ARES

Asociația ARES

Asociația pentru Reziliență, Evaluare și Securitate

DOCUMENT PROFESIONAL M–01

STANDARD PROFESIONAL ARES

Metodologia ARES–SECURITAS

Metodologie profesională pentru organizarea, dezvoltarea, fundamentarea și redactarea analizei de risc la securitatea fizică.

METODĂ · STRUCTURĂ · APLICARE

EVALUATORI DE RISC LA SECURITATEA FIZICĂ

Publicație profesională · Asociația ARES

EDIȚIA 2026

Actualizat 25.07.2026

M–01 · METODOLOGII

Metodologia ARES–SECURITAS

Metodologie profesională pentru organizarea, dezvoltarea, fundamentarea și redactarea analizei de risc la securitatea fizică.

09	5.347	≈ 24	2026
CAPITOLE	CUVINTE	MINUTE DE LECTURĂ	EDIȚIE PROFESIONALĂ

NOTĂ PROFESIONALĂ

Documentul nu are natura unui act normativ și se aplică în completarea legislației în vigoare, fără a înlocui ori modifica obligațiile legale aplicabile.

CUPRINS

CAPITOLUL 1
S — Scopul evaluării și pregătirea evaluării

CAPITOLUL 2
E — Evaluarea amplasării geografice și a contextului

CAPITOLUL 3
C — Cadrul organizațional

CAPITOLUL 4
U — Unitățile de risc

CAPITOLUL 5
R — Riscurile analizate

CAPITOLUL 6
I — Identificarea, analizarea și estimarea riscurilor

CAPITOLUL 7
T — Tratarea riscurilor și măsurile de securitate

CAPITOLUL 8
A — Analiza și estimarea costurilor de securitate

CAPITOLUL 9
S — Soluțiile finale, concluziile și documentația finală

FORMULA OFICIALĂ ARES–SECURITAS

NUCLEUL METODOLOGIC CORECT

CONCLUZIE

Metodologie profesională pentru analiza de risc la securitatea fizică

STANDARD PROFESIONAL ARES–SECURITAS

Prezentul document reprezintă o metodologie și un standard profesional elaborat de Asociația pentru Reziliență, Evaluare și Securitate (ARES) și nu are natura unui act normativ. El se aplică în completarea legislației în vigoare și nu înlocuiește ori modifică obligațiile stabilite prin Legea nr. 333/2003, HG nr. 301/2012 și Instrucțiunile M.A.I. nr. 9/2013.

Metodologia ARES–SECURITAS reprezintă un model profesional de organizare, dezvoltare, fundamentare și redactare a analizei de risc la securitatea fizică, construit în concordanță cu exigențele impuse de Instrucțiunile M.A.I. nr. 9/2013, cu normele metodologice aprobate prin HG nr. 301/2012 și cu obligațiile generale stabilite prin Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor. Ea urmărește să ofere evaluatorului un cadru unitar de lucru prin care analiza de risc să nu rămână la nivel descriptiv sau formal, ci să devină un instrument juridic, tehnic și organizațional apt să fundamenteze, în mod serios și verificabil, măsurile de securitate necesare fiecărui obiectiv.

Metodologia are la bază ideea că analiza de risc la securitatea fizică nu se confundă nici cu simpla descriere a obiectivului, nici cu proiectarea tehnică a unui sistem de securitate și nici cu elaborarea unei oferte comerciale. Ea reprezintă o activitate profesională de identificare a amenințărilor și vulnerabilităților, de determinare a zonelor de impact, de analizare și estimare a riscurilor și de stabilire a măsurilor necesare pentru aducerea acestora în domeniul riscului acceptabil. Din această perspectivă, analiza de risc este fundamentul legal și metodologic al planului de pază, al măsurilor organizatorice, al dotărilor mecanofizice, al sistemelor tehnice de protecție și alarmare și, după caz, al necesității serviciilor de pază umană.

Formula ARES–SECURITAS exprimă succesiunea logică și profesională a evaluării:

S — Scopul evaluării și pregătirea evaluării
E — Evaluarea amplasării geografice și a contextului
C — Cadrul organizațional
U — Unitățile de risc
R — Riscurile analizate
I — Identificarea, analizarea și estimarea riscurilor
T — Tratarea riscurilor și măsurile de securitate
A — Analiza și estimarea costurilor de securitate
S — Soluțiile finale, concluziile și documentația finală

Prin această structură, metodologia ARES–SECURITAS oferă un traseu de lucru clar: de la definirea obiectivului și a cadrului legal, la înțelegerea contextului și a organizării interne, la localizarea vulnerabilităților și a amenințărilor, la formularea riscurilor relevante, la evaluarea juridică prin grilă și, în final, la stabilirea măsurilor obligatorii, a recomandărilor și a opțiunilor de tratare.

M–01 · 01

CAPITOLUL 1

S — Scopul evaluării și pregătirea evaluării

Primul capitol stabilește fundamentul evaluării. În această etapă se definește unitatea evaluată, se individualizează obiectul de activitate, se determină scopul analizei, se delimitează aria evaluării, se identifică baza legală aplicabilă și se stabilește instrumentul juridic de cuantificare a riscului. Tot în această etapă se clarifică raporturile dintre evaluator și beneficiar, limitele misiunii profesionale și rolul concret al analizei de risc în sistemul general de securitate fizică al unității.

