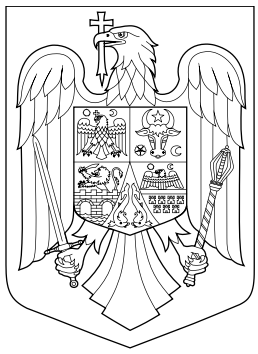


GUVERNUL ROMÂNIEI
PRIMUL-MINISTRU

DECIZIE
privind aprobarea normelor metodologice pentru realizarea/echivalarea/revizuirea planurilor de securitate ale proprietarilor/operatorilor/administratorilor de infrastructură critică națională/europeană, a structurii cadru a planului de securitate al proprietarului/operatorului/administratorului deţinător de infrastructură critică națională/europeană şi a atribuțiilor ofițerului de legătură pentru securitate din cadrul compartimentului specializat desemnat la nivelul autorităților publice responsabile şi la nivelul proprietarului/operatorului/administratorului de infrastructură critică națională/europeană

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

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

primul-ministru emite prezenta decizie.

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

Art. 2. – Se aprobă structura cadru a planului de securitate al proprietarului /operatorului /administratorului deținător de infrastructură critică națională / europeană prevăzută în anexa nr. 2.

Art. 3. – Se aprobă atribuțiile ofițerului de legătură pentru securitate din cadrul compartimentului specializat desemnat la nivelul autorităților publice responsabile și la nivelul proprietarului / operatorului / administratorului de infrastructură critică națională / 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

București, 19 martie 2013
Nr. 166

Anexa nr. 1

NORME METODOLOGICE
PENTRU REALIZAREA/ECHIVALAREA/REVIZUIREA PLANURILOR DE SECURITATE ALE PROPRIETARILOR/OPERATORILOR/ADMINISTRATORILOR DE INFRASTRUCTURĂ CRITICĂ NAȚIONALĂ/EUROPEANĂ

CAPITOLUL I
Dispoziții generale

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

Art. 2 - Scopul prezentelor norme metodologice este de a asigura o concepție unitară de realizare a PSO, conform prevederilor legale aplicabile.

Art. 3 - Termenii utilizați în cuprinsul prezentelor norme metodologice sunt definiți la art.3 din OUG nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice aprobată cu modificări prin Legea nr. 18/2011, denumită în continuare *OUG nr. 98/2010* iar terminologia generală are sensul conform definițiilor date în cuprinsul documentelor normative aplicabile.

CAPITOLUL II
Planurile de securitate ale proprietarilor/operatorilor/administratorilor de infrastructuri critice naționale/europene

SECȚIUNEA 1
Dispoziții comune

Art. 4. - (1) Proprietarii/operatorii/administratorii de infrastructuri critice naționale / europene, elaborează, echivalează sau actualizează, după caz, PSO având la bază cel puțin aspectele precizate în anexa nr. 3 a O.U.G. nr. 98/2010.

(2) În acest scop, proprietarii/operatorii/administratorii de infrastructuri critice naționale / europene pot utiliza scenariile de amenințare, 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 cerințele specifice de protecție a infrastructurilor critice.

Art. 5. - (1) Scenariile de amenințări se întocmesc de către proprietarii/operatorii/administratorii de infrastructuri critice naționale / europene pe baza coordonatelor stabilite de către autoritatea publică responsabilă în domeniu.

(2) Proprietarii/operatorii/administratorii de infrastructuri critice naționale din sectorul "tehnologia informației și comunicații" pot utiliza pentru realizarea analizei de risc și alte instrumente sau tehnici din domeniul managementului riscului.

Art. 6 - La elaborarea scenariilor vor fi avute în vedere, după caz, amenințări de tipul:

a) fenomene meteorologice periculoase;
b) fenomene distructive de origine geologică;
c) accidente, avarii, explozii, incendii;
d) poluări de ape;

e) prăbușiri de construcții, instalații, amenajări;
f) accident nuclear major sau urgență radiologică cu efect transfrontalier;
g) accident major în care sunt implicate substanțe periculoase;
h) boli transmisibile care pot afecta sănătatea publică (epidemii/pandemii);
i) amenințări teroriste;
j) grave tulburări sociale;
k) alte amenințări cu specific sectorial, conform criteriilor aprobate în sectorul respectiv;
l) evenimente internaționale și/sau cu caracter geo-politic sau de natura amenințărilor militare, dacă acestea pot genera amenințări suplimentare la nivelul infrastructurilor critice naționale.

Art. 7 - Responsabilitatea generală pentru stabilirea unor scenarii de amenințări credibile, în sensul art. 5 și 6 din prezentele norme metodologice, revine autorităților publice responsabile. Pentru stabilirea unor elemente concrete, specifice, ale acestor scenarii, autoritățile publice responsabile se pot consulta asupra aspectelor din domeniile specifice de competență.

Art. 8 - Consultarea între autoritățile publice responsabile și structurile cu atribuții, la care se face referire în art. 7, se poate realiza în mod direct sau prin intermediul Centrului de coordonare a protecției infrastructurilor critice din cadrul Ministerului Afacerilor Interne, denumit în continuare CCPIC. Consultarea prin intermediul CCPIC este obligatorie pentru aspectele care cad sub incidența 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, autoritățile publice responsabile informează CCPIC, în scris, asupra elementelor de scenarii stabilite, înainte de realizarea analizelor de risc și vulnerabilitate.

Art. 9 - În scopul asigurării unui cadru unitar de realizare a PSO, CCPIC poate organiza ședințe, ateliere de lucru și seminarii în vederea armonizării acestuia la nivel național.

SECȚIUNEA 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 naționale/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 internaționale (ISO), ce definesc principii și linii directoare, cât şi prin diverse tehnici de evaluare a riscurilor existente, pentru fiecare sector de activitate la nivel național și internațional.

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

a) una dintre metodele sau tehnicile descrise de standardele internaționale în materie;
b) o altă metodă de analiză standardizată pe plan internațional, cu indicarea standardului public aplicabil;
c) o metodă sau tehnică nestandardizată de analiză ori un procedeu nestandardizat de estimare a consecințelor, în măsura în care operatorul de infrastructură critică poate să ofere documentație detaliată cu privire la modul de aplicare a acesteia/acestuia, să justifice necesitatea și 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 inițiale avute în vedere, valorile parametrilor inițiali sau intermediari introduși în algoritmi și aproximările realizate, astfel încât exclusiv pe baza informațiilor disponibile, o terță parte să poată expertiza, în cazul în care se consideră necesar, nivelul de conformitate.

Art. 12 .- Proprietarii/operatorii/administratorii de infrastructuri critice naționale / europene și autoritățile publice responsabile vor realiza activitățile organizatorice și administrative necesare pentru respectarea prevederilor standardelor internaționale aplicabile, atât pentru desfășurarea activităților interne legate de managementul riscurilor, cât și pentru a asigura interfața în procesele de consultare și comunicare externă.

Art. 13. - (1) În realizarea prevederilor art. 12 al prezentei metodologii, proprietarii / operatorii / administratorii de infrastructuri critice naționale / europene și autoritățile publice responsabile vor acorda o atenție deosebită următoarelor etape ale managementului riscului:

a) stabilirea contextului;
b) identificarea riscurilor/amenințărilor;
c) analiza riscurilor;
d) evaluarea riscurilor;
e) modalitatea de abordare a riscurilor;
f) măsuri de protecție, compensare și recuperare post – incident;
g) evaluare globală;

(2) Etapele prevăzute la alin. (1) lit. a) „stabilirea contextului" și lit. b) „identificarea riscurilor/ amenințărilor" sunt definitorii pentru realizarea, în bune condiții și la un nivel de calitate comparabil pentru toate părțile vizate, a scenariilor de amenințări și a condițiilor de realizare a analizelor de risc și vulnerabilitate, după cum se precizează în cuprinsul Secțiunii I – „Dispoziții comune".

