CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ
«Autoritatea Națională pentru Securitatea Rețelelor și Sistemelor Informatice»

GHID PRACTIC

ELABORARE DOCUMENTAȚIA DE AUTOEVALUARE A ÎNDEPLINIRII CERINȚELOR MINIME DE SECURITATE

București, 02 octombrie 2019

Nr. 2100

CUPRINS

Capitolul I. Date generale

1. **Ghidul practic de elaborare a documentației de autoevaluare a îndeplinirii cerințelor minime de securitate** are la bază Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice și Ordinul MCSI nr. 599/2019 privind aprobarea Normelor metodologice de identificare a operatorilor de servicii esențiale și furnizorilor de servicii digitale.

2. Următorii termeni sunt utilizați pe parcursul procesului de elaborarea a documentației de autoevaluare:

DAICMS – Documentația de autoevaluare a îndeplinirii cerințelor minime de securitate.

Legea NIS – Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare.

NIS – rețelele și sistemele informatice.

OENIS – Operatorii economici și celelalte entități care operează ori furnizează servicii în cadrul sectoarelor și subsectoarelor definite în anexa la Legea NIS ori furnizează servicii esențiale din lista prevăzută la art. 20 lit. r din aceeași lege.

PEIOR – procesul de identificare și înscriere a operatorilor de servicii esențiale în ROSE.

Responsabil NIS – personal responsabil cu securitatea rețelelor și sistemelor informatice și desemnat pentru legătura cu CERT-RO/ANSRSI.

ROSE – Registrul operatorilor de servicii esențiale.

3. DAICMS se întocmește în primii doi ani de la intrarea în vioare a acestei legi, respectiv până la data de 12.01.2021, conform art. 14 alin. (3) din OMCSI nr. 599/2018 și în baza art. 43 din Legea NIS, și se utilizează în cadrul procesului de evaluare și înscriere a operatorilor de servicii esențiale în Registrul operatorilor de servicii esențiale.

4. În DAICMS este prezentat stadiul implementării cerințelor minime de securitate în raport cu art. 25 alin. (5) lit. a) ÷ h) din Legea NIS.

5. În conformitate cu art. 43 din Legea NIS și în baza art. 14 alin. (3) din OMCSI nr. 599/2019, în etapa a 2-a din PEIOR, notificarea pentru înscrierea în ROSE va fi transmisă/depusă de către OENIS la CERT-RO împreună cu Declarația pe propria răspundere (Anexa nr. 7 la Normele tehnice aprobate prin OMCSI nr. 599/2019) însoțită obligatoriu de DAICMS.

6. DAICMS presupune identificarea modului de implementare a cerințelor minime de securitate, descrierea acestora și anexarea unor scheme, grafice și tabele, acolo unde e cazul.

7. În vederea elaborării DAICMS, personalul de specialitate (din domeniul securității cibernetice, IT etc.) desemnat ca responsabil(ii) NIS va identifica datele/informațiile necesare întocmirii documentului, va elabora documentul în conformitate cu modelul de la capitolul II, sub formă text, completat cu tabele, grafice și scheme reprezentative.

8. DAICMS va cuprinde toate capitolele precizate în modelul de la capitolul II. În acest sens se vor actualiza/adapta capitolele I și X, iar capitolele II – IX se completează cu datele specificate în model ținând cont de precizările de la fiecare capitol.

9. În susținerea descrierilor, DAICMS se completează, în anexă, cu tabele, grafice, rapoarte și scheme reprezentative.

10. În cazul în care se utilizează instrumente de testare/evaluare a implementării cerințelor minime de securitate la nivelul NIS, rapoartele generate vor fi în limba română și vor însoți DAICMS ca anexă la document.

11. DAICMS se elaborează la nivelul tuturor operatorilor economici, OENIS, pe parcursul procesului de evaluare și notificare în vederea înscrierii în ROSE de către personalul de specialitate (desemnat ca **responsabil NIS** și/sau nominalizat pentru această activitate). DAICMS se semnează de către cel care întocmește documentul și se asumă în numele instituției de către cei în drept.

12. Tabelul cu semnături și aprobări se identifică pe pagina a doua a DAICMS conform modelului de mai jos.

13. În cazul în care activitatea de implementare a cerințelor minime de securitate NIS și/sau de asigurare a funcționării NIS este externalizată, DAICMS va fi elaborată de responsabilul NIS sau o persoană de specialitate din cadrul furnizorului, semnată de acesta și asumată inclusiv de responsabilul NIS.