Scopul evaluării este determinarea riscurilor la securitatea fizică ale unității și stabilirea măsurilor necesare pentru ca acestea să fie încadrate în domeniul riscului acceptabil. Analiza de risc nu urmărește numai constatarea unei stări de fapt, ci și fundamentarea cerințelor de securitate necesare raportat la specificul obiectivului, la vulnerabilitățile sale, la expunerea sa și la obligațiile legale incidente. În mod corect înțeleasă, analiza de risc reprezintă documentul profesional care justifică de ce anumite măsuri sunt necesare, de ce altele sunt insuficiente și de ce unele soluții nu au caracter opțional, ci obligatoriu.

În această etapă, evaluatorul trebuie să colecteze și să studieze documentele relevante privind unitatea evaluată: date de identificare, obiect de activitate, regim juridic, amplasament, program de funcționare, fluxuri operaționale, tipuri de bunuri și valori, documente privind măsuri de securitate deja existente, contracte de pază, contracte de monitorizare, documente de mentenanță, planuri sau relevee disponibile, proceduri interne, regulamente de acces, registre și alte informații utile. Pregătirea evaluării include și stabilirea metodei de lucru, a instrumentelor utilizate, a planificării activităților de teren, precum și a setului de întrebări și chestionare necesare pentru obținerea informațiilor funcționale.

Tot în capitolul introductiv se face documentarea legislativă. Evaluatorul trebuie să identifice cadrul general aplicabil securității fizice, normele speciale care țin de obiectul de activitate al unității, existența unor cerințe minimale de securitate prevăzute de HG nr. 301/2012, eventualele obligații referitoare la numerar, valori, bunuri cu regim special, informații protejate, transporturi, mecanofizică, control acces sau sisteme de alarmare. Nu orice obiectiv este supus acelorași exigențe, iar analiza corectă presupune o încadrate juridică exactă încă de la început.

Din perspectiva Legii nr. 333/2003, acest capitol trebuie să arate expres că securitatea fizică nu este o opțiune lăsată la aprecierea liberă a beneficiarului, ci o obligație legală. Unitățile care dețin bunuri ori valori sunt obligate să asigure paza acestora, iar răspunderea pentru luarea măsurilor de asigurare a pazei revine conducătorilor unităților. De asemenea, organizarea pazei se face în funcție de importanța, specificul și valoarea bunurilor, iar acolo unde nu este posibilă realizarea unui sistem organizat de pază, conducătorii unităților au obligația de a executa împrejmuiri, grilaje, obloane, încuietori sigure, iluminat de securitate, sisteme de alarmă sau alte mijloace necesare asigurării pazei și integrității bunurilor.

Așadar, evaluarea riscului nu creează obligația de securitate, ci o particularizează și o motivează profesional. Evaluatorul nu inventează nevoi de securitate, ci le identifică, le structurează și le justifică în baza legii și a stării reale a obiectivului.

În această etapă trebuie precizat și faptul că analiza de risc nu se confundă cu proiectarea tehnică. Evaluatorul nu execută proiectul sistemului de alarmare, nu instalează, nu modifică și nu pune în funcțiune sisteme, nu redactează planul de pază în locul conducerii unității și nu întocmește oferte comerciale ori devize de execuție. El stabilește necesitatea și nivelul măsurilor de securitate, nu soluția comercială finală a unui furnizor anume.

Un alt element esențial al capitolului introductiv este confidențialitatea. Datele privind vulnerabilitățile obiectivului, punctele sensibile, procedurile interne, valorile păstrate, lipsurile de organizare sau deficiențele sistemelor existente sunt informații sensibile. Înainte de elaborarea analizei, evaluatorul trebuie să se afle într-un raport profesional clar cu beneficiarul și să trateze toate informațiile obținute cu confidențialitatea cerută de natura lor.

În final, acest capitol fixează grila aplicabilă. Pentru acele categorii de unități pentru care există grile specifice de evaluare, cuantificarea se va realiza prin grila specială aferentă obiectului principal de activitate. Dacă în aceeași incintă există activități distincte, fiecare cu profil diferit și cu cerințe proprii de securitate, se impune completarea unor grile distincte. Fiecare activitate trebuie analizată și încadrată separat în domeniul riscului acceptabil.

M–01 · 02

CAPITOLUL 2

E — Evaluarea amplasării geografice și a contextului

Al doilea capitol privește mediul extern al obiectivului. Dacă primul capitol stabilește identitatea juridică și funcțională a unității, aici evaluatorul examinează contextul în care aceasta există și operează. Riscul de securitate fizică nu este generat exclusiv din interiorul obiectivului; el este influențat în mod direct de amplasament, de vecinătăți, de accesibilitate, de posibilitatea de observare sau disimulare, de tipul căilor de acces, de izolarea ori expunerea obiectivului și de specificul mediului local.

