ORDONANŢĂ DE URGENŢĂ Nr. 98 din 3 noiembrie 2010

privind identificarea, desemnarea şi protecţia infrastructurilor critice

Text în vigoare începând cu data de 19 martie 2011

Text actualizat în baza actelor normative modificatoare, publicate în Monitorul Oficial al României, Partea I, până la 16 martie 2011.

Act de bază

#B: Ordonanţa de urgenţă a Guvernului nr. 98/2010

Acte modificatoare

#M1: Legea nr. 18/2011

Modificările şi completările efectuate prin actul modificator sunt scrise cu font italic. În faţa fiecărei modificări sau completări este indicat actul normativ care a efectuat modificarea sau completarea respectivă, în forma #M1.

#CIN

NOTĂ:

Ordonanţa de urgenţă a Guvernului nr. 98/2010 a fost aprobată cu modificări prin Legea nr. 18/2011 (#M1).

#B

Având în vedere că asigurarea unui nivel corespunzător de protecţie a infrastructurilor critice este esenţială pentru dezvoltarea economică, menţinerea funcţiilor vitale ale societăţii şi siguranţa cetăţenilor, precum şi faptul că neadoptarea unei astfel de reglementări în regim de urgenţă ar putea aduce atingere securităţii naţionale datorită impactului semnificativ generat de incapacitatea de a menţine respectivele funcţii până la crearea cadrului normativ pentru protecţia infrastructurilor critice,

având în vedere obligativitatea transpunerii, până la data de 12 ianuarie 2011, a prevederilor Directivei 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora, publicată în Jurnalul Oficial al Uniunii Europene nr. L 345 din 23 decembrie 2008,

ţinând seama de necesitatea adoptării la termenul menţionat a unui set de acte normative indispensabile procesului de implementare a prevederilor directivei,

luând în considerare procedurile pentru identificarea şi desemnarea infrastructurilor critice naţionale şi europene care trebuie realizate până la data menţionată,

întrucât realizarea cadrului normativ secundar, respectiv parcurgerea unor proceduri specifice este condiţionată de existenţa reglementărilor primare în materia protecţiei infrastructurilor critice,

având în vedere faptul că întârzierea îndeplinirii obligaţiei de transpunere corectă şi completă a Directivei 2008/114/CE a Consiliului din 8 decembrie 2008 va aduce prejudicii importante României, constând în îngreunarea procesului de accesare a fondurilor europene puse la dispoziţie prin Programul Comisiei Europene de prevenire, pregătire şi management al consecinţelor actelor teroriste şi al altor riscuri legate de securitate pentru perioada 2007 - 2013, blocarea posibilităţilor de încheiere în timp util a acordurilor între România şi statele membre ale Uniunii Europene implicate în desemnarea infrastructurilor critice europene, nefinalizarea la termenul stabilit a procesului de identificare şi desemnare a infrastructurilor critice şi, pe cale de consecinţă, ar conduce la declanşarea de către Comisia Europeană a procedurii de infrigement împotriva României,

având în vedere că întârzierea încheierii acordurilor bilaterale/multilaterale cu statele membre ale Uniunii Europene pentru desemnarea infrastructurilor critice ar pune România în situaţia de a nu beneficia de o informare imediată şi completă asupra unor posibile efecte transfrontaliere dezastruoase datorate perturbării unor instalaţii, servicii sau sisteme vitale României, aflate pe teritoriul acelor state membre, de aplicarea unor măsuri coordonate şi integrate la nivel european pentru asigurarea protecţiei infrastructurilor critice, precum şi de instrumente pentru limitarea şi eliminarea consecinţelor negative ale perturbării sau distrugerii unor astfel de infrastructuri,

luând în considerare că toate aceste aspecte sunt de interes public şi reprezintă situaţii extraordinare a căror reglementare nu poate fi amânată,

în temeiul art. 115 alin. (4) din Constituţia României, republicată,

Guvernul României adoptă prezenta ordonanţă de urgenţă.

CAPITOLUL I

Dispoziţii generale

Obiect de reglementare

ART. 1

Prezenta ordonanţă de urgenţă stabileşte cadrul legal privind identificarea, desemnarea infrastructurilor critice naţionale/europene şi evaluarea necesităţii de a îmbunătăţi protecţia acestora, în scopul creşterii capacităţii de asigurare a stabilităţii, securităţii şi siguranţei sistemelor economico-sociale şi protecţiei persoanelor.

Domeniul de aplicare

ART. 2

(1) Prevederile prezentei ordonanţe de urgenţă se aplică sectoarelor şi subsectoarelor prevăzute în anexa nr. 1.

(2) Prevederile prezentei ordonanţe de urgenţă se aplică în mod corespunzător sectoarelor stabilite prin directive ale Uniunii Europene.

Definiţii

ART. 3

În sensul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie:

a) infrastructură critică naţională, denumită în continuare ICN - un element, un sistem sau o componentă a acestuia, aflat pe teritoriul naţional, care este esenţial pentru menţinerea funcţiilor vitale ale societăţii, a sănătăţii, siguranţei, securităţii, bunăstării sociale ori economice a persoanelor şi a cărui perturbare sau distrugere ar avea un impact semnificativ la nivel naţional ca urmare a incapacităţii de a menţine respectivele funcţii;

b) infrastructură critică europeană, denumită în continuare ICE - o infrastructură critică naţională, a cărei perturbare sau distrugere ar avea un impact semnificativ asupra a cel puţin două state membre ale Uniunii Europene, denumite în continuare state membre. Importanţa impactului se evaluează din perspectiva criteriilor intersectoriale. Acesta include efectele ce rezultă din relaţiile intersectoriale de dependenţă de alte tipuri de infrastructuri;

c) protecţia infrastructurilor critice, denumită în continuare PIC - orice activitate care are drept scop asigurarea funcţionalităţii, a continuităţii şi a integrităţii ICN/ICE pentru a descuraja, diminua şi neutraliza o ameninţare, un risc sau un punct vulnerabil. Într-o enumerare neexhaustivă, PIC cuprinde activităţile desfăşurate succesiv privind evaluarea şi analiza riscurilor, asigurarea protecţiei informaţiilor clasificate, realizarea planurilor de securitate ale operatorilor de infrastructură critică, denumite în continuare PSO, stabilirea ofiţerilor de legătură şi a modului de realizare a comunicaţiilor, precum şi exerciţii, rapoarte, reevaluări şi actualizări ale documentelor elaborate;

d) analiză de risc - analizarea scenariilor de ameninţări semnificative, pentru a evalua vulnerabilitatea şi impactul potenţial al perturbării sau al distrugerii ICN/ICE;

e) autorităţi publice responsabile - autorităţile publice prevăzute în anexa nr. 1;

f) proprietari/operatori/administratori de ICN/ICE sunt acele entităţi responsabile cu investiţiile într-un element, sistem sau componentă a acestuia, desemnat ca ICN sau ICE, conform prezentei ordonanţe de urgenţă, şi/sau cu operarea/administrarea curentă a acestora;

g) praguri critice - valori-limită stabilite în funcţie de gravitatea impactului, perturbării sau al distrugerii unei infrastructuri şi care determină identificarea acesteia ca ICN/ICE;

h) Reţeaua de alertă privind infrastructurile critice, denumită în continuare CIWIN - sistem securizat de informare şi comunicare destinat asistenţei instituţiilor naţionale şi celorlalte state membre pentru schimbul de informaţii referitoare la vulnerabilităţile, măsurile adecvate reducerii acestora şi strategiile de diminuare a riscurilor;

i) informaţii sensibile privind protecţia infrastructurilor critice - informaţii cu privire la o infrastructură critică ce ar putea fi utilizate, în cazul divulgării, în scopul planificării şi al realizării unor acţiuni care să determine perturbarea sau distrugerea instalaţiilor unor infrastructuri critice;

j) servicii esenţiale - acele servicii, facilităţi ori activităţi care sunt sau ar putea fi necesare pentru a asigura un standard minim de trai şi bunăstare a societăţii şi a căror degradare sau întrerupere a furnizării lor, ca urmare a perturbării ori distrugerii sistemului fizic de bază, ar afecta semnificativ siguranţa sau securitatea populaţiei şi funcţionarea instituţiilor statului.

CAPITOLUL II

Roluri şi responsabilităţi

#M1

Coordonarea naţională

ART. 4

(1) Coordonarea, la nivel naţional, a activităţilor privind identificarea, desemnarea şi protecţia infrastructurilor critice se realizează de către primul-ministru prin consilierul desemnat.

#B

(2) Responsabilitatea pentru organizarea şi desfăşurarea activităţilor necesare implementării prezentei ordonanţe de urgenţă, respectiv realizarea cooperării între autorităţile publice responsabile şi structurile neguvernamentale revin Ministerului Administraţiei şi Internelor, denumit în continuare M.A.I., prin Centrul de coordonare a PIC, care va asigura punctul naţional de contact în relaţia cu alte state membre, Comisia Europeană, Organizaţia Tratatului Atlanticului de Nord şi alte structuri internaţionale, precum şi managementul reţelei CIWIN la nivel naţional.

#M1

Organisme pentru PIC

ART. 5

(1) La nivelul Guvernului, sub coordonarea consilierului desemnat potrivit art. 4 alin. (1), se înfiinţează şi funcţionează grupul de lucru interinstituţional pentru PIC.

#B

(2) Componenţa, atribuţiile şi modul de organizare a Grupului de lucru interinstituţional se stabilesc prin hotărâre a Guvernului.

Evaluări şi rapoarte privind PIC

ART. 6

(1) Autorităţile publice responsabile efectuează, împreună cu proprietarii/operatorii/administratorii de ICN/ICE, o evaluare a riscurilor şi ameninţărilor subsectoarelor ICN/ICE, în termen de un an de la desemnarea infrastructurii critice drept ICN/ICE în cadrul subsectoarelor respective. Evaluarea conţine inclusiv propuneri cu privire la necesitatea îmbunătăţirii protecţiei ICN/ICE desemnate în cadrul subsectoarelor şi se prezintă spre aprobare primului-ministru. Ulterior, evaluarea se realizează anual.

(2) Proprietarii/operatorii/administratorii de ICN/ICE au obligaţia de a informa autorităţile publice responsabile despre orice modificare survenită la nivelul ICN/ICE desemnată.

(3) M.A.I., prin Centrul de coordonare a PIC, transmite Comisiei Europene la fiecare doi ani un raport sinteză cu date generale privind tipurile de riscuri, ameninţări şi puncte vulnerabile identificate în fiecare dintre sectoarele în care a fost desemnată o ICE în temeiul art. 10 şi care se află pe teritoriul naţional.

(4) M.A.I., prin Centrul de coordonare a PIC, transmite Comisiei Europene informări anuale referitoare la numărul de infrastructuri pe sector cu privire la care s-au purtat dezbateri privind pragurile criteriilor intersectoriale.

(5) Raportul prevăzut la alin. (3) va fi analizat în cadrul grupului de lucru interinstituţional pentru PIC, se clasifică, în funcţie de informaţiile pe care le cuprinde, în conformitate cu legislaţia naţională privind informaţiile clasificate şi se transmite Comisiei Europene sub semnătura primului-ministru.

(6) Autorităţile publice responsabile, împreună cu Comisia Europeană şi autorităţile responsabile din celelalte state membre evaluează, în baza rapoartelor bienale, necesitatea de a prevedea măsuri de protecţie suplimentare pentru ICE, la nivel comunitar.

Atribuţiile autorităţilor publice responsabile

ART. 7

(1) M.A.I., prin Centrul de coordonare a PIC, sprijină autorităţile publice responsabile şi proprietarii/operatorii/administratorii de ICN/ICE desemnate, asigurându-le accesul la informaţii cu privire la cele mai bune practici şi metode disponibile, precum şi prin facilitarea participării la acţiunile coordonate de către Comisia Europeană în materie de formare şi de schimb de informaţii privind noi evoluţii tehnice în materie de PIC.

(2) Autorităţile publice responsabile au următoarele atribuţii:

a) stabilesc criteriile sectoriale/intersectoriale şi pragurile critice aferente acestora;

b) coordonează activităţile specifice procesului de identificare a ICN/ICE, în domeniul de responsabilitate;

c) propun desemnarea ICN/ICE corespunzător sectoarelor aflate în responsabilitate;

#M1

d) informează Guvernul, prin consilierul desemnat potrivit art. 4 alin. (1), asupra stadiului de implementare a actelor normative în domeniu;

#B

e) verifică modul de îndeplinire de către proprietarii/operatorii/administratorii de ICN/ICE a obligaţiilor stabilite prin prezenta ordonanţă de urgenţă şi aplică, prin personalul împuternicit, sancţiuni pentru nerespectarea acestora;

f) avizează PSO pentru sectoarele aflate în domeniul de responsabilitate;

g) participă, la solicitarea M.A.I. prin Centrul de coordonare a PIC, la discuţiile bilaterale/multilaterale în vederea încheierii acordurilor pentru desemnarea ICE;

h) stabilesc/dispun, după caz, măsuri de îmbunătăţire a activităţii specifice ICN/ICE în domeniul de responsabilitate;

i) informează M.A.I. asupra stadiului identificării ICN/ICE din domeniul de responsabilitate;

j) asigură resursele financiare necesare organizării şi desfăşurării activităţilor specifice în domeniul PIC;

k) participă, la solicitarea Comisiei Europene, la elaborarea orientărilor pentru aplicarea criteriilor sectoriale şi intersectoriale şi la aproximarea valorilor pragurilor critice care se utilizează pentru identificarea ICE.

(3) Autorităţile publice responsabile şi structurile abilitate conform legii se asigură că informaţiile clasificate cu privire la protecţia ICN/ICE utilizate la nivel naţional, precum şi cele transmise statelor membre sau Comisiei Europene nu sunt utilizate în alt scop decât cel al PIC.

Compartimentul specializat în domeniul ICN/ICE

ART. 8

(1) Autorităţile publice responsabile şi fiecare proprietar/operator/administrator de ICN/ICE au obligaţia să desemneze, din cadrul structurii proprii, un compartiment specializat în domeniul ICN/ICE, care va îndeplini şi rol de punct de contact pentru aspectele care ţin de securitatea infrastructurilor critice între proprietarul/operatorul/administratorul de ICN/ICE şi autorităţile publice responsabile.

(2) Compartimentul prevăzut la alin. (1) este condus de un ofiţer de legătură pentru securitatea ICN/ICE şi se află în directa subordonare a conducătorului autorităţii publice responsabile sau a proprietarului/operatorului/administratorului de ICN/ICE.

(3) Personalul din cadrul compartimentului specializat în domeniul ICN/ICE are atribuţii privind elaborarea, aplicarea, evaluarea şi actualizarea permanentă a planului de măsuri elaborat la nivelul autorităţii publice responsabile, respectiv a PSO.

(4) Autorităţile publice responsabile stabilesc şi implementează un mecanism de comunicare adecvat cu ofiţerii de legătură pentru securitate din cadrul ICN/ICE, în scopul schimbului de date relevante privind riscurile şi ameninţările identificate în legătură cu ICN/ICE respectivă, cu asigurarea securităţii informaţiilor sensibile referitoare la protecţia infrastructurilor critice, conform reglementărilor în vigoare privind accesul la informaţii clasificate.

(5) În termen de maximum 2 ani de la data abilitării, în condiţiile legii, de către instituţiile cu competenţe în domeniu a unităţilor de învăţământ pentru formare şi certificare profesională în domeniul PIC, autorităţile publice responsabile şi proprietarii/operatorii/administratorii de ICN/ICE sunt obligaţi să asigure pregătirea personalului desemnat să îndeplinească funcţia de ofiţer de legătură pentru securitatea infrastructurilor critice.

CAPITOLUL III

Identificarea, desemnarea şi protecţia ICN/ICE

Identificarea ICN/ICE

ART. 9

(1) În conformitate cu procedura prevăzută în anexa nr. 2, autorităţile publice responsabile identifică potenţialele ICN/ICE care corespund criteriilor sectoriale şi intersectoriale şi se încadrează în definiţiile prevăzute la art. 3 lit. a) şi b).

(2) Criteriile sectoriale şi pragurile critice aferente, definite în funcţie de gravitatea impactului perturbării sau al distrugerii unei anumite infrastructuri, se stabilesc prin ordine ale conducătorilor autorităţilor publice responsabile, potrivit domeniilor din responsabilitate, pentru ICN şi potenţiale ICE.

(3) Criteriile intersectoriale ce stau la baza identificării ICN/ICE sunt următoarele:

a) criteriul privind victimele, evaluat în funcţie de numărul posibil de decese sau vătămări;

b) criteriul privind efectele economice, evaluat în funcţie de importanţa pierderilor economice şi/sau a degradării produselor sau serviciilor, inclusiv eventualele efecte asupra mediului;

c) criteriul privind efectul asupra populaţiei, evaluat în funcţie de impactul asupra încrederii acesteia, suferinţa fizică sau perturbarea vieţii cotidiene, inclusiv pierderea de servicii esenţiale.

(4) Criteriile intersectoriale nu sunt cumulative pentru identificarea ICN/ICE.

(5) Pragurile critice aferente criteriilor intersectoriale, definite în funcţie de gravitatea impactului perturbării sau al distrugerii unei anumite infrastructuri se stabilesc prin hotărâre a Guvernului.

(6) Proprietarii/Operatorii/Administratorii de ICN/ICE, precum şi proprietarii, operatorii şi administratorii infrastructurilor care fac obiectul procedurii de identificare şi desemnare ca ICN/ICE au obligaţia de a participa, la solicitarea autorităţilor publice responsabile, la procesul de stabilire a criteriilor şi pragurilor critice.

(7) Pentru stabilirea criteriilor şi a pragurilor critice aferente, autorităţile publice responsabile pot colabora şi cu alte autorităţi sau persoane juridice în condiţiile în care ICN/ICE ar putea genera efecte în domeniul de responsabilitate al acestora.

(8) Sectoarele stabilite pentru punerea în aplicare a prezentei ordonanţe de urgenţă sunt cele prevăzute în anexa nr. 1, iar autorităţile publice responsabile pot identifica ulterior şi alte sectoare, în cazul ICE acordându-se prioritate sectorului Tehnologia informaţiei şi comunicaţii.

