GHID PRACTIC PENTRU OSE

Implementarea măsurilor minime de asigurare a securității rețelelor și sistemelor informatice



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ



ISACA®
Romania Chapter

Editura Sitech 2021

ISBN 978-606-11-7971-8, e-book: https://dnsc.ro/vezi/document/ghid-ose

Autori:

Adrian Munteanu este profesor universitar doctor în cadrul Facultății de Economie și Administrarea Afacerilor – Univ. Alexandru Ioan Cuza din Iași, unde predă cursuri despre securitatea informațiilor, auditul sistemelor informaționale, guvernare și managementul serviciilor IT. A fost co-președintele filialei din România a IAPP (International Association of Privacy Professionals), membership director al ISACA Romania Chapter și instructor pentru cursurile CISA (Certified Information Systems Auditor) și CIPM (Certified Information Privacy Manager).

Adrian este auditor de securitate cibernetică atestat DNSC, expert ENISA (European Union Agency for Network and Information Security) în domeniul managementului riscurilor și deține certificări relevante cum ar fi CISA, CRISC, CDPSE, CIPM, COBIT Foundation, ITIL Foundation. Are o experiență de peste 15 ani în misiuni de audit, consultanță și instruire în industrii diferite.

Adrian Păuna este auditor de securitate cibernetică atestat DNSC, specialist în domeniul securității cibernetice cu o experiență de mai mult de 15 ani. A lucrat în zona administrației publice participând la crearea primului CERT guvernamental. Ulterior a activat la ENISA - Agenția Uniunii Europene pentru Securitate Cibernetică unde a elaborat o serie de studii în zona securității ICS/SCADA. In ultimii ani își desfășoară activitatea într-o mare companie IT unde executa activități de Pentest, audit intern ISO 27001 si PCI DSS. Adrian a obținut titlul de doctor in științe inginerești, domeniul securitatea informatică la Academia Tehnica Militară din București. Deține o serie de certificări in domeniul securității cibernetice din care menționăm: CISSP, CISA, OSCP, CEH, CREST CRT, ISO 27001:2013 LA.

Claudiu Constantinescu a fost administrator de rețele și sisteme înainte de a fi auditor IT și de securitatea informației. Acum, după 15 ani de consultanță și audit în domeniul securității, continuității și managementului fraudelor, poate spune că a lucrat cu organizații din toate zonele de business, mari și mici, fiind implicat inclusiv în proiecte pentru multinaționale la nivel global. Printre certificări se numără și CISA, CISM, ISO27001 Lead Auditor și Lead Implementer.

Grațiela Măgdălinoiu este Președinte al Boardului ISACA Romania Chapter, contribuind in ultimii 5 ani la dezvoltarea comunității de specialiști si crearea unor parteneriate solide cu instituții academice, publice sau alte asociații profesionale in

domeniu, fiind in același timp implicata in mod activ in inițiative locale de reglementare si grupuri de lucru.

Grațiela are peste 15 ani de experiență in proiecte de guvernanta, conformitate, audit si management al riscului in securitatea informației, acumulata atât in mediul corporate cat si cel antreprenorial. A condus proiecte complexe, cu interacțiune si raportare către nivelul executiv superior al organizațiilor, lărgindu-și aria de expertiza in timp, si acoperind nu numai tehnologia și securitatea informației ci si programe ABAC, protecția datelor cu caracter personal sau etica si conformitate de business. Deține certificări relevante in domeniu precum: CISA, ISO 27001, ISO 20000, CDSPE, CIPP.