Evaluarea amplasării geografice presupune descrierea localizării obiectivului în mediul urban sau rural, identificarea zonei în care acesta funcționează, analiza vecinătăților imediate și apropiate, a căilor de acces și a modului în care configurația terenului ori a zonei construite poate favoriza sau descuraja materializarea unor evenimente de securitate. Se are în vedere dacă obiectivul este amplasat într-o zonă circulată sau izolată, dacă există rute multiple de apropiere și de retragere, dacă există zone slab iluminate, locuri de mascare, căi laterale de acces, pasaje, curți interioare, terenuri virane sau alte elemente care pot influența vulnerabilitatea.

Evaluatorul trebuie să analizeze și raportul dintre obiectiv și vecinătățile sale. Unele vecinătăți reduc riscul, de exemplu prin prezența permanentă a altor activități, supraveghere naturală, trafic constant sau control public sporit. Alte vecinătăți îl pot crește, cum ar fi spațiile abandonate, zonele slab frecventate, incintele industriale dezafectate, localurile cu activitate nocturnă intensă, zonele cu acces dificil sau imobilele care permit observarea ori accesarea facilă a obiectivului. Nu este suficientă descrierea acestora; evaluatorul trebuie să explice în ce mod concret ele influențează securitatea fizică.

Contextul extern include și aspecte legate de incidența unor forme de criminalitate relevante, de frecvența evenimentelor de ordine publică, de existența unor antecedente locale privind furturi, pătrunderi, agresiuni, vandalism ori alte manifestări cu impact asupra tipului de activitate analizate. Aici pot fi folosite date statistice, date locale, observații de teren și informații obținute de la beneficiar sau din vecinătate, în măsura în care acestea sunt verificate și utilizate responsabil.

Rolul metodologic al acestui capitol este acela de a arăta în ce măsură mediul exterior exercită presiune asupra obiectivului și cum afectează el probabilitatea de materializare a unor riscuri. Capitolul nu stabilește încă măsuri de tratare, ci definește contextul extern în care evaluarea internă va trebui să se înscrie. O unitate expusă într-o zonă izolată, cu căi multiple de apropiere și retragere și cu supraveghere naturală redusă va fi analizată diferit față de una situată într-o zonă intens circulată, bine iluminată și vizibilă.

Acest capitol trebuie redactat narativ, în limbaj concret și aplicat. Nu este suficient să se noteze „obiectivul se află în mediul urban”; trebuie explicat dacă mediul urban este central sau periferic, dacă accesul este direct din arteră principală ori din stradă secundară, dacă parcările, aleile, curțile și zonele adiacente favorizează observarea sau, dimpotrivă, disimularea. În mod similar, nu este suficient să se menționeze existența vecinătăților; trebuie explicat dacă acestea produc risc suplimentar sau contribuie la protecția naturală a amplasamentului.

M–01 · 03

CAPITOLUL 3

C — Cadrul organizațional

Capitolul al treilea privește mediul intern al unității din punct de vedere organizațional. Oricât de bună sau de slabă ar fi situația din exterior, securitatea obiectivului este puternic determinată de modul în care acesta este organizat intern, de cine răspunde de securitate, de ce reguli există, de cum circulă persoanele, bunurile și valorile și de măsura în care activitatea este structurată ori, dimpotrivă, vulnerabilă prin improvizație, neclaritate și lipsă de responsabilitate.

Acest capitol trebuie să identifice cadrul organizațional intern, politicile și responsabilitățile privind securitatea fizică, programul de lucru, structura funcțională, personalul relevant, fluxurile operaționale și procedurile interne existente. El trebuie să stabilească dacă unitatea are reguli clare de acces, dacă responsabilitățile sunt nominalizate, dacă există persoane desemnate pentru relația cu securitatea fizică, dacă sunt clar delimitate zonele sensibile, dacă există proceduri pentru deschidere, închidere, manipularea valorilor, predarea cheilor, gestionarea incidentelor și raportarea evenimentelor.

Un punct central îl reprezintă zonele funcționale. Potrivit HG nr. 301/2012, conducătorii unităților deținătoare de bunuri și valori au obligația de a identifica și stabili zonele funcționale corespunzător activității desfășurate și de a adopta măsurile necesare protecției vieții, integrității persoanelor și siguranței valorilor. Prin urmare, evaluatorul nu creează el însuși, în mod arbitrar, zone funcționale noi, ci verifică dacă acestea au fost identificate, dacă delimitarea lor este adecvată activității și dacă ele sunt utile și suficiente pentru analiza de risc. Dacă lipsesc ori sunt necorespunzător configurate, evaluatorul constată acest aspect și îl tratează ca vulnerabilitate.

În structura legală consacrată de normele metodologice, zonele funcționale sunt: zona de acces în unitate și zona perimetrală, zona de tranzacționare, zona de depozitare, zona de expunere, zona de transfer, zona de procesare, zona echipamentelor de securitate, zona de tranzacții cu automate bancare și alte zone cu regim de securitate ridicat. Metodologia ARES–SECURITAS respectă această clasificare și nu o substituie. Orice grupare metodologică suplimentară are doar rol de lucru și nu poate modifica delimitarea legală.