(9) La solicitarea Comisiei Europene, autorităţile publice competente sau proprietarii/operatorii/administratorii de ICN/ICE, după caz, vor participa la elaborarea orientărilor pentru aplicarea criteriilor sectoriale/intersectoriale şi

aproximarea valorilor pragurilor care se utilizează pentru identificarea ICE. Utilizarea acestor orientări este opţională pentru autorităţile publice responsabile.

Desemnarea ICN/ICE

ART. 10

(1) În urma procesului de identificare a potenţialelor ICN, autorităţile publice responsabile propun desemnarea ICN.

(2) Desemnarea ICN se aprobă prin hotărâre a Guvernului.

(3) M.A.I., în urma procesului de identificare a potenţialelor ICE, informează statele membre care pot fi afectate în mod semnificativ de o posibilă ICE cu privire la identitatea acesteia şi motivele de desemnare a infrastructurii respective drept potenţială ICE.

(4) Autorităţile publice responsabile se implică, la solicitarea M.A.I. prin Centrul de coordonare a PIC, în dezbateri bilaterale şi/sau multilaterale cu celelalte state membre care pot fi afectate în mod semnificativ de o potenţială ICE situată pe teritoriul naţional sau care pot afecta în mod semnificativ teritoriul naţional, în cazul potenţialelor ICE situate în alte state membre.

#M1

(5) În situaţia în care autorităţile publice responsabile au motive să creadă că teritoriul naţional ar putea fi afectat în mod semnificativ de o potenţială ICE situată într-un alt stat membru, aceasta nefiind însă identificată ca atare de către statul membru pe teritoriul căruia se află potenţiala ICE, informează primul-ministru, prin consilierul desemnat potrivit art. 4 alin. (1). În urma deciziei acestuia, Centrul de coordonare a PIC din cadrul M.A.I. informează Comisia Europeană cu privire la intenţia României de a participa la dezbaterile bilaterale şi/sau multilaterale pe această temă, în vederea solicitării acceptului statului membru pe al cărui teritoriu se află infrastructura care urmează să fie desemnată drept ICE.

#B

(6) Desemnarea ICE se realizează în urma unui acord între România şi statele membre care ar putea fi afectate semnificativ cu acceptul statului membru pe al cărui teritoriu se află infrastructura care urmează să fie desemnată drept ICE.

(7) M.A.I., prin Centrul de coordonare a PIC, informează anual Comisia Europeană cu privire la numărul de ICE desemnate pe fiecare sector, precum şi cu privire la numărul de state membre dependente de fiecare ICE desemnată.

(8) Autorităţile publice responsabile informează proprietarul/operatorul/administratorul de ICN/ICE cu privire la desemnarea acesteia ca ICN/ICE în termen de 10 zile de la intrarea în vigoare a actului normativ de desemnare.

(9) Informaţiile sensibile privind protecţia infrastructurilor critice se clasifică la un nivel adecvat, în condiţiile legii. Diseminarea acestor informaţii se face potrivit principiului nevoii de a cunoaşte, atât în relaţia cu proprietarii/operatorii/administratorii de ICN/ICE, cât şi cu celelalte state membre.

Protecţia ICN/ICE

ART. 11

(1) În termen de 9 luni de la desemnarea unei infrastructuri drept ICN/ICE, proprietarul/operatorul/administratorul de ICN/ICE elaborează PSO şi îl transmite spre avizare autorităţilor publice responsabile.

(2) PSO identifică elementele de infrastructură critică ale ICN/ICE şi soluţiile de securitate existente sau care urmează să fie puse în aplicare pentru protecţia acestora.

(3) Cerinţele minime privind conţinutul PSO sunt prevăzute în anexa nr. 3.

(4) Fiecare autoritate publică responsabilă se asigură, în termen de un an de la desemnarea în sectorul de responsabilitate a unei infrastructuri drept ICN/ICE desemnate, că există un PSO sau un echivalent al acestuia şi că acestea sunt revizuite periodic. Termenul poate fi prelungit în cazuri excepţionale cu acordul primului-ministru şi notificarea Comisiei Europene în acest sens de către Centrul de coordonare a PIC din cadrul M.A.I.

(5) În cazul în care se constată un echivalent al PSO, acesta este evaluat, testat şi, dacă este necesar, revizuit şi actualizat de către proprietarul/operatorul/administratorul de ICN/ICE, conform cerinţelor minime privind conţinutul PSO.

(6) PSO este evaluat, testat şi, dacă este necesar, revizuit şi actualizat de către proprietar/operator/administrator de ICN/ICE, periodic, la intervale de cel mult 2 ani.

(7) În cazul în care există deja acorduri de supraveghere sau de supervizare în privinţa unei ICE, aceste acorduri nu sunt afectate de prezentul articol, iar autoritatea naţională responsabilă pentru sectorul din care face parte ICE respectivă are rolul de autoritate de supraveghere în conformitate cu prevederile acordurilor existente.

CAPITOLUL IV

Contravenţii şi sancţiuni

Contravenţii

ART. 12

Constituie contravenţii următoarele fapte săvârşite de către proprietarii/operatorii/administratorii de ICN/ICE:

a) neluarea măsurilor de constituire a compartimentului specializat în domeniul ICN/ICE, conform art. 8 alin. (1);

b) neîndeplinirea obligaţiilor prevăzute la art. 8 alin. (5);

c) nerespectarea dispoziţiilor privind participarea la procesul de stabilire a criteriilor şi pragurilor critice, conform art. 9 alin. (6);

d) neîntocmirea PSO conform art. 11 alin. (1);

e) nerespectarea obligaţiei de evaluare, revizuire şi actualizare a PSO prevăzută la art. 11 alin. (6), precum şi neîndeplinirea sarcinilor prevăzute în PSO ori a măsurilor stabilite de autorităţile publice responsabile în scopul avizării PSO.

Sancţiuni

ART. 13

(1) Contravenţiile prevăzute la art. 12 se sancţionează după cum urmează:

a) cu amendă de la 2.000 lei la 5.000 lei, contravenţiile prevăzute la art. 12 lit. a) - c);

b) cu amendă de la 10.000 lei la 30.000 lei, contravenţiile prevăzute la art. 12 lit. d) şi e).

(2) Constatarea contravenţiilor şi aplicarea sancţiunilor prevăzute în prezenta ordonanţă de urgenţă se fac de către personalul împuternicit din cadrul autorităţilor publice responsabile.

(3) Contravenţiilor prevăzute la art. 12 le sunt aplicabile dispoziţiile Ordonanţei Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare.

CAPITOLUL V

Dispoziţii finale

Aplicarea prezentei ordonanţe de urgenţă

ART. 14*)

(1) Procesul de identificare şi desemnare a ICN se încheie la data de 30 noiembrie 2010 şi se revizuieşte periodic.

(2) Procesul de identificare şi desemnare a ICE se încheie până la 12 ianuarie 2011 şi se revizuieşte periodic.

(3) După finalizarea activităţilor prevăzute la alin. (2) CE va fi informată de îndată, de către Centrul de coordonare a PIC din cadrul M.A.I., asupra măsurilor dispuse pentru transpunerea prevederilor directivei, transmiţând totodată textele şi tabelul de concordanţă.

#CIN

*) Conform art. II alin. (1) din Legea nr. 18/2011 (#M1), pentru încheierea procesului de identificare şi desemnare a ICN, prevăzut la art. 14 alin. (1) din Ordonanţa de urgenţă a Guvernului nr. 98/2010, se instituie un nou termen, 30 iunie 2011.

#B

Acte normative suplimentare

ART. 15*)

(1) Prin hotărâre a Guvernului se aprobă:

a) componenţa, atribuţiile şi modul de organizare a Grupului de lucru interinstituţional, prevăzute la art. 5 alin. (2), în termen de 30 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă;

b) pragurile critice aferente criteriilor intersectoriale, prevăzute la art. 9 alin. (5), în termen de 60 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă;

c) desemnarea ICN, prevăzută la art. 10 alin. (2), până la data de 30 noiembrie 2010.

(2) Ordinele conducătorilor autorităţilor publice, prevăzute la art. 9 alin. (2) se emit în termen de 60 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă.

#CIN

*) Conform art. II alin. (2) din Legea nr. 18/2011 (#M1), pentru desemnarea ICN, prevăzută la art. 15 alin. (1) lit. c) din Ordonanţa de urgenţă a Guvernului nr. 98/2010, se instituie un nou termen, 30 iunie 2011.

#B

Anexe

ART. 16

Anexele nr. 1 - 3 fac parte integrantă din prezenta ordonanţă de urgenţă.

*

Prezenta ordonanţă de urgenţă transpune prevederile Directivei 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora, publicată în Jurnalul Oficial al Uniunii Europene nr. L 345 din 23 decembrie 2008.

ANEXA 1

LISTA

sectoarelor, subsectoarelor infrastructurii critice naţionale/infrastructurii critice europene (ICN/ICE) şi autorităţilor publice responsabile

1.1. Lista sectoarelor ICN şi a autorităţilor publice responsabile

---

Nr. crt.	Autorităţi publice responsabile	Sectorul	Subsectorul
1.	Ministerul Economiei, Comerţului şi Mediului de Afaceri	Energetic	1.1. Energie electrică, inclusiv nuclearelectrică - capacităţi şi instalaţii pentru producere, depozitare/stocare, reţele de distribuţie şi transport
			1.2. Petrol şi derivate petroliere - capacităţi şi instalaţii pentru extracţie/ producţie, rafinare, tratare, depozitare/stocare, distribuţie şi transport prin conducte, terminale
			1.3. Gaze naturale şi derivate din gaze naturale - capacităţi şi instalaţii pentru extracţie/ producţie, rafinare, tratare, depozitare/stocare, distribuţie şi transport prin conducte, terminale
			1.4. Resurse minerale

#M1

2.	Ministerul Comunicaţiilor şi Societăţii Informaţionale Ministerul Apărării Naţionale Ministerul Educaţiei, Cercetării, Tineretului	Tehnologia informaţiei şi comunicaţii	2.1. Sistemele, reţelele şi serviciile de comunicaţii 2.2. Sisteme de prelucrare, procesare şi stocare a datelor, inclusiv a serviciilor publice electronice 2.3. Infrastructuri de securitate informatică

	şi Sportului		2.4. Sistemele şi reţelele de
	Serviciul de		comunicaţii pentru cifrul de
	Telecomunicaţii Speciale		stat
	Serviciul de Informaţii		2.5. Infrastructuri de emisie
	Externe		radio-tv
	Serviciul Român de		2.6. Servicii poştale la nivel
	Informaţii		naţional

#B

3.	Ministerul Sănătăţii	Alimentare cu	3.1. Furnizarea de apă potabilă
	Ministerul Mediului şi	apă	3.2. Controlul calităţii apei
	Pădurilor		3.3. Îndiguirea şi controlul
			calitativ al apei

#M1

4.	Ministerul Agriculturii	Alimentaţie	4.1. Producţia şi furnizarea de
	şi Dezvoltării Rurale		hrană, asigurarea securităţii
	Autoritatea Naţională		şi siguranţei alimentelor
	Sanitară Veterinară şi		
	pentru Siguranţa		
	Alimentelor		
	Ministerul Economiei,		
	Comerţului şi Mediului		
	de Afaceri		
	Ministerul Educaţiei,		
	Cercetării, Tineretului		
	şi Sportului		

#B

5.	Ministerul Sănătăţii	Sănătate	5.1. Asistenţa medicală şi
	Ministerul Educaţiei,		spitalicească
	Cercetării, Tineretului		5.2. Medicamente, seruri,
	şi Sportului		vaccinuri, produse farmaceutice
			5.3. Biolaboratoare şi

			bioagenţi
			5.4. Servicii de urgenţă
			medicală şi transport sanitar
6.	Ministerul Apărării Naţionale Ministerul Administraţiei şi Internelor Serviciul Român de Informaţii Serviciul de Informaţii Externe Ministerul Economiei, Comerţului şi Mediului de Afaceri Serviciul de Telecomunicaţii Speciale	Securitate naţională	6.1. Apărarea ţării, ordinea publică şi siguranţa naţională 6.2. Sistemul integrat pentru securitatea frontierei de stat 6.3. Industria de apărare, capacităţi şi instalaţii de producţie şi depozitare
7.	Ministerul Administraţiei şi Internelor	Administraţie	7.1. Serviciile şi administraţia 7.2. Serviciile de urgenţă
8.	Ministerul Transporturilor şi Infrastructurii	Transporturi	8.1. Transportul rutier 8.2. Transportul feroviar 8.3. Transportul aerian 8.4. Transportul naval
9.	Ministerul Economiei, Comerţului şi Mediului de Afaceri Ministerul Educaţiei, Cercetării, Tineretului şi Sportului	Industria chimică şi nucleară	9.1. Producţia, procesarea, depozitarea şi utilizarea substanţelor chimice şi materialelor nucleare şi radioactive 9.2. Conductele de produse/

| | | | substanţe chimice periculoase |

| 10.| Ministerul Educaţiei, Cercetării, Tineretului şi Sportului Agenţia Spaţială Română | Spaţiu şi cercetare | 10.1. Spaţiul cosmic
10.2. Cercetare |

1.2. Lista sectoarelor ICE şi a autorităţilor publice responsabile

Autoritatea publică responsabilă	Sectorul	Subsectorul
Ministerul Economiei, Comerţului şi Mediului de Afaceri	I. Energetic	Energie	1.1. Infrastructuri şi electrică| instalaţii pentru producerea, transportul şi distribuţia energiei electrice, inclusiv resursele energetice folosite
		Petrol	1.2. Producţia de petrol, rafinarea, tratarea, depozitarea şi distribuţia prin conducte
		Gaze	1.3. Producţia de gaze, rafinarea, tratarea, depozitarea şi distribuţia prin conducte
			1.4. Terminale GNL
Ministerul Transporturilor şi	II. Transporturi	2.1. Transportul rutier
		2.2. Transportul feroviar

Infrastructurii		
		2.3. Transportul aerian
		2.4. Transportul pe căi navigabile interioare
		2.5. Transportul maritim pe distanţe mici şi porturi

NOTĂ:

Prezenta listă este stabilită în concordanţă cu prevederile Directivei 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora şi se completează pe măsura emiterii directivelor Uniunii Europene pentru desemnarea ICE.

ANEXA 2

PROCEDURA DE IDENTIFICARE

de către autorităţile publice responsabile de infrastructuri critice care pot fi desemnate drept infrastructuri critice naţionale/infrastructuri critice europene (ICN/ICE)

I. Procedura de identificare de către autorităţile publice responsabile de infrastructuri care pot fi desemnate drept ICN

1. Autorităţile publice responsabile identifică infrastructurile critice care pot fi desemnate drept ICN prin parcurgerea următoarelor etape consecutive.

O potenţială ICN care nu satisface cerinţele uneia dintre următoarele etape este considerată non-ICN şi este exclusă din procedură.

2. O potenţială ICN care îndeplineşte cerinţele stabilite face obiectul următoarelor etape ale acestei proceduri.

3. Autoritatea publică responsabilă împreună cu proprietarii/operatorii/administratorii identifică potenţiale ICN, parcurgând următoarele etape:

a) etapa 1 - aplicarea criteriilor şi pragurilor critice sectoriale;

b) etapa 2 - evaluarea preliminară prin aplicarea definiţiei prevăzute la art. 3 lit. a) din ordonanţa de urgenţă;

c) etapa 3 - aplicarea criteriilor şi pragurilor critice intersectoriale;

d) etapa 4 - formularea propunerilor pentru desemnarea ICN.

II. Procedura de identificare de către autorităţile publice responsabile de infrastructuri care pot fi desemnate drept ICE

1. Autorităţile publice responsabile identifică infrastructurile critice care pot fi desemnate drept potenţiale ICE prin parcurgerea următoarelor etape consecutive.

2. O ICE potenţială care nu satisface cerinţele uneia dintre următoarele etape este considerată non-ICE şi este exclusă din procedură.

3. O ICE potenţială care îndeplineşte cerinţele stabilite face obiectul următoarelor etape ale acestei proceduri:

a) etapa 1 - autorităţile publice responsabile aplică ICN desemnate, criteriile sectoriale pentru a efectua o primă selecţie a ICE din cadrul unui sector;

b) etapa 2 - autorităţile publice responsabile aplică definiţia ICE, în temeiul art. 3 lit. b) din ordonanţa de urgenţă, potenţialei ICE identificate în cadrul primei etape. Importanţa impactului se determină fie prin utilizarea metodelor naţionale de identificare a ICE, fie în raport cu criteriile intersectoriale, la un nivel naţional corespunzător. În cazul unei infrastructuri care asigură un serviciu esenţial, se va ţine seama de disponibilitatea unor alternative, precum şi de durata perturbării/repunerii în funcţiune;

c) etapa 3 - autorităţile publice responsabile aplică elementul transfrontalier al definiţiei ICE, în temeiul art. 3 lit. b) din ordonanţa de urgenţă, potenţialei ICE care a trecut de primele două etape ale procedurii. O ICE potenţială care corespunde definiţiei face obiectul următoarei etape a procedurii. În cazul unei infrastructuri care asigură un serviciu esenţial, se va ţine seama de disponibilitatea unor alternative, precum şi de durata perturbării/repunerii în funcţiune;

d) etapa 4 - autorităţile publice responsabile aplică criterii intersectoriale potenţialelor ICE selectate. În cadrul criteriilor intersectoriale se ţine seama de gravitatea impactului şi, în cazul infrastructurilor care furnizează servicii esenţiale, de disponibilitatea unor alternative şi de durata perturbării/repunerii în funcţiune.

4. În procesul de identificare este suficientă îndeplinirea unui criteriu intersectorial pentru ca potenţiala ICE să treacă de această etapă.

5. O potenţială ICE care nu îndeplineşte criteriile intersectoriale nu este considerată ICE.

6. O potenţială ICE care a parcurs această procedură este comunicată doar statelor membre care pot fi afectate în mod semnificativ de ICE potenţială respectivă.

ANEXA 3

PROCEDURĂ

privind planul de securitate pentru operator

1. Prin planul de securitate pentru operator vor fi identificate elementele de infrastructură critică naţională/infrastructură critică europeană (ICN/ICE) şi soluţiile de securitate existente sau care sunt puse în aplicare pentru protecţia acestora.

