătoare.
- Stațiile de lucru cu acces la registre sau date confidențiale beneficiază de controale tehnice suplimentare (criptare disc, MFA, restricții USB).

4. Metodologia de Evaluare a Riscurilor – Matricea 5×5

Analiza riscurilor utilizează o metodologie cantitativă și calitativă cu evaluare pe trei niveluri obligatorii: INERENT, REZIDUAL și ȚINTĂ. Fiecare nivel este calculat pe baza formulei: Scor Risc = Impact (1–5) × Probabilitate (1–5).

4.1. Cele trei niveluri obligatorii de evaluare

Nivel de evaluare	Definiție
INERENT	Scorul de risc în absența oricărui control – reflectă expunerea teoretică maximă.
REZIDUAL	Scorul după aplicarea controalelor existente documentate (MFA, antivirus, backup, proceduri). Reprezintă riscul actual al CSPA.
ȚINTĂ	Scorul estimat după implementarea tuturor măsurilor suplimentare propuse în planul de acțiuni. Apetitul CSPA: SCĂZUT = tolerabil; MEDIU și superior = intolerabil.

4.2. Scara de impact și probabilitate

Impact (I): 1 = Minor, 2 = Mediu, 3 = Major, 4 = Grav, 5 = Dramatic.

Probabilitate (P): 1 = Aproape imposibil, 2 = Puțin posibil, 3 = Posibil, 4 = Foarte posibil, 5 = Cert.

4.3. Matricea de risc (Impact × Probabilitate)

Prob. \ Impact	I=5 Dramatic	I=4 Grav	I=3 Major	I=2 Mediu	I=1 Minor
P=5 Cert (aproape sigur)	S=25 CRITIC	S=20 CRITIC	S=15 ÎNALT	S=10 ÎNALT	S=5 MEDIU
P=4 Foarte posibil	S=20 CRITIC	S=16 CRITIC	S=12 ÎNALT	S=8 SEMNIFICATIV	S=4 MEDIU
P=3 Posibil	S=15 ÎNALT	S=12 ÎNALT	S=9 SEMNIFICATIV	S=6 MEDIU	S=3 SCĂZUT
P=2 Puțin posibil	S=10 ÎNALT	S=8 SEMNIFICATIV	S=6 MEDIU	S=4 MEDIU	S=2 SCĂZUT
P=1 Aproape imposibil	S=5 MEDIU	S=4 MEDIU	S=3 SCĂZUT	S=2 SCĂZUT	S=1 SCĂZUT

4.4. Nivelurile de risc și acțiunile corespunzătoare

Nivel risc / Scor	Acțiune necesară
CRITIC ≥ 16	Tratare imediată – intolerabil; escaladare Director + Manager TIC
ÎNALT 10–15	Plan de acțiuni cu termene clare; monitorizare lunară
SEMNIFICATIV 8–9	Intolerabil – tratare planificată în 6–9 luni; monitorizare trimestrială
MEDIU 4–7	Intolerabil – tratare planificată în 9–12 luni; monitorizare trimestrială
SCĂZUT 1–3	Tolerabil – monitorizare anuală; asumare risc rezidual documentată

Conform apetitului de risc CSPA: nivelul SCĂZUT este tolerabil; orice risc MEDIU și superior este intolerabil și necesită tratare, transfer sau monitorizare controlată.

4.5. Procedura operațională de evaluare

Pentru fiecare exercițiu de evaluare se întocmește un dosar de analiză care trebuie să conțină cel puțin: inventarul activelor analizate, lista amenințărilor și vulnerabilităților relevante, descrierea controalelor existente, foile de calcul ale riscurilor, ipotezele utilizate și concluziile echipei.

Pentru fiecare risc se descriu: scenariul de amenințare, activele afectate, cauza/vulnerabilitatea, controalele existente, scorul inerent, scorul rezidual, scorul țintă și măsurile propuse.

4.6. Periodicitatea și reevaluarea extraordinară

Periodicitatea minimă și termenii de reacție sunt următorii:

- evaluarea completă – cel puțin o dată pe an;
- reevaluarea punctuală – înainte de punerea în producție a unui sistem nou sau a unei schimbări majore;
- reevaluarea extraordinară – inițiată în maximum 10 zile lucrătoare după producerea unui incident semnificativ, după constatarea unei vulnerabilități critice, după control/audit extern sau după emiterea unor recomandări de către ASC;
- reevaluarea de confirmare – în termen de maximum 30 zile lucrătoare după implementarea unei măsuri majore ori după finalizarea unui proiect de remediere.

Reevaluarea extraordinară poate fi țintită (doar pentru activele/procesele afectate) sau completă, dacă evenimentul relevă o deficiență sistemică sau o schimbare majoră de profil de risc.

4.7. Validarea și aprobarea rezultatelor

Rezultatele evaluării sunt validate de deținătorii de procese și de Managerul TIC. Riscurile MEDIU și superior se prezintă Directorului CSPA și, după caz, Comitetului de supraveghere a CSPA, împreună cu planul de tratare și resursele estimate.

5. Calculul Impactului Financiar pe Componente

Calculul impactului financiar este obligatoriu pentru orice risc identificat cu scor rezidual ≥ 4 (MEDIU sau superior). Expunerea totală estimată se calculează ca sumă a celor patru componente:

- Impact Operațional Direct – pierderi din indisponibilitatea sistemelor (ore de muncă pierdute, întârzieri în procesarea cererilor, costuri de oportunitate).
- Amenzi și Sancțiuni – penalități de reglementare estimate conform HG 562/2025, Legii 195/2024 (GDPR) și reglementărilor ASC.
- Costuri de Recuperare – investigarea incidentului, restaurarea din backup, ore suplimentare, consultanți IT, notificări obligatorii.
- Pierderi Reputaționale – costul pierderii încrederii în capacitatea CSPA de a proteja datele personale ale auditorilor și entităților de audit.

Se vor evalua explicit și riscurile reziduale provenite de la furnizorii de servicii TIC (TPRM – Third Party Risk Management), în special dependența de Microsoft 365 și de eventualii furnizori de găzduire a registrelor.

6. Clasificarea Pragurilor de Expunere Financiară

Severitatea financiară a riscului se raportează la pragurile de mai jos, exprimate în MDL (adaptate la bugetul modest al CSPA):

Nivel Expunere Financiară	Prag (MDL)
Dramatică	**> 500.000 MDL**
Gravă	**200.001 – 500.000 MDL**
Majoră	**50.001 – 200.000 MDL**
Medie	**10.001 – 50.000 MDL**
Minoră	**≤ 10.000 MDL**

7. Criterii de Acceptare a Riscului și Apetitul la Risc

Apetitul la risc al CSPA este conservator, axat pe protecția datelor cu caracter personal și pe asigurarea continuității activității minime.

7.1. Regula fundamentală de acceptare

Sunt acceptate implicit doar riscurile clasificate ca SCĂZUTE (Scor 1–3) cu o expunere financiară de nivel Minor (≤ 10.000 MDL). Orice risc cu scor ≥ 4 (MEDIU și superior) este intolerabil.