Din perspectiva Legii nr. 333/2003, cadrul organizațional trebuie analizat și prin prisma obligațiilor conducerii unității. Conducătorii unităților răspund de organizarea și funcționarea pazei, analizează nevoile stricte de pază, stabilesc efectivele necesare în raport cu natura, importanța, mărimea și vulnerabilitatea obiectivului, asigură selecția personalului, instruirea acestuia, amenajările și instalațiile necesare, introducerea, întreținerea și menținerea în funcțiune a sistemelor tehnice de pază și alarmă, stabilesc reguli de acces și responsabilități pentru structurile interne.

Această obligație legală are o consecință metodologică importantă: lipsa regulilor interne, lipsa responsabilităților nominalizate, absența procedurilor sau inexistența unor măsuri organizatorice elementare nu sunt simple neajunsuri administrative, ci vulnerabilități relevante pentru analiza de risc. Într-o unitate în care nimeni nu răspunde clar de securitate, accesul nu este reglementat, cheile circulă fără evidență, zonele nu sunt delimitate și incidentele nu sunt raportate, riscul este crescut nu doar prin lipsa tehnicii, ci prin lipsa cadrului organizațional.

Cadrul organizațional trebuie deci descris nu formal, ci funcțional. Nu este suficient să se consemneze că există un regulament intern; trebuie arătat dacă el are conținut aplicabil securității. Nu este suficient să se menționeze existența personalului de pază; trebuie văzut dacă acesta este integrat într-un sistem coerent, dacă are consemn clar, dacă punctele vulnerabile sunt cunoscute, dacă regulile de acces sunt efectiv aplicate și dacă activitatea este controlată.

M–01 · 04

CAPITOLUL 4

U — Unitățile de risc

Capitolul al patrulea introduce una dintre cele mai importante componente ale metodologiei ARES–SECURITAS: unitățile de risc. Acestea reprezintă componentele fizice sau funcționale ale obiectivului asupra cărora se pot manifesta riscurile la securitatea fizică și în interiorul cărora o amenințare poate exploata una sau mai multe vulnerabilități. Conceptul de unitate de risc permite evaluatorului să iasă din descrierea generală a obiectivului și să lucreze pe segmente analizabile, identificabile și evaluabile.

În metodologia ARES–SECURITAS, unitățile de risc pot fi grupate de lucru în zona perimetrală, zona învelișului, zona interioară și zonele critice sau sensibile. Zona perimetrală privește limita fizică exterioară a obiectivului și spațiile imediat adiacente. Zona învelișului include toate elementele fizice care fac trecerea dintre exterior și interior: uși, porți, ferestre, ziduri, împrejmuiri, puncte de acces, pasaje tehnice și alte elemente similare. Zona interioară privește spațiile operaționale interne, iar zonele critice sau sensibile includ acele locații în care sunt concentrate valori, informații, echipamente esențiale, comenzi de securitate, infrastructuri vitale sau activități a căror afectare produce consecințe disproporționate.

Această grupare este una metodologică și nu înlocuiește zonele funcționale prevăzute de HG nr. 301/2012. Ea este folosită doar pentru a ordona munca evaluatorului și pentru a facilita identificarea vulnerabilităților și a amenințărilor.

Pentru fiecare unitate de risc trebuie identificate vulnerabilitățile, amenințările relevante, zona de impact, evenimentele de securitate posibile, cauzele probabile și consecințele potențiale. Această etapă trebuie realizată cu exactitate, întrucât omisiunea unor vulnerabilități ori amenințări sau utilizarea unor date nereale ori incorecte poate compromite analiza și îi poate afecta valabilitatea profesională și juridică.

Legea nr. 333/2003 întărește metodologic această abordare prin faptul că impune personalului de pază obligația de a cunoaște locurile și punctele vulnerabile din perimetrul obiectivului, pentru a preveni producerea oricăror fapte de natură să aducă prejudicii unității. Aceasta arată că noțiunea de vulnerabilitate nu este o construcție teoretică exterioară regimului legal, ci un element intrinsec activității de securitate.

Zona de impact, în sensul metodologiei ARES–SECURITAS, reprezintă partea obiectivului ori a activității asupra căreia se produc efectele materializării riscului. Ea poate privi persoanele, bunurile, valorile, datele, activitatea, imaginea, continuitatea operațională sau combinații între acestea. Identificarea zonei de impact este esențială pentru că permite legarea riscului de efectul său real și împiedică analiza să rămână abstractă.

În mod corect realizată, identificarea unităților de risc permite evaluatorului să răspundă la întrebări concrete: unde se poate produce pătrunderea neautorizată, unde se poate produce sustragerea, unde sunt concentrate valorile, unde este punctul de comandă al securității, unde poate fi neutralizat sistemul de protecție, unde o eroare de acces produce efecte majore, unde o agresiune afectează persoanele ori activitatea. Fără această segmentare, analiza rămâne generală și își pierde precizia.

M–01 · 05

CAPITOLUL 5

R — Riscurile analizate

Acest capitol stabilește logica centrală a metodologiei. El trebuie să clarifice raportul dintre vulnerabilitate, amenințare, risc, eveniment de securitate, modus operandi, probabilitate, impact și consecințe. Una dintre cele mai frecvente erori din practica evaluării constă în amestecarea acestor noțiuni: riscul este confundat cu evenimentul, evenimentul cu modul de operare, iar modul de operare cu categoria de risc. Metodologia ARES–SECURITAS urmărește tocmai eliminarea acestei confuzii.