(3) Efectuarea analizelor de risc se realizează în conformitate cu prevederile Secțiunii I – „Dispoziții comune" și cu cerințele art. 2, lit. b din Anexa nr. 3 – „Procedură privind planul de securitate pentru operator" a OUG nr. 98/2010; estimarea impacturilor potențiale este descrisă la etapa prevăzută la alin. (1) lit. c) „analiza riscurilor".

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

SECȚIUNEA a 3-a
Elaborarea și avizarea PSO

Art. 14 - (1) Pentru a facilita elaborarea unitară a PSO, autoritățile publice responsabile emit ordine sau formulează recomandări, aplicabile la nivel de sector ori subsector, cu privire la forma, structura și cuprinsul planurilor de securitate ale operatorilor.

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

Art. 15. - PSO se elaborează și se transmit, spre avizare, în 2 (două) exemplare originale, autorităților publice responsabile.

Art. 16. - Proprietarii/Operatorii/Administratorii de infrastructuri critice naționale / europene transmit, în 2 (două) exemplare originale, autorităților publice responsabile documentele ce urmează a fi echivalate cu PSO, prezentând într-un memoriu sau într-o notă justificativă elementele de echivalență și analiza de suficiență, din care să reiasă satisfacerea necesităților 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 națională / europeană a PSO sau a documentelor de echivalare, autoritățile publice responsabile vor realiza, după caz, una dintre următoarele acțiuni:

a) avizarea și returnarea unui exemplar original avizat, cu comunicarea îndeplinirii de către proprietarul/operatorul/administratorul de infrastructură critică națională / europeană, a cerinței prevăzute la art. 11, alin. (3) din OUG nr. 98/2010;
b) avizarea și returnarea unui exemplar original, cu obiecții, motivația obiecțiilor, măsurile de corectare și termenele de conformare;

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

(2) În cazurile prevăzute alin. (1) lit. a) sau b), autoritățile publice responsabile vor transmite către CCPIC, în termen de 30 zile, un raport-sinteză cu privire la evaluarea riscurilor și amenințărilor, inclusiv propuneri cu privire la necesitatea îmbunătățirii protecției infrastructurilor critice naționale / 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 națională / europeană către autoritățile publice responsabile, în conformitate cu prevederile art. 15 și 16, vor fi clasificate în raport cu conținutul acestora, conform prevederilor legale.

SECȚIUNEA a 4-a

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

Art. 19 - (1) PSO și 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 ofițerul de legătură pentru securitate, denumit în continuare *OLS*, de la nivelul autorității publice responsabile, prevăzut la art. 8, alin. (2) din OUG nr. 98/2010.

(2) Pentru analizarea conținutului capitolelor de specialitate din cuprinsul PSO sau al documentelor echivalente PSO care necesită un înalt nivel de expertiză tehnico-științifică ori cunoștințe detaliate despre natura proceselor analizate, autoritățile publice responsabile pot coopta și reprezentanți ai altor structuri specializate din România sau pot angaja experți, persoane fizice și/sau juridice, cu rol consultativ, fără ca aceștia să facă parte din comisia de evaluare prevăzută la alin. (1). Pentru angajare, reprezentanții structurilor specializate din România sau experții, persoane fizice și/sau juridice, trebuie să obțină în prealabil de la autoritatea națională competentă un certificat de acces la date și documente clasificate.

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

Art. 20 - (1) PSO și planurile sau documentele echivalente PSO se testează prin exerciții (interne, naționale, internaționale – numai pentru ICE), organizate și desfășurate cu o periodicitate de minimum un exercițiu pe an.

(2) Anumite componente ale PSO sau ale documentelor echivalente PSO se vor testa atât prin exerciții parțiale (în teren, în punctele de comandă, exerciții simulate, exerciții tematice cu forțe și mijloace etc.), cât și prin exerciții de alertare, desfășurate în mod periodic și astfel încât să acopere, în timp, o gamă variată de condiții (anunțate/neanunțate, cu scenariul cunoscut/parțial cunoscut/necunoscut, ziua/noaptea, iarna/vara, în timpul/afara programului, în weekend/în timpul săptămânii etc.).

(3) Normele de organizare, desfășurare și evaluare a exercițiilor sunt elaborate de către fiecare autoritate publică responsabilă și aprobate prin ordin sau dispoziție al/a conducătorului acesteia.

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

(5) Exercițiile organizate și desfășurate în conformitate cu prevederile alin. (1) și (2) se vor finaliza prin elaborarea unui raport de evaluare a fiecărui exercițiu.

Art. 21. - (1) PSO și planurile sau documentele echivalente PSO se revizuiesc și se actualizează la intervale de cel mult doi ani, în conformitate cu prevederile art. 11, alin. (6) din OUG nr. 98/2010.

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

(3) Actualizarea PSO implică aducerea la zi a unor informații, denumiri, cantități, valori etc. din cuprinsul PSO, fără modificarea substanțială a conținutului acestuia și fără necesitatea de reluare a procesului de avizare a PSO. Modificările aduse PSO în timpul actualizărilor sunt aprobate de conducătorii operatorilor de infrastructuri critice și sunt comunicate autorităților publice responsabile.

(4) Revizuirea PSO constă în reanalizarea și modificarea substanțială a uneia sau mai multora dintre

elementele componente ale PSO și necesită reluarea procesului de avizare prevăzut în cuprinsul prezentelor norme metodologice.

CAPITOLUL III
Dispoziții finale

Art. 22 - Prezentele norme metodologice intră în vigoare de la data publicării în Monitorul Oficial al României, Partea I.

Anexa nr. 2

STRUCTURA – CADRU*)
a planului de securitate al proprietarului / operatorului / administratorului deținător de infrastructură critică națională și/sau europeană

- Structura cadru -

AVIZAT

CONDUCĂTORUL AUTORITĂȚII
PUBLICE RESPONSABILE

VERIFICAT

APROB

(ofițer de legătura al APR)

(proprietar/operator/administrator)

PLANUL DE SECURITATE

al _____ pentru
(proprietarului / operatorului / administratorului de infrastructură critică națională / europeană)

_____
(infrastructura critică națională /europeană)

Versiunea: ____
(după completare documentul se clasifică la nivelul corespunzător)

ÎNTOCMIT

(ofițer de legătură pentru securitate al proprietarului/operatorului/administratorului)

*) Structura-cadru este reprodusă in facsimil.

CAPITOLUL I **- Dispoziții Generale**

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

NOTĂ:

Planul de securitate este un document strategic care:

- definește scopul și obiectivele de securitate ale proprietarului / operatorului / administratorului, pe baza unei evaluări a riscurilor de securitate;
- stabilește cadrul general de lucru, cu acoperirea întregului spectru de securitate (prevenire, diminuare, răspuns și revenire la starea de normalitate), fundamentat pe baza concluziilor rezultate în urma evaluării riscurilor și amenințărilor la adresa securității;
- reflectă o abordare coordonată a securității sistemelor unui proprietar / operator / administrator care integrează toate resursele disponibile pentru asigurarea unei mai bune protecții a infrastructurii critice;
- identifică elementele-cheie care necesită protecție (ca rezultat al evaluării riscurilor de securitate);
- stabilește 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 incidență în domeniul securității (Plan de analiză și acoperire a riscurilor - PAAR, Plan de evacuare în situații de urgență, Plan de apărare împotriva incendiilor, etc.), procedurile, protocoalele, acordurile și responsabilitățile operatorului în acest domeniu;
- definește un parcurs sau un plan de acțiune pentru stabilirea de noi măsuri care vizează contracararea riscurilor tratate prioritar, in funcție de impact (măsuri imediate sau pe termen mediu și lung, după necesitate);
- stabilește acțiunile și resursele necesare pentru sprijinirea procesului de implementare a măsurilor pe care le conține (de exemplu: măsuri de îndepărtare a surselor de risc, de diminuare a consecințelor, de asigurare a securității cibernetice, securitatea tehnologiei informației, pentru controlul documentelor clasificate, pentru gestionarea alertelor, etc.).