Nivel risc	Scor	Decizie
SCĂZUT	1–3	Tolerabil – acceptare documentată; monitorizare anuală
MEDIU	4–7	Intolerabil – tratare obligatorie sau transfer; nu poate fi acceptat fără aprobare scrisă Comitetului de supraveghere
SEMNIFICATIV	8–9	Intolerabil – tratare planificată în max. 6–9 luni; monitorizare trimestrială
ÎNALT	10–15	Intolerabil – plan de acțiuni cu termene clare; monitorizare lunară
CRITIC	≥ 16	Intolerabil – tratare imediată; escaladare Director + Manager TIC

7.2. Procesul de acceptare excepțională

- Riscurile cu scor rezidual ≥ 4 nu pot fi acceptate implicit.
- În cazuri excepționale documentate, acceptarea unui risc rezidual MEDIU se poate face exclusiv prin aprobarea scrisă a Comitetului de supraveghere, cu precizarea justificării și a termenului de reevaluare.
- Riscurile SEMNIFICATIVE, ÎNALTE și CRITICE nu pot fi acceptate – necesită obligatoriu tratare sau transfer.
- Toate deciziile de acceptare excepțională se consemnează în Registrul Riscurilor și se raportează ASC, conform cerințelor HG 562/2025.

8. Planul de Tratare a Riscurilor – Priorități P1–P4

Tratarea riscurilor este structurată pe 4 niveluri de prioritate, bazate pe analiza cost-beneficiu. Riscurile de nivel MEDIU, SEMNIFICATIV, ÎNALT și CRITIC sunt intolerabile.

8.1. Cadrul de priorități

Prioritate	Tip acțiune	Termen orientativ
P1 – URGENTE	Măsuri organizatorice și procedurale, configurații tehnice cost-zero (ex. activare MFA, revizuire drepturi acces, actualizare antivirus).	**Q1–Q4 202_**
P2 – INVESTIȚII MODERATE	Achiziții hardware/software (ex. licențe suplimentare, upgrade soluții backup, echipamente de rețea).	**Q1–Q4 202_**
P3 – ACȚIUNI CONTRACTUALE	Negociere clauze de securitate cu furnizorii (Microsoft, suport IT, găzduire).	**Q1–Q4 202_**
P4 – TRANSFER / MONITORIZARE	Transfer risc; monitorizare controlată prin controale compensatorii.	**Q4 202_ / Continuu**

8.2. Opțiunile de tratare permise

- **DIMINUARE (Atenuare)** – aplicarea de controale tehnice suplimentare (ex. criptare disc, backup off-site, restricții USB, politici de parole).
- **EVITARE** – eliminarea procesului sau activității care generează riscul (ex. renunțarea la stocarea locală a registrelor în favoarea cloud guvernamental securizat).
- **TRANSFER** – externalizarea riscului prin clauze contractuale cu furnizorii (SLA pentru disponibilitate, confidențialitate).
- **ACCEPTARE** – doar pentru riscuri SCĂZUTE sau cu aprobare explicită a Comitetului de supraveghere lui CSPA conform secțiunii 7.
- **MONITORIZARE CONTROLATĂ** – aplicarea controalelor compensatorii și reevaluarea periodică (pentru riscuri cu soluții tehnice limitate).

8.3. Principii de implementare

Toate acțiunile cu cost zero (organizatorice și procedurale) se implementează prioritar.

Termenele asumate în planul de acțiuni sunt monitorizate de Managerul TIC și raportate Directorului CSPA.

Orice măsură suplimentară implementată se documentează cu data finalizării și se actualizează în Registrul Riscurilor.

8.4. Formarea planului de măsuri

Pentru fiecare risc intolerabil se întocmește o fișă de măsură care include:

- descrierea măsurii și riscurile vizate;
- tipul măsurii (organizatorică, tehnică, contractuală, de instruire);

- responsabilul de implementare;
- termenul de implementare și dependențele;
- estimarea costului (CAPEX/OPEX);
- scorul rezidual estimat după implementare.

Planul de măsuri se consolidează anual de Managerul TIC și se actualizează la fiecare reevaluare.

8.5. Măsurile care necesită finanțare

Pentru măsurile care necesită finanțare:

- Managerul TIC întocmește o notă de fundamentare (risc, justificare, cost, efect asupra scorului, urgență).
- Măsurile cu impact bugetar se propun pentru includere în proiectul de buget sau în rectificări.
- În lipsa finanțării aprobate, riscul nu se consideră tratat; se aplică măsuri compensatorii, se documentează motivul amânării și se stabilește termen de reevaluare.

9. Monitorizarea Conformității și Revizuirea Procedurii

9.1. Raportare periodică

Managerul TIC prezintă Directorului CSPA un raport de conformitate cu starea riscurilor reziduale, progresul planului de acțiuni și jurnalele de excepții.

Monitorizarea tehnică a controalelor (antivirus, jurnalizare, backup, actualizări) se efectuează continuu de Managerul TIC.

Progresul măsurilor se verifică trimestrial pentru riscurile MEDIU/SEMNIFICATIV și lunar pentru riscurile ÎNALT/CRITIC.

9.2. Frecvența revizuirii

Analiza Riscurilor Cibernetice este revizuită anuală sau după orice incident semnificativ.

Prezenta Procedură Internă este revizuită la fiecare 2 ani sau în urma oricărei modificări semnificative a peisajului amenințărilor, a cadrului normativ sau a arhitecturii IT a CSPA.

Inventarul activelor – actualizat la orice modificare majoră și revizuit anual.

9.3. Instruire și conștientizare

Toți angajații CSPA participă anual la instruiri de conștientizare a securității cibernetice, cu focus pe:

- identificarea e-mailurilor de phishing și a tehnicilor de inginerie socială;
- procedura de raportare a incidentelor;
- manipularea securizată a datelor cu caracter personal;
- utilizarea corectă a MFA și a parolelor puternice.

Angajații cu acces privilegiat la registre (operatori) beneficiază de instruiri suplimentare și de controale tehnice întărite.

9.4. Reevaluări repetate în urma incidentelor, controalelor și schimbărilor

În cazul producerii unui incident, al unei constatări de audit/control sau al unei schimbări majore, evaluarea riscurilor se reia după următoarea regulă practică:

- După incident semnificativ – reevaluare țintită a activelor și controalelor afectate, corelată cu analiza post-incident.
- După constatări ale ASC, auditului intern sau extern – fiecare constatare se transpune într-un risc nou sau actualizarea unui risc existent, cu plan de măsuri.

- După schimbări tehnologice sau contractuale (ex. migrare în cloud, schimbare furnizor) – reevaluare înainte de punerea în exploatare.
- După implementarea măsurilor – reevaluare de eficacitate pentru a confirma reducerea scorului rezidual la nivelul țintă.

9.5. Evidențe și arhivare

Toate evaluările, reevaluările, corespondența cu furnizorii și ASC, foile de calcul, planurile de măsuri, aprobările și dovezile de implementare se păstrează în dosarul evaluării (format electronic) timp de minimum 5 ani, pentru a putea fi prezentate la cererea conducerii, a auditorilor sau a ASC

10. Anexe

Anexa 1. Lista orientativă a amenințărilor relevante pentru CSPA

Lista de mai jos se utilizează ca bază minimă la identificarea riscurilor și la justificarea măsurilor de securitate selectate pentru implementarea HG nr. 562/2025. Echipa de evaluare poate adăuga amenințări suplimentare în funcție de schimbările de arhitectură, servicii, incidente și controale externe.