În logica sa corectă, vulnerabilitatea este starea, caracteristica, slăbiciunea sau condiția exploatabilă existentă în obiectiv. Amenințarea este factorul intern sau extern capabil să exploateze această vulnerabilitate. Din relația dintre vulnerabilitate și amenințare rezultă riscul potențial. Riscul se poate materializa printr-un eveniment de securitate. Evenimentul se produce printr-un anumit modus operandi. Acesta afectează o zonă de impact și generează consecințe de natură și gravitate variabile. Estimarea juridică finală a nivelului de risc se validează prin grila de evaluare și prin raportarea la pragul critic.

Metodologia ARES–SECURITAS pornește de la ideea că riscurile analizate trebuie ancorate în fapte relevante din punct de vedere juridic, fără ca analiza să se transforme într-o calificare penală. Evaluatorul nu este chemat să stabilească vinovății sau să tipifice juridic în sens penal o situație, dar este obligat să construiască o analiză serioasă în jurul acelor afectări pe care sistemul de securitate fizică trebuie să le prevină: pătrunderea neautorizată, sustragerea, agresiunea, constrângerea, compromiterea unor spații sau informații, afectarea continuității activității, neutralizarea mijloacelor de protecție.

Din această perspectivă, categoriile metodologice de risc trebuie formulate clar și corect. Ele pot include: riscul de pătrundere neautorizată; riscul de sustragere de bunuri sau valori; riscul de agresiune asupra persoanelor; riscul de lipsire ilegală de libertate sau constrângere; riscul de amenințare sau șantaj; riscul de violare a vieții private și de acces neautorizat la informații; riscul de afectare a zonelor, valorilor ori echipamentelor protejate; riscul de afectare a continuității activității; riscul de distrugere, degradare ori neutralizare a elementelor de protecție.

Această formulare este metodologic superioară expresiilor improprii de tipul „risc de efracție”. Efracția nu este risc; este mod de operare. Ea descrie felul în care cineva pătrunde, nu categoria de afectare care trebuie evaluată. În mod similar, escaladarea, folosirea unei chei adevărate, folosirea unei chei mincinoase, inducerea în eroare a personalului, disimularea, fraudarea unui acces legitim ori scoaterea din funcțiune a unui sistem nu sunt riscuri autonome, ci modalități concrete prin care amenințarea exploatează vulnerabilitatea și produce evenimentul.

Pentru consistență juridică, evaluatorul poate ancora aceste riscuri în repere din Codul penal. Riscul de pătrundere neautorizată se corelează cu fapte precum violarea de domiciliu sau violarea sediului profesional. Riscul de sustragere se corelează cu furtul, furtul calificat și alte forme relevante. Riscul de agresiune se raportează la lovire, vătămare, amenințare, tâlhărie ori alte manifestări violente. Riscul de violare a vieții private

și al informațiilor privește fapte care afectează confidențialitatea, integritatea vieții private și accesul neautorizat la date sau informații protejate. Riscurile privind sistemele și continuitatea includ și situațiile în care sunt afectate dispozitive ori sisteme de semnalizare, alarmare, supraveghere sau intervenție.

Evenimentul de securitate reprezintă manifestarea concretă a riscului. El poate consta în pătrundere neautorizată, sustragere de bunuri sau valori, agresiune asupra personalului ori publicului, compromiterea unei zone protejate, captarea sau divulgarea fără drept a unor informații, distrugerea ori neutralizarea unui sistem de protecție sau perturbarea activității unității.

Consecințele pot privi persoanele, bunurile, valorile, activitatea, imaginea, credibilitatea, continuitatea operațională, datele și informațiile protejate. Evaluatorul trebuie să le identifice într-o manieră concretă și aplicată. Nu este suficient să menționeze generic „pierderi materiale”; el trebuie să arate ce tip de prejudiciu este posibil, cine este afectat, ce activitate este perturbată, ce date sunt compromise și ce impact poate avea evenimentul asupra funcționării normale a unității.

M–01 · 06

CAPITOLUL 6

I — Identificarea, analizarea și estimarea riscurilor

Acest capitol urmează ordinea impusă de Instrucțiunile M.A.I. nr. 9/2013: identificarea riscurilor, analizarea riscurilor și estimarea riscurilor. Este etapa în care elementele deja colectate și clarificate în capitolele anterioare sunt puse în lucru și transformate într-un raționament evaluativ.

Identificarea riscurilor presupune corelarea, pentru fiecare unitate de risc, a amenințărilor relevante cu vulnerabilitățile existente, cu zonele de impact, cu evenimentele de securitate posibile, cu cauzele probabile și cu consecințele previzibile. Această operațiune nu este o listare arbitrară de pericole, ci un exercițiu de raționament aplicat. Nu orice amenințare este relevantă pentru orice obiectiv și nu orice vulnerabilitate are aceeași greutate. Relevanța se stabilește în funcție de specificul activității, de valorile protejate, de configurarea obiectivului și de contextul intern și extern.