2. Procedura privind planul de securitate pentru operator al ICN/ICE va acoperi cel puţin următoarele aspecte:

a) identificarea elementelor importante;

b) efectuarea unei analize de risc bazate pe scenarii de ameninţări majore, pe punctele vulnerabile ale fiecărui element şi pe impactul potenţial;

c) identificarea, selectarea şi stabilirea priorităţilor în ceea ce priveşte contramăsurile şi procedurile, făcându-se distincţie între măsurile permanente de securitate, care identifică investiţiile de securitate indispensabile şi mijloacele care sunt relevante pentru utilizarea în orice situaţie. În acest capitol vor fi incluse informaţii referitoare la măsuri de ordin general, cum sunt măsurile tehnice - inclusiv instalarea de mijloace de detectare, de control al accesului, de protecţie şi de prevenire -, măsuri organizatorice - inclusiv proceduri pentru gestionarea alertelor şi a crizelor -, măsuri de control şi verificare, comunicare, sensibilizare şi formare, măsuri de securitate graduale, care pot fi activate în funcţie de diferitele niveluri ale riscurilor şi ameninţărilor, precum şi măsuri în domeniul securităţii sistemelor de informaţii.

DECIZIE nr. 166 din 19 martie 2013 privind aprobarea Normelor metodologice pentru realizarea/echivalarea/revizuirea planurilor de securitate ale proprietarilor/operatorilor/administratorilor de infrastructura critica nationala/europeana, a structurii-cadru a planului de securitate al proprietarului/operatorului/administratorului detinator de infrastructura critica nationala/europeana si a atributiilor ofiterului de legatura pentru securitate din cadrul compartimentului specializat desemnat la nivelul autoritatilor publice responsabile si la nivelul proprietarului/operatorului/administratorului de infrastructura critica nationala/europeana

EMITENT: GUVERNUL - PRIM-MINISTRUL

PUBLICAT: MONITORUL OFICIAL nr. 150 din 21 martie 2013

Având în vedere prevederile art. 4 alin. (1) din Ordonanţa de urgenţă a Guvernului nr. 98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice, aprobată cu modificări prin Legea nr. 18/2011,

în temeiul art. 19 din Legea nr. 90/2001 privind organizarea şi funcţionarea Guvernului României şi a ministerelor, cu modificările şi completările ulterioare,

prim-ministrul emite prezenta decizie.

ART. 1

Se aprobă Normele metodologice pentru realizarea/echivalarea/revizuirea planurilor de securitate ale proprietarilor/operatorilor/administratorilor de infrastructură critică naţională/europeană prevăzute în anexa nr. 1.

ART. 2

Se aprobă structura-cadru a planului de securitate al proprietarului/operatorului/administratorului deţinător de infrastructură critică naţională/europeană, prevăzută în anexa nr. 2.

ART. 3

Se aprobă atribuţiile ofiţerului de legătură pentru securitate din cadrul compartimentului specializat desemnat la nivelul autorităţilor publice responsabile şi la nivelul proprietarului/operatorului/administratorului de infrastructură critică naţională/europeană prevăzute în anexa nr. 3.

ART. 4

Anexele nr. 1-3 fac parte integrantă din prezenta decizie.

PRIM-MINISTRU
VICTOR-VIOREL PONTA

Contrasemnează:

Secretarul general al Guvernului,
Ion Moraru

Bucureşti, 19 martie 2013.
Nr. 166.

ANEXA 1

NORME METODOLOGICE
pentru realizarea/echivalarea/revizuirea planurilor de securitate ale proprietarilor/operatorilor/administratorilor de infrastructură critică naţională/europeană

CAP. I
Dispoziţii generale

ART. 1
Prezentele norme metodologice se aplică pentru elaborarea şi avizarea planurilor de securitate ale proprietarilor/operatorilor/administratorilor de infrastructuri critice naţionale/europene, denumite în continuare PSO, respectiv pentru evaluarea şi testarea planurilor de securitate existente în vederea echivalării acestora ca PSO, cât şi pentru revizuirea periodică şi actualizarea acestora.

ART. 2
Scopul prezentelor norme metodologice este de a asigura o concepţie unitară de realizare a PSO, conform prevederilor legale aplicabile.

ART. 3
Termenii utilizaţi în cuprinsul prezentelor norme metodologice sunt definiţi la art. 3 din Ordonanţa de urgenţă a Guvernului nr. 98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice, aprobată cu modificări prin Legea nr. 18/2011, denumită în continuare OUG nr. 98/2010, iar terminologia generală are sensul conform definiţiilor date în cuprinsul documentelor normative aplicabile.

CAP. II
Planurile de securitate ale proprietarilor/operatorilor/administratorilor de infrastructuri critice naţionale/europene

SECŢIUNEA 1
Dispoziţii comune

ART. 4
(1) Proprietarii/Operatorii/Administratorii de infrastructuri critice naţionale/europene elaborează, echivalează sau actualizează, după caz, PSO având la bază cel puţin aspectele precizate în anexa nr. 3 la OUG nr. 98/2010.
(2) În acest scop, proprietarii/operatorii/administratorii de infrastructuri critice naţionale/europene pot utiliza scenariile de ameninţare, acolo unde acestea sunt disponibile, prin procedura de autorizare a operatorului de infrastructură critică.
(3) Echivalarea unor documente existente cu PSO se va realiza respectând principiile ce stau la baza emiterii acestuia, astfel încât acestea să asigure alinierea la cerinţele specifice de protecţie a infrastructurilor critice.

ART. 5
(1) Scenariile de ameninţări se întocmesc de către proprietarii/operatorii/administratorii de infrastructuri critice naţionale/europene pe baza coordonatelor stabilite de către autoritatea publică responsabilă în domeniu.

(2) Proprietarii/Operatorii/Administratorii de infrastructuri critice naţionale din sectorul "tehnologia informaţiei şi comunicaţii" pot utiliza pentru realizarea analizei de risc şi alte instrumente sau tehnici din domeniul managementului riscului.

ART. 6

La elaborarea scenariilor vor fi avute în vedere, după caz, ameninţări de tipul:

a) fenomene meteorologice periculoase;

b) fenomene distructive de origine geologică;

c) accidente, avarii, explozii, incendii;

d) poluări de ape;

e) prăbuşiri de construcţii, instalaţii, amenajări;

f) accident nuclear major sau urgenţă radiologică cu efect transfrontalier;

g) accident major în care sunt implicate substanţe periculoase;

h) boli transmisibile care pot afecta sănătatea publică (epidemii/pandemii);

i) ameninţări teroriste;

j) grave tulburări sociale;

k) alte ameninţări cu specific sectorial, conform criteriilor aprobate în sectorul respectiv;

l) evenimente internaţionale şi/sau cu caracter geopolitic sau de natura ameninţărilor militare, dacă acestea pot genera ameninţări suplimentare la nivelul infrastructurilor critice naţionale.

ART. 7

Responsabilitatea generală pentru stabilirea unor scenarii de ameninţări credibile, în sensul art. 5 şi 6 din prezentele norme metodologice, revine autorităţilor publice responsabile. Pentru stabilirea unor elemente concrete, specifice, ale acestor scenarii, autorităţile publice responsabile se pot consulta asupra aspectelor din domeniile specifice de competenţă.

ART. 8

Consultarea între autorităţile publice responsabile şi structurile cu atribuţii, la care se face referire în art. 7, se poate realiza în mod direct sau prin intermediul Centrului de coordonare a protecţiei infrastructurilor critice din cadrul Ministerului Afacerilor Interne, denumit în continuare CCPIC. Consultarea prin intermediul CCPIC este obligatorie pentru aspectele care cad sub incidenţa art. 6 alin. (3) din OUG nr. 98/2010 sau, în cazul în care din motive obiective această consultare tripartită nu s-a putut realiza, autorităţile publice responsabile informează CCPIC, în scris, asupra elementelor de scenarii stabilite, înainte de realizarea analizelor de risc şi vulnerabilitate.

ART. 9

În scopul asigurării unui cadru unitar de realizare a PSO, CCPIC poate organiza şedinţe, ateliere de lucru şi seminare în vederea armonizării acestuia la nivel naţional.

SECŢIUNEA a 2-a

Cadrul de management al riscului

ART. 10

(1) PSO este documentul de planificare la nivel strategic, cu caracter operativ prin procedurile asociate, destinat realizării managementului riscurilor de la nivelul infrastructurilor critice naţionale/europene.

(2) Structura-cadru a PSO este prezentată în anexa nr. 2 la decizie.

ART. 11

(1) Cadrul general aplicabil pentru managementul riscurilor este stabilit atât prin standarde internaţionale (ISO), ce definesc principii şi linii directoare, cât şi prin diverse tehnici de evaluare a riscurilor existente, pentru fiecare sector de activitate la nivel naţional şi internaţional.

(2) Pentru efectuarea analizelor de risc, proprietarii/operatorii/administratorii de infrastructuri critice naţionale/europene pot utiliza orice metodă sau tehnică de analiză, atât timp cât aceasta este acceptată de autorităţile publice responsabile, astfel:

a) una dintre metodele sau tehnicile descrise de standardele internaţionale în materie;

b) o altă metodă de analiză standardizată pe plan internaţional, cu indicarea standardului public aplicabil;

c) o metodă sau tehnică nestandardizată de analiză ori un procedeu nestandardizat de estimare a consecinţelor, în măsura în care operatorul de infrastructură critică poate să ofere documentaţie detaliată cu privire la modul de aplicare a acesteia/acestuia, să justifice necesitatea şi avantajele alegerii acestei abordări, iar autoritatea publică responsabilă să îşi exprime, în scris, avizul pentru utilizarea respectivei metode sau respectivului procedeu.

(3) Analizele de risc precizează în cuprinsul acestora, în mod obligatoriu, denumirea/tipul metodei utilizate, presupunerile iniţiale avute în vedere, valorile parametrilor iniţiali sau intermediari introduşi în algoritmi şi aproximările realizate, astfel încât, exclusiv pe baza informaţiilor disponibile, o terţă parte să poată expertiza, în cazul în care se consideră necesar, nivelul de conformitate.

ART. 12

Proprietarii/Operatorii/Administratorii de infrastructuri critice naţionale/europene şi autorităţile publice responsabile vor realiza activităţile organizatorice şi administrative necesare pentru respectarea prevederilor ISO aplicabile, atât pentru desfăşurarea activităţilor interne legate de managementul riscurilor, cât şi pentru a asigura interfaţa în procesele de consultare şi comunicare externă.

ART. 13

(1) În realizarea prevederilor art. 12, proprietarii/operatorii/administratorii de infrastructuri critice naţionale/europene şi autorităţile publice responsabile vor acorda o atenţie deosebită următoarelor etape ale managementului riscului:

a) stabilirea contextului;

b) identificarea riscurilor/ameninţărilor;

c) analiza riscurilor;

d) evaluarea riscurilor;

e) modalitatea de abordare a riscurilor;

f) măsuri de protecţie, compensare şi recuperare post- incident;

g) evaluare globală.

(2) Etapele prevăzute la alin. (1) lit. a) "stabilirea contextului" şi lit. b) "identificarea riscurilor/ameninţărilor" sunt definitorii pentru realizarea, în bune condiţii şi la un nivel de calitate comparabil pentru toate părţile vizate, a scenariilor de

ameninţări şi a condiţiilor de realizare a analizelor de risc şi vulnerabilitate, după cum se precizează în cuprinsul secţiunii 1 - "Dispoziţii comune".

(3) Efectuarea analizelor de risc se realizează în conformitate cu prevederile secţiunii 1 "Dispoziţii comune" şi cu cerinţele art. 2 lit. b) din anexa nr. 3 "Procedură privind planul de securitate pentru operator" la OUG nr. 98/2010; estimarea impacturilor potenţiale este descrisă la etapa prevăzută la alin. (1) lit. c) "analiza riscurilor".

(4) Aplicarea etapelor prevăzute la alin. (1) lit. d) "evaluarea riscurilor" şi lit. e) "modalitatea de abordare a riscurilor" este destinată să completeze cadrul general de management al riscurilor şi să ofere planificatorilor şi factorilor decizionali implicaţi informaţiile necesare pentru întocmirea PSO.

SECŢIUNEA a 3-a
Elaborarea şi avizarea PSO

ART. 14

(1) Pentru a facilita elaborarea unitară a PSO, autorităţile publice responsabile emit ordine sau formulează recomandări, aplicabile la nivel de sector ori subsector, cu privire la forma, structura şi cuprinsul planurilor de securitate ale operatorilor.

(2) Ordinele emise de autorităţile publice responsabile nu pot intra în vigoare mai târziu de 6 (şase) luni înainte de termenul prevăzut la art. 11 alin. (1) din OUG nr. 98/2010.

ART. 15

PSO se elaborează şi se transmit, spre avizare, în 2 (două) exemplare originale, autorităţilor publice responsabile.

ART. 16

Proprietarii/Operatorii/Administratorii de infrastructuri critice naţionale/europene transmit, în 2 (două) exemplare originale, autorităţilor publice responsabile documentele ce urmează a fi echivalate cu PSO, prezentând într-un memoriu sau într-o notă justificativă elementele de echivalenţă şi analiza de suficienţă, din care să reiasă satisfacerea necesităţilor PSO, fără elaborarea unui document distinct în acest sens.

ART. 17

(1) În termen de 30 (treizeci) de zile de la primirea de la proprietarii/operatorii/administratorii de infrastructură critică naţională/europeană a PSO sau a documentelor de echivalare, autorităţile publice responsabile vor realiza, după caz, una dintre următoarele acţiuni:

a) avizarea şi returnarea unui exemplar original avizat, cu comunicarea îndeplinirii de către proprietarul/operatorul/administratorul de infrastructură critică naţională/europeană a cerinţei prevăzute la art. 11 alin. (3) din OUG nr. 98/2010;

b) avizarea şi returnarea unui exemplar original, cu obiecţii, motivaţia obiecţiilor, măsurile de corectare şi termenele de conformare;

c) neavizarea şi returnarea ambelor exemplare, cu precizarea motivelor neavizării şi a termenelor de conformare şi retransmitere a documentelor pentru avizare.

(2) În cazurile prevăzute la alin. (1) lit. a) sau b), autorităţile publice responsabile vor transmite către CCPIC, în

termen de 30 de zile, un raport-sinteză cu privire la evaluarea riscurilor şi ameninţărilor, inclusiv propuneri cu privire la necesitatea îmbunătăţirii protecţiei infrastructurilor critice naţionale/europene, în conformitate cu prevederile art. 6 alin. (1) din OUG nr. 98/2010.

ART. 18

Documentele transmise de către proprietarii/operatorii/administratorii de infrastructură critică naţională/europeană către autorităţile publice responsabile, în conformitate cu prevederile art. 15 şi 16, vor fi clasificate în raport cu conţinutul acestora, conform prevederilor legale.

SECŢIUNEA a 4-a

Evaluarea, testarea, revizuirea şi actualizarea PSO şi a planurilor sau documentelor echivalente PSO

ART. 19

(1) PSO şi planurile sau documentele echivalente PSO se evaluează, cu ocazia procesului de avizare la care se face referire în art. 17, de către o comisie compusă din minimum 3 persoane, din care una trebuie să fie ofiţerul de legătură pentru securitate, denumit în continuare OLS, de la nivelul autorităţii publice responsabile, prevăzut la art. 8 alin. (2) din OUG nr. 98/2010.

(2) Pentru analizarea conţinutului capitolelor de specialitate din cuprinsul PSO sau al documentelor echivalente PSO care necesită un înalt nivel de expertiză tehnico-ştiinţifică ori cunoştinţe detaliate despre natura proceselor analizate, autorităţile publice responsabile pot coopta şi reprezentanţi ai altor structuri specializate din România ori pot angaja experţi, persoane fizice şi/sau juridice, cu rol consultativ, fără ca aceştia să facă parte din comisia de evaluare prevăzută la alin. (1). Pentru angajare, reprezentanţii structurilor specializate din România sau experţii, persoane fizice şi/sau juridice, trebuie să obţină în prealabil de la autoritatea naţională competentă un certificat de acces la date şi documente clasificate.

(3) Procesul de evaluare se încheie prin întocmirea unui raport de evaluare, document semnat de toţi membrii comisiei.

ART. 20

(1) PSO şi planurile sau documentele echivalente PSO se testează prin exerciţii (interne, naţionale, internaţionale - numai pentru ICE), organizate şi desfăşurate cu o periodicitate de minimum un exerciţiu pe an.

(2) Anumite componente ale PSO sau ale documentelor echivalente PSO se vor testa atât prin exerciţii parţiale (în teren, în punctele de comandă, exerciţii simulate, exerciţii tematice cu forţe şi mijloace etc.), cât şi prin exerciţii de alertare, desfăşurate în mod periodic şi astfel încât să acopere, în timp, o gamă variată de condiţii (anunţate/neanunţate, cu scenariul cunoscut/parţial cunoscut/necunoscut, ziua/noaptea, iarna/vara, în timpul/în afara programului, în weekend/în timpul săptămânii etc.).

(3) Normele de organizare, desfăşurare şi evaluare a exerciţiilor sunt elaborate de către fiecare autoritate publică responsabilă şi aprobate prin ordin sau dispoziţie al/a conducătorului acesteia.

(4) Normele prevăzute la alin. (3) vor preciza modul de evaluare a exerciţiilor, utilizându-se în acest scop metodologii şi sisteme

organizatorice deja consacrate pe plan internaţional (evaluatori-controlori etc.)

(5) Exerciţiile organizate şi desfăşurate în conformitate cu prevederile alin. (1) şi (2) se vor finaliza prin elaborarea unui raport de evaluare a fiecărui exerciţiu.

ART. 21

(1) PSO şi planurile sau documentele echivalente PSO se revizuiesc şi se actualizează la intervale de cel mult 2 ani, în conformitate cu prevederile art. 11 alin. (6) din OUG nr. 98/2010.

(2) Baza pentru revizuirea şi actualizarea PSO o constituie rapoartele de evaluare a exerciţiilor, elaborate de autorităţile publice responsabile în conformitate cu prevederile art. 20 alin. (5).