Prin planul de securitate pentru operator vor fi identificate soluțiile de securitate existente sau care sunt puse în aplicare pentru protecția elementelor de infrastructură critică națională / europeană.

Această structură cadru a PSO este aplicabilă tuturor categoriilor de proprietari / operatori / administratori de infrastructură critică națională / europeană și se adresează tuturor tipurilor de riscuri care amenință funcționarea corespunzătoare a proprietarilor / operatorilor / administratorilor deținători de infrastructură critică națională / europeană.

1.2 Scop și obiective

1.2.1 Scop

Scopul PSO este de a contribui la îmbunătățirea protecției infrastructurii critice naționale / europene aflate în responsabilitatea proprietarului / operatorului / administratorului de infrastructură critică națională / europeană, prin coordonarea măsurilor de protecție / securitate existente și instituirea unor măsuri noi în baza unui proces de management al riscului.

PSO identifică elementele de infrastructură critică ale infrastructurii critice naționale / europeană și soluțiile de securitate existente sau care urmează să fie puse în aplicare pentru protecția acestora.

PSO contribuie la îmbunătățirea nivelului existent al securității și protecției infrastructurii critice naționale / europeană, nivel care poate fi afectat de diferite tipuri de amenințări sau vulnerabilități.

1.2.2 Obiective

PSO trebuie să asigure îndeplinirea a cel puțin următoarelor obiective:

- îmbunătățirea abilității operatorului de planificare, prevenire, răspuns și restaurare a stării de normalitate, în urma producerii unui eveniment ce a afectat infrastructura critică pentru protecția căreia se elaborează PSO;

- descrierea elementelor componente ale planului de securitate și definirea măsurilor de control al riscurilor, pentru asigurarea securității infrastructurii critice națională / europeană;
- definirea rolurilor și responsabilităților personalului cu atribuții în domeniul securității infrastructurii critice națională / europeană;
- fundamentarea necesității includerii măsurilor de securitate în activitățile curente ale operatorului;
- stabilirea proceselor pentru elaborarea, menținerea, actualizarea, evaluarea și modificarea PSO;
- stabilirea proceselor de identificare și primire a feedbackului de la părțile interesate (angajați, contractanți, populație, ș.a.), privind aspectele legate de securitate, incidentele de securitate, activitățile periculoase, etc.;
- stabilirea modalității de interacționare cu părțile externe interesate;
- identificarea cerințelor de pregătire a personalului/partenerilor în ceea ce privește implementarea planului de securitate și planificarea activităților de instruire;
- stabilirea modalității de investigare a tuturor incidentelor de securitate sau activităților care pot genera astfel de evenimente;
- instituirea unui proces de evaluare a eventualelor implicații de securitate atunci când se iau decizii în ceea ce privește activitățile operatorului;
- reprezentarea clară și sistematică asupra componentelor infrastructurii critice națională / europeană din responsabilitatea operatorilor de infrastructură critică;
- reprezentarea amenințărilor și vulnerabilităților la adresa infrastructurii critice națională / europeană din responsabilitatea operatorilor de infrastructură critică și a riscurilor induse de acestea;
- identificarea măsurilor de securitate existente și a celor necesare suplimentar pentru controlul riscurilor la adresa infrastructurii critice naționale / europene aflate în responsabilitatea operatorilor de infrastructură critică;
- instituirea capabilităților de răspuns si recuperare a infrastructurii critice naționale/ europene la nivelul operatorilor de infrastructură critică, corelat cu scenariile de amenințare și cooperarea cu autoritățile relevante;
- reprezentarea cadrului organizatoric relevant pentru protecția infrastructurii critice în cadrul operatorilor de infrastructură critică, inclusiv a proceselor necesare pentru funcționarea acestuia;
- planificarea activităților relevante pentru protecția infrastructurii critice pe perioada de valabilitate;
- stabilirea cadrului de dialog și cooperare pe probleme de protecția infrastructurii critice.

1.3. Întocmire, avizare și aprobare

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

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

1.4 Confidențialitate

Informațiile sensibile privind protecția infrastructurilor critice se clasifică la un nivel adecvat, în condițiile legii. Diseminarea acestor informații se face potrivit principiului nevoii de a cunoaște, atât în relația cu proprietarii / operatorii / administratorii de infrastructură critică națională / europeană, cât și cu celelalte state membre în condițiile legislației privind protecția informațiilor clasificate și se supune în totalitate dispozițiilor acesteia.

CAPITOLUL II

Descriere organizațională

2.1 Structura organizațională*)

Autoritatea publică responsabilă: ...
Compartiment specializat în domeniul infrastructurii critice națională / europeană al autorității publice responsabile: ...
OLS al autorității publice responsabile: …
Compartiment specializat în domeniul infrastructurii critice națională / europeană al proprietarului / operatorului / administratorului de infrastructură critică națională / europeană: ...
OLS al operatorului/proprietarului/administratorului de infrastructură critică națională / europeană: ...
Organigrama proprietarului / operatorului / administratorului de infrastructură critică națională / europeană: ...

2.2 Cadrul legislativ

Legi: ...
Ordonanțe de urgență ale Guvernului ...
Ordonanțe ale Guvernului …
Hotărâri ale Guvernului ...
Ordine ale ministrului ...
Standarde naționale/internaționale (funcție de fiecare caz în parte) ...
Acorduri internaționale / naționale ...
Alte documente ...

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

Pentru stabilirea caracteristicilor unității administrativ-teritoriale pot fi utilizate informațiile din Planul județean de analiză și acoperire a riscurilor aprobat de prefect și întocmit în conformitate cu Ordinul ministrului administrației și internelor nr. 132/ 2007 pentru aprobarea Metodologiei de elaborare a Planului de analiză și acoperire a riscurilor și a Structurii-cadru a Planului de analiză și acoperire a riscurilor.

2.4 Sisteme de operare

Tipul sistemului: • ... Harta sistemului • ...

Tipul serviciului furnizat/serviciilor furnizate • ... Statistici privind serviciul furnizat • ...

*) Tabelele sunt reproduse în facsimil.

2.5 Descrierea infrastructurii, facilităților și echipamentelor din infrastructura critică națională / europeană

Se vor menționa elementele fizice, organizaționale și facilitățile necesare funcționării serviciului esențial.

Infrastructuri, facilități și echipamente *(în acest tabel se vor menționa elementele fizice, organizaționale și facilitățile necesare funcționării serviciului esențial, date tehnice,etc.)*	
Stații de alimentare	
Hub - uri	
Servere	
Depozite	
Ateliere de întreținere	
Clădiri administrative	
Puncte de comandă	
...	
Alți proprietari	

2.6 Personal

Se introduc informații referitoare la numărul și categoriile de personal care lucrează în cadrul infrastructurii critice națională / europeană. Acest lucru permite atât furnizarea unui indicator al dimensiunilor relative și al semnificației activității desfășurate de operator cât și un indicator privind riscurile asociate și provocările existente legate de îmbunătățirea securității globale a respectivei infrastructuri critice naționale / europene.