14. După data de 12.01.2021, DAICMS nu se mai elaborează și va fi înlocuită de Raportul de audit elaborat de un auditor de securitate NIS atestat de către CERT-RO/ANSRSI.

Capitolul II. Model DAICSM

Neclasificat

SIGLA/ LOGO	OENIS (Denumirea operatorului ...)

Documentație de autoevaluare a îndeplinirii cerințelor minime de securitate

a

... OENIS ...

Localitatea, .../...../..... *(data)*

Nr. ...

Întocmit /Avizat / Aprobat[1]	**Prenume Nume**	**Funcție**	**Departament**	**Data**	**Semnătura**
Aprobat	...	...			
Avizat	...	....			
Întocmit	Ion IONESCU	Responsabil NIS ... etc	...		

[1] Se va completa în funcție de fiecare OENIS și de personalul implicat în elaborarea/aprobarea DAICMS.

Capitolul I. Introducere

Documentația de autoevaluare a îndeplinirii cerințelor minime de securitate a fost întocmită conform art. 14 alin. (3) din *Ordinul MCSI nr. 599/2018 privind aprobarea Normelor metodologice de identificare a operatorilor de servicii esențiale și furnizorilor de servicii digitale* și în baza art. 43 din *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice* în cadrul procesului de evaluare și înscriere a operatorilor de servicii esențiale în ROSE.

DAICMS prezintă stadiul implementării la nivelul ..... *(denumirea OENIS)* a cerințelor minime de securitate în raport cu art. 25 alin. (5) lit. a) ÷ h) din Legea NIS.

În procesul de elaborare a DAICMS, responsabilul NIS (sau persoana nominalizată) a identificat toate rețelele și sistemele informatice care susțin furnizarea serviciilor esențiale stabilite/identificate, modul de implementare a cerințelor minime de securitate, a descris cele identificate și a elaborat și anexat scheme, grafice și tabele, acolo unde a fost cazul.

Capitolul II. Rețelele și sistemele informatice care susțin furnizarea serviciilor esențiale

În acest capitol **se identifică și se descriu rețelele și sistemele informatice care susțin fiecare serviciu esențial și se elaborează/prezintă arhitectura NIS** la nivelul OENIS.

Obiective: identificarea NIS; identificarea elementelor componente și a arhitecturii NIS; stabilirea interdependenței și interconectării NIS cu alte NIS ale altor operatori de servicii esențiale ori furnizori de servicii digitale; identificarea punctelor critice NIS.

Sarcini: descrierea NIS; descrierea/precizarea interconectării NIS cu alți OSE/FSD atât din România, cât și din afara țării; tabele interconectări/interdependențe; lista punctelor critice; scheme, grafice etc.; arhitectura NIS.

Rezultate: asigurarea unui nivel ridicat de securitate NIS; stabilirea măsurilor de securitate NIS; determinarea impactului unui incident de securitate cibernetică, atunci când este cazul (obligație cei revine statului român, prin CERT-RO în calitate de CSIRT național, conform Directivei NIS[2] și în baza capitolului IV, secțiunea a 3-a, din Legea NIS).

... se completează ...

Capitolul III. Politicile și planurile proprii de securitate a rețelelor și sistemelor informatice

În acest capitol **se identifică și se descrie politicile și planurile proprii de securitate NIS, precum și modurile de implementare a acestora** la nivelul OENIS.

Obiective: identificarea politicilor și planurilor de securitate la nivelul NIS; modul de implementare a fiecărui plan și a politicilor NIS; stabilirea responsabililor cu implementarea politicilor și a planurilor de securitate.

[2] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, publicată în Jurnalul Oficial al Uniunii Europene seria L nr. 194 din 19 iulie 2016.

Sarcini: enumerare și descriere politici și planuri de securitate; descrierea modalităților de implementare a politicilor și planurilor proprii de securitate NIS; tabele responsabili; scheme, grafice reprezentative etc.