(3) Actualizarea PSO implică aducerea la zi a unor informaţii, denumiri, cantităţi, valori etc. din cuprinsul PSO, fără modificarea substanţială a conţinutului acestuia şi fără necesitatea de reluare a procesului de avizare a PSO. Modificările aduse PSO în timpul actualizărilor sunt aprobate de conducătorii operatorilor de infrastructuri critice şi sunt comunicate autorităţilor publice responsabile.

(4) Revizuirea PSO constă în reanalizarea şi modificarea substanţială a uneia sau mai multora dintre elementele componente ale PSO şi necesită reluarea procesului de avizare prevăzut în cuprinsul prezentelor norme metodologice.

CAP. III
Dispoziţii finale

ART. 22

Prezentele norme metodologice intră în vigoare de la data publicării în Monitorul Oficial al României, Partea I.

ANEXA 2

STRUCTURA-CADRU
a planului de securitate al
proprietarului/operatorului/administratorului deţinător
de infrastructură critică naţională/europeană

NOTĂ(CTCE)

Imaginea reprezentând "Structura-cadru a planului de securitate al proprietarului/operatorului/administratorului deţinător de infrastructură critică naţională/europeană" se găseşte în Monitorul Oficial al României, Partea I, nr. 150 din 21 martie 2013, la pagina 15 (a se vedea imaginea asociată).

CAPITOLUL I
Dispoziţii generale

1.1. Rolul planului de securitate al proprietarului/operatorului/administratorului deţinător de infrastructură critică naţională/europeană

NOTĂ:

Planul de securitate este un document strategic care:

- defineşte scopul şi obiectivele de securitate ale proprietarului/operatorului/administratorului, pe baza unei evaluări

ariscurilor de securitate;

- stabileşte cadrul general de lucru, cu acoperirea întregului spectru de securitate (prevenire, diminuare, răspuns şi revenire la starea de normalitate), fundamentat pe baza concluziilor rezultate în urma evaluării riscurilor şi ameninţărilor la adresa securităţii;

- reflectă o abordare coordonată a securităţii sistemelor unui proprietar/operator/administrator care integrează toate resursele disponibile pentru asigurarea unei mai bune protecţii a infrastructurii critice;

- identifică elementele-cheie care necesită protecţie (ca rezultat al evaluării riscurilor de securitate);

- stabileşte măsurile de diminuare a riscurilor identificate în urma evaluării riscurilor de securitate, inclusiv măsurile aplicabile pentru fiecare nivel de alertare;

- identifică cu exactitate planurile cu incidenţă în domeniul securităţii (Plan de analiză şi acoperire a riscurilor - PAAR, Plan de evacuare în situaţii de urgenţă, Plan de apărare împotriva incendiilor etc.), procedurile, protocoalele, acordurile şi responsabilităţile operatorului în acest domeniu;

- defineşte un parcurs sau un plan de acţiune pentru stabilirea de noi măsuri care vizează contracararea riscurilor tratate prioritar, în funcţie de impact (măsuri imediate sau pe termen mediu şi lung, după necesitate);

- stabileşte acţiunile şi resursele necesare pentru sprijinirea procesului de implementare a măsurilor pe care le conţine (de exemplu: măsuri de îndepărtare a surselor de risc, de diminuare a consecinţelor, de asigurare a securităţii cibernetice, securitatea tehnologiei informaţiei, pentru controlul documentelor clasificate, pentru gestionarea alertelor etc.).

Prin planul de securitate pentru operator vor fi identificate soluţiile de securitate existente sau care sunt puse în aplicare pentru protecţia elementelor de infrastructură critică naţională/europeană.

Această structură-cadru a PSO este aplicabilă tuturor categoriilor de proprietari/operatori/administratori de infrastructură critică naţională/europeană şi se adresează tuturor tipurilor de riscuri care ameninţă funcţionarea corespunzătoare a proprietarilor/operatorilor/administratorilor deţinători de infrastructură critică naţională/europeană.

1.2. Scop şi obiective

1.2.1. Scop

Scopul PSO este de a contribui la îmbunătăţirea protecţiei infrastructurii critice naţionale/europene aflate în responsabilitatea proprietarului/operatorului/administratorului de infrastructură critică naţională/europeană, prin coordonarea măsurilor de protecţie/securitate existente şi instituirea unor măsuri noi în baza unui proces de management al riscului.

PSO identifică elementele de infrastructură critică ale infrastructurii critice naţionale/europene şi soluţiile de securitate existente sau care urmează să fie puse în aplicare pentru protecţia acestora.

PSO contribuie la îmbunătăţirea nivelului existent al securităţii şi protecţiei infrastructurii critice naţionale/europene, nivel care poate fi afectat de diferite tipuri de ameninţări sau vulnerabilităţi.

1.2.2. Obiective

PSO trebuie să asigure îndeplinirea a cel puţin următoarelor obiective:

- îmbunătăţirea abilităţii operatorului de planificare, prevenire, răspuns şi restaurare a stării de normalitate, în urma producerii unui eveniment ce a afectat infrastructura critică pentru protecţia căreia se elaborează PSO;
- descrierea elementelor componente ale planului de securitate şi definirea măsurilor de control al riscurilor, pentru asigurarea securităţii infrastructurii critice naţionale/europene;
- definirea rolurilor şi responsabilităţilor personalului cu atribuţii în domeniul securităţii infrastructurii critice naţionale/europene;
- fundamentarea necesităţii includerii măsurilor de securitate în activităţile curente ale operatorului;
- stabilirea proceselor pentru elaborarea, menţinerea, actualizarea, evaluarea şi modificarea PSO;
- stabilirea proceselor de identificare şi primire a feedbackului de la părţile interesate (angajaţi, contractanţi, populaţie ş.a.), privind aspectele legate de securitate, incidentele de securitate, activităţile periculoase etc.;
- stabilirea modalităţii de interacţionare cu părţile externe interesate;
- identificarea cerinţelor de pregătire a personalului/partenerilor în ceea ce priveşte implementarea planului de securitate şi planificarea activităţilor de instruire;
- stabilirea modalităţii de investigare a tuturor incidentelor de securitate sau activităţilor care pot genera astfel de evenimente;
- instituirea unui proces de evaluare a eventualelor implicaţii de securitate atunci când se iau decizii în ceea ce priveşte activităţile operatorului;
- reprezentarea clară şi sistematică asupra componentelor infrastructurii critice naţionale/europene din responsabilitatea operatorilor de infrastructură critică;
- reprezentarea ameninţărilor şi vulnerabilităţilor la adresa infrastructurii critice naţionale/europene din responsabilitatea operatorilor de infrastructură critică şi a riscurilor induse de acestea;
- identificarea măsurilor de securitate existente şi a celor necesare suplimentar pentru controlul riscurilor la adresa infrastructurii critice naţionale/europene aflate în responsabilitatea operatorilor de infrastructură critică;
- instituirea capabilităţilor de răspuns şi recuperare a infrastructurii critice naţionale/europene la nivelul operatorilor de infrastructură critică, corelat cu scenariile de ameninţare şi cooperarea cu autorităţile relevante;
- reprezentarea cadrului organizatoric relevant pentru protecţia infrastructurii critice în cadrul operatorilor de infrastructură critică, inclusiv a proceselor necesare pentru funcţionarea acestuia;
- planificarea activităţilor relevante pentru protecţia infrastructurii critice pe perioada de valabilitate;
- stabilirea cadrului de dialog şi cooperare pe probleme de protecţia infrastructurii critice.

1.3. Întocmire, avizare şi aprobare

În termen de 9 luni de la desemnarea unei infrastructuri drept infrastructură critică naţională/europeană, proprietarul/operatorul/administratorul deţinător al acesteia elaborează PSO şi îl transmite spre avizare autorităţilor publice responsabile.

PSO este întocmit de OLS al proprietarului/operatorului/administratorului de infrastructură critică naţională/europeană, aprobat de proprietarul/operatorul/administratorul acesteia, verificat de OLS al autorităţii publice responsabile şi avizat de conducătorul acesteia.

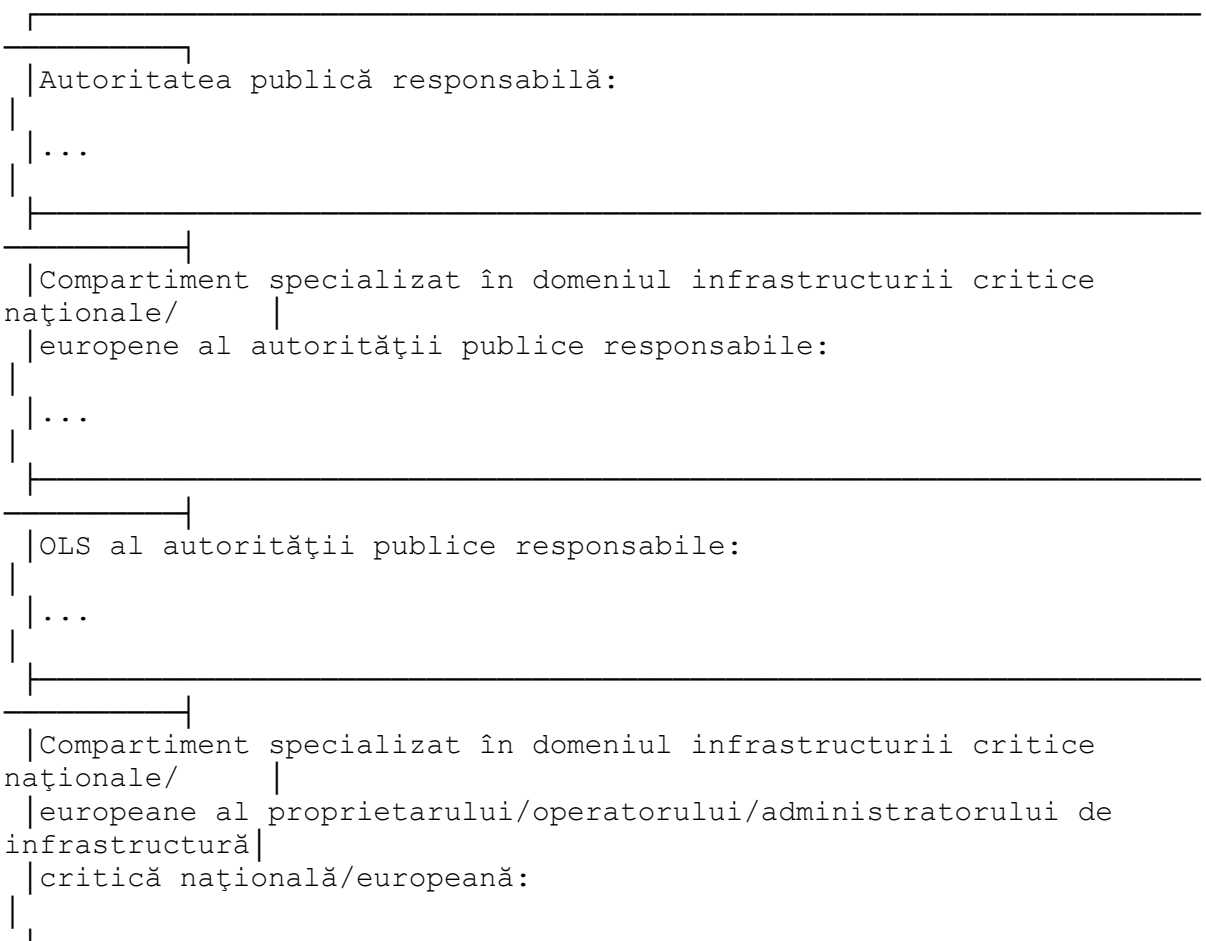
1.4. Confidenţialitate

Informaţiile sensibile privind protecţia infrastructurilor critice se clasifică la un nivel adecvat, în condiţiile legii. Diseminarea acestor informaţii se face potrivit principiului nevoii de a cunoaşte, atât în relaţia cu proprietarii/operatorii/administratorii de infrastructură critică naţională/europeană, cât şi cu celelalte state membre în condiţiile legislaţiei privind protecţia informaţiilor clasificate, şi se supune în totalitate dispoziţiilor acesteia.

CAPITOLUL II

Descriere organizaţională

2.1. Structura organizaţională



OLS al operatorului/proprietarului/administratorului de infrastructură critică naţională/europeană:
...
Organigrama proprietarului/operatorului/administratorului de infrastructură critică naţională/europeană:
...

2.2. Cadrul legislativ

Legi:
...
Ordonanţe de urgenţă ale Guvernului
...
Ordonanţe ale Guvernului
...
Hotărâri ale Guvernului
...
Ordine ale ministrului
...
Standarde naţionale/internaţionale (în funcţie de fiecare caz în parte)
...

Acorduri internaţionale/naţionale
...
Alte documente
...

2.3. Caracteristici ale unităţii administrativ-teritoriale pe raza căreia este amplasată infrastructura critică

Pentru stabilirea caracteristicilor unităţii administrativ-teritoriale pot fi utilizate informaţiile din planul judeţean de analiză şi acoperire a riscurilor aprobat de prefect şi întocmit în conformitate cu Ordinul ministrului administraţiei internelor nr. 132/2007 pentru aprobarea Metodologiei de elaborare a Planului de analiză şi acoperire a riscurilor şi a Structurii-cadru a Planului de analiză şi acoperire a riscurilor.

2.4. Sisteme de operare

Tipul sistemului:
• ...
Harta sistemului
• ...
Tipul serviciului furnizat/serviciilor furnizate
• ...
Statistici privind serviciul furnizat
• ...

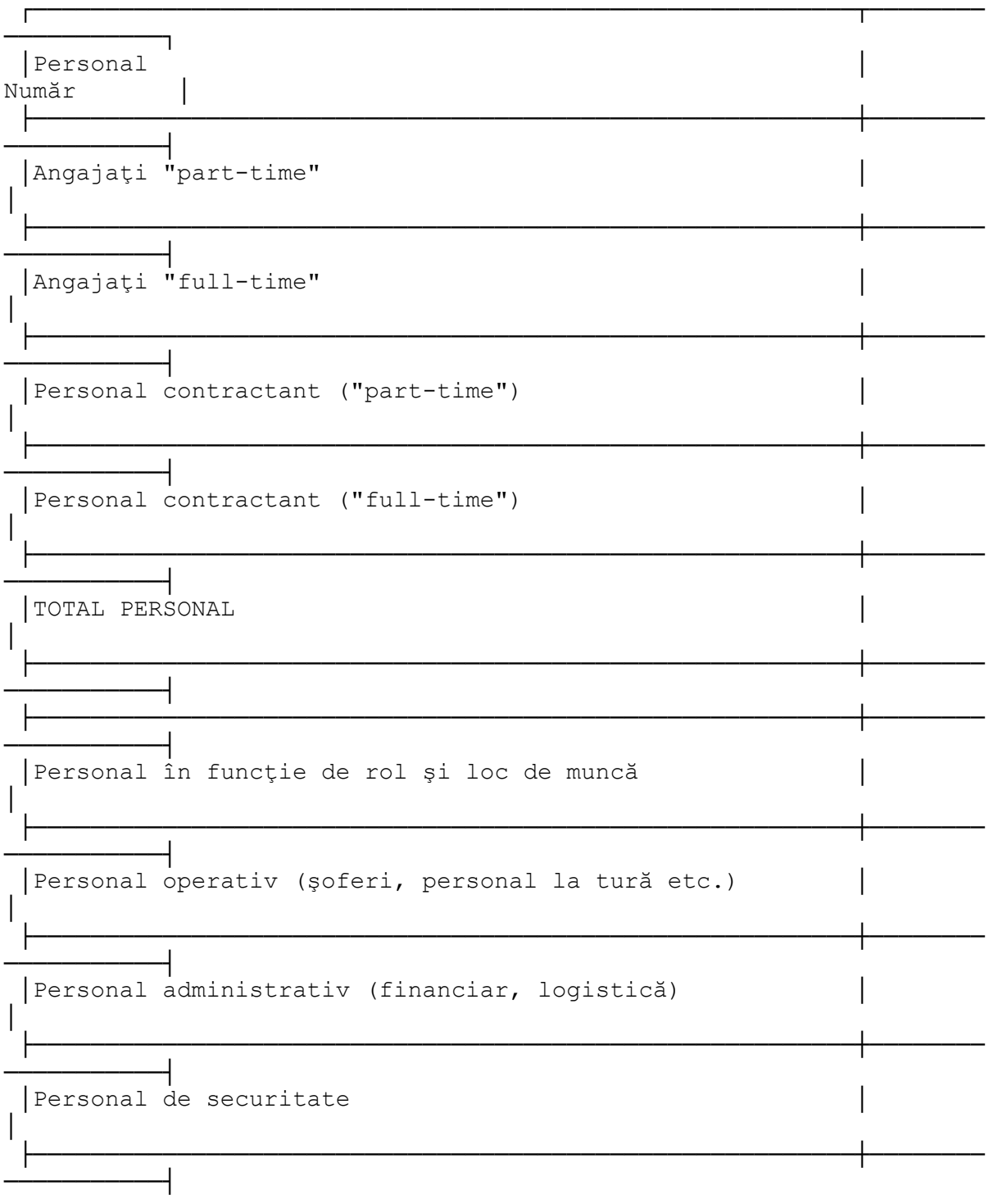
2.5. Descrierea infrastructurii, facilităţilor şi echipamentelor din infrastructura critică naţională/europeană

Se vor menţiona elementele fizice, organizaţionale şi facilităţile necesare funcţionării serviciului esenţial.

Infrastructuri, facilităţi şi echipamente (în acest tabel se vor menţiona elementele fizice, organizaţionale şi facilităţile necesare funcţionării serviciului esenţial, date tehnice etc.)
Staţii de alimentare
Hub-uri
Servere
Depozite
Ateliere de întreţinere
Clădiri administrative
Puncte de comandă
...
Alţi proprietari

2.6. Personal

Se introduc informaţii referitoare la numărul şi categoriile de personal care lucrează în cadrul infrastructurii critice naţionale/europene. Acest lucru permite atât furnizarea unui indicator al dimensiunilor relative şi al semnificaţiei activităţii desfăşurate de operator, cât şi un indicator privind riscurile asociate şi provocările existente legate de îmbunătăţirea securităţii globale a respectivei infrastructuri critice naţionale/europene.