Personal	Număr
Angajați „part-time”	
Angajați „full-time”	
Personal contractant („part-time”)	
Personal contractant („full-time”)	
TOTAL PERSONAL	
Personal în funcție de rol și loc de muncă	Număr
Personal operativ (șoferi, personal la tură, etc.)	
Personal administrativ (financiar, logistică)	
Personal de securitate	
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 securității se bazează pe scenariile de amenințări, identificarea punctelor vulnerabile ale fiecărui element al infrastructurii critice națională / europeană și impactul asupra acesteia în cazul producerii unui eveniment nedorit (în cazul exploatării unei vulnerabilități de către o amenințare).

3.2 Istoricul incidentelor

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

3.3 Facilitățile și operațiunile cu grad ridicat de risc

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

PSO trebuie să identifice acele surse de risc (facilități și operațiuni interne sau externe) și vulnerabilități care ar putea genera sau favoriza riscul perturbării sau distrugerii infrastructurii critice națională / europeană pentru care se elaborează PSO.

Pentru a se realiza acest lucru, trebuie să se ia în considerare toate sursele plauzibile și semnificative de risc, precum și o gamă cât mai largă de consecințe ale riscului.

3.4 Elementele planului de securitate

3.4.1 Generalități

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

3.4.2 Securitatea fizică a infrastructurii critice naționale / europene și controlul accesului

Se identifică punctele vulnerabile ale infrastructurii critice națională / europeană și se menționează documentele în care sunt menționate/stabilite măsurile: de prevenire a evenimentelor, de diminuare a impactului, de facilitare a intervenției sau de restabilire a serviciilor furnizate de infrastructura critică națională / europeană în cazul în care acestea devin indisponibile.

Vor fi precizate pe scurt elementele de protecție perimetrală, sistemele de detecție și semnalizare a efracției, sistemele de control a accesului, de management al identității, de management al vizitatorilor, de detecție și stingere a incendiilor, de supraveghere video perimetrală și a căilor de acces, ș.a.

Nr. crt.	Infrastructura critică națională / europeană (componenta critică)	Elemente de securitate *(controlul accesului, managementul identității, elemente de protecție la explozie, ieșiri de urgență, căi de evacuare, sisteme de detecție a efracției, sisteme de supraveghere video, etc.)*	Rolul elementelor de securitate *(detectare / descurajare / , întârziere atac, reducere vulnerabilitate sau amenințare, alarmare eveniment, ș.a.)*	Informații suplimentare *(nr. de înregistrare și documentele care conțin detalii privind securitatea acesteia)*
1				
2				
...				
n				

3.4.3 Inspecții privind securitatea fizică

Se descriu facilitățile, vehiculele și alte elemente care necesită inspecție periodică, precum și modul în care se efectuează verificările. Se vor preciza deficiențele constatate cu ocazia inspecțiilor și frecvența lor, precum și aspectele referitoare la viabilitatea procedurilor de raportare a constatărilor.

Constatările inspecțiilor de securitate trebuie să se refere la:

- elementele mecanice de protecție perimetrală (bariere, garduri, porți de acces auto și persoane, mijloace de iluminat perimetral, ș.a.);
- elemente de protecție cu echipamente de detecție și semnalizare a efracției sau cu camere de supraveghere video, după caz;
- elemente de blocare, restricționare, identificare și autentificare;
- sisteme de urmărire și control al accesului;
- sisteme de detectare rapidă a debutului de incendiu și de stingere a incendiului.

3.4.4 Tehnologia informațiilor și rețele de comunicații

Se identifică și 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 și tehnologiile existente pentru protecția, păstrarea, distrugerea, multiplicarea, arhivarea, ținerea evidenței și 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 națională / europeană

Nr. crt.	Nume și prenume	Loc de muncă	Tipologie *(gardian, paznic, operator echipament de securitate, ș.a.)*	Pregătire în domeniu / Atestat profesional	Nivel acces / responsabilități
Angajații operatorului					
1					
2					
...					
n					
Personal contractant din afara operatorului					
1					
2					
...					

n					
Alte situații					
1					
2					
...					
n					
TOTAL					

3.4.7 Echipamente și tehnologii legate de securitate

Se identifică și descriu succint tehnologiile deținute și programele instalate pe echipamentele operatorului (de exemplu, butoanele de alarmare, de pornire / oprire a instalațiilor de stingere a incendiilor, ș.a.).

Nr. crt.	Tehnologii și programe	Modelul echipamentului	Echipamentele dotate	Informații suplimentare
1				
2				
...				
n				

3.4.8 Tehnologia comunicațiilor

Se identifică și se descriu succint tehnologia și procesele utilizate pentru comunicare în situație de urgență atât cu personalul operatorului cât și cu poliția, pompierii, ambulanța și alte servicii publice. De asemenea, trebuie menționate și eventualele redundanțe ale sistemelor de comunicații prevăzute pentru evitarea defecțiunilor echipamentelor de bază.

3.4.9 Resurse și instrumente mixte

Suplimentar aspectelor precizate în celelalte secțiuni, această secțiune trebuie să identifice și să descrie succint celelalte instrumente și resurse utilizate de operator pentru îmbunătățirea abilității 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 și procese pentru îmbunătățirea securității; planuri de urgență; planuri de intervenție în diferite situații; echipamente speciale precum camerele de luat vederi, detectoarele de fum, dispozitivele electronice de control a accesului, ș.a.; proceduri de manipulare a unei bombe; identificarea și manipularea pachetelor suspecte; proceduri de urmat în cazul unei explozii sau a unui incendiu, etc.).

CAPITOLUL IV
Managementul PSO, responsabilități și atribuții

4.1 Revizuirea și actualizarea PSO

Responsabilități	Funcția / Structura	Nume și prenume
Întocmit	*OLS* *Compartimentul specializat în domeniul infrastructurii critice națională / europeană al autorității publice responsabile*	
Avizat	 *Conducător al autorității publice responsabile*	
Aprobat	*conducătorul proprietarului / operatorului / administratorului deţinător de infrastructură critică națională / europeană* 	

Întocmit revizuire / actualizare	*OLS* *Compartimentul specializat al autorității publice responsabile*	
Avizat revizuire / actualizare	 *Autoritatea publică responsabilă*	
Aprobat revizuire / actualizare	*conducătorul proprietarului / operatorului / administratorului deţinător de infrastructură critică națională / europeană* 	
Responsabil distribuire la sau extrase	 	
Alte responsabilități (verificare, avizare, autorizare, etc.)	 	

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

4.2 Rolul și responsabilitățile angajaților

4.2.1 Generalități

PSO trebuie să conțină responsabilitățile tuturor structurilor operatorului (departamente, direcții, servicii, birouri compartimente etc.) cu atribuții în domeniul securității infrastructurii critice națională / europeană.

De exemplu, structurile cu atribuții de planificare, de management financiar, al resurselor umane, de securitatea muncii, de mentenanță, de management al riscului, de asigurare logistică, etc.

4.2.2 Rolul și responsabilitățile OLS

Vor fi specificate rolul și responsabilitățile ofițerului de legătură pentru securitate în domeniul protecției infrastructurilor critice.

4.2.3 Roluri-cheie și responsabilități – Personalul de securitate

În această secțiune vor fi specificate rolurile și responsabilitățile, ce revin personalului de securitate și care vor fi atribuite pozițiilor corespunzătoare din statul de funcțiuni al operatorului. Trebuie menționat că la anumiți operatori mai mici poate exista și cumul de funcții.

4.2.4. Alte categorii de personal

Se vor specifica rolurile și responsabilitățile ce revin și altor categorii de personal ale operatorului, în domeniul securității infrastructurilor critice.