Ilie Voinea este un specialist în domeniul protecției datelor și securității informației. Are o experiență de cel puțin 10 ani in managementul IT într-un mare grup de firme. In ultimii ani activează ca Data Protection Officer si Consultant IT. Deține certificări din partea IAPP, ISACA si PECB: CDPSE, CIPP/E, CDPO, Lead Auditor 27001:2013

Larisa Găbudeanu este un profesionist în domeniul protecției datelor și securității informației. Autor/co-autor a mai multor volume, inclusiv despre gestionarea riscului în domeniul tehnologiei informatice și a datelor personale, cadru didactic asociat și lector în numeroase conferințe naționale și internaționale. Având experiență academică în domeniul dreptului și al securității informațiilor, activitatea sa se axează pe aspecte privind dreptul informatic, criminalitatea informatică, infracțiuni în cadrul afacerilor, securitatea informației și protecția datelor personale. De asemenea, a susținut examinări și deține certificări relevante în aceste domenii, precum, CDPSE, CISA, CRISC, CISM, CIPM, CIPP/E. Are o experiență vastă într-o firmă de avocatură internațională, acordând consultanță clienților internaționali și coordonând proiecte în drept bancar, drept informatic, infracțiuni privind afacerile și protecția datelor personale, precum și experiență în protecția datelor și securitatea informatică în cadrul unui grup regional bancar.

Tiberiu Anghel este membru al Board-ului ISACA Romania Chapter de peste 3 ani si are mai bine de 10 ani de experiență în securitate cibernetica, atât in domeniul public cat si in domeniul privat. Tiberiu este specializat in zona de detecție și răspuns la incidente de securitate cibernetica, având o bună înțelegere a proceselor, tehnologiilor și a cerințelor privind specialiștii. Mai mult, el a participat in diverse proiecte de consultanta privind implementarea proceselor si a sistemelor de securitate cibernetică, lucrând cu companii din multiple industrii: retail, energie, banking, fintech, insurance. Tiberiu a urmat cursurile masterului in Managementul Inovatiei din cadrul University of Amsterdam si este certificat CISM.

CUPRINS

CUVÂNT ÎNAINTE 5

CAPITOLUL 1: INTRODUCERE 8

1.1 Concepte generale 8
1.2 Domeniul de securitate Guvernanță 11
Analiza riscurilor de securitate a sistemelor informatice 11
Politica de securitate a sistemului informatic 11
Acreditarea securității sistemului informatic 11
Indicatori de evaluare a conformității securității sistemului informatic 12
Auditul de securitate al sistemului informatic 12
Securitatea resurselor umane 12
Gestionarea activelor 12
Cartografierea ecosistemului 13
Relațiile ecosistemului 13
1.3 Domeniul de securitate Protecție 13
Configurarea sistemelor 13
Segregarea sistemelor 14
Filtrarea traficului 14
Criptografie 14
Conturi pentru administrare 14
Administrarea sistemelor informatice 15
Autentificare și identificare 15
Drepturile de acces 16
Mentenanța securității IT 16
Sisteme de control industrial 17
Securitate fizică și a mediului de lucru 17
1.4 Domeniul de securitate Apărare 17
Detectare 17
Înregistrarea evenimentelor/Logare 17
Corelarea și analiza jurnalelor 18
Răspuns la incidente de securitate 18
Raport incidente 18
Comunicarea cu autoritățile competente și CSIRT Național 18
1.5 Domeniul de securitate Reziliență 19
1.6 Managementul riscurilor 20
1.6.1 Introducere 20
1.6.2 Managementul riscurilor conform standardelor ISO 22

CAPITOLUL 2: IMPLEMENTAREA CERINȚELOR MINIME DE SECURITATE 26

2.1 Domeniul de securitate : A - GUVERNANȚĂ 27
2.1.1 Categoria de activități de securitate: A 1 - Managementul securității informației 27
2.1.2 Categoria de activități de securitate: A 2 - Managementul ecosistemului 49

2.3 Domeniul de securitate : B - PROTECŢIE 54
2.3.1 Categoria de activități de securitate: B 1 - Managementul arhitecturii 54
2.3.2 Categoria de activități de securitate: B 2 - Managementul administrării 65
2.3.3 Categoria de activități de securitate B3 - Managementul identității și accesului 72
2.3.4 Categoria de activități de securitateB4 - Managementul mentenanței 78
2.4 Domeniul de