Analizarea riscurilor presupune examinarea relației dintre probabilitatea de materializare și impactul potențial asupra zonei de impact. Probabilitatea nu trebuie înțeleasă exclusiv ca frecvență statistică, ci ca apreciere profesională rezultată din context, expunere, accesibilitate, atractivitatea țintei, istoricul evenimentelor, nivelul vulnerabilităților și gradul de control existent. Impactul privește gravitatea efectelor asupra persoanelor, bunurilor, valorilor, activității și continuității operaționale.

Totuși, în metodologia ARES–SECURITAS, probabilitatea și impactul au rol metodologic de susținere a raționamentului, nu înlocuiesc instrumentul juridic central. Evaluarea finală, în sens legal, se face prin grila de evaluare aplicabilă obiectului. Grila este instrumentul normativ prin care se cuantifică riscul și se stabilește dacă obiectivul se încadrează sau nu în domeniul riscului acceptabil.

Estimarea riscurilor se finalizează, prin urmare, prin completarea și aplicarea grilei corespunzătoare. În această etapă, evaluatorul lucrează cu categoriile de criterii prevăzute de reglementările aplicabile: criterii specifice obiectivului, criterii de securitate, criterii funcționale și alte criterii. Elementele relevante identificate în teren și în documentare trebuie transpuse corect în grilă, fără a forța încadrări artificiale și fără a omite aspecte cu relevanță reală.

Pragul critic de 60% joacă aici un rol decisiv. Domeniul riscului acceptabil este asociat valorilor estimate sub pragul critic, iar domeniul riscului inacceptabil valorilor de peste pragul critic. Din punct de vedere juridic și metodologic, cerințele de securitate fizică sunt considerate îndeplinite numai atunci când riscul evaluat se încadrează în domeniul acceptabil. Aceasta înseamnă că analiza nu se încheie cu simpla completare a grilei, ci cu concluzia motivată privind suficiența sau insuficiența măsurilor existente ori propuse.

În situațiile în care grila nu acoperă explicit anumite elemente relevante, evaluatorul poate utiliza zona de „alte criterii” ori de detaliere, pentru a introduce factorii care cresc sau diminuează riscul și care au rezultat din observația directă, din specificul activității sau din particularitățile obiectivului. Această libertate metodologică trebuie exercitată cu rigoare, justificând fiecare element și evitând arbitrarul.

M–01 · 07

CAPITOLUL 7

T — Tratarea riscurilor și măsurile de securitate

Acest capitol stabilește răspunsul la riscurile identificate și evaluate. Dacă analiza se oprește la constatare, ea rămâne incompletă. Rolul său final este acela de a fundamenta măsurile prin care riscurile sunt reduse, controlate, limitate sau eliminate, astfel încât obiectivul să fie adus ori menținut în domeniul riscului acceptabil.

Măsurile de securitate pot fi organizatorice, procedurale, fizice și tehnice. Măsurile organizatorice privesc repartizarea responsabilităților, stabilirea fluxurilor, desemnarea persoanelor responsabile, controalele interne și integrarea securității în funcționarea curentă a unității. Măsurile procedurale privesc regulile de acces, gestionarea cheilor și a codurilor, deschiderea și închiderea obiectivului, manipularea valorilor, reacția la incidente, raportarea evenimentelor, controlul vizitatorilor, accesul personalului și alte reguli de operare. Măsurile fizice privesc compartimentările, împrejmuirile, grilajele, obloanele, încuietorile, ușile rezistente, seifurile, dulapurile metalice, geamurile protejate și alte elemente mecano-fizice. Măsurile tehnice privesc sistemele de alarmare, detectoarele, butoanele de panică, controlul accesului, televiziunea cu circuit închis, monitorizarea, dispecerizarea și alte componente tehnice.

Legea nr. 333/2003 este deosebit de importantă în acest punct, întrucât definește expres elementele de protecție mecano-fizice și sistemul de alarmare împotriva efracției. În sensul legii, elementele de protecție mecano-fizice includ ziduri, plase, blindaje, case de fier, seifuri, dulapuri metalice, geamuri și folie de protecție, grilaje, uși și încuietori. Sistemul de alarmare împotriva efracției este ansamblul de echipamente electronice care poate include centrală de comandă și semnalizare optică și acustică, detectoare, butoane și pedale de panică, control de acces și televiziune cu circuit închis cu posibilități de înregistrare și stocare a imaginilor și datelor, corespunzător gradului de siguranță impus de caracteristicile obiectivului păzit.

În aceeași logică, Legea nr. 333/2003 stabilește obligația conducătorilor unităților care dețin bunuri, valori sau suporturi de stocare a documentelor, datelor și informațiilor cu caracter secret de stat de a asigura paza, mijloacele mecano-fizice de protecție și sistemele de alarmare în locurile de păstrare, depozitare și manipulare, precum și în locurile unde se desfășoară activități cu un asemenea caracter.

Din punct de vedere metodologic, acest capitol trebuie să facă două delimitări clare.