CAPITOLUL V
MANAGEMENTUL RISCULUI

5.1 Evaluarea riscurilor de securitate

În această secțiune vor fi incluse informații referitoare la măsuri de ordin general, cum sunt:

- măsuri organizatorice
  - proceduri documentate (ex: pentru gestionarea alertelor, comunicare, conștientizare și sensibilizare personal ș.a.);
  - acțiuni de control / verificare periodică a funcționalității sistemelor tehnice de securitate și a capacității de răspuns și revenire;
  - planificare și realizare activități de formare și perfecționare a personalului în domeniul securității

infrastructurilor critice;

- măsuri de control și verificare, comunicare, sensibilizare și formare;
- măsuri de securitate graduale, care pot fi activate în funcție de diferitele niveluri ale riscurilor și amenințărilor;
- măsuri în domeniul securității sistemelor de informații;
- măsuri tehnice care includ instalarea de:
  - sisteme de protecție fizică perimetrală (garduri, bariere, porți de acces ș.a.);
  - sisteme de protecție și alarmare împotriva efracției (cu senzori în infraroșu, microunde, magnetici, de vibrații sau acustici);
  - sisteme de control al accesului (biometrie, smart card, proximitate);
  - sisteme de management al vizitatorilor;
  - sisteme de supraveghere video pe timp de zi și noapte (camere TVCI);
  - dispecerate de monitorizare, comandă și control;
  - sisteme de detecție și stingere a incendiului;
  - sisteme de securitate cibernetică (pentru infrastructuri IT și de comunicații).

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

5.1.1 Prevenire, control și diminuare a riscului

Identificarea, selectarea și stabilirea priorităților în ceea ce privește contramăsurile și procedurile, realizându-se distincție între măsurile permanente - *măsurile permanente de securitate* (de natură tehnică), care identifică investițiile de securitate indispensabile, și *măsurile nepermanente de securitate* (de natură organizatorică), care pot fi activate gradual în funcție de diferitele niveluri ale riscurilor și amenințărilor identificate.

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

Măsurile de control a riscului trebuie stabilite pentru fiecare din elementele care fac parte din spectrul securității.

Măsurile de prevenire și 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 Intervenția sau răspunsul în cazul apariției riscului de securitate

Măsurile de securitate referitoare la faza de intervenție sau răspuns trebuie să fie prevăzute în planurile specifice de intervenție în situații de urgență. PSO trebuie să precizeze cum și de unde se pot obține anumite informații din planurile specifice de intervenție, în cazul producerii anumitor incidente de securitate.

5.1.3 Reconstrucția sau restabilirea stării de normalitate după manifestarea riscului de securitate

Măsurile de securitate în faza de reconstrucție trebuie să fie prevăzute în planurile de asigurare a continuității serviciului. PSO trebuie să precizeze cum și de unde se pot obține anumite informații din planurile de asigurare a continuității serviciului.

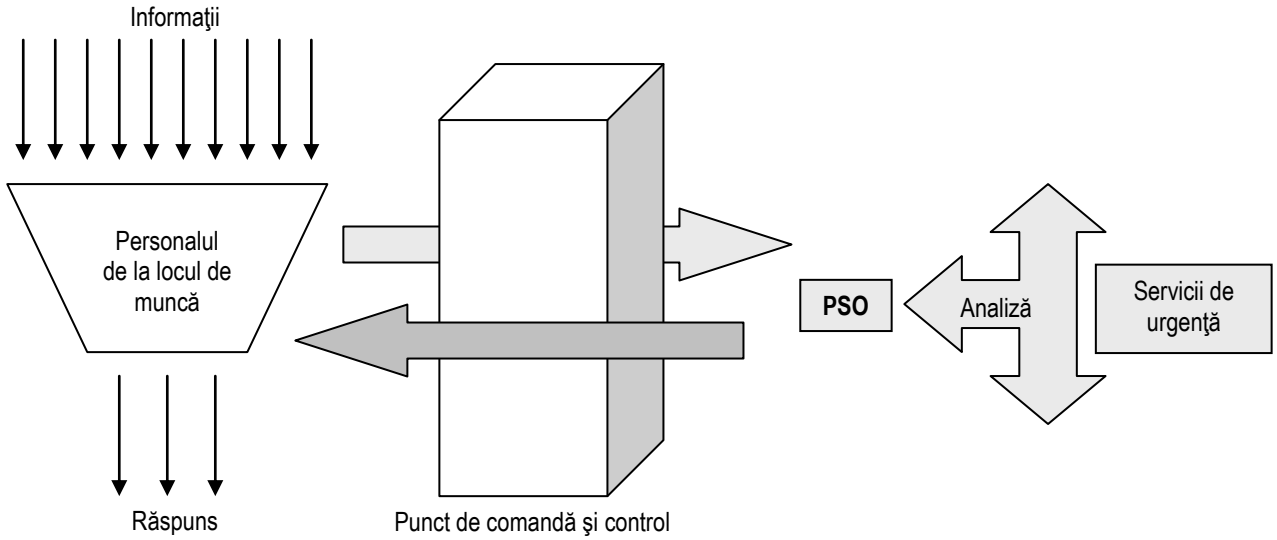
5.2 Punctul de comandă și control (dispeceratul)

Intervenția efectivă în cazul producerii unui eveniment cu urmări pentru securitatea ICN/ICE, necesită luarea unor decizii complexe**,** spre deosebire de operațiunile care se desfășoară în mod curent la nivelul operatorului. PSO trebuie să conțină informații despre sistemul de management al crizelor**,** documentat la nivelul operatorului de infrastructură critică națională / europeană, dacă există un astfel de sistem, iar dacă nu,

să facă trimitere la modul de acțiune și persoanele care dispun de autoritatea de decizie în astfel de situații, conform planului de intervenție specific.

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

Diagrama procesului de schimb de informații în domeniul securității ICN/ICE*)



*)Diagrama este reprodus[in facsimil.

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

CAPITOLUL VI
Niveluri de alertă

6.1 Generalități

Măsurile preventive sunt luate pentru a menține un nivel acceptabil de securitate a infrastructurii critice naționale/ europene în cauză, precum și pentru a permite asigurarea unui nivel minim de funcționare corespunzătoare a serviciilor esențiale pe care le furnizează populației 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 națională / europeană. Măsurile preventive sunt întreprinse pentru a menține la un nivel acceptabil securitatea infrastructurii critice națională / europeană, precum și pentru a permite furnizarea continuă către populație a serviciului esențial asigurat de respectiva infrastructurii critice națională / europeană.

6.2 Stabilirea nivelurilor de alertă

Operatorii trebuie să stabilească un sistem de alertare pe niveluri. PSO trebuie să descrie acest sistem și 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 amenințărilor care pot genera evenimente cu consecințe foarte grave.

Sistemul de alertare pe niveluri trebuie să conțină următoarele elemente:

- definirea fiecărui nivel de alertă;
- criterii pentru declanșarea alertei și nivelul acesteia;
- stabilirea persoanelor cu drept de alertare pe tipuri și niveluri de alertă;

- măsurile de securitate care corespund fiecărui nivel de alertă;

- un element care să indice dacă trebuie pus în aplicare planul de intervenție pentru situații de urgență (în general, acest plan este pus în aplicare atunci când este necesară activarea punctului de comandă care permite cooperarea cu alte autorități cu responsabilități de intervenție);

- detalierea aspectelor referitoare la diseminarea informației privind nivelul de alertă (mecanisme de diseminare a informației, destinatarul informației, nivelul de urgență al transmiterii informației), precum și măsurile ce trebuie întreprinse pentru fiecare nivel de alertă în parte.