Rezultate: identificarea modului de implementare a politicilor de securitate în vederea asigurării unui nivel comun ridicat de securitate NIS; stabilirea personalului responsabil cu implementarea și gestionarea activităților; punct de pornire în stabilirea unor modele naționale comune de securitate și a ghidurilor de implementare sectoriale/naționale, precum și în identificarea cerințelor de securitate și stabilirea cerințelor specifice de asigurare a securității NIS la nivel sectorial/subsectorial și național (îndeplinirea cerințelor stabilite în capitolul IV și capitolul VI din Legea NIS).

... se completează ...

Capitolul IV. Managementul incidentelor care afectează securitatea rețelelor și sistemelor informatice

În acest capitol **se identifică și se descrie modul de organizare și implementare a managementului incidentelor** la nivelul OENIS.

Obiective: identificarea proceselor managementului incidentelor care afectează securitatea NIS; stabilirea responsabililor cu implementarea și gestionarea managementului incidentelor; identificarea modalităților de stabilire a impactului unui incident de securitate cibernetică; identificarea modalităților de prevenire, limitare și combatere a efectelor unui incident cibernetic; stabilirea modalităților de notificare a autorității naționale – CERT-RO; cooperarea cu alte instituții/ autorități și informare în procesul de management al incidentelor.

Sarcini: descrierea modului de organizare și implementare a managementului incidentelor; tabele/ liste responsabili implementare și gestionare; descrierea modalități de notificare și informare; liste cooperare și informare; scheme intervenție, planuri, grafice reprezentative etc.

Rezultate: identificarea modului de administrare a unui incident de securitate cibernetică; identificarea unor modalități de limitare și contracarare a efectelor incidentelor; stabilirea unor modalități de cooperare de specialitate atât la nivel sector/subsector, cât și național/internațional; limitarea pierderilor, financiare și economice, precum și asigurarea continuității furnizării serviciului esențial (îndeplinirea cerințelor stabilite în capitolul IV din Legea NIS).

... se completează ...

Capitolul V. Accesul la rețelele și sistemele informatice

În acest capitol **se descrie modul de utilizare și accesare a NIS** la nivelul OENIS.

Obiective: prevenirea accesului neautorizat la NIS; stabilirea modului de administrare/gestionare a NIS; stabilirea modului de realizare a accesului la NIS; monitorizarea și controlul accesului la NIS.

Sarcini: descrierea modului de organizare și implementare a managementului accesului la NIS; tabele/liste responsabili/administratori etc.; descrierea modului de monitorizare și control a accesului la resursele NIS; scheme, planuri, grafice etc.

Rezultate: limitarea și prevenirea accesului neautorizat la NIS; identificarea modului de monitorizare și control a accesului la resursele NIS; creșterea nivelului de securitate a NIS; stabilirea unor ghiduri de bune practici atât la nivel sector/subsector, cât și național (îndeplinirea cerințelor stabilite în capitolul IV din Legea NIS).

... se completează ...

Capitolul VI. Diseminarea datelor deținute la nivelul rețelelor și sistemelor informatice

În acest capitol **se descrie modul de accesare/procesare/stocare a datelor/informațiilor din NIS, precum și modalitățile de diseminare a acestora** la nivelul OENIS.

Obiective: prevenirea diseminării neautorizate; stabilirea persoanelor autorizate să dețină sau să utilizeze datele gestionate în NIS; stabilirea modului de remediere a incidentelor semnalate cu privire la diseminarea neautorizată a datelor de la nivelul NIS.

Sarcini: descrierea modului de organizare și implementare a managementului accesului la NIS; tabele/liste responsabili/administratori etc.; descrierea modului de monitorizare și control a accesului la resursele NIS; scheme, planuri, grafice etc.

Rezultate: limitarea și prevenirea accesului neautorizat la NIS; controlul accesului la informațiile NIS, instruirea și conștientizarea personalului privind accesul la datele instituției; creșterea nivelului de securitate a NIS; limitarea pierderilor de date/informații (îndeplinirea cerințelor stabilite în capitolul IV din Legea NIS).

... se completează ...

Capitolul VII. Sistemului de management al riscului

În acest capitol **se descrie modul de implementarea a sistemului de management al riscului** la nivelul OENIS.

Obiective: identificarea modului de implementare a sistemului de management al riscului; stabilirea modalităților de continuitatea a funcționării NIS în cazul unor riscuri identificate; stabilirea unor registre a riscurilor de securitate, dacă e cazul.