Categoria amenințării	Exemple pentru CSPA	Active / procese afectate	Justificarea relevanței
Compromiterea identității și accesului	furt de credențiale, phishing, abuz de cont privilegiat, bypass MFA	Microsoft, VPN, conturi de acces la registre	CSPA procesează date personale; accesul neautorizat poate duce la divulgare sau modificare.
Malware / ransomware	criptarea fișierelor, troieni	Stații de lucru, fișiere de serviciu	Poate bloca activitatea administrativă și accesul la registre.
Indisponibilitatea infrastructurii externalizate	cădere internet, indisponibilitate cloud găzduire registre	Registre publice, email, colaborare	Dependența de furnizori externi; necesită planuri de continuitate.
Defecțiuni de rețea și comunicații	cădere VPN, întrerupere internet, defecțiune echipamente rețea locală	Acces la sisteme, comunicare cu participanții, lucru de la distanță	Afectează disponibilitatea serviciilor CSPA.
Vulnerabilități și patching insuficient	sisteme neactualizate, firmware vulnerabil, biblioteci compromise	Stații, aplicații, echipamente de rețea	HG 562/2025 impune patch management; risc de exploatare.
Schimbări necontrolate / erori de configurare	configurări greșite, release fără testare, modificări neautorizate	Aplicații, reguli firewall, permisiuni acces	Poate produce indisponibilitate sau breșe de securitate.
Exfiltrare / divulgare neautorizată	email greșit, upload neautorizat, print, USB personal	Date deținători registre, documente	CSPA trebuie să prevină scurgerile de date personale.
Erori umane și insider threat	operare greșită, nerespectare proceduri, conflict de interese	Operațiuni în registre, administrare acces	Modelul operațional presupune intervenție umană; necesită segregare atribuții.
Compromiterea backup-ului sau restaurării	backup incomplet, restaurare nereușită, copii nevalidate	Date operaționale, fișiere de serviciu	Fără backup valid, RTO/RPO nu pot fi respectate.
Furnizori și supply-chain	incident la Microsoft, la furnizorul de găzduire, actualizări compromise	Toate serviciile externalizate	HG 562/2025 cere gestionarea riscurilor lanțului de aprovizionare.
Securitate fizică și utilități	incendiu, lipsă energie, acces neautorizat în sediu	Sediu CSPA, stații, documente pe hârtie	Afectează atât activitatea, cât și protecția informațiilor.
Evenimente externe / dezastre	cutremur, inundație, indisponibilitate clădire	Sediu CSPA, personal	Necesită BIA și plan de continuitate (ex. lucru de la distanță).
Compromiterea identității și accesului	furt de credențiale, phishing, abuz de cont privilegiat, bypass MFA	Microsoft, VPN, conturi de acces la registre	CSPA procesează date personale; accesul neautorizat poate duce la divulgare sau modificare.
Malware / ransomware	criptarea fișierelor, troieni	Stații de lucru, fișiere de serviciu	Poate bloca activitatea administrativă și accesul la registre.

Anexa 2. Justificarea selecției măsurilor din HG nr. 562/2025

Selecția măsurilor de securitate se justifică pe baza unei analize documentate a riscurilor și a caracteristicilor operaționale ale CSPA, după următoarele principii obligatorii:

- corelarea măsurii cu activele critice, procesele esențiale, cerințele de continuitate și obligațiile legale ale CSPA;

- corelarea măsurii cu amenințările și vulnerabilitățile identificate în Anexa 1 și în evaluarea curentă a riscurilor;
- analiza proporționalității: expunerea la risc, probabilitatea, impactul financiar/operațional/reputațional și fezabilitatea măsurii;
- luarea în considerare a externalizării serviciilor, inclusiv a controalelor deja existente la furnizor și a limitelor de control direct ale CSPA;
- preluarea constatărilor din incidente, audituri și controale externe, inclusiv recomandările ASC;
- prioritizarea măsurilor care reduc riscurile intolerabile, în special pe confidențialitate, integritate, acces privilegiat, backup/recuperare, jurnalizare și gestionarea furnizorilor

Pentru fiecare măsură selectată din HG nr. 562/2025, echipa de evaluare va documenta cel puțin: cerința HG, riscul/amenințarea tratată, activul/procesul vizat, justificarea aplicării sau neaplicării, măsura alternativă (dacă există), responsabilul, termenul, costul estimat și dovada implementării. Această documentare servește drept bază pentru Documentul de Aplicabilitate (SoA) și pentru raportările către ASC.

CONSILIUL DE SUPRAVEGHERE
PUBLICĂ A AUDITULUI

ANALIZA
riscurilor cibernetice

Aprobare:
Decizia Comitetului de supraveghere a auditului nr. 31 din 25.06.2026

web: www.cspa.md | email: cspa@cspa.md

Cuprins

1. Sinteză

Prezenta analiză consolidează identificarea, evaluarea și planul de tratare a riscurilor de securitate cibernetică pentru Consiliul de supraveghere publică a auditului, în calitate de entitate critică desemnată de către Agenția pentru Securitate Cibernetică. Evaluarea a acoperit toate activele informaționale, infrastructura IT, procesele operaționale și dependențele externe, utilizând metodologia matricei 5×5 (Impact × Probabilitate). Riscurile au fost evaluate pe trei niveluri obligatorii — INERENT, REZIDUAL și ȚINTĂ — asigurând trasabilitatea completă de la starea brută la obiectivul de securitate asumat.

Principalele constatări

Registrele publice naționale — sunt stocate în fișiere pe calculator, fără backup automatizat. Compromiterea, modificarea neautorizată — inclusiv prin eroare umană accidentală — sau pierderea acestora ar afecta direct sistemul de audit.

Absența unui Domain Controller face imposibilă aplicarea centralizată a politicilor de securitate: gestionare parole, revocare acces, patch management, criptare, audit log centralizat.

Routerul MikroTik administrat exclusiv de Moldtelecom — CSPA nu are vizibilitate sau control asupra perimetrului de rețea propriu. Emailul instituțional administrat de STISC.

Condițiile actuale sunt optime pentru un atac ransomware cu impact catastrofal și ireversibil: date critice în fișiere neprotejate, email expus la phishing, router fără control CSPA, fără EDR și fără backup funcțional testat.

Există neconformități clare cu HG 562/2025, care pot atrage sancțiuni administrative, amenzi și răspundere juridică a conducerii. CSPA nu dispune de plan de continuitate (BCP/DRP) și nici de proceduri de răspuns la incidente — obligații legale exprese pentru entitățile critice.

Absența oricărei colectări centralizate a jurnalelor de securitate (SIEM) face imposibilă detectarea incidentelor înainte de producerea efectelor vizibile și îngreunează respectarea obligației legale de raportare la ASC în termen de 24 de ore.

Rezultatele evaluării

Au fost identificate 24 de riscuri, dintre care 3 sunt CRITICE (scor ≥ 16), 14 sunt ÎNALTE (scor 10–15) și 7 sunt SEMNIFICATIVE (scor 8–9). Niciun risc nu se află în zona tolerabilă.

Riscurile critice vizează pierderea ireversibilă a Registrelor publice (R-REG-01, S=20), atacurile de phishing vizând angajații (R-EMAIL-01, S=16) și neconformitatea cu cerințele legale aplicabile entităților critice (R-CONF-01, S=16).