6.3 Comunicarea și armonizarea

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

6.4 Cadrul legal

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

6.5 Procedurile de alertare

În această secțiune trebuie specificat cum sunt declanșate, 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, amenințările și punctele vulnerabile la adresa infrastructurii critice naționale / europene
- **Anexa nr. 2** - Lista cu măsurile de prevenire a producerii evenimentelor nedorite și de diminuare a riscurilor identificate ca fiind prioritare pentru infrastructura critică națională / europeană
- **Anexa nr. 3** - Lista cu revizuirile PSO
- **Anexa nr. 4** - Glosar de termeni și definiții în domeniul protecției infrastructurilor critice
- **Anexa nr. 5** - Acronime
- **Anexa nr. 6** - Fișă raportare incident de securitate
- **Anexa nr. 7** - Lista cu datele de contact ale persoanelor cu responsabilități în domeniul securității
- **Anexa nr. 8** - Organigrama proprietarului / operatorului / administratorului deținător de infrastructură critică națională / europeană
- **Anexa nr. 9** - Fluxul informațional – decizional în cazul producerii unui incident de securitate
- **Anexa nr. 10** - Relația între PSO și alte documente în domeniul securității
- **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 nr. 1)*
la planul de securitate

DATE GENERALE
privind riscurile, amenințările și punctele vulnerabile la adresa infrastructurii critice națională / europeană
"_____"

INFRASTRUCTURA CRITICĂ NAȚIONALĂ / EUROPEANĂ

1. Autoritatea publică responsabilă: Date: zz-ll-aaaa
   ...
2. Administrator / proprietar / operator de ICN/ICE:
   ...
3. Conducător:
   ...
4. Ofițer de legătură pentru securitate:
   ...
5. Adresa:
   ...
6. Telefon:
   ...
7. E-mail:
   ...

PUNCTELE VULNERABILE ALE ICN/ICE

 = Vulnerabilitate foarte ridicată = Vulnerabilitate ridicată = Vulnerabilitate medie = Vulnerabilitate scăzută = Vulnerabilitate foarte scăzută	Estimare nivelurilor de vulnerabilitate din cadrul PSO (Se indică nivelul de vulnerabilitate)
Puncte vulnerabile Introduceti punctul vulnerabil	
Introduceti punctul vulnerabil	
Introduceti punctul vulnerabil	
Introduceti punctul vulnerabil	
Introduceti punctul vulnerabil	
Introduceti punctul vulnerabil	
Introduceti punctul vulnerabil	

*)Anexa nr.1 este reprodusa in facsimil.

AMENINȚĂRILE

Nr. crt.	Tipuri de amenințări
1	Introduceti amenințarea
2	Introduceti amenințarea
3	Introduceti amenințarea

4	Introduceti amenințarea
5	Introduceti amenințarea
6	Introduceti amenințarea
...	
n	Introduceti amenințarea

RISCURI DE SECURITATE

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

NIVELUL AFERENT PENTRU FIECARE TIP DE RISC

PROBABILITATE						
	Foarte probabil (5)	...	...	...	...	...
	Probabil (4)	...	...	...	...	...
	Probabilitate redusă (3)	...	...	...	...	...
	Puțin probabil (2)	...	...	...	...	...
	Improbabil (1)	...	...	...	...	...
Risc foarte ridicat		Foarte scăzut (1)	Scăzut (2)	Mediu (3)	Ridicat (4)	Foarte ridicat (5)
Risc ridicat						
Risc mediu				NIVELUL IMPACTULUI		
Risc scăzut						
Risc foarte scăzut						

NOTĂ:
Fiecare tip de risc va fi trecut în matricea riscului în căsuța aferentă după stabilirea nivelului impactului și a probabilității de producere.

ANEXA nr. 2)*
la planul de securitate

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

Nr. crt.	Riscul de securitate identificat	Măsuri de prevenire	Măsuri de diminuare (reducere)	Costuri aproximative	Data implementării	Responsabil implementare măsură și raportare rezultate	Stadiul de îndeplinire
1	...	...	...				...
2	...	...	...				...
3	...	...	...				...
4	...	...	...				...
5	...	...	...				...
6	...	...	...				...
7	...	...	...				...
...							
n	...	...	...				...

***)**Anexa nr.2 este reprodusa in facsimil.

ANEXA nr. 3)*
la planul de securitate

LISTA
cu revizuirile PSO

Nr. crt.	Numărul de înregistrare	Secțiunile revizuite	Data revizuirii	Observații
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
...				
n				

***)**Anexa nr.3 este reprodusa in facsimil.

ANEXA nr. 4)*
la planul de securitate

GLOSAR
de termeni și definiții în domeniul protecției infrastructurilor critice

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
Ș
T
Ț
U
V
X
Z
Y
W

***)**Anexa nr. 4 este reprodusa in facsimil.

*ANEXA nr. 5 *)*
la planul de securitate

Acronime

Acronime	Detaliere
ICE	Infrastructură critică europeană
ICN	Infrastructură critică națională
PIC	Protecția infrastructurilor critice
OLS	Ofițer de legătură pentru securitate
APR	Autoritate publică responsabilă
PSO	Plan de securitate pentru operator
TIC	Tehnologia informației și comunicațiilor
…	

***)**Anexa nr.5 este reprodusa in facsimil.

ANEXA nr. 6)*
la planul de securitate

Fișă raportare incident de securitate

Secțiunea A. Informații generale de contact ale raportorului incidentului

Nume: ...	Prenume: ...
Structura: ...	Funcția: ...
Telefon fix: ...	Telefon mobil: ...
Fax: ...	E-mail: ...

Secțiunea B. Informații generale privind incidentul de securitate

Data producerii incidentului: zz-ll-aaaa	Data detecției incidentului: zz-ll-aaaa
Ora producerii incidentului: hh:mm	Ora detecției incidentului: hh:mm
Data încetării incidentului: zz-ll-aaaa	Ora încetării incidentului: hh:mm
Zona incidentului: ...	Locația specifică: ...
Descrierea incidentului	Observații

Secțiunea C. Informații privind impactul incidentului de securitate

Gravitate impact:	Nivelul 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 ...			
Angajați evacuați (DA, NU, NEC) ...			

Secțiunea D. Informații privind persoanele implicate

Nr. crt.	Nume și prenume	Data nașterii / vârstă / sex	Adresa	Localitate	Nr. de telefon	E-mail
1	...	...	...	...	...	...
...	...	...	...	...	...	...
n	...	...	...	...	...	...

Secțiunea E. Informații generale privind infrastructura critică națională / europeană afectată

Situația infrastructurii critice naționala / europeană	Distrusă	...
	Avariată	...
	Vandalizată	...
	Activitate suspectă	...
	Breșă	...
Denumire ICN: ...	Locația: ...	
Suprafață: ...	Nr. angajați: ...	
Daune interne: ...	Daune externe: ...	

***)** Anexa nr. 6 este reprodusa in facsimil.

Secțiunea F. Informații privind notificarea producerii incidentului

Nr. crt.	Serviciul anunțat	Data și ora anunțării	Data și ora sosirii	Persoana	Alte informații
1	Poliția	...	...	...	...
2	Poliția locală	...	...	...	...
3	Firmă de pază	...	...	...	...
4	Jandarmerie	...	...	...	...
5	Pompieri	...	...	...	...
6	Ambulanță	...	...	...	...
7	Alte servicii de salvare	...	...	...	...