Personal de serviciu (portari, administratori, paznici etc.)	
Personal	
TOTAL PERSONAL	

CAPITOLUL III
Analiza mediilor de securitate

3.1. Aspecte generale privind analiza riscurilor legate de securitate

Analiza riscurilor la adresa securităţii se bazează pe scenariile de ameninţări, identificarea punctelor vulnerabile ale fiecărui element al infrastructurii critice naţionale/europene şi impactul asupra acesteia în cazul producerii unui eveniment nedorit (în cazul exploatării unei vulnerabilităţi de către o ameninţare).

3.2. Istoricul incidentelor

Nr. crt.	Data	Locaţia şi ora incidentului	Tipul incidentului	Scurtă descriere	Cauzele incidentului	Pagube	Echipa care a investigat incidentul
1							
2							
3							
4							
5							
...							

n						

3.3. Facilităţile şi operaţiunile cu grad ridicat de risc

PSO trebuie să identifice acele facilităţi sau aspecte operaţionale care se confruntă cu riscurile cele mai mari. În acest mod măsurile de securitate sunt direcţionate acolo unde pot avea cel mai bun efect.

PSO trebuie să identifice acele surse de risc (facilităţi şi operaţiuni interne sau externe) şi vulnerabilităţi care ar putea genera ori favoriza riscul perturbării sau distrugerii infrastructurii critice naţionale/europene pentru care se elaborează PSO.

Pentru a se realiza acest lucru, trebuie să se iaîn considerare toate sursele plauzibile şi semnificative de risc, precum şi o gamă cât mai largă de consecinţe ale riscului.

3.4. Elementele planului de securitate

3.4.1. Generalităţi

Se vor preciza descriptiv unele aspecte privind capacităţile de securitate ale operatorului (politici, proceduri de securitate, sisteme tehnice şi/sau informatice de securitate etc.).

3.4.2. Securitatea fizică a infrastructurii critice naţionale/europene şi controlul accesului

Se identifică punctele vulnerabile ale infrastructurii critice naţionale/europene şi se menţionează documentele în care sunt menţionate/stabilite măsurile: de prevenire a evenimentelor, de diminuare a impactului, de facilitare a intervenţiei sau de restabilire a serviciilor furnizate de infrastructura critică naţională/europeană în cazul în care acestea devin indisponibile.

Vor fi precizate pe scurt elementele de protecţie perimetrală, sistemele de detecţie şi semnalizare a efracţiei, sistemele de control al accesului, de management al identităţii, de management al vizitatorilor, de detecţie şi stingere a incendiilor, de supraveghere video perimetrală şi a căilor de acces ş.a.

Nr. crt.	Infrastructura critică naţională/europeană (componenta critică)	Elemente de securitate (controlul accesului, managementul identităţii, elemente de protecţie la explozie, ieşiri de urgenţă, căi de evacuare, sisteme de detecţie a efracţiei, sisteme de supraveghere video etc.)	Rolul elementelor de securitate (detectare/ descurajare/, întârziere atac, reducere vulnerabilitate sau amenînţare, alarmare eveniment ş.a.)	Informaţii suplimentare (nr. de înregistrare şi documentele care conţin detalii privind securitatea acesteia

1				
2				
...				
n				

3.4.3. Inspecţii privind securitatea fizică

Se descriu facilităţile, vehiculele şi alte elemente care necesită inspecţie periodică, precum şi modul în care se efectuează verificările. Se vor preciza deficienţele constatate cu ocazia inspecţiilor şi frecvenţa lor, precum şi aspectele referitoare la viabilitatea procedurilor de raportare a constatărilor.

Constatările inspecţiilor de securitate trebuie să se refere la:

- elementele mecanice de protecţie perimetrală (bariere, garduri, porţi de acces auto şi persoane, mijloace de iluminat perimetral ş.a.);
- elemente de protecţie cu echipamente de detecţie şi semnalizare a efracţiei sau cu camere de supraveghere video, după caz;
- elemente de blocare, restricţionare, identificare şi autentificare;
- sisteme de urmărire şi control al accesului;
- sisteme de detectare rapidă a debutului de incendiu şi de stingere a incendiului.

3.4.4. Tehnologia informaţiilor şi reţele de comunicaţii

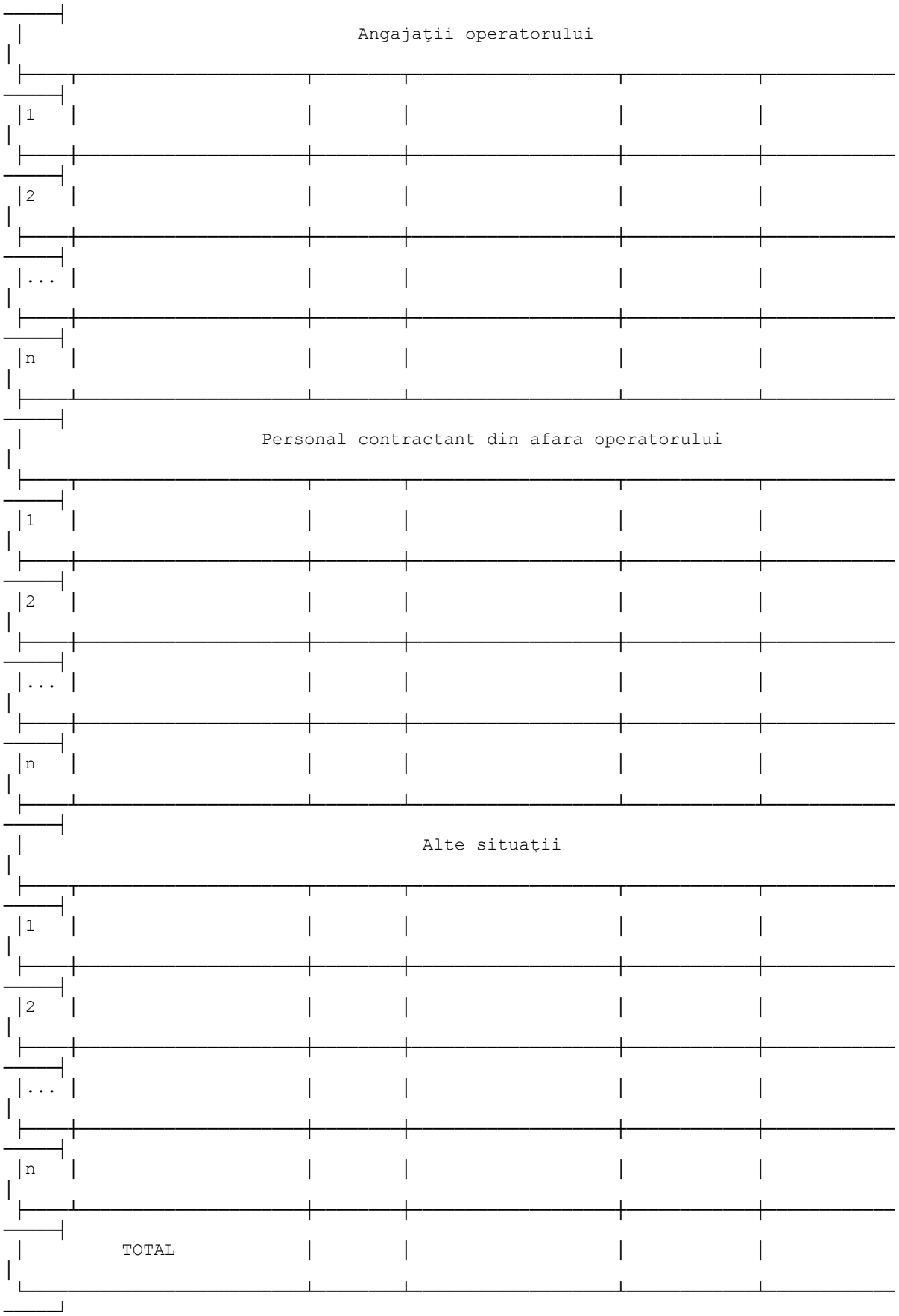
Se identifică şi se descriu succint măsurile sau tehnologiile existente pentru protejarea sistemelor IT împotriva atacurilor cibernetice, intruziunilor electronice sau distrugerilor fizice.

3.4.5. Controlul documentelor

Se indică succint măsurile şi tehnologiile existente pentru protecţia, păstrarea, distrugerea, multiplicarea, arhivarea, ţinerea evidenţei şi limitarea accesului la documente clasificate (planuri de securitate, evaluări de risc, rapoarte de "intelligence", alte documente legate de infrastructuri critice).

3.4.6. Personalul de securitate aferent infrastructurii critice naţionale/europene

Nr. crt.	Numele şi prenumele	Locul de muncă	Tipologia (gardian, paznic operator echipament de securitate ş.a)	Pregătire în domeniu/ Atestat profesional	Nivel acces/ Responsabilităţi



3.4.7. Echipamente şi tehnologii legate de securitate

Se identifică şi se descriu succint tehnologiile deţinute şi programele instalate pe echipamentele operatorului (de exemplu, butoanele de alarmare, de pornire/oprire a instalaţiilor de stingere a incendiilor ş.a.).

Nr. crt.	Tipologii şi programe echipamentului	Modelul	Echipamentele dotate	Informaţii suplimentare
1				
2				
...				
n				

3.4.8. Tehnologia comunicaţiilor

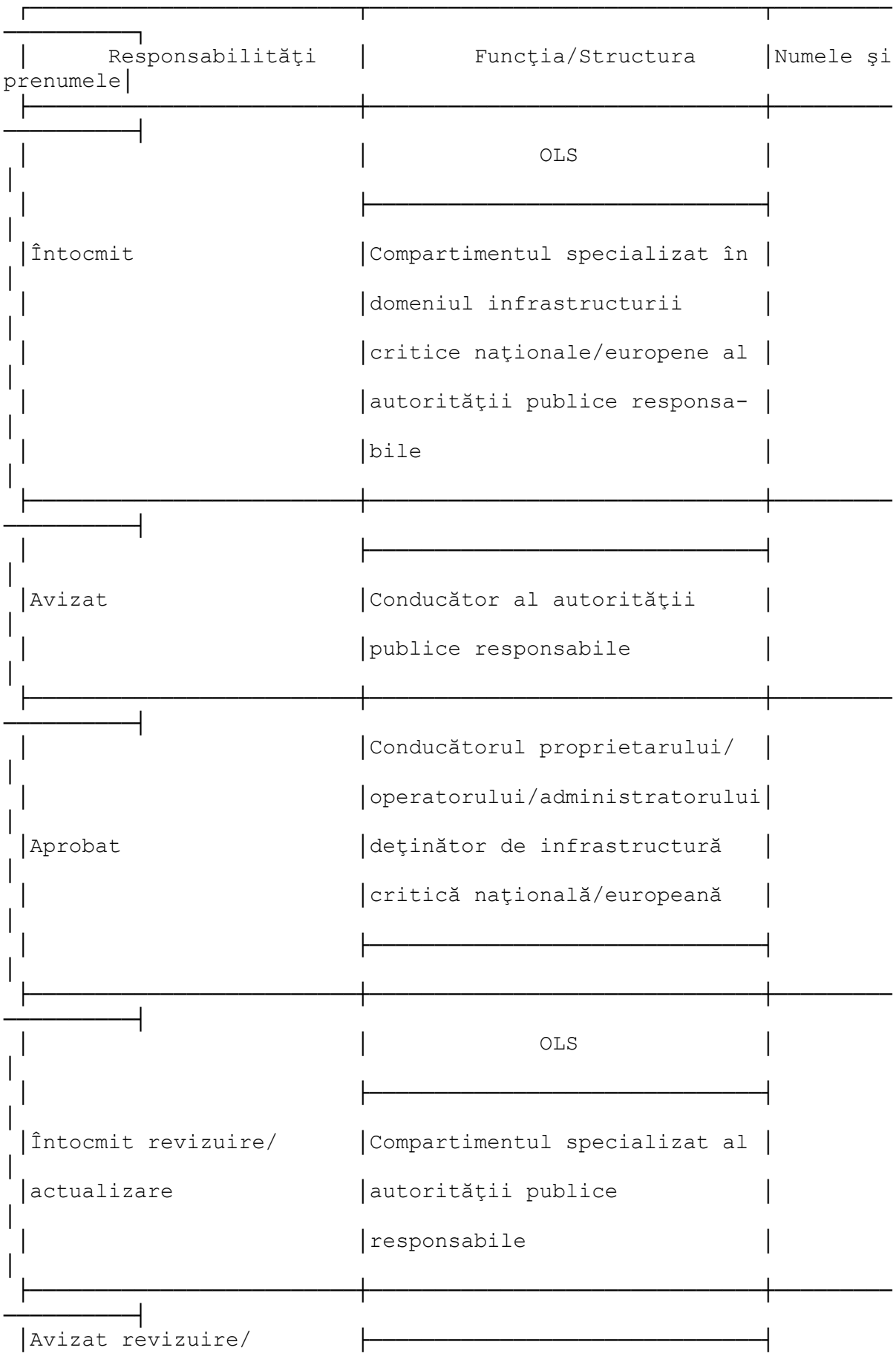
Se identifică şi se descriu succint tehnologia şi procesele utilizate pentru comunicare în situaţie de urgenţă atât cu personalul operatorului, cât şi cu poliţia, pompierii, ambulanţa şi alte servicii publice. De asemenea, trebuie menţionate şi eventualele redundanţe ale sistemelor de comunicaţii prevăzute pentru evitarea defecţiunilor echipamentelor de bază.

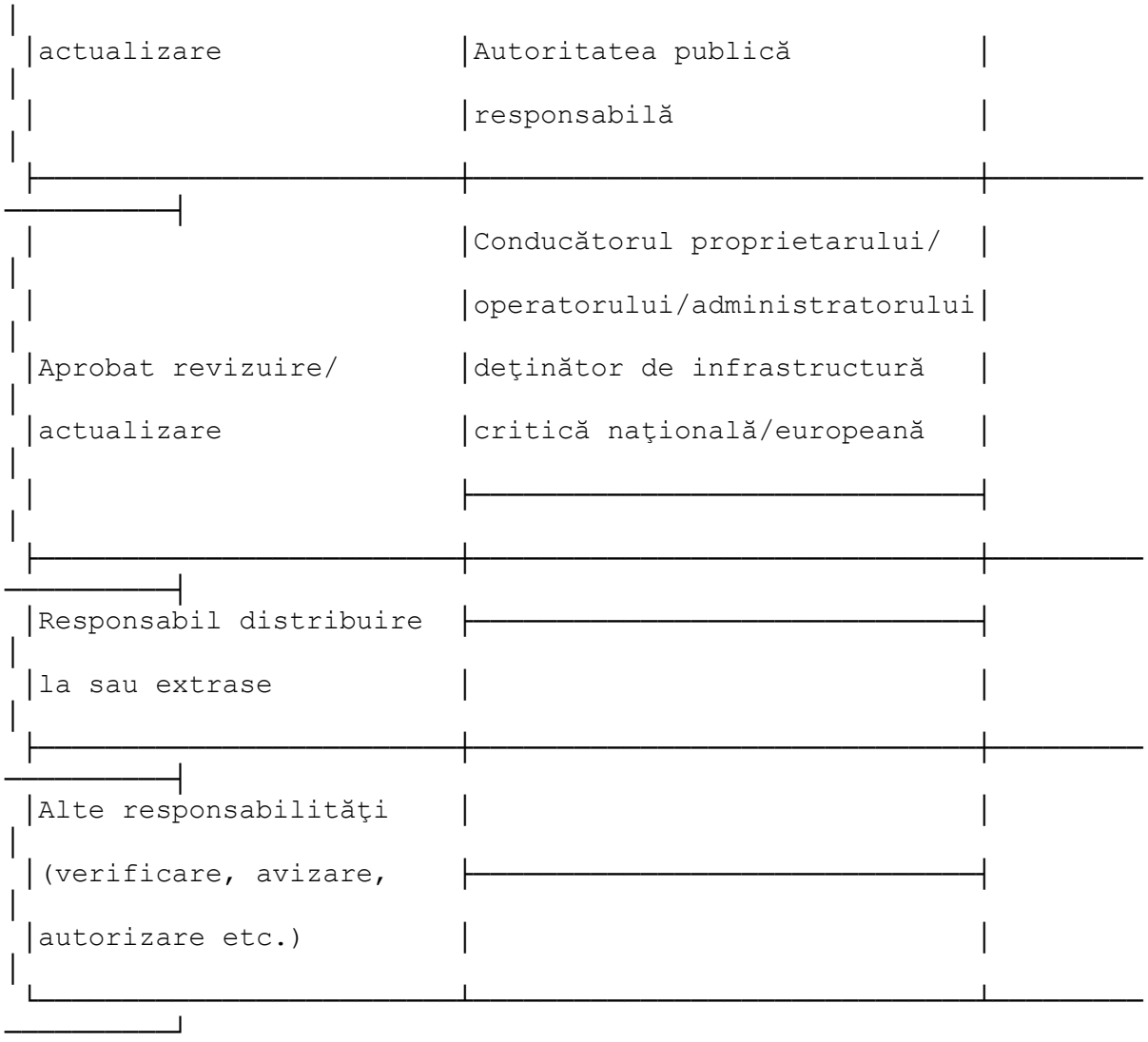
3.4.9. Resurse şi instrumente mixte

Suplimentar aspectelor precizate în celelalte secţiuni, această secţiune trebuie să identifice şi să descrie succint celelalte instrumente şi resurse utilizate de operator pentru îmbunătăţirea abilităţii acestuia de a preveni, de a reduce, de a interveni sau de a restabili starea de normalitate în urma producerii unui eveniment (diferite planuri, proceduri şi procese pentru îmbunătăţirea securităţii; planuri de urgenţă; planuri de intervenţie în diferite situaţii; echipamente speciale precum camerele de luat vederi, detectoarele de fum, dispozitivele electronice de control al accesului ş.a.; proceduri de manipulare a unei bombe; identificarea şi manipularea pachetelor suspecte; proceduri de urmat în cazul unei explozii sau al unui incendiu etc.).