Riscul identificat R-LOG-01 (absența jurnalizării centralizate / SIEM, S=12 ÎNALT) evidențiază incapacitatea actuală de a detecta incidentele de securitate înainte de producerea efectelor vizibile, cu implicații directe asupra obligației legale de raportare la ASC în termen de 24 de ore. Implementarea Wazuh SIEM reduce scorul țintă la S=4.

Recomandări și buget

Planul de acțiuni este structurat pe patru priorități (P1–P4). Majoritatea măsurilor din Prioritatea 1 nu necesită costuri suplimentare (ex. activare BitLocker, configurare Windows Firewall, elaborare proceduri).

Bugetul total estimat pentru implementarea integrală a planului este de aproximativ ~77.000 MDL/an + ~127.500 MDL unic (+ 50.000–120.000 MDL opțional pentru audit extern independent).

2. Dispoziții generale

Prezenta analiză este elaborată în temeiul Hotărârii Guvernului nr. 562/2025 privind cerințele de securitate cibernetică pentru entitățile din sectoarele critice, ca urmare a desemnării a Consiliului de supraveghere publică a auditului (CSPA) ca entitate critică de către Agenția pentru Securitate Cibernetică a Republicii Moldova.

Metodologia de evaluare aplică standardele internaționale, utilizând o matrice de risc 5×5 (Impact × Probabilitate).

Profilul CSPA:

Instituție	I.P. Consiliul de Supraveghere Publică a Auditului (CSPA)
Statut juridic	Instituție Publică autonomă cu statut de persoană juridică
Sediu	str. Mitropolit Gavriil Banulescu-Bodoni 57/1, et.4, MD-2005 Chișinău
Funcții principale	Certificare auditori · Înregistrare entități de audit · Control calitate · Supraveghere stagiari
Active critice	Registrul public al auditorilor · Registrul public al entităților de audit · Dosare certificare · Date personale auditori/stagiari
Desemnare ASC	Entitate critică — sector: servicii financiare / reglementare audit național
Email instituțional	Administrat de STISC (externalizat)
Internet	Moldtelecom — router Mikrotik (fără acces de administrare pentru CSPA)
Infrastructură AD	Fără Domain Controller — stații autonome cu conturi locale
Stocare Registre	Fișiere Word/Excel pe calculator (fără bază de date, fără backup automatizat)

Metodologia de evaluare

Riscurile sunt evaluate pe o scală 1–5 pentru Impact și 1–5 pentru Probabilitate, rezultând un Scor de Risc = I × P (max 25). Evaluarea se realizează obligatoriu pe trei niveluri: INERENT (fără niciun control), REZIDUAL (după controalele existente) și ȚINTĂ (după implementarea tuturor măsurilor propuse).

Nivel Risc	Scor I×P	Tolerabilitate	Acțiune necesară
CRITIC	≥ 16	INTOLERABIL	Tratare imediată
ÎNALT	10–15	INTOLERABIL	Plan de acțiuni cu termene clare ≤ 90 zile
SEMNIFICATIV	8–9	INTOLERABIL	Tratare planificată ≤ 6–9 luni; monitorizare trimestrială
MEDIU	4–7	INTOLERABIL	Tratare planificată ≤ 12 luni; monitorizare trimestrială
SCĂZUT	1–3	TOLERABIL	Acceptare documentată; monitorizare anuală

Apetitul de risc al CSPA

Consiliul de supraveghere publică a auditului (CSPA), în calitate de entitate critică desemnată de Agenția pentru Securitate Cibernetică, își asumă următorul apetit de risc pentru securitatea cibernetică:

1. Toleranță zero pentru pierderea, coruperea sau indisponibilitatea ireversibilă a Registrului public al auditorilor și a Registrului public al entităților de audit. Orice risc care poate duce la distrugerea sau inaccesibilitatea acestor registre este considerat intolerabil și necesită tratare imediată, indiferent de cost.

2. Toleranță foarte scăzută pentru modificările neautorizate sau frauduloase ale datelor din registrele publice, precum și pentru încălcarea confidențialității datelor cu caracter personal ale auditorilor și stagiarilor.

3. Toleranță scăzută pentru neconformitatea cu cerințele legale aplicabile entităților critice (HG 562/2025). CSPA nu acceptă riscuri care pot atrage sancțiuni administrative, amenzi sau răspunderea juridică a conducerii.

4. Toleranță moderată pentru întreruperile temporare de servicii necritice (ex. website, comunicare neoficială), cu condiția ca acestea să nu afecteze îndeplinirea obligațiilor legale de bază și să fie remediate în termen de 48 de ore.

5. Orice risc evaluat ca SEMNIFICATIV (scor 8–9), ÎNALT (10–15) sau CRITIC (≥16) este considerat intolerabil și necesită tratare. Acceptarea formală a unui risc se poate face doar pentru riscuri SCĂZUTE (scor 1–3) și numai cu aprobarea scrisă a Directorului CSPA.

Prezentul apetit de risc este aprobat de conducerea CSPA și va fi revizuit anual sau ori de câte ori intervin modificări semnificative în infrastructură, cadrul legal sau misiunea instituției.

3. Inventarul activelor informatice

Identificarea și clasificarea activelor informaționale reprezintă primul pas obligatoriu în analiza riscurilor cibernetice. Registrul de mai jos prezintă activele CSPA cu clasificarea criticalității, locația de stocare și vulnerabilitatea principală identificată.

ID	Activ informațional	Tip	Locație stocare	Criticalitate	Vulnerabilitate principală
A1	**Registrul public al auditorilor**	Date critice	PC	**CRITICĂ**	SPOF, fără backup, fără control acces, fără audit trail
A2	**Registrul public al entităților de audit**	Date critice	Word/Excel pe PC angajat	**CRITICĂ**	SPOF, fără backup, fără control acces, fără audit trail
A3	Infrastructura de rețea (MikroTik + Moldtelecom)	Infrastructură	Fizic în sediu	**CRITICĂ**	Zero vizibilitate și control configurație; CVE Mikrotik nepatchate
A4	Serviciul de poștă electronică (@cspa.md)	Serviciu extern	Administrat de STISC	**ÎNALTĂ**	Dependență externă, fără MFA, fără vizibilitate anti-phishing
A5	Calculatoarele angajaților (8 stații de lucru)	Endpoint	Fizic în sediu	**ÎNALTĂ**	Fără politici centralizate, patch management absent, USB necontrolat
A6	Documente administrative și corespondență oficială	Date operaționale	Local pe PC-uri	**ÎNALTĂ**	Fără backup centralizat, fără clasificare, fără versioning
A7	Pagina web CSPA	Serviciu public	Găzduit extern	**ÎNALTĂ**	CMS posibil neactualizat
A8	Date cu caracter personal ale auditorilor și stagiarilor	Date personale	Incluse în registrele A1, A2	**CRITICĂ**	Expunere necontrolată; fără criptare

4. Registrul riscurilor

Evaluare la nivel REZIDUAL (după controalele existente). Toate riscurile cu nivel SEMNIFICATIV și superior sunt INTOLERABILE conform apetitului de risc al entității critice. Scor Risc = Impact × Probabilitate (max 25).