ANEXA nr. 7)*
la planul de securitate

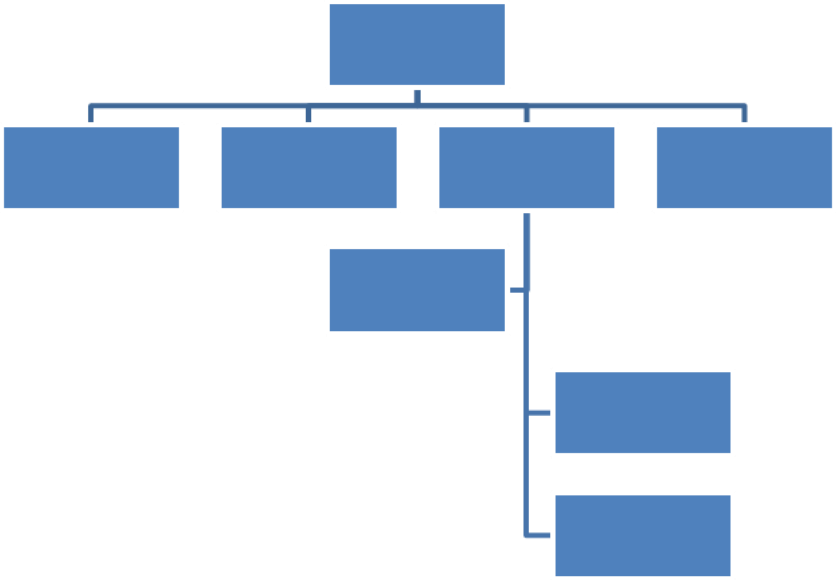
Listă cu datele de contact
ale persoanelor cu responsabilități în domeniul securității

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

***)** Anexa nr. 7 este reprodusa in facsimil.

ANEXA nr. 8)*
la planul de securitate

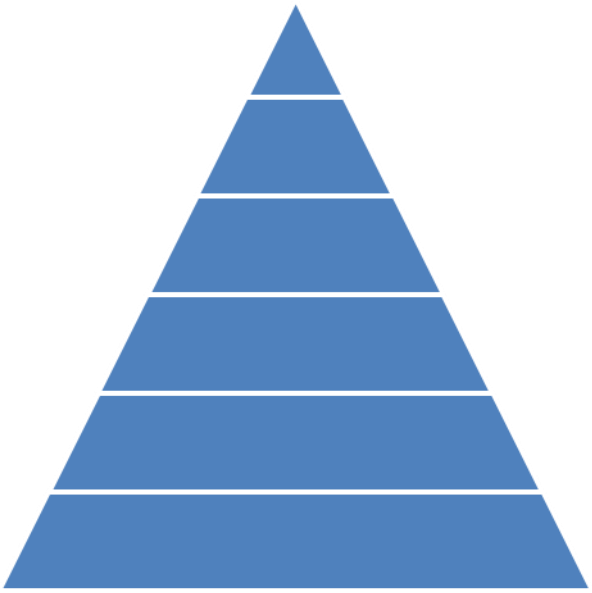
ORGANIGRAMA
proprietarului / operatorului / administratorului deținător de infrastructură critică națională / europeană



*)Anexa nr. 8 este reprodusa in facsimil.

ANEXA nr. 9)*
la planul de securitate

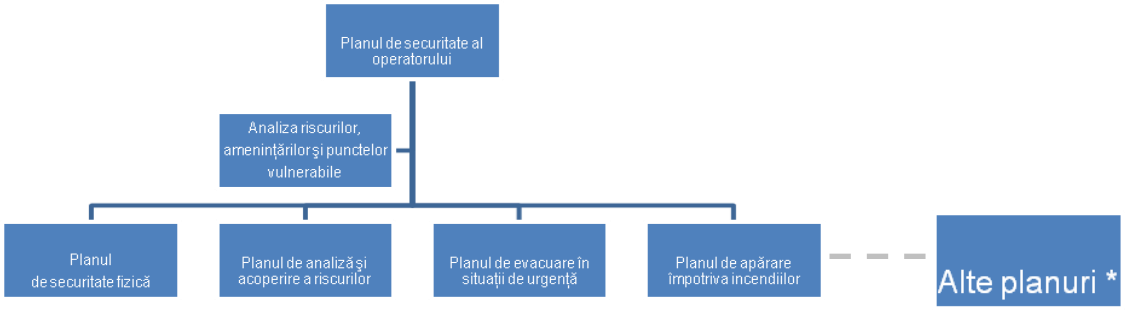
FLUXUL INFORMAȚIONAL – DECIZIONAL
în cazul producerii unui incident de securitate



*)Anexa nr. 9 este reprodusa in facsimil.

ANEXA nr. 10
la planul de securitate

Relația dintre PSO și alte documente în domeniul securității



[1]) Anexa nr. 10 este reprodusa in facsimil.
* Pentru situațiile în care instituția/operatorul economic gestionează informații clasificate în condițiile Legii nr.182/2002 privind protecţia informaţiilor clasificate, cu modificările şi completările ulterioare, la acest punct trebuie menționat ca document distinct „Programul de Prevenire a scurgerii de informații clasificate".

ANEXA nr. 11)*
la planul de securitate

Sistem de alertare pe niveluri

Nivelul 1 de alertă – „Conștientizare crescută" – COD VERDE					
Criterii de alertare	**Punerea în aplicare a planului de intervenție în situații de urgență**	**Informare**	**Măsuri**	**Interdependențe**	**Alte specificații**
Introducere criterii	DA / NU / PROBABIL	Introducere informări *(Ex.: Informarea tuturor angajaților privind necesitatea unei atenții sporite)*	Introducere măsuri *(Ex.: sunt trimise în plus echipe de cercetare în zonele expuse riscului; se întrunește conducerea pentru analiza potențialelor amenințări l*	Introducere infrastructuri critice naționale potențial afectate	
Nivelul 2 de alertă – „Securitate crescută" – COD GALBEN					
Criterii de alertare	**Punerea în aplicare a planului de intervenție în situații de urgență**	**Informare**	**Măsuri**	**Interdependențe**	**Alte specificații**
Introducere criterii	DA / NU / PROBABIL	Introducere informări *(Ex.: Nivel 1 de informare + informarea populației deservită ce urmează să fie afectată)*	Introducere măsuri *(Ex.: măsuri de nivel 1 + întărirea capacității de prevenire a apariției tipului de risc)*	Introducere infrastructuri critice naționale potențial afectate	
Nivelul 3 de alertă – „Securitate maximă" – COD ROȘU					
Criterii de alertare	**Punerea în aplicare a planului de intervenție în situații de urgență**	**Informare**	**Măsuri**	**Interdependențe**	**Alte specificații**
Introducere criterii	DA / NU / PROBABIL	Introducere informări *(Ex.: Nivel 2 de informare + punerea în aplicare a tuturor prevederilor celorlalte planuri de intervenție și răspuns privind informarea)*	Introducere măsuri *(Ex.: măsuri de nivel 2 + punerea în aplicare a măsurilor stabilite prin planurile specifice pentru tipurile de risc specifice)*	Introducere infrastructuri critice naționale potențial afectate	

*) Anexa nr. 11 este reprodusa in facsimil.

Anexa Nr. 3

ATRIBUȚIILE
ofițerului de legătură pentru securitate din cadrul compartimentului specializat desemnat la nivelul autorităților publice responsabile și la nivelul proprietarului / operatorului / administratorului de infrastructură critică națională / europeană

I. Ofițerul de legătură pentru securitate este șeful compartimentului specializat (constituit din minim 3 persoane) desemnat la nivelul autorităților publice responsabile sau la nivelul proprietarului / operatorului / administratorului de infrastructură critică națională / europeană, se află în directa subordonare a conducătorului autorității publice responsabile sau proprietarului / operatorului / administratorului deținător de infrastructură critică națională / europeană și este:

- persoana responsabilă cu activitatea în domeniul protecției infrastructurilor critice/șeful compartimentului, la nivelul autorităților publice responsabile;
- șeful compartimentului specializat în domeniul infrastructurii critice națională / europeană, la nivelul proprietarului/ operatorului/administratorului de infrastructură critică națională / europeană.