Prima delimitare privește **limita competenței evaluatorului**. Evaluatorul stabilește necesitatea, categoria, rolul și nivelul măsurilor, dar nu substituie activitatea de proiectare, instalare, modificare ori execuție. El poate arăta că este necesar controlul accesului, dar nu alege în locul proiectantului modelul comercial exact al echipamentului. El poate arăta că sunt necesare compartimentări ori elemente mecano-fizice suplimentare, dar nu execută proiectul de detaliu al lucrărilor. El poate arăta că este necesară conectarea la dispecerat ori monitorizarea, dar nu redactează contractul comercial în locul beneficiarului.

A doua delimitare privește raportul dintre **măsurile obligatorii** și **măsurile recomandate**. Nu toate măsurile propuse au aceeași natură. Unele sunt obligatorii deoarece lipsa lor menține obiectivul în domeniul riscului inacceptabil ori deoarece ele decurg din cerințe legale sau din standardul minim necesar de protecție. Altele

sunt recomandări de optimizare, eficientizare sau consolidare suplimentară. Această diferențiere nu trebuie lăsată pentru final în mod implicit, ci pregătită încă din capitolul de tratare a riscurilor.

Pentru obiectivele existente, evaluatorul trebuie să lucreze pornind de la starea de fapt. El va analiza contractele de pază, monitorizare, instalare și mentenanță, documentele de punere în funcțiune, existența avizărilor necesare, starea dotărilor mecano-fizice, verificările funcționale și modul real de utilizare a măsurilor existente. Pentru obiectivele noi, evaluarea privește măsurile necesare care trebuie prevăzute și implementate astfel încât obiectivul să fie adus de la început într-o stare de securitate conformă.

M–01 · 08

CAPITOLUL 8

A — Analiza și estimarea costurilor de securitate

Estimarea costurilor de securitate este o componentă obligatorie a Raportului de evaluare și tratare a riscurilor la securitatea fizică. Potrivit art. 7 alin. (2) lit. h) din Instrucțiunile M.A.I. nr. 9/2013, raportul trebuie să cuprindă estimarea costurilor de securitate în funcție de măsurile de securitate propuse și de nivelul de risc asumat. Prin urmare, această componentă trebuie inclusă în fiecare analiză de risc întocmită potrivit Instrucțiunilor M.A.I. nr. 9/2013 și nu poate fi tratată ca o secțiune facultativă.

Caracterul obligatoriu al estimării nu transformă raportul într-un deviz, într-o ofertă comercială sau într-un proiect tehnic. Rolul evaluatorului este de a prezenta, într-o manieră justificată și verificabilă, implicația economică a măsurilor propuse și raportul dintre cost, reducerea riscului și nivelul de risc asumat de beneficiar.

Estimarea poate fi exprimată prin valori orientative, intervale de cost, categorii de efort investițional ori alte repere motivate, folosind informații actuale și surse identificabile. Evaluatorul trebuie să precizeze ipotezele utilizate și să se abțină de la stabilirea unor prețuri contractuale ferme atunci când acestea depind de proiectare, cantități, soluții tehnice de detaliu sau oferte ale furnizorilor autorizați.

Costul poate influența prioritizarea, etapizarea și alegerea între opțiuni de tratare echivalente, dar nu poate înlătura o măsură impusă de lege ori indispensabilă încadrării riscului în domeniul acceptabil. Pentru fiecare opțiune de tratare, raportul trebuie să arate atât efectul estimat asupra riscului, cât și ordinul de mărime al efortului economic necesar.

M–01 · 09

CAPITOLUL 9

S — Soluțiile finale, concluziile și documentația finală

Capitolul final închide analiza de risc și trebuie redactat cu deosebită claritate, deoarece aici se transformă întregul raționament anterior într-o concluzie profesională și juridică. Acest capitol nu trebuie să fie o simplă listă de observații, ci o sinteză ordonată care să stabilească explicit: care este situația finală a obiectivului, care este încadrarea sa în raport cu pragul critic, ce măsuri sunt obligatorii, ce măsuri sunt recomandate, ce opțiuni alternative există, care este nivelul de risc rezidual estimat și care este documentația finală ce susține analiza.

În mod obligatoriu, metodologia ARES–SECURITAS trebuie să distingă clar între **măsurile obligatorii** și **recomandări**.

Măsurile obligatorii sunt acele măsuri fără de care obiectivul nu poate fi considerat adus în domeniul riscului acceptabil ori fără de care nu sunt îndeplinite cerințele legale ori minimale de securitate. Ele rezultă fie din legislația aplicabilă, fie din constatarea că lipsa lor menține riscul la un nivel inacceptabil. Aceste măsuri trebuie formulate clar, ferm și fără echivoc. Ele nu se prezintă ca simple sugestii și nu se amestecă cu soluții opționale. Dacă, spre exemplu, lipsa controlului accesului într-o zonă critică, lipsa unui sistem de alarmare, inexistența unor elemente mecano-fizice minimale sau absența unor reguli interne elementare mențin obiectivul în afara domeniului acceptabil, acestea trebuie indicate ca obligații de implementare.