CAPITOLUL IV
Managementul PSO, responsabilităţi şi atribuţii

4.1. Revizuirea şi actualizarea PSO


Responsabilităţi
Funcţia/Structura
Numele şi prenumele
OLS
Întocmit
Compartimentul specializat în domeniul infrastructurii critice naţionale/europene al autorităţii publice responsabile
Avizat
Conducător al autorităţii publice responsabile
Aprobat
Conducătorul proprietarului/ operatorului/administratorului deţinător de infrastructură critică naţională/europeană
OLS
Întocmit revizuire/ actualizare
Compartimentul specializat al autorităţii publice responsabile
Avizat revizuire/



Pentru ca PSO să reflecte cu acurateţe capabilităţile mediilor de securitate ale operatorului, acesta trebuie revizuit şi modificat, dacă este necesar, în fiecare an sau ori de câte ori situaţia o impune. Analiza de risc trebuie revizuită periodic.

4.2. Rolul şi responsabilităţile angajaţilor

4.2.1. Generalităţi

PSO trebuie să conţină responsabilităţile tuturor structurilor operatorului (departamente, direcţii, servicii, birouri compartimente etc.) cu atribuţii în domeniul securităţii infrastructurii critice naţionale/europene.

De exemplu, structurile cu atribuţii de planificare, de management financiar, al resurselor umane, de securitate a muncii, de mentenanţă, de management al riscului, de asigurare logistică etc.

4.2.2. Rolul şi responsabilităţile OLS

Vor fi specificate rolul şi responsabilităţile ofiţerului de legătură pentru securitate în domeniul protecţiei infrastructurilor critice.

4.2.3. Roluri-cheie şi responsabilităţi - Personalul de securitate

În această secţiune vor fi specificate rolurile şi

responsabilităţile ce revin personalului de securitate şi care vor fi atribuite poziţiilor corespunzătoare din statul de funcţiuni al operatorului. Trebuie menţionat că la anumiţi operatori mai mici poate exista şi cumul de funcţii.

4.2.4. Alte categorii de personal

Se vor specifica rolurile şi responsabilităţile ce revin şi altor categorii de personal ale operatorului, în domeniul securităţii infrastructurilor critice.

CAPITOLUL V
Managementul riscului

5.1. Evaluarea riscurilor de securitate

În această secţiune vor fi incluse informaţii referitoare la măsuri de ordin general, cum sunt:

- măsuri organizatorice
- proceduri documentate (de exemplu pentru gestionarea alertelor, comunicare, conştientizare şi sensibilizare personal ş.a.);
- acţiuni de control/verificare periodică al/a funcţionalităţii sistemelor tehnice de securitate şi al/a capacităţii de răspuns şi revenire;
- planificare şi realizare de activităţi de formare şi perfecţionare a personalului în domeniul securităţii infrastructurilor critice;
- măsuri de control şi verificare, comunicare, sensibilizare şi formare;
- măsuri de securitate graduale, care pot fi activate în funcţie de diferitele niveluri ale riscurilor şi ameninţărilor;
- măsuri în domeniul securităţii sistemelor de informaţii;
- măsuri tehnice care includ instalarea de:
- sisteme de protecţie fizică perimetrală (garduri, bariere, porţi de acces ş.a.);
- sisteme de protecţie şi alarmare împotriva efracţiei (cu senzori în infraroşu, microunde, magnetici, de vibraţii sau acustici);
- sisteme de control al accesului (biometrie, smart card, proximitate);
- sisteme de management al vizitatorilor;
- sisteme de supraveghere video pe timp de zi şi noapte (camere TVCI);
- dispecerate de monitorizare, comandă şi control;
- sisteme de detecţie şi stingere a incendiului;
- sisteme de securitate cibernetică (pentru infrastructuri IT şi de comunicaţii).

Lista privind tipurile de riscuri, ameninţările şi punctele vulnerabile identificate în urma analizei de risc efectuate la ICN/ICE desemnată se găseşte în anexa nr. 1, care face parte integrantă din prezentul plan de securitate.

5.1.1. Prevenire, control şi diminuare a riscului

Identificarea, selectarea şi stabilirea priorităţilor în ceea ce priveşte contramăsurile şi procedurile, realizându-se distincţie între măsurile permanente - măsurile permanente de securitate (de natură tehnică), care identifică investiţiile de securitate indispensabile, şi măsurile nepermanente de securitate (de natură organizatorică), care pot fi activate gradual în funcţie de

diferitele niveluri ale riscurilor şi ameninţărilor identificate.

Măsurile de prevenire şi diminuare a riscului derivă din evaluarea de risc efectuată. În cuprinsul acestei secţiuni trebuie precizată şi modalitatea de implementare a acestor măsuri.

Măsurile de control al riscului trebuie stabilite pentru fiecare dintre elementele care fac parte din spectrul securităţii.

Măsurile de prevenire şi diminuare a riscului pentru fiecare tip de risc identificat sunt precizate în anexa nr. 2, care face parte integrantă din prezentul plan de securitate.

5.1.2. Intervenţia sau răspunsul în cazul apariţiei riscului de securitate

Măsurile de securitate referitoare la faza de intervenţie sau de răspuns trebuie să fie prevăzute în planurile specifice de intervenţie în situaţii de urgenţă. PSO trebuie să precizeze cum şi de unde se pot obţine anumite informaţii din planurile specifice de intervenţie, în cazul producerii anumitor incidente de securitate.

5.1.3. Reconstrucţia sau restabilirea stării de normalitate după manifestarea riscului de securitate

Măsurile de securitate în faza de reconstrucţie trebuie să fie prevăzute în planurile de asigurare a continuităţii serviciului. PSO trebuie să precizeze cum şi de unde se pot obţine anumite informaţii din planurile de asigurare a continuităţii serviciului.

5.2. Punctul de comandă şi control (dispeceratul)

Intervenţia efectivă în cazul producerii unui eveniment cu urmări pentru securitatea ICN/ICE necesită luarea unor decizii complexe, spre deosebire de operaţiunile care se desfăşoară în mod curent la nivelul operatorului. PSO trebuie să conţină informaţii despre sistemul de management al crizelor, documentat la nivelul operatorului de infrastructură critică naţională/europeană, dacă există un astfel de sistem, iar dacă nu, să facă trimitere la modul de acţiune şi la persoanele care dispun de autoritatea de decizie în astfel de situaţii, conform planului de intervenţie specific.

În anexa nr. 9, care face parte integrantă din prezentul plan de securitate, este precizat Fluxul informaţional-decizional în cazul producerii unui incident de securitate care poate perturba sau distruge o infrastructură critică naţională/europeană.

Diagrama procesului de schimb de informaţii în domeniul securităţii ICN/ICE

NOTĂ(CTCE)

Imaginea reprezentând "Diagrama procesului de schimb de informaţii în domeniul securităţii ICN/ICE" se găseşte în Monitorul Oficial al României, Partea I nr. 150 din 21 martie 2013, la pagina 22 (a se vedea imaginea asociată).

În anexa nr. 7, care face parte integrantă din prezentul plan de securitate, sunt precizate datele de contact ale persoanelor cu responsabilităţi în domeniul securităţii ICN/ICE.

CAPITOLUL VI
Niveluri de alertă

6.1. Generalităţi

Măsurile preventive sunt luate pentru a menţine un nivel acceptabil de securitate a infrastructurii critice

naţionale/europene în cauză, precum şi pentru a permite asigurarea unui nivel minim de funcţionare corespunzătoare a serviciilor esenţiale pe care le furnizează populaţiei pe timpul crizei respective.

Nivelurile de alertă trebuie stabilite pentru punerea în aplicare a măsurilor de securitate în momentul producerii unui eveniment cu impact asupra infrastructurii critice naţionale/europene. Măsurile preventive sunt întreprinse pentru a menţine la un nivel acceptabil securitatea infrastructurii critice naţionale/europene, precum şi pentru a permite furnizarea continuă către populaţie a serviciului esenţial asigurat de respectiva infrastructură critică naţională/europeană.

6.2. Stabilirea nivelurilor de alertă

Operatorii trebuie să stabilească un sistem de alertare pe niveluri. PSO trebuie să descrie acest sistem şi să stabilească măsurile de securitate ce trebuie puse în aplicare la fiecare nivel de alertă. În mod normal, nivelurile cele mai ridicate de alertă corespund ameninţărilor care pot genera evenimente cu consecinţe foarte grave.

Sistemul de alertare pe niveluri trebuie să conţină următoarele elemente:

- definirea fiecărui nivel de alertă;
- criterii pentru declanşarea alertei şi nivelul acesteia;
- stabilirea persoanelor cu drept de alertare pe tipuri şi pe niveluri de alertă;
- măsurile de securitate care corespund fiecărui nivel de alertă;
- un element care să indice dacă trebuie pus în aplicare planul de intervenţie pentru situaţii de urgenţă (în general, acest plan este pus în aplicare atunci când este necesară activarea punctului de comandă care permite cooperarea cu alte autorităţi cu responsabilităţi de intervenţie);
- detalierea aspectelor referitoare la diseminarea informaţiei privind nivelul de alertă (mecanisme de diseminare a informaţiei, destinatarul informaţiei, nivelul de urgenţă al transmiterii informaţiei), precum şi măsurile ce trebuie întreprinse pentru fiecare nivel de alertă în parte.

6.3. Comunicarea şi armonizarea

Dacă există un sistem de alertare extern în aria de desfăşurare a activităţii operatorului de infrastructură critică naţională/europeană, acesta trebuie să ia în considerare că este necesară armonizarea propriului sistem cu cel extern, pentru a evita conflictele de interese şi confuziile.

6.4. Cadrul legal

În situaţia în care legislaţia obligă operatorul să utilizeze un anumit sistem de alertare, acest aspect trebuie specificat în PSO. În această secţiune vor fi specificate actele normative care reglementează sistemul de alertare.

6.5. Procedurile de alertare

În această secţiune trebuie specificat cum sunt declanşate, anulate sau modificate alertele. În anexa nr. 11 care face parte integrantă din prezentul plan de securitate este descris un model de sistem de alertare pe niveluri.

CAPITOLUl VII
Anexe

- Anexa nr. 1	- Date generale privind riscurile, ameninţările şi punctele vulnerabile la adresa infrastructurii critice naţionale/ europene
- Anexa nr. 2	- Lista cu măsurile de prevenire a producerii evenimentelor nedorite şi de diminuare a riscurilor identificate ca fiind prioritare pentru infrastructura critică naţională/europeană
- Anexa nr. 3	- Lista cu revizuirile PSO
- Anexa nr. 4	- Glosar de termeni şi definiţii în domeniul protecţiei infrastructurilor critice
- Anexa nr. 5	- Acronime
- Anexa nr. 6	- Fişă raportare incident de securitate
- Anexa nr. 7	- Lista cu datele de contact ale persoanelor cu responsabilităţi în domeniul securităţii
- Anexa nr. 8	- Organigrama proprietarului/operatorului/administratorului deţinător de infrastructură critică

naţională/europeană	
- Anexa nr. 9	- Fluxul informaţional-decizional în cazul producerii unui incident de securitate
- Anexa nr. 10	- Relaţia între PSO şi alte documente în domeniul securităţii
- Anexa nr. 11	- Sistem de alertare pe niveluri

NOTĂ:
Anexele nr. 3, 4, 5, 6, 8 şi 10 se completează de către deţinătorul de ICN/ICE în funcţie de situaţie, ţinând cont de specificul domeniului de responsabilitate.

ANEXA 1
----
la planul de securitate

DATE GENERALE
privind riscurile, ameninţările şi punctele vulnerabile la adresa infrastructurii critice naţionale/europene
"

_____ "

INFRASTRUCTURA CRITICĂ NAŢIONALĂ/EUROPEANĂ
Date: zz-ll-aaaa
1. Autoritatea publică responsabilă:
...
2. Administrator/proprietar/operator de ICN/ICE:
...
3. Conducător:

| ... |

| 4. Ofiţer de legătură pentru securitate: |

| ... |

| 5. Adresa: |

| ... |

| 6. Telefon: |

| ... |

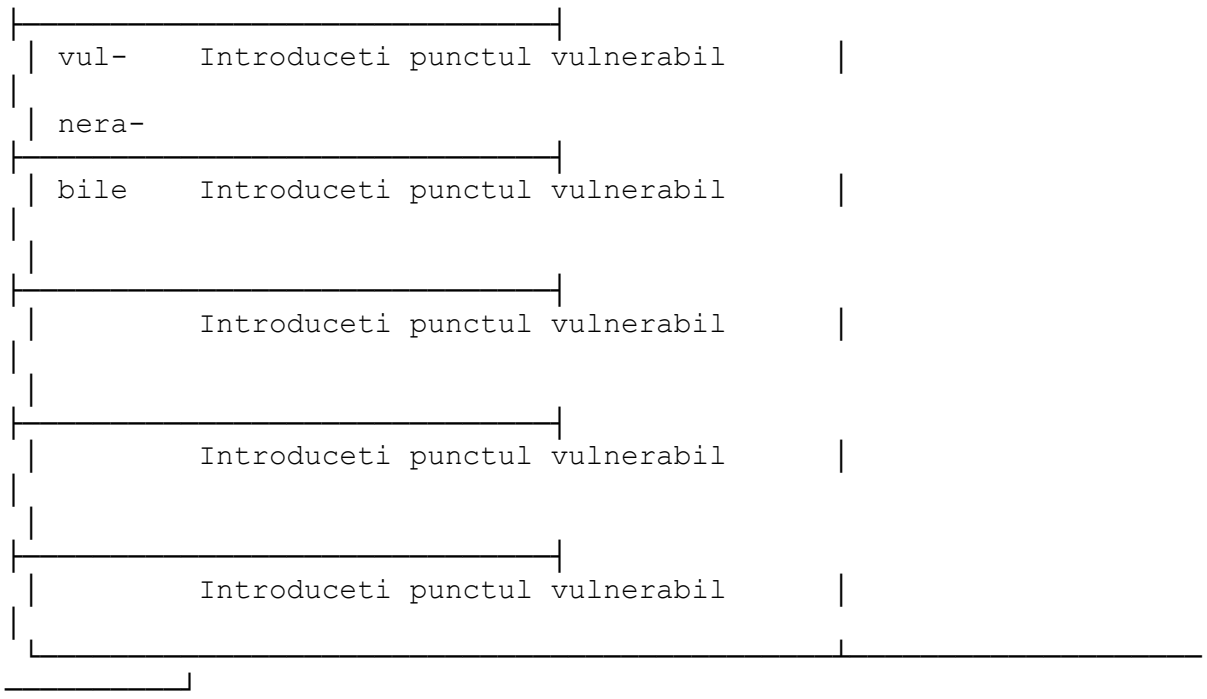
| 7. E-mail: |

| ... |

| PUNCTELE VULNERABILE ALE ICN/ICE |

■■■■■ - Vulnerabilitate foarte ridicată	Estimarea nivelurilor din cadrul PSO (Se indică nivelul de vulnerabilitate)
■■■■ - Vulnerabilitate ridicată	
■■■ - Vulnerabilitate medie	
■■ - Vulnerabilitate scăzută	
■ - Vulnerabilitate foarte scăzută	
Introduceti punctul vulnerabil	
Introduceti punctul vulnerabil	

| Puncte |



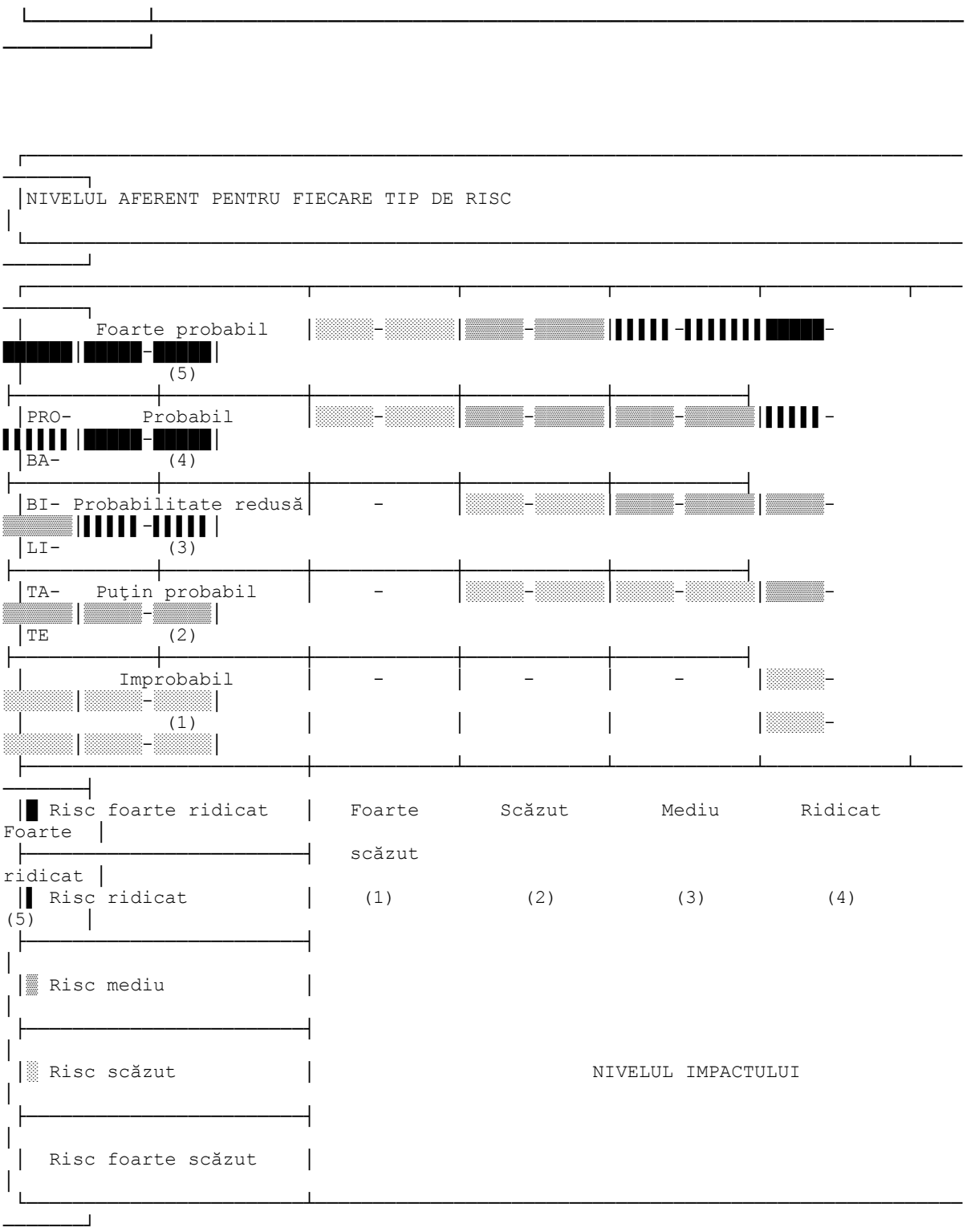
AMENINŢĂRILE

Nr. crt.	Tipuri de ameninţări
1	Introduceţi ameninţarea
2	Introduceţi ameninţarea
3	Introduceţi ameninţarea
4	Introduceţi ameninţarea
5	Introduceţi ameninţarea

6	Introduceţi ameninţarea
...	Introduceţi ameninţarea
n	Introduceţi ameninţarea

RISCURI DE SECIRITATE

Nr. crt.	Tipuri de risc
1	Introduceţi riscul
2	Introduceţi riscul
3	Introduceţi riscul
4	Introduceţi riscul
5	Introduceţi riscul
6	Introduceţi riscul
...	Introduceţi riscul
n	Introduceţi riscul



NOTĂ:

Fiecare tip de risc va fi trecut în matricea riscului în căsuţa aferentă după stabilirea nivelului impactului şi a probabilităţii de producere.