REGISTRE CRITICE

ID	Categorie / Amenințare	Vulnerabilitate principală	I Rez	P Rez	S Rez	S In	S Țintă	Nivel	Decizie tratare	Expunere Fin. (MDL)	Prio-ritate
R-REG-01	Pierdere permanentă sau corupere a Registrului public al auditorilor	Stocat pe un singur calculator; fără backup automatizat; fără bază de date; defect disc, ransomware sau ștergere accidentală = pierdere ireversibilă	**5**	**4**	**20**	**25**	**3**	**CRITIC**	**DIMINUARE URGENTĂ**	~850.000 MDL	**P1**
R-REG-02	Modificare neautorizată sau frauduloasă a datelor din Registrul entităților de audit	Fișierul Excel/Word nu are audit trail sau autentificare; orice utilizator cu acces poate modifica fără urmă — inclusiv prin eroare umană accidentală (suprascriere, ștergere greșită, tastare eronată), la fel de probabilă ca modificarea intenționată sau frauduloasă	5	3	**15**	**20**	**4**	**ÎNALT**	**DIMINUARE URGENTĂ**	~280.000 MDL	**P1**
R-REG-03	Acces neautorizat la date cu caracter personal din registre	Fișiere locale fără criptare; fără politică de clasificare; posibil transmis prin email necriptat; GDPR/Legea 133/2011	4	3	**12**	**16**	**3**	**ÎNALT**	DIMINUARE	~170.000 MDL	**P1**

INFRASTRUCTURĂ REȚEA

ID	Categorie / Amenințare	Vulnerabilitate principală	I Rez	P Rez	S Rez	S In	S Țintă	Nivel	Decizie tratare	Expunere Fin. (MDL)	Prio-ritate
R-NET-01	Compromiterea routerului Mikrotik de un actor extern	Administrat exclusiv de Moldtelecom; CSPA fără vizibilitate, fără patch-uri, fără firewall propriu; CVE în RouterOS exploatate activ de grupări APT	5	3	**15**	**20**	**8**	**ÎNALT**	DIMINUARE + TRANSFER	~120.000 MDL	**P2**
R-NET-02	Interceptarea traficului de rețea intern (MITM/sniffing)	Absența DC înseamnă fără politici centralizate; autentificare locală pe fiecare stație; trafic intern posibil necriptat; fără segmentare VLAN	4	2	**8**	**12**	**3**	**SEMNIFICATIV**	DIMINUARE	~35.000 MDL	**P2**
R-NET-03	Atac DDoS sau întrerupere serviciu internet (unicul ISP)	Un singur furnizor ISP (Moldtelecom) fără redundanță; întreruperea blochează emailul (STISC), servicii cloud și comunicarea externă	3	3	**9**	**12**	**6**	**SEMNIFICATIV**	DIMINUARE	~25.000 MDL	**P3**

EMAIL ȘI COMUNICAȚII

ID	Categorie / Amenințare	Vulnerabilitate principală	I Rez	P Rez	S Rez	S In	S Țintă	Nivel	Decizie tratare	Expunere Fin. (MDL)	Prio-ritate
R-EMAIL-01	Phishing/spear-phishing vizând angajații CSPA	Email administrat de STISC — CSPA nu controlează setările anti-spam, DMARC, DKIM, SPF;	4	4	**16**	**20**	**6**	**CRITIC**	**DIMINUARE URGENTĂ**	~350.000 MDL	**P1**
R-EMAIL-02	Compromiterea contului de email prin parole slabe sau refolosite	Fără DC → fără politică centralizată de parole; fără MFA impus; angajații pot folosi parole identice pe servicii personale și profesionale	4	3	**12**	**16**	**3**	**ÎNALT**	DIMINUARE	~85.000 MDL	**P1**
R-EMAIL-03	Transmitere accidentală a informațiilor confidențiale prin email necriptat	Nu există DLP; angajații pot trimite fișierele cu date personale ale auditorilor direct prin email; STISC administrează serverul fără vizibilitate DLP pentru CSPA	3	3	**9**	**12**	**4**	**SEMNIFICATIV**	DIMINUARE	~45.000 MDL	**P3**

STAȚII DE LUCRU (ENDPOINT)

ID	Categorie / Amenințare	Vulnerabilitate principală	I Rez	P Rez	S Rez	S In	S Țintă	Nivel	Decizie tratare	Expunere Fin. (MDL)	Prio-ritate
R-EP-01	Infectare cu ransomware — Registrele ca țintă primară	Registrele sunt pe stații locale; fără GPO de restricționare execuție; combinație ideală: fișiere Office neprotejate, fără DC, email expus la phishing, router fără control; țintă prioritară pentru actori APT	5	3	**15**	**20**	**4**	**ÎNALT**	**DIMINUARE URGENTĂ**	~420.000 MDL	**P2**
R-EP-02	Furt sau pierdere calculator cu Registrele (singurul punct de stocare)	Registrele sunt pe un singur calculator; furtul fizic = pierderea totală a Registrelor publice naționale; fără criptare disc → datele accesibile imediat	5	2	**10**	**15**	**4**	**ÎNALT**	DIMINUARE	~380.000 MDL	**P1**
R-EP-03	Sistem de operare/aplicații neactualizate cu vulnerabilități CVE critice	Fără DC → fără WSUS/patch management centralizat; actualizările depind de fiecare angajat; stații cu Windows vechi = vectori de atac prin documente malițioase	4	3	**12**	**16**	**3**	**ÎNALT**	DIMINUARE	~95.000 MDL	**P2**
R-EP-04	Utilizare dispozitive USB externe necontrolate pe stațiile cu Registre	Fără DC → fără GPO de restricționare USB; angajații pot conecta USB-uri personale cu malware; exfiltrare date prin USB imposibil de detectat	3	3	**9**	**12**	**2**	**SEMNIFICATIV**	DIMINUARE	~30.000 MDL	**P2**

IDENTITATE ȘI ACCES (IAM) + AMENINȚARE INTERNĂ

ID	Categorie / Amenințare	Vulnerabilitate principală	I Rez	P Rez	S Rez	S In	S Țintă	Nivel	Decizie tratare	Expunere Fin. (MDL)	Prio-ritate
R-IAM-01	Absența autentificării centralizate — imposibil revocat accesul angajat plecat	Fără DC, fiecare stație are conturi locale independente; la plecarea angajatului cu acces la Registre, contul rămâne activ; fără audit log centralizat al activităților	4	3	**12**	**16**	**3**	**ÎNALT**	DIMINUARE	~75.000 MDL	**P2**
R-IAM-02	Acces privilegiat necontrolat + amenințare internă (Insider Threat)	Fără separare rol admin/utilizator; un angajat cu drepturi admin poate instala software, dezactiva antivirus, accesa orice	4	2	**8**	**12**	**3**	**SEMNIFICATIV**	DIMINUARE	~150.000 MDL	**P2**

ID	Categorie / Amenințare	Vulnerabilitate principală	I Rez	P Rez	S Rez	S In	S Țintă	Nivel	Decizie tratare	Expunere Fin. (MDL)	Prio-ritate
		fișier; risc fraudă internă; statistic 1 din 3 incidente implică actori interni									
R-IAM-03	Dependență critică de un singur angajat (deținătorul stației cu Registrele)	Dacă angajatul este indisponibil (boală, demisie, accident), Registrele sunt inaccesibile; CSPA nu poate îndeplini obligațiile legale; nicio redundanță identificată	4	3	12	16	6	ÎNALT	DIMINUARE	~110.000 MDL	**P2**