Sarcini: descrierea modului de implementare a sistemului de management al riscului; lista/registrul riscurilor; descrierea modului de acțiune și implementare a măsurilor de atenuare a riscurilor; scheme, grafice etc.

Rezultate: reducerea riscurilor identificate; implementarea unor măsuri adecvate de atenuare/limitare a riscurilor identificate; stabilirea personalului și a resurselor necesare; creșterea nivelului de securitate a NIS; limitarea pierderilor financiare și realizarea furnizării optime a serviciului esențial (îndeplinirea cerințelor stabilite în capitolul IV din Legea NIS).

... se completează ...

Capitolul VIII. Planuri de acțiune pe niveluri de alertă de securitate a rețelelor și sistemelor informatice

În acest capitol **se identifica și descrie modul de implementare a planurilor de acțiune, în funcție de nivelurile de alertă de securitate NIS** la nivelul OENIS.

Obiective: identificarea planurilor de acțiune; identificare modului de implementare a planurilor de acțiune pe niveluri de alertă de securitate NIS; stabilirea personalului responsabil pentru implementarea planurilor de acțiune.

Sarcini: descrierea modului de implementare a planurilor de acțiune pe niveluri de alertă de securitate NIS; lista/registrul personalului responsabil cu implementarea; descrierea modului de acțiune în caz de alertă de securitate NIS; scheme, grafice etc.

Rezultate: reducerea impactului unei alerte de securitate asupra NIS; implementarea unor măsuri adecvate de acțiune în cazul unor alerte de securitate NIS; stabilirea personalului responsabil cu aplicarea/implementarea planurilor; creșterea nivelului de securitate a NIS; limitarea pierderilor financiare, economice și asigurarea continuității furnizării serviciului esențial (îndeplinirea cerințelor stabilite în capitolul IV din Legea NIS).

... se completează ...

Capitolul IX. Asigurarea continuității serviciilor

În acest capitol **se descrie modul de asigurarea a continuității serviciilor, inclusiv mijloacele alternative de furnizare a serviciului esențial** la nivelul OENIS.

Obiective: identificarea modalităților de asigurare a serviciilor în cazul unor atacuri cibernetice și/sau alerte; identificarea modului de remediere/recuperare a datelor și informațiilor afectate de un incident/ dezastru; identificarea mijloacelor alternative pentru furnizarea serviciului esențial; stabilirea resurselor și a personalului responsabil pentru asigurarea continuității serviciului.

Sarcini: descrierea modului de asigurarea a continuității serviciilor; descrierea modalităților de recuperare a datelor/informațiilor; nominalizarea și descrierea mijloacelor alternative pentru furnizarea serviciului esențial; lista/registrul resurselor și personalului responsabil cu asigurarea continuității; scheme, grafice etc.

Rezultate: asigurarea continuității serviciului indiferent de situația creată, atacuri cibernetice, alerte de securitate etc.; implementarea unor mijloace alternative de asigurare a continuității serviciilor; stabilirea personalului responsabil și modalităților de acțiune în vederea asigurării continuității serviciilor; creșterea nivelului de securitate a NIS; limitarea pierderilor financiare, economice și asigurarea continuității furnizării serviciului esențial (îndeplinirea cerințelor stabilite în capitolul IV din Legea NIS).

... se completează ...

Capitolul X. Dispoziții finale

În acest capitol **se precizează date cu privire la DAICMS despre responsabili, instituție, locație, anexe (dacă e cazul) și volumul.**

Prezentul DAICMS a fost elaborat la data de *.... /..../.... (data)* la sediul *..... (denumirea OENIS)* situat în localitatea *..... (localitatea)*, județul *..... (județul)*, de către *..... (numele și prenumele)*, desemnat responsabil NIS prin *.... (tipul actului de numire),* nr. *..... (numărul actului)* din *../../..... (data actului)*.

Prezentul DAICMS cuprinde xx file (xx pagini).

Anexele[3] 1 – xx *(se trece numărul de anexe)* fac parte integrantă din DAICMS.

Anexe DAICMS:

Anexa nr. 1 .... *(denumire anexă)*, ... file / ... pagini

Anexa nr. xx ..... *(denumire anexă)*, ... file / ... pagini

[3] Referința la anexe se face direct în text, iar aici la final se trece numărul total al anexelor.