Atribuțiile compartimentului desemnat se stabilesc pe baza și în concordanță cu prevederile legislației în domeniul protecției infrastructurilor critice în vigoare.

II. În îndeplinirea responsabilităților, ofițerul de legătură pentru securitate al autorităților publice responsabile are următoarele atribuții principale:

a) reprezintă punctul de contact al autorității publice responsabile în relația cu Centrul de coordonare a protecției infrastructurilor critice, cu proprietarii/operatorii/administratorii de infrastructură critică națională / europeană din sectorul/subsectorul aflat în responsabilitate și celelalte autorități publice responsabile, pentru aspectele care țin de securitatea infrastructurilor critice;

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

c) răspunde de actualizarea bazei de date aferente mecanismului de comunicare național în domeniul protecției infrastructurilor critice, privind riscurile, amenințările și vulnerabilitățile identificate la adresa infrastructurii critice națională / europeană din responsabilitate;

d) asigură monitorizarea permanentă a evoluției riscurilor, amenințărilor și vulnerabilităților la adresa infrastructurii critice națională / europeană din responsabilitate;

e) informează, în dinamică, Centrul de coordonare a protecției infrastructurilor critice și celelalte structuri interdependente asupra evoluției riscurilor, amenințărilor și vulnerabilităților la adresa infrastructuri critice națională / europeană, din aria de responsabilitate;

f) propune măsurile cu caracter imediat în situația identificării unor riscuri la nivelul infrastructurii critice națională / europeană din responsabilitate;

g) participă, în calitate de reprezentant desemnat al autorității publice responsabile, la procesul de stabilire a criteriilor și pragurilor critice pentru infrastructura critică națională / europeană din responsabilitate;

h) coordonează activitatea de elaborare a planurilor anuale de verificare prin exerciții și activități specifice, a viabilității PSO sau a documentelor echivalente, existente la nivelul proprietarilor/operatorilor/ administratorilor de infrastructură critică națională / europeană, din aria de responsabilitate;

i) propune conducerii autorității publice responsabile avizarea PSO elaborate la nivelul proprietarilor/operatorilor/administratorilor de infrastructură critică națională / europeană;

j) propune nominalizarea de către conducătorul autorității publice responsabile, a unui expert responsabil din cadrul compartimentului desemnat la nivelul autorității publice responsabile pe problematica protecției infrastructurilor critice, pentru a asigura consiliere operatorilor de infrastructuri critice, inclusiv în faza de elaborare a scenariilor de amenințări și de stabilire a condițiilor de realizare a analizelor de risc;

k) participă, de regulă, la ședințele Grupului de lucru interinstituțional pentru protecția infrastructurilor critice;

l) propune spre aprobare conducătorului autorității publice responsabile componența nominală a Comisiei de evaluare a PSO;

m) informează periodic Centrul de coordonare a protecției infrastructurilor critice cu privire la existența/actualizarea PSO;

n) urmărește respectarea de către proprietarii/operatorii/administratorii de infrastructură critică națională / europeană a prevederilor legale privind protecția infrastructurilor critice;

o) asigură, la solicitarea ofițerului de legătură al proprietarului / operatorului / administratorului de infrastructură critică națională / europeană, consultarea celorlalte autorități publice responsabile / institute de profil, în vederea elaborării scenariilor de amenințări;

p) cooperează cu Centrul de coordonare a protecției infrastructurilor critice în vederea realizării schimbului de informații în domeniul protecției infrastructurilor critice;

q) coordonează elaborarea și transmiterea, la solicitarea Centrului de coordonare a protecției infrastructurilor critice, a informărilor, analizelor, materialelor documentare privind infrastructurile critice din sfera de responsabilitate;

r) participă, la solicitarea Centrului de coordonare a protecției infrastructurilor critice, la activități specifice domeniului (workshop-uri, simpozioane, exerciții de verificare și testare a PSO etc.);

s) propune, în condițiile legii, măsuri pentru asigurarea pregătirii personalului desemnat să îndeplinească funcția de ofițer de legătură pentru securitatea infrastructurilor critice de la nivelul proprietarilor /operatorilor /administratorilor de infrastructură critică națională / europeană;

t) organizează și coordonează activitatea de elaborare și transmitere a documentelor clasificate, aferente infrastructurii critice națională / europeană din aria de responsabilitate, asigurând respectarea normelor în vigoare;

u) verifică modul de îndeplinire de către proprietarii/operatorii/ administratorii de infrastructură critică națională / europeană, din sectorul de responsabilitate, a obligațiilor stabilite de legislația în vigoare și propune conducătorului autorității publice responsabile aplicarea, în condițiile legii, de sancțiuni pentru nerespectarea acestora;

v) elaborează rapoartele de evaluare a exercițiilor desfășurate;

w) coordonează procesul anual de actualizare a listei cu infrastructurile critice din sectorul aflat în competență și informează Centrul de coordonare a protecției infrastructurilor critice cu privire la necesitatea actualizării anexei la Hotărârea Guvernului nr. 1198/2012 privind desemnarea infrastructurilor critice naționale;

x) urmărește permanent, îndeplinirea, potrivit competențelor, a obligațiilor prevăzute de legislația națională în domeniu.

III. În îndeplinirea responsabilităților, ofițerul de legătură pentru securitate al proprietarului/operatorului/administratorului de infrastructură critică națională / europeană are următoarele atribuții principale:

a) reprezintă punctul de contact al proprietarului/operatorului/ administratorului de infrastructură critică națională / europeană în relația cu autoritatea publică responsabilă, cu Centrul de coordonare a protecției infrastructurilor critice precum și alte structuri cu care se află în relație de interdependență, pentru aspectele care țin de securitatea infrastructurilor critice;

b) elaborează și/sau actualizează analiza de risc și identifică punctele vulnerabile privind infrastructură critică națională / europeană din responsabilitate sau propune inițierea demersurilor, în condițiile legii, pentru desemnarea unei persoane fizice/juridice atestate, care să execute aceste activități;

c) elaborează scenariile de amenințări la adresa infrastructurii critice națională / europeană din responsabilitate;

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

e) răspunde de actualizarea bazei de date aferente mecanismului de comunicare național în domeniul protecției infrastructurilor critice, privind riscurile, amenințările și vulnerabilitățile identificate la adresa infrastructurii critice națională / europeană din responsabilitate;

f) asigură monitorizarea permanentă a evoluției situației privind riscurile, amenințările și vulnerabilitățile la adresa infrastructurii critice națională / europeană din responsabilitate;

g) informează, în dinamică, autoritățile publice responsabile și celelalte structuri interdependente asupra evoluției riscurilor, amenințărilor și vulnerabilităților la adresa infrastructurii critice națională / europeană;

h) propune măsurile cu caracter imediat în situația producerii unor riscuri la nivelul infrastructurii critice națională / europeană din responsabilitate;

i) participă, la solicitarea autorității publice responsabile, la procesul de stabilire a criteriilor și pragurilor critice pentru infrastructura critică națională / europeană din responsabilitate;

j) răspunde de evaluarea, testarea și, după caz, actualizarea și revizuirea PSO la termenele stabilite de legislația în vigoare;

k) organizează și conduce exercițiile și activitățile specifice cu ocazia testării PSO sau a documentelor echivalente;

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

m) planifică și asigură, în condițiile legii, participarea personalului din subordine la activități de pregătire de specialitate;

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

o) urmărește permanent îndeplinirea obligațiilor prevăzute de legislația națională în domeniu.