AMENINȚĂRI EXTERNE

ID	Categorie / Amenințare	Vulnerabilitate principală	I Rez	P Rez	S Rez	S In	S Țintă	Nivel	Decizie tratare	Expunere Fin. (MDL)	Prio-ritate
R-EXT-01	Atac APT — exfiltrare date despre auditorii entităților de interes public	Ca entitate critică ASC, CSPA deține date despre auditorii EIP; un actor statal/criminal poate folosi aceste date pentru recunoaștere, fraudă sau compromitere a auditului financiar național; infrastructura practic neprotejată	5	2	10	15	4	ÎNALT	DIMINUARE + NOTIFICARE ASC	~450.000 MDL	**P4**
R-EXT-02	Defacement sau compromitere website	Site-ul publică date din Registre și decizii oficiale; dacă compromis, atacatorul poate publica date false (suspendare fictivă) sau folosi site-ul pentru phishing; CSPA nu controlează direct hosting-ul	4	2	8	12	3	SEMNIFICATIV	DIMINUARE	~25.000 MDL	**P3**
R-EXT-03	Social engineering și inginerie socială — manipularea Registrelor publice	Organizație mică (8 persoane) fără departament IT dedicat și fără training formal; angajații pot fi manipulați prin telefon, email sau prezentare fizică să acorde acces sau să modifice date; fără proceduri de verificare identitate solicitanți	4	3	12	16	3	ÎNALT	DIMINUARE	~130.000 MDL	**P2**

JURNALIZARE ŞI DETECTARE

ID	Categorie / Amenințare	Vulnerabilitate principală	I Rez	P Rez	S Rez	S In	S Țintă	Nivel	Decizie tratare	Expunere Fin. (MDL)	Prio-ritate
R-LOG-01	Absența jurnalizării centralizate a evenimentelor de securitate (SIEM)	Fără DC și fără SIEM, evenimentele de securitate sunt stocate local pe fiecare stație (Windows Event Log). Nu există colectare centralizată, corelare sau alertare. Un incident poate rămâne nedetectat zile sau săptămâni — detectat abia după efecte vizibile (date criptate, fișiere șterse, cont compromis).	**3**	**4**	**12**	**20**	**4**	**ÎNALT**	DIMINUARE	~65.000 MDL	**P2**

CONFORMITATE LEGALĂ + CONTINUITATE ACTIVITATE

ID	Categorie / Amenințare	Vulnerabilitate principală	I Rez	P Rez	S Rez	S In	S Țintă	Nivel	Decizie tratare	Expunere Fin. (MDL)	Prio-ritate
R-CONF-01	Neconformitate cu HG 562/2025 cerințe securitate cibernetică entitate critică	HG 562/2025 impune obligații specifice (politici securitate, audit, raportare incidente, BCP); starea actuală — fără DC, registre în Excel, router neadministrat — contravine majorității cerințelor;	4	4	**16**	**20**	**3**	**CRITIC**	**DIMINUARE URGENTĂ**	~320.000 MDL	**P1**
R-CONF-02	Incapacitate de raportare incident de securitate cibernetică către ASC în termenul legal de 24h	Nu există proceduri de răspuns la incidente, sistem de detecție sau responsabil desemnat; în caz de incident, CSPA nu va ști că a suferit un incident — sancțiune suplimentară pentru neraportare	3	4	**12**	**15**	**3**	**ÎNALT**	**DIMINUARE URGENTĂ**	~95.000 MDL	**P1**
R-BCP-01	Indisponibilitate totală CSPA în urma unui incident cibernetic sau fizic	Niciun plan BCP/DRP; internet prin Moldtelecom; dacă oricare cade simultan, CSPA nu poate certifica, înregistra sau comunica; obligații legale cu termene fixe	4	3	**12**	**16**	**3**	**ÎNALT**	DIMINUARE	~200.000 MDL	**P3**
R-BCP-02	Dependență de furnizori externi fără SLA de securitate (lanț de aprovizionare)	CSPA depinde de STISC (email) și Moldtelecom (internet) fără SLA cu cerințe de securitate; nicio clauză de notificare incident; nicio alternativă planificată; firmware MikroTik posibil neactualizat de Moldtelecom	3	3	**9**	**12**	**4**	**SEMNIFICATIV**	DIMINUARE	~45.000 MDL	**P3**

Nivel	Nr. Riscuri	Scor	Riscuri principale
CRITIC	**3**	≥ 16	R-REG-01 (pierdere Registre, S=20), R-EMAIL-01 (phishing, S=16), R-CONF-01 (neconformitate HG562, S=16)
ÎNALT	**14**	10–15	R-REG-02, R-REG-03, R-NET-01, R-EMAIL-02, R-EP-01, R-EP-02, R-EP-03, R-IAM-01, R-IAM-03, R-EXT-01, R-EXT-03, R-CONF-02, R-BCP-01, R-LOG-01
SEMNIFICATIV	**7**	8–9	R-NET-02, R-NET-03, R-EMAIL-03, R-EP-04, R-IAM-02, R-EXT-02, R-BCP-02
MEDIU	**0**	4-7	Niciun risc cu scor pur MEDIU (4–7) identificat în starea actuală;
SCĂZUT	0	1–3	Niciun risc scăzut identificat — toate riscurile necesită tratare
TOTAL	**24**	—	**0 riscuri tolerabile în starea actuală a infrastructurii CSPA**

5. Analiza detaliată a riscurilor prioritare

Secțiunea prezintă analiza aprofundată a riscurilor cu nivel CRITIC și a celor mai semnificative riscuri ÎNALTE, cu scenarii de materializare, consecințe și recomandări specifice.

R-REG-01 + R-EP-01 — Punct Unic de Eșec și Ransomware pe Registrele Publice

Severitate: CRITIC (S=20) · Impact: 5 — Catastrofal · Probabilitate: 4 — Așteptat
Active afectate: A1, A2, A5, A8 — Registrele auditorilor, entităților de audit, date personale

Descriere

Ambele registre publice — Registrul public al auditorilor și Registrul public al entităților de audit — sunt păstrate exclusiv în fișiere pe calculator, fără backup automatizat, fără bază de date și fără control al versiunilor. Aceasta reprezintă cel mai sever risc identificat. Combinația cu absența Domain Controller-ului, lipsa politicilor de securitate centralizate și expunerea la phishing creează condiții ideale pentru un atac ransomware cu impact catastrofal și ireversibil.