Recomandările sunt acele măsuri care, fără a fi strict indispensabile pentru coborârea sub pragul critic ori fără a decurge direct dintr-o obligație minimală, contribuie la creșterea nivelului de securitate, la redundanță, la eficiență, la ușurința administrării sau la consolidarea protecției. Ele pot viza modernizări, extinderi, optimizări, soluții suplimentare de control, integrarea unor funcții tehnice, îmbunătățirea iluminatului, proceduri interne mai sofisticate, instruiri suplimentare ori alte elemente care sporesc calitatea sistemului de securitate.

Opțiunile alternative de tratare trebuie de asemenea prezentate distinct. Există situații în care riscul poate fi adus în domeniul acceptabil prin mai multe combinații rezonabile de măsuri. De exemplu, o anumită vulnerabilitate poate fi tratată prin pază umană permanentă, prin alarmare combinată cu monitorizare și intervenție ori printr-o soluție mixtă de control acces, protecție mecano-fizică și supraveghere video. În asemenea cazuri, evaluatorul nu trebuie să forțeze artificial o singură formulă, ci poate prezenta opțiuni alternative, cu condiția ca fiecare să fie suficientă pentru atingerea nivelului acceptabil și să fie clar delimitată de măsurile care rămân obligatorii indiferent de opțiune.

Capitolul final trebuie să cuprindă și **nivelul de risc rezidual**. Chiar dacă instrumentul legal central rămâne grila și încadrarea în raport cu pragul critic, din punct de vedere metodologic este util și profesionist ca evaluatorul să exprime riscul rămas după implementarea măsurilor propuse. Aceasta nu trebuie formulată speculativ, ci ca apreciere tehnico-metodologică: dacă măsurile obligatorii și opțiunea de tratare aleasă sunt implementate integral și corect, obiectivul poate fi considerat adus ori menținut în domeniul riscului acceptabil.

În concluziile finale, evaluatorul trebuie să spună explicit dacă obiectivul, în starea existentă, se află ori nu în domeniul riscului acceptabil; dacă nu se află, ce trebuie implementat pentru a ajunge acolo; dacă se află deja, ce măsuri sunt necesare pentru menținere și ce recomandări sunt formulate pentru consolidare. Formulările

trebuie să fie clare, juridice și lipsite de ambiguitate. Nu este suficientă formula vagă „se recomandă luarea unor măsuri”; trebuie precizat ce anume are caracter obligatoriu, ce are caracter recomandat și de ce.

Documentația finală a analizei de risc trebuie să includă raportul de evaluare și tratare a riscurilor, grila de evaluare și documentele-suport. Raportul și grila se semnează de evaluator, iar documentele-suport pot include chestionare, declarații, note de constatare, fotografii, schițe, extrase documentare, contracte analizate, date obținute în teren și orice alte materiale relevante utilizate în procedura de evaluare. Din perspectiva Legii nr. 333/2003, trebuie avut în vedere și faptul că paza se organizează și se efectuează potrivit planului de pază, întocmit de unitate și avizat potrivit legii, plan prin care se stabilesc caracteristicile obiectivului, posturile, personalul, amenajările, instalațiile și mijloacele tehnice de pază și alarmare, regulile de acces și modul de acțiune în diferite situații. Astfel, concluziile analizei de risc trebuie să fie suficient de clare pentru a putea fundamenta, ulterior, măsurile ce vor fi transpuse în planul de pază și în proiectele ori implementările tehnice necesare.

M–01 · 10

FORMULA OFICIALĂ ARES–SECURITAS

ARES–SECURITAS este expresia unei ordini profesionale a evaluării:

S — Scopul evaluării și pregătirea evaluării
E — Evaluarea amplasării geografice și a contextului
C — Cadrul organizațional
U — Unitățile de risc
R — Riscurile analizate
I — Identificarea, analizarea și estimarea riscurilor
T — Tratarea riscurilor și măsurile de securitate
A — Analiza și estimarea costurilor de securitate
S — Soluțiile finale, concluziile și documentația finală

M–01 · 11

NUCLEUL METODOLOGIC CORECT

Forma metodologică finală, curată și coerentă, este următoarea:

vulnerabilitate + amenințare = risc potențial
riscul se poate materializa printr-un eveniment de securitate
evenimentul se produce printr-un modus operandi
evenimentul afectează o zonă de impact și produce consecințe
estimarea legală finală se validează prin grila de evaluare și pragul critic de 60%

M–01 · 12

CONCLUZIE

Metodologia ARES–SECURITAS, în forma sa consolidată, reprezintă un model profesional complet pentru analiza de risc la securitatea fizică. Ea respectă delimitările corecte dintre noțiunile fundamentale, păstrează exactitatea juridică a zonelor funcționale, folosește grila de evaluare ca instrument legal central, ancorează tipurile de riscuri în afectări juridic relevante și integrează obligațiile esențiale care rezultă din Legea nr. 333/2003 privind organizarea pazei, responsabilitatea conducerii unității, planul de pază, mijloacele mecano-fizice și sistemele de alarmare.

În această formă, metodologia nu mai este doar o schemă de lucru, ci poate deveni fundamentul unui **ghid oficial al evaluatorului de risc la securitatea fizică**, redactat în limbaj juridic continuu, apt să susțină atât practica profesională, cât și argumentarea tehnică și legală a raportului de evaluare.