ANEXA 2

---

la planul de securitate

LISTA
cu măsurile de prevenire a producerii evenimentelor nedorite şi de diminuare a riscurilor identificate ca fiind prioritare pentru infrastructura critică naţională/europeană

Nr. crt.	Riscul de securitate identificat	Măsuri de aproximative implementării	Măsuri de prevenire diminuare implementare (reducere)	Costuri îndepli- nire	Data	Responsabil Stadiu de măsură şi raportare rezultate
1	...	...	...			
2	...	...	...			
3	...	...	...			
4	...	...	...			
5	...	...	...			
6	...	...	...			
7	...	...	...			
...	...	...	...			
n	...	...	...			

ANEXA 3
----
la planul de securitate

LISTA
cu revizuirile PSO

Nr. crt.	Numărul de înregistrare	Secţiunile revizuite	Data revizuirii	Observaţii
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
...				
11				

ANEXA 4
----
la planul de securitate

GLOSAR
de termeni şi definiţii în domeniul protecţiei infrastructurilor critice

A
B
C
D
E
F
G
H
I
J
K

L
M
N
O
P
R
S
Ş
T
Ţ
U
V
X
Z
Y
W

ANEXA 5
----
la planul de securitate

ACRONIME

Acronime	Detaliere
ICE	Infrastructură critică europeană
ICN	Infrastructură critică naţională
PIC	Protecţia infrastructurilor critice
OLS	Ofiţer de legătură pentru securitate
APR	Autoritate publică responsabilă
PSO	Plan de securitate pentru operator
TIC	Tehnologia informaţiei şi comunicaţiilor
...	

ANEXA 6
----
la planul de securitate

Fişă raportare incident de securitate

Secţiunea A. Informaţii generale de contact ale raportorului incidentului

Nume: ... 	Prenume: ...
Structură: ... 	Funcţia: ...
Telefon fix: ... 	Telefon mobil: ...
Fax: ... 	E-mail: ...

Secţiunea B. Informaţii generale privind incidentul de securitate

Data producerii incidentului: zz-ll-aaaa 	Data detecţiei incidentului: zz-ll-aaaa
Ora producerii incidentului: hh:mm 	Ora detecţiei incidentului: hh:mm
Data încetării incidentului: zz-ll-aaaa 	Ora încetării incidentului: hh:mm
Zona incidentului: ... 	Locaţia specifică: ...

Descrierea incidentului	Observaţii

Secţiunea C. Informaţii privind impactul incidentului de securitate

*Font 9

Gravitate impact:		Nivel de impact al incidentului	Impact asupra altor servicii (efect DOMINO):
Nivelul de impact asupra fiecăruia din serviciile afectate			
▉ Foarte ridicat	...		
▉ Ridicat	...		
▒ Mediu	...		
▒ Scăzut	...		
Foarte scăzut	...		
Angajaţi evacuaţi (DA, NU, NEC)			
...			

Secţiunea D. Informaţii privind persoanele implicate

Nr. crt.	Nume şi prenume	Data naşterii/ vârsta/sex	Adresa	Localitate	Nr. de telefon	E-mail

1	...	...	...	...	...	...
...	...	...	...	...	...	...
n	...	...	...	...	...	...

Secţiunea E. Informaţii generale privind infrastructura critică naţională/europeană afectată

Situaţia infrastructurii critice naţionale/europene	Distrusă	...
	Avariată	...
	Vandalizată	...
	Activitate suspectă	...
	Breşă	...
Denumirea ICN: ...	Locaţia: ...	
Suprafaţă: ...	Nr. angajaţi: ...	
Daune interne: ...	Daune externe: ...	

Secţiunea F. Informaţii privind notificarea producerii incidentului

Nr. crt.	Serviciul anunţat	Data şi ora anunţării	Data şi ora sosirii	Persoana informaţii	Alte
1	Poliţia	...	...	...	...
2	Poliţia locală	...	...	...	...
3	Firmă de pază	...	...	...	...
4	Jandarmerie	...	...	...	...
5	Pompieri	...	...	...	...
6	Ambulanţă	...	...	...	...
7	Alte servicii de salvare	...	...	...	...

ANEXA 7
----
la planul de securitate

Listă cu datele de contact ale persoanelor cu responsabilităţi în domeniul securităţii

Nr. crt.	Nume şi prenume	Structura	Funcţia	Telefon fix	Telefon mobil	E-mail	Fax
1	...	...	...	...	...	...	...
2	...	...	...	...	...	...	...
3	...	...	...	...	...	...	...
4	...	...	...	...	...	...	...
5	...	...	...	...	...	...	...
6	...	...	...	...	...	...	...
7	...	...	...	...	...	...	...
8	...	...	...	...	...	...	...
9	...	...	...	...	...	...	...
10	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...
n	...	...	...	...	...	...	...

ANEXA 8
----
la planul de securitate

ORGANIGRAMA
proprietarului/operatorului/administratorului deţinător de infrastructură critică naţională/europeană

NOTĂ(CTCE)
Imaginea reprezentând "Organigrama proprietarului/operatorului/administratorului deţinător de infrastructură critică naţională/europeană" se gaseşte în Monitorul Oficial al României, Partea I, nr. 150 din 21 martie 2013, la pagina 29 (a se vedea imaginea asociată).

ANEXA 9
----
la planul de securitate

FLUXUL INFORMAŢIONAL-DECIZIONAL
în cazul producerii unui incident de securitate

NOTĂ(CTCE)
Imaginea reprezentând "Fluxul informaţional-decizional în cazul producerii unui incident de securitate" se găseşte în Monitorul Oficial al României, Partea I, nr. 150 din 21 martie 2013, la pagina 29 (a se vedea imaginea asociată).

ANEXA 10
----
la planul de securitate

Relaţia dintre PSO şi alte documente în domeniul securităţii

NOTĂ(CTCE)
Imaginea reprezentând "Relaţia dintre PSO şi alte documente în domeniul securităţii" se găseşte în Monitorul Oficial al României, Partea I, nr. 150 din 21 martie 2013, la pagina 30 (a se vedea imaginea asociată).

ANEXA 11
----
la planul de securitate

Sistem de alertare pe niveluri

Nivelul 1 de alertă - "Conştientizare crescută" - COD VERDE

Criterii de alertare specificaţii	Punerea în aplicare a planului de intervenţie în situaţii de urgenţă	Informare	Măsuri	Interdependenţe	Alte
Introducere criterii	DA/NU/ PROBABIL	Introducere informări (Ex.: Informarea tuturor angajaţilor privind necesitatea unei atenţii sporite)	Introducere măsuri (Ex.: sunt trimise în plus echipe de cercetare în zonele expuse riscului; se întruneşte conducerea pentru analiza potenţialelor ameninţări)	Introducere infrastructuri critice naţionale potenţial afectate	
Nivelul 2 de alertă - "Securitate crescută" - COD GALBEN					
Criterii de alertare specificaţii	Punerea în aplicare a planului de intervenţie în situaţii de urgenţă	Informare	Măsuri	Interdependenţe	Alte
Introducere criterii	DA/NU/ PROBABIL	Introducere informări	Introducere măsuri	Introducere infrastructuri	

				critice	
		(Ex.: Nivel 1	(Ex.: măsuri de	naţionale	
		de informare +	nivel 1 + întă-	potenţial	
		informarea po-	rirea capacită-	afectate	
		pulaţiei deser-	ţii de preveni-		
		vită ce urmează	re a apariţiei		
		să fie	tipului de		
		afectată)	risc)		
Nivelul 3 de alertă - "Securitate maximă" - COD ROŞU					
Criterii de alertare specificaţii	Punerea în aplicare a planului de intervenţie în situaţii de urgenţă	Informare	Măsuri	Interdependenţe	Alte
Introducere criterii	DA/NU/ PROBABIL	Introducere informări	Introducere măsuri	Introducere infrastructuri critice	
		(Ex.: Nivel 2	(Ex.: măsuri de	naţionale	
		de informare +	nivel 2 + pune-	potenţial	
		punerea în a-	rea în aplicare	afectate	
		plicare a tutu-	a măsurilor		
		ror prevederi-	stabilite prin		
		lor celorlalte	planurile		
		planuri de	specifice		
		intervenţiei	pentru tipurile		
		şi răspuns	de risc		
		privind	specifice)		
		informarea)			

ANEXA 3

ATRIBUŢIILE
ofiţerului de legătură pentru securitate din cadrul compartimentului specializat desemnat la nivelul autorităţilor publice responsabile şi la nivelul proprietarului/operatorului/administratorului de infrastructură critică naţională/europeană

I. Ofiţerul de legătură pentru securitate este şeful compartimentului specializat (constituit din minimum 3 persoane) desemnat la nivelul autorităţilor publice responsabile sau la nivelul proprietarului/operatorului/administratorului de infrastructură critică naţională/europeană, se află în directa subordonare a conducătorului autorităţii publice responsabile sau a proprietarului/operatorului/administratorului deţinător de infrastructură critică naţională/europeană şi este:

- persoana responsabilă cu activitatea în domeniul protecţiei infrastructurilor critice/şeful compartimentului, la nivelul autorităţilor publice responsabile;
- şeful compartimentului specializat în domeniul infrastructurii critice naţionale/europene, la nivelul proprietarului/operatorului/administratorului de infrastructură critică naţională/europeană.

Atribuţiile compartimentului desemnat se stabilesc pe baza şi în concordanţă cu prevederile legislaţiei în domeniul protecţiei infrastructurilor critice în vigoare.

II. În îndeplinirea responsabilităţilor, ofiţerul de legătură pentru securitate al autorităţilor publice responsabile are următoarele atribuţii principale:

a) reprezintă punctul de contact al autorităţii publice responsabile în relaţia cu Centrul de coordonare a protecţiei infrastructurilor critice, cu proprietarii/operatorii/administratorii de infrastructură critică naţională/europeană din sectorul/subsectorul aflat în responsabilitate şi celelalte autorităţi publice responsabile, pentru aspectele care ţin de securitatea infrastructurilor critice;

b) organizează, coordonează şi răspunde de activitatea de reevaluare şi actualizare periodică a documentelor specifice domeniului protecţiei infrastructurilor critice elaborate la nivelul compartimentului de specialitate aflat în responsabilitate;

c) răspunde de actualizarea bazei de date aferente mecanismului de comunicare naţional în domeniul protecţiei infrastructurilor critice, privind riscurile, ameninţările şi vulnerabilităţile identificate la adresa infrastructurii critice naţionale/europene din responsabilitate;

d) asigură monitorizarea permanentă a evoluţiei riscurilor, ameninţărilor şi vulnerabilităţilor la adresa infrastructurii critice naţionale/europene din responsabilitate;

e) informează, în dinamică, Centrul de coordonare a protecţiei infrastructurilor critice şi celelalte structuri interdependente asupra evoluţiei riscurilor, ameninţărilor şi vulnerabilităţilor la adresa infrastructurii critice naţionale/europene din aria de responsabilitate;

f) propune măsurile cu caracter imediat în situaţia identificării unor riscuri la nivelul infrastructurii critice

naţionale/europene din responsabilitate;
g) participă, în calitate de reprezentant desemnat al autorităţii publice responsabile, la procesul de stabilire a criteriilor şi pragurilor critice pentru infrastructura critică naţională/europeană din responsabilitate;
h) coordonează activitatea de elaborare a planurilor anuale de verificare prin exerciţii şi activităţi specifice a viabilităţii PSO sau a documentelor echivalente, existente la nivelul proprietarilor/operatorilor/administratorilor de infrastructură critică naţională/europeană din aria de responsabilitate;
i) propune conducerii autorităţii publice responsabile avizarea PSO elaborate la nivelul proprietarilor/operatorilor/administratorilor de infrastructură critică naţională/europeană;
j) propune nominalizarea de către conducătorul autorităţii publice responsabile a unui expert responsabil din cadrul compartimentului desemnat la nivelul autorităţii publice responsabile pe problematica protecţiei infrastructurilor critice, pentru a asigura consiliereoperatorilor de infrastructuri critice, inclusiv în faza de elaborare a scenariilor de ameninţări şi de stabilire a condiţiilor de realizare a analizelor de risc;
k) participă, de regulă, la şedinţele Grupului de lucru interinstituţional pentru protecţia infrastructurilor critice;
l) propune spre aprobare conducătorului autorităţii publice responsabile componenţa nominală a Comisiei de evaluare a PSO;
m) informează periodic Centrul de coordonare a protecţiei infrastructurilor critice cu privire la existenţa/actualizarea PSO;
n) urmăreşte respectarea de către proprietarii/operatorii/administratorii de infrastructură critică naţională/europeană a prevederilor legale privind protecţia infrastructurilor critice;
o) asigură, la solicitarea ofiţerului de legătură al proprietarului/operatorului/administratorului de infrastructură critică naţională/europeană, consultarea celorlalte autorităţi publice responsabile/institute de profil, în vederea elaborării scenariilor de ameninţări;
p) cooperează cu Centrul de coordonare a protecţiei infrastructurilor critice în vederea realizării schimbului de informaţii în domeniul protecţiei infrastructurilor critice;
q) coordonează elaborarea şi transmiterea, la solicitarea Centrului de coordonare a protecţiei infrastructurilor critice, a informărilor, analizelor, materialelor documentare privind infrastructurile critice din sfera de responsabilitate;
r) participă, la solicitarea Centrului de coordonare a protecţiei infrastructurilor critice, la activităţi specifice domeniului (workshopuri, simpozioane, exerciţii de verificare şi testare a PSO etc.);
s) propune, în condiţiile legii, măsuri pentru asigurarea pregătirii personalului desemnat să îndeplinească funcţia de ofiţer de legătură pentru securitatea infrastructurilor critice de la nivelul proprietarilor/operatorilor/administratorilor de infrastructură critică naţională/europeană;
t) organizează şi coordonează activitatea de elaborare şi transmitere a documentelor clasificate, aferente infrastructurii critice naţionale/europene din aria de responsabilitate, asigurând respectarea normelor în vigoare;

u) verifică modul de îndeplinire de către proprietarii/operatorii/administratorii de infrastructură critică naţională/europeană din sectorul de responsabilitate a obligaţiilor stabilite de legislaţia în vigoare şi propune conducătorului autorităţii publice responsabile aplicarea, în condiţiile legii, de sancţiuni pentru nerespectarea acestora;

v) elaborează rapoartele de evaluare a exerciţiilor desfăşurate;

w) coordonează procesul anual de actualizare a listei cu infrastructurile critice din sectorul aflat în competenţă şi informează Centrul de coordonare a protecţiei infrastructurilor critice cu privire la necesitatea actualizării anexei la Hotărârea Guvernului nr. 1.198/2012 privind desemnarea infrastructurilor critice naţionale;

x) urmăreşte permanent îndeplinirea, potrivit competenţelor, a obligaţiilor prevăzute de legislaţia naţională în domeniu.

III. În îndeplinirea responsabilităţilor, ofiţerul de legătură pentru securitate al proprietarului/operatorului/administratorului de infrastructură critică naţională/europeană are următoarele atribuţii principale:

a) reprezintă punctul de contact al proprietarului/operatorului/administratorului de infrastructură critică naţională/europeană în relaţia cu autoritatea publică responsabilă, cu Centrul de coordonare a protecţiei infrastructurilor critice, precum şi alte structuri cu care se află în relaţie de interdependenţă, pentru aspectele care ţin de securitatea infrastructurilor critice;

b) elaborează şi/sau actualizează analiza de risc şi identifică punctele vulnerabile privind infrastructura critică naţională/europeană din responsabilitate sau propune iniţierea demersurilor, în condiţiile legii, pentru desemnarea unei persoane fizice/juridice atestate, care să execute aceste activităţi;

c) elaborează scenariile de ameninţări la adresa infrastructurii critice naţionale/europene din responsabilitate;

d) răspunde de actualizarea periodică a documentelor elaborate la nivelul compartimentului de specialitate al proprietarului/operatorului/administratorului de infrastructură critică naţională/europeană;

e) răspunde de actualizarea bazei de date aferente mecanismului de comunicare naţional în domeniul protecţiei infrastructurilor critice, privind riscurile, ameninţările şi vulnerabilităţile identificate la adresa infrastructurii critice naţionale/europene din responsabilitate;

f) asigură monitorizarea permanentă a evoluţiei situaţiei privind riscurile, ameninţările şi vulnerabilităţile la adresa infrastructurii critice naţionale/europene din responsabilitate;

g) informează, în dinamică, autorităţile publice responsabile şi celelalte structuri interdependente asupra evoluţiei riscurilor, ameninţărilor şi vulnerabilităţilor la adresa infrastructurii critice naţionale/europene;

h) propune măsurile cu caracter imediat în situaţia producerii unor riscuri la nivelul infrastructurii critice naţionale/europene din responsabilitate;

i) participă, la solicitarea autorităţii publice responsabile, la procesul de stabilire a criteriilor şi pragurilor critice pentru infrastructura critică naţională/europeană din responsabilitate;

j) răspunde de evaluarea, testarea şi, după caz, actualizarea şi

revizuirea PSO la termenele stabilite de legislaţia în vigoare;

k) organizează şi conduce exerciţiile şi activităţile specifice cu ocazia testării PSO sau a documentelor echivalente;

l) asigură întocmirea şi înaintarea către autoritatea publică responsabilă, în vederea avizării, a PSO elaborat la nivelul compartimentului de specialitate al proprietarului/operatorului/administratorului de infrastructură critică naţională/europeană;

m) planifică şi asigură, în condiţiile legii, participarea personalului din subordine la activităţi de pregătire de specialitate;

n) asigură elaborarea/transmiterea documentelor clasificate, aferente infrastructurii critice naţionale/europene din aria de responsabilitate, urmărind respectarea prevederilor legale privind accesul la documentele clasificate;

o) urmăreşte permanent îndeplinirea obligaţiilor prevăzute de legislaţia naţională în domeniu.