Scenarii de materializare

- Defectarea HDD/SSD a calculatorului angajatului → pierdere totală și ireversibilă a datelor
- Infectare ransomware prin email de phishing (PDF/Word macro/Excel malițios) → criptarea și imposibilitatea accesării registrelor
- Ștergere accidentală sau intenționată (amenințare internă la demisie) → pierdere nedetectabilă
- Furt fizic al calculatorului sau al mediilor de stocare → pierdere totală + expunere date personale
- Absența angajatului (concediu, boală, demisie bruscă) → blocarea accesului instituțional
- Propagare laterală a malware-ului prin rețeaua internă nesegmentată → infectarea tuturor stațiilor

Consecințe

- Operațional: Imposibilitatea îndeplinirii obligațiilor legale de publicitate a registrelor de stat
- Reputațional: Pierderea credibilității instituționale la nivel național și internațional
- Financiar: Costuri de reconstituire estimate la 6–18 luni de muncă; cerere de răscumpărare (double extortion)

Recomandări specifice

- Migrare imediată cu versioning automat și backup zilnic
- Implementarea strategiei de backup 3-2-1: 3 copii, 2 medii diferite, 1 offsite/cloud (MCloud); testare lunară a restaurării
- Soluție EDR (Bitdefender GravityZone Business sau Defender for Business) pe toate stațiile; activare Controlled Folder Access anti-ransomware
- Desemnarea unui angajat backup responsabil cu actualizarea registrelor (principiul celor 4 ochi)

R-IAM-01 + R-IAM-02 — Absența Controlului Centralizat al Identităților (Fără Domain Controller)

Severitate: ÎNALT (S=12) · Impact: 4 — Sever · Probabilitate: 3 — Probabil
Active afectate: A5, A6 — Calculatoarele angajaților, documente administrative

Descriere

Absența unui Domain Controller (Active Directory sau echivalent) înseamnă că nu există niciun mecanism centralizat de autentificare, autorizare, gestionare a parolelor, aplicare a politicilor de securitate (GPO), monitorizare a sesiunilor sau revocare rapidă a accesului. Fiecare calculator funcționează ca o insulă independentă, cu conturi locale necontrolate. Fără DC, fără separarea rol administrator/utilizator, un angajat cu drepturi de administrator poate instala software, dezactiva antivirusul și accesa orice fișier — risc de fraudă internă și modificare nedetectată a Registrelor.

Scenarii de materializare

- Angajat demisionat păstrează accesul la stații și date după plecare; contul local rămâne activ nedefinit
- Parolele nu expiră și nu respectă cerințe de complexitate; refolosire parole identice pe servicii personale și profesionale
- Instalarea software neautorizat (inclusiv malware) de către orice angajat cu drepturi admin
- Fără criptare discuri (BitLocker necesită GPO pentru activare centralizată)
- Fără patch management centralizat → vulnerabilități necorectate → exploatare prin documente malițioase

Recomandări specifice

- Pe termen mediu: Implementarea unui Domain Controller
- Utilizarea unui gestionar de parole
- Proceduri documentate de onboarding/offboarding cu checklist de revocare acces; audit manual anual al conturilor active
- Activare BitLocker pe toate stațiile de lucru (funcție inclusă în Windows 10/11 Pro)

R-NET-01 — Lipsa Vizibilității și Controlului Rețelei (Router MikroTik fără Acces Admin)

Severitate: ÎNALT (S=15) · Impact: 5 — Catastrofal · Probabilitate: 3 — Probabil
Active afectate: A3 — Infrastructura de rețea

Descriere

Routerul MikroTik este administrat exclusiv de Moldtelecom, fără niciun acces de administrare pentru personalul CSPA sau managerul TIC. CSPA nu poate configura firewall-ul, crea segmente de rețea (VLAN), bloca trafic suspect, monitoriza conexiunile, activa VPN sau răspunde rapid la un incident de securitate. Botnet-ul Meris (2021) a compromis sute de mii de routere MikroTik la nivel global prin vulnerabilități CVE necorecte — risc real și documentat.

Recomandări specifice

- Solicitare formală scrisă către Moldtelecom pentru acces de administrare al routerului sau înlocuire cu echipament propriu CSPA
- Activarea imediată a DNS-over-HTTPS cu filtrare (Cloudflare 1.1.1.1 for Families sau NextDNS — gratuit) pe toate stațiile
- Separarea rețelei VLAN (rețea CSPA vs. vizitatori); documentarea topologiei de rețea existente

R-EMAIL-01 + R-EMAIL-02 — Phishing și Compromitere Email (Poșta Electronică via STISC)

Severitate: CRITIC (S=16) · Impact: 4 — Sever · Probabilitate: 4 — Așteptat
Active afectate: A4 — Serviciu email administrat extern; cel mai frecvent vector de atac în sectorul public

Descriere

Emailul instituțional este furnizat și administrat de STISC. CSPA nu deține controlul complet asupra configurației de securitate: lipsă MFA, posibile configurații DMARC/DKIM/SPF deficitare, absența filtrelor avansate anti-phishing și expunerea adreselor instituționale în documente publice. Phishing-ul este vectorul #1 de atac în sectorul public, vizând în special organizații mici cu resurse limitate de conștientizare.

Scenarii de materializare

- Phishing țintit (spear-phishing) împotriva directorului sau angajatului cu acces la registre → execuție malware → criptare registre
- BEC (Business Email Compromise) → instrucțiuni frauduloase de plată sau de modificare urgentă a datelor din registre
- Spoofing al adresei CSPA → comunicări frauduloase trimise auditorilor sau partenerilor instituționali
- Compromiterea contului de email → acces la corespondența sensibilă cu entitățile auditate

Recomandări specifice

- Verificarea/solicitarea configurației DMARC=reject, DKIM și SPF pentru domeniul cspa.md
- Politică internă: date sensibile nu se transmit pe email necriptat
- Training obligatoriu anti-phishing cu simulări periodice pentru toți angajații
- Pe termen mediu: Evaluare migrare email la Microsoft 365 Business (control complet DMARC/DKIM, DLP, MFA nativ)

R-CONF-01 + R-CONF-02 — Neconformitate Legală și Incapacitate de Raportare la ASC

Severitate: CRITIC (S=16) · Impact: 4 — Sever · Probabilitate: 4 — Așteptat
Temeiul legal: HG 562/2025 · obligație raportare incident 24h la ASC

Descriere

HG 562/2025 impune obligații specifice pentru entitățile critice: politici de securitate, audit periodic, raportare incidente la ASC în maxim 24 ore, continuitate activitate (BCP/DRP). Starea actuală a infrastructurii CSPA contravine majorității acestor cerințe. Mai grav: în cazul unui incident, CSPA nu are proceduri de detectare și raportare, ceea ce conduce la sancțiune dublă (pentru incident + pentru neraportare).

Recomandări specifice

- Audit intern de conformitate față de HG 562/2025; Responsabil Securitate Cibernetică
- Elaborare Procedură de Răspuns la Incidente Cibernetice: detectare, izolare, notificare ASC 24h, recuperare

- Elaborare BCP/DRP minim viabil: pentru registrele critice; exercițiu de simulare criză cel puțin o dată pe an
- Prezentarea prezentei analize de riscuri Comitetului de Supraveghere și includerea în planul de activitate al Consiliului
- Solicitarea unui audit de securitate cibernetică independent prin ASC sau furnizor acreditat pentru validarea externă (~50.000–120.000 MDL)

6. Harta riscurilor – Matricea Impact x Probabilitate

Pozițiile riscurilor la nivel REZIDUAL pe matricea 5×5. Toate riscurile se află în zona intolerabilă (SEMNIFICATIV–CRITIC). Niciun risc nu se află în zona tolerabilă.