NORME METODOLOGICE din 19 martie 2013 pentru realizarea/echivalarea/revizuirea planurilor de securitate ale proprietarilor/operatorilor/administratorilor de infrastructura critica nationala/europeana

EMITENT: GUVERNUL - PRIM-MINISTRUL

PUBLICAT: MONITORUL OFICIAL nr. 150 din 21 martie 2013

CAP. I
Dispoziţii generale

ART. 1
Prezentele norme metodologice se aplică pentru elaborarea şi avizarea planurilor de securitate ale proprietarilor/operatorilor/administratorilor de infrastructuri critice naţionale/europene, denumite în continuare PSO, respectiv pentru evaluarea şi testarea planurilor de securitate existente în vederea echivalării acestora ca PSO, cât şi pentru revizuirea periodică şi actualizarea acestora.

ART. 2
Scopul prezentelor norme metodologice este de a asigura o concepţie unitară de realizare a PSO, conform prevederilor legale aplicabile.

ART. 3
Termenii utilizaţi în cuprinsul prezentelor norme metodologice sunt definiţi la art. 3 din Ordonanţa de urgenţă a Guvernului nr. 98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice, aprobată cu modificări prin Legea nr. 18/2011, denumită în continuare OUG nr. 98/2010, iar terminologia generală are sensul conform definiţiilor date în cuprinsul documentelor normative aplicabile.

CAP. II
Planurile de securitate ale proprietarilor/operatorilor/administratorilor de infrastructuri critice naţionale/europene

SECŢIUNEA 1
Dispoziţii comune

ART. 4
(1) Proprietarii/Operatorii/Administratorii de infrastructuri critice naţionale/europene elaborează, echivalează sau actualizează, după caz, PSO având la bază cel puţin aspectele precizate în anexa nr. 3 la OUG nr. 98/2010.
(2) În acest scop, proprietarii/operatorii/administratorii de infrastructuri critice naţionale/europene pot utiliza scenariile de ameninţare, acolo unde acestea sunt disponibile, prin procedura de autorizare a operatorului de infrastructură critică.
(3) Echivalarea unor documente existente cu PSO se va realiza respectând principiile ce stau la baza emiterii acestuia, astfel încât acestea să asigure alinierea la cerinţele specifice de protecţie a infrastructurilor critice.

ART. 5
(1) Scenariile de ameninţări se întocmesc de către

proprietarii/operatorii/administratorii de infrastructuri critice naţionale/europene pe baza coordonatelor stabilite de către autoritatea publică responsabilă în domeniu.

(2) Proprietarii/Operatorii/Administratorii de infrastructuri critice naţionale din sectorul "tehnologia informaţiei şi comunicaţii" pot utiliza pentru realizarea analizei de risc şi alte instrumente sau tehnici din domeniul managementului riscului.

ART. 6

La elaborarea scenariilor vor fi avute în vedere, după caz, ameninţări de tipul:

a) fenomene meteorologice periculoase;

b) fenomene distructive de origine geologică;

c) accidente, avarii, explozii, incendii;

d) poluări de ape;

e) prăbuşiri de construcţii, instalaţii, amenajări;

f) accident nuclear major sau urgenţă radiologică cu efect transfrontalier;

g) accident major în care sunt implicate substanţe periculoase;

h) boli transmisibile care pot afecta sănătatea publică (epidemii/pandemii);

i) ameninţări teroriste;

j) grave tulburări sociale;

k) alte ameninţări cu specific sectorial, conform criteriilor aprobate în sectorul respectiv;

l) evenimente internaţionale şi/sau cu caracter geopolitic sau de natura ameninţărilor militare, dacă acestea pot genera ameninţări suplimentare la nivelul infrastructurilor critice naţionale.

ART. 7

Responsabilitatea generală pentru stabilirea unor scenarii de ameninţări credibile, în sensul art. 5 şi 6 din prezentele norme metodologice, revine autorităţilor publice responsabile. Pentru stabilirea unor elemente concrete, specifice, ale acestor scenarii, autorităţile publice responsabile se pot consulta asupra aspectelor din domeniile specifice de competenţă.

ART. 8

Consultarea între autorităţile publice responsabile şi structurile cu atribuţii, la care se face referire în art. 7, se poate realiza în mod direct sau prin intermediul Centrului de coordonare a protecţiei infrastructurilor critice din cadrul Ministerului Afacerilor Interne, denumit în continuare CCPIC. Consultarea prin intermediul CCPIC este obligatorie pentru aspectele care cad sub incidenţa art. 6 alin. (3) din OUG nr. 98/2010 sau, în cazul în care din motive obiective această consultare tripartită nu s-a putut realiza, autorităţile publice responsabile informează CCPIC, în scris, asupra elementelor de scenarii stabilite, înainte de realizarea analizelor de risc şi vulnerabilitate.

ART. 9

În scopul asigurării unui cadru unitar de realizare a PSO, CCPIC poate organiza şedinţe, ateliere de lucru şi seminare în vederea armonizării acestuia la nivel naţional.

SECŢIUNEA a 2-a

Cadrul de management al riscului

ART. 10

(1) PSO este documentul de planificare la nivel strategic, cu

caracter operativ prin procedurile asociate, destinat realizării managementului riscurilor de la nivelul infrastructurilor critice naţionale/europene.

(2) Structura-cadru a PSO este prezentată în anexa nr. 2 la decizie.

ART. 11

(1) Cadrul general aplicabil pentru managementul riscurilor este stabilit atât prin standarde internaţionale (ISO), ce definesc principii şi linii directoare, cât şi prin diverse tehnici de evaluare a riscurilor existente, pentru fiecare sector de activitate la nivel naţional şi internaţional.

(2) Pentru efectuarea analizelor de risc, proprietarii/operatorii/administratorii de infrastructuri critice naţionale/europene pot utiliza orice metodă sau tehnică de analiză, atât timp cât aceasta este acceptată de autorităţile publice responsabile, astfel:

a) una dintre metodele sau tehnicile descrise de standardele internaţionale în materie;

b) o altă metodă de analiză standardizată pe plan internaţional, cu indicarea standardului public aplicabil;

c) o metodă sau tehnică nestandardizată de analiză ori un procedeu nestandardizat de estimare a consecinţelor, în măsura în care operatorul de infrastructură critică poate să ofere documentaţie detaliată cu privire la modul de aplicare a acesteia/acestuia, să justifice necesitatea şi avantajele alegerii acestei abordări, iar autoritatea publică responsabilă să îşi exprime, în scris, avizul pentru utilizarea respectivei metode sau respectivului procedeu.

(3) Analizele de risc precizează în cuprinsul acestora, în mod obligatoriu, denumirea/tipul metodei utilizate, presupunerile iniţiale avute în vedere, valorile parametrilor iniţiali sau intermediari introduşi în algoritmi şi aproximările realizate, astfel încât, exclusiv pe baza informaţiilor disponibile, o terţă parte să poată expertiza, în cazul în care se consideră necesar, nivelul de conformitate.

ART. 12

Proprietarii/Operatorii/Administratorii de infrastructuri critice naţionale/europene şi autorităţile publice responsabile vor realiza activităţile organizatorice şi administrative necesare pentru respectarea prevederilor ISO aplicabile, atât pentru desfăşurarea activităţilor interne legate de managementul riscurilor, cât şi pentru a asigura interfaţa în procesele de consultare şi comunicare externă.

ART. 13

(1) În realizarea prevederilor art. 12, proprietarii/operatorii/administratorii de infrastructuri critice naţionale/europene şi autorităţile publice responsabile vor acorda o atenţie deosebită următoarelor etape ale managementului riscului:

a) stabilirea contextului;

b) identificarea riscurilor/ameninţărilor;

c) analiza riscurilor;

d) evaluarea riscurilor;

e) modalitatea de abordare a riscurilor;

f) măsuri de protecţie, compensare şi recuperare post- incident;

g) evaluare globală.

(2) Etapele prevăzute la alin. (1) lit. a) "stabilirea

contextului" şi lit. b) "identificarea riscurilor/ameninţărilor" sunt definitorii pentru realizarea, în bune condiţii şi la un nivel de calitate comparabil pentru toate părţile vizate, a scenariilor de ameninţări şi a condiţiilor de realizare a analizelor de risc şi vulnerabilitate, după cum se precizează în cuprinsul secţiunii 1 - "Dispoziţii comune".

(3) Efectuarea analizelor de risc se realizează în conformitate cu prevederile secţiunii 1 "Dispoziţii comune" şi cu cerinţele art. 2 lit. b) din anexa nr. 3 "Procedură privind planul de securitate pentru operator" la OUG nr. 98/2010; estimarea impacturilor potenţiale este descrisă la etapa prevăzută la alin. (1) lit. c) "analiza riscurilor".

(4) Aplicarea etapelor prevăzute la alin. (1) lit. d) "evaluarea riscurilor" şi lit. e) "modalitatea de abordare a riscurilor" este destinată să completeze cadrul general de management al riscurilor şi să ofere planificatorilor şi factorilor decizionali implicaţi informaţiile necesare pentru întocmirea PSO.

SECŢIUNEA a 3-a
Elaborarea şi avizarea PSO

ART. 14

(1) Pentru a facilita elaborarea unitară a PSO, autorităţile publice responsabile emit ordine sau formulează recomandări, aplicabile la nivel de sector ori subsector, cu privire la forma, structura şi cuprinsul planurilor de securitate ale operatorilor.

(2) Ordinele emise de autorităţile publice responsabile nu pot intra în vigoare mai târziu de 6 (şase) luni înainte de termenul prevăzut la art. 11 alin. (1) din OUG nr. 98/2010.

ART. 15

PSO se elaborează şi se transmit, spre avizare, în 2 (două) exemplare originale, autorităţilor publice responsabile.

ART. 16

Proprietarii/Operatorii/Administratorii de infrastructuri critice naţionale/europene transmit, în 2 (două) exemplare originale, autorităţilor publice responsabile documentele ce urmează a fi echivalate cu PSO, prezentând într-un memoriu sau într-o notă justificativă elementele de echivalenţă şi analiza de suficienţă, din care să reiasă satisfacerea necesităţilor PSO, fără elaborarea unui document distinct în acest sens.

ART. 17

(1) În termen de 30 (treizeci) de zile de la primirea de la proprietarii/operatorii/administratorii de infrastructură critică naţională/europeană a PSO sau a documentelor de echivalare, autorităţile publice responsabile vor realiza, după caz, una dintre următoarele acţiuni:

a) avizarea şi returnarea unui exemplar original avizat, cu comunicarea îndeplinirii de către proprietarul/operatorul/administratorul de infrastructură critică naţională/europeană a cerinţei prevăzute la art. 11 alin. (3) din OUG nr. 98/2010;

b) avizarea şi returnarea unui exemplar original, cu obiecţii, motivaţia obiecţiilor, măsurile de corectare şi termenele de conformare;

c) neavizarea şi returnarea ambelor exemplare, cu precizarea motivelor neavizării şi a termenelor de conformare şi retransmitere

a documentelor pentru avizare.

(2) În cazurile prevăzute la alin. (1) lit. a) sau b), autorităţile publice responsabile vor transmite către CCPIC, în termen de 30 de zile, un raport-sinteză cu privire la evaluarea riscurilor şi ameninţărilor, inclusiv propuneri cu privire la necesitatea îmbunătăţirii protecţiei infrastructurilor critice naţionale/europene, în conformitate cu prevederile art. 6 alin. (1) din OUG nr. 98/2010.

ART. 18

Documentele transmise de către proprietarii/operatorii/administratorii de infrastructură critică naţională/europeană către autorităţile publice responsabile, în conformitate cu prevederile art. 15 şi 16, vor fi clasificate în raport cu conţinutul acestora, conform prevederilor legale.

SECŢIUNEA a 4-a

Evaluarea, testarea, revizuirea şi actualizarea PSO şi a planurilor sau documentelor echivalente PSO

ART. 19

(1) PSO şi planurile sau documentele echivalente PSO se evaluează, cu ocazia procesului de avizare la care se face referire în art. 17, de către o comisie compusă din minimum 3 persoane, din care una trebuie să fie ofiţerul de legătură pentru securitate, denumit în continuare OLS, de la nivelul autorităţii publice responsabile, prevăzut la art. 8 alin. (2) din OUG nr. 98/2010.

(2) Pentru analizarea conţinutului capitolelor de specialitate din cuprinsul PSO sau al documentelor echivalente PSO care necesită un înalt nivel de expertiză tehnico-ştiinţifică ori cunoştinţe detaliate despre natura proceselor analizate, autorităţile publice responsabile pot coopta şi reprezentanţi ai altor structuri specializate din România ori pot angaja experţi, persoane fizice şi/sau juridice, cu rol consultativ, fără ca aceştia să facă parte din comisia de evaluare prevăzută la alin. (1). Pentru angajare, reprezentanţii structurilor specializate din România sau experţii, persoane fizice şi/sau juridice, trebuie să obţină în prealabil de la autoritatea naţională competentă un certificat de acces la date şi documente clasificate.

(3) Procesul de evaluare se încheie prin întocmirea unui raport de evaluare, document semnat de toţi membrii comisiei.

ART. 20

(1) PSO şi planurile sau documentele echivalente PSO se testează prin exerciţii (interne, naţionale, internaţionale - numai pentru ICE), organizate şi desfăşurate cu o periodicitate de minimum un exerciţiu pe an.

(2) Anumite componente ale PSO sau ale documentelor echivalente PSO se vor testa atât prin exerciţii parţiale (în teren, în punctele de comandă, exerciţii simulate, exerciţii tematice cu forţe şi mijloace etc.), cât şi prin exerciţii de alertare, desfăşurate în mod periodic şi astfel încât să acopere, în timp, o gamă variată de condiţii (anunţate/neanunţate, cu scenariul cunoscut/parţial cunoscut/necunoscut, ziua/noaptea, iarna/vara, în timpul/în afara programului, în weekend/în timpul săptămânii etc.).

(3) Normele de organizare, desfăşurare şi evaluare a exerciţiilor sunt elaborate de către fiecare autoritate publică responsabilă şi aprobate prin ordin sau dispoziţie al/a

conducătorului acesteia.

(4) Normele prevăzute la alin. (3) vor preciza modul de evaluare a exerciţiilor, utilizându-se în acest scop metodologii şi sisteme organizatorice deja consacrate pe plan internaţional (evaluatori-controlori etc.)

(5) Exerciţiile organizate şi desfăşurate în conformitate cu prevederile alin. (1) şi (2) se vor finaliza prin elaborarea unui raport de evaluare a fiecărui exerciţiu.

ART. 21

(1) PSO şi planurile sau documentele echivalente PSO se revizuiesc şi se actualizează la intervale de cel mult 2 ani, în conformitate cu prevederile art. 11 alin. (6) din OUG nr. 98/2010.

(2) Baza pentru revizuirea şi actualizarea PSO o constituie rapoartele de evaluare a exerciţiilor, elaborate de autorităţile publice responsabile în conformitate cu prevederile art. 20 alin. (5).

(3) Actualizarea PSO implică aducerea la zi a unor informaţii, denumiri, cantităţi, valori etc. din cuprinsul PSO, fără modificarea substanţială a conţinutului acestuia şi fără necesitatea de reluare a procesului de avizare a PSO. Modificările aduse PSO în timpul actualizărilor sunt aprobate de conducătorii operatorilor de infrastructuri critice şi sunt comunicate autorităţilor publice responsabile.

(4) Revizuirea PSO constă în reanalizarea şi modificarea substanţială a uneia sau mai multora dintre elementele componente ale PSO şi necesită reluarea procesului de avizare prevăzut în cuprinsul prezentelor norme metodologice.

CAP. III
Dispoziţii finale

ART. 22

Prezentele norme metodologice intră în vigoare de la data publicării în Monitorul Oficial al României, Partea I.

LEGE
pentru modificarea Ordonanţei de urgenţă a Guvernului nr. 98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice

Parlamentul României adoptă prezenta lege.

ARTICOL UNIC

Ordonanţa de urgenţă a Guvernului nr. 98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice, publicată în Monitorul Oficial al României, Partea I, nr. 757 din 12 noiembrie 2010, aprobată cu modificări prin Legea nr. 18/2011, se modifică după cum urmează:

1. La articolul 7 alineatul (2), litera g) va avea următorul cuprins:

„g) participă, la solicitarea M.A.I. prin Centrul de coordonare a protecţiei infrastructurilor critice, la discuţiile bilaterale/multilaterale în vederea identificării ICE şi realizării schimbului de scrisori necesare desemnării ICE”;

2. Alineatul (6) al articolului 10 va avea următorul cuprins:

„(6) Desemnarea ICE se realizează prin schimb de scrisori între autorităţile competente din România şi din statele membre care ar putea fi afectate semnificativ cu acceptul statului membru pe al cărui teritoriu se află infrastructura care urmează să fie desemnată drept ICE şi se aprobă prin hotărâre a Guvernului.”

Bucureşti, 2015.
Nr.