I ↓ / P →	P=1 Rar	P=2 Posibil	P=3 Probabil	P=4 Așteptat	P=5 Cert
I=5 Catastrofal	S=5	S=10 R-EP-02 R-EXT-01	S=15 R-REG-02 R-NET-01 R-EP-01	S=20 R-REG-01	S=25
I=4 Sever	S=4	S=8 R-NET-02 R-IAM-02 R-EXT-02	S=12 R-REG-03 R-EMAIL-02 R-EP-03 R-IAM-01 R-IAM-03 R-EXT-03 R-BCP-01 R-CONF-02 R-LOG-01	S=16 R-EMAIL-01 R-CONF-01	S=20
I=3 Moderat	S=3	S=6	S=9 R-NET-03 R-EMAIL-03 R-EP-04 R-BCP-02		S=15
I=2 Minor	—	—	—	—	—

7. Planul de acțiuni pentru tratarea riscurilor

Planul este prioritizat pe 4 niveluri.

PRIORITATEA 1 — URGENTE

ID Risc	Măsura Propusă	Responsabil	Termen	Cost Est.	Tip	Justificare
R-REG-01 R-EP-01	Control acces pe roluri și backup zilnic automatizat	Director + Manager IT	60 zile	0 MDL	Tehnică	SPOF absolut — pierderea Registrelor = incapacitate funcționare; ROI infinit
R-CONF-01	Audit conformitate HG 562/2025; elaborare Plan de Conformare; desemnare Responsabil Securitate Cibernetică; raportare la ASC în termen legal	Director + Manager IT	60 zile	0 MDL	Org./Legal	Obligație legală entitate critică; neconformitate = sancțiuni ASC
R-CONF-02	Elaborare Procedură Răspuns la Incidente Cibernetice: detectare, izolare, notificare ASC 24h, recuperare; test anual	Director + Manager IT	60 zile	0 MDL	Organizatorică	Fără procedură = sancțiune dublă; șabloane disponibile ASC/CERT-MD
R-EMAIL-01	(1) confirmare DMARC/DKIM/SPF pe cspa.md; (2) activare filtre anti-phishing avansate;	Director + Manager IT	60 zile	0 MDL	Contractuală	Phishing = risc CRITIC cu scor 16; configurări tehnice implementate de STISC la solicitare
R-EP-02 R-REG-01	Activare BitLocker pe toate stațiile de lucru CSPA; inventar complet active IT;	Manager IT	30 zile	0 MDL	Tehnică	BitLocker = funcție inclusă în Windows 10/11 Pro; protejează la furt fizic
R-REG-01 R-REG-02	Backup imediat al registrelor (strategie 3-2-1): copie pe NAS; testare lunară a restaurării efective	Director + Manager IT	60-360 zile	~17.500 MDL	Tehnică	Măsura minimă; testarea restaurării este obligatorie
R-EP-03 R-IAM-02	Verificare/activare antivirus pe toate stațiile; dezactivare macro-uri Office pentru fișiere din surse externe; audit conturi locale active	Manager IT	60 zile	0 MDL	Tehnică	Windows Defender + dezactivare macro = reducere imediată risc ransomware

PRIORITATEA 2 — INVESTIȚII MODERATE (Q3 2026-Q1 2027)

ID Risc	Măsura Propusă	Responsabil	Termen	Cost Est.	Tip	Justificare
R-IAM-01 R-IAM-02	Implementare AD Linux	Manager IT	Q3 2026	0 MDL	Tehnică	DC on-premise; revocare acces în secunde
R-EP-01 R-EP-04	Instalare soluție EDR (Bitdefender GravityZone Business sau echivalent) pe toate stațiile; activare Controlled Folder	Manager IT + Director	Q1 2027	~9.000 MDL/an	Tehnică	GravityZone = ~15 USD/stație/an × 8; protecție ransomware = prioritate pentru stațiile de lucru

ID Risc	Măsura Propusă	Responsabil	Termen	Cost Est.	Tip	Justificare
	Access anti-ransomware; patch management centralizat					
R-NET-01	Negociere Moldtelecom acces read-only la consola Mikrotik; activare DNS filtering	Manager IT	60 zile	0 MDL	Tehnică	Perimetru securitate independent de ISP
R-EXT-03 R-EMAIL-01	Training obligatoriu securitate cibernetică pentru toți 8 angajații (phishing, social engineering, BEC); politică utilizare acceptabilă IT semnată	Manager IT	Q2-Q3 2026	0 MDL	Organizatorică	Factorul uman = principal vector de atac;
R-LOG-01	Implementare Wazuh SIEM open-source (gratuit) pe un server dedicat (sau VM) pentru colectarea centralizată a jurnalelor de securitate de pe toate stațiile; configurare alerte automate la evenimente suspecte; alternativ Microsoft Sentinel (inclus M365 Business Premium)	Manager IT	Q4 2026	~10.000 MDL software + resurse hardware	Tehnică	Wazuh = SIEM open-source gratuit, adoptat de mii de organizații; esențial pentru detecția incidentelor şi respectarea obligației de raportare ASC 24h

PRIORITATEA 3 — ACȚIUNI PLANIFICATE (Q3 2026 – Q3 2027)

ID Risc	Măsura Propusă	Responsabil	Termen	Cost Est.	Tip	Justificare
R-REG-02 R-REG-03	Migrare Registre în bază de date dedicată cu separare roluri creare/aprobare/vizualizare și audit trail nativ	Manager IT+Director	Q3 2027	~100.000 MDL	Tehnică	Audit trail obligatoriu pentru date publice oficiale; elimină riscul modificare nedetectată
R-BCP-01	Elaborare BCP minimal: proceduri funcționare offline temporară, RTO ≤ 4 ore / RPO ≤ 24 ore, locație alternativă, contacte urgență, exerciții de simulare criză (tabletop) anual	Director	Q4 2026	0 MDL	Organizatorică	Obligație HG 562/2025
R-REG-03	Audit GDPR al Registrelor	Jurist + Director	Q4 2026	0 MDL	Legal	Legea 133/2011; Registrele conțin CNP, adrese, sancțiuni;

ID Risc	Măsura Propusă	Responsabil	Termen	Cost Est.	Tip	Justificare
						sancțiune până la 10.000 EUR
R-EMAIL-01 R-EMAIL-02 R-EP-01 R-EP-03	Migrare Microsoft 365 E3	Manager IT+Director	Q3 2027	~68.000 MDL/an	Tehnică	Microsoft 365 E3 = ~39 USD/stație/lunar × 8; protecție = prioritate pentru stațiile de lucru
R-EXT-01 R-CONF-01	OPTIONAL — Audit de securitate cibernetică independent prin ASC sau furnizor acreditat pentru validarea externă a posturii de securitate și conformității cu HG 562/2025	Director	Q4 2026	**50.000–120.000 MDL**	Extern / Audit	Entitate critică ASC; validare externă independentă a măsurilor implementate; confirmare conformitate; recomandat anual

Categorie investiție	Cost estimat
Prioritatea 1 — Urgente (BitLocker, backup, proceduri)	17,500 MDL (unic)
Prioritatea 2 — Investiții moderate (EDR, AD, UTM)	~10.000 MDL (unic) + ~9,000 MDL (anual)
Prioritatea 3 — Acțiuni planificate (M365)	~68.000 MDL/an + ~100.000 MDL unic
Audit de securitate independent (opțional, P3)	*50.000–120.000 MDL (unic)*
BUGET TOTAL ESTIMAT PLAN DE ACȚIUNI (fără audit extern)	**~77.000 MDL/an + ~127.500 MDL unic (+ 50.000–120.000 MDL audit extern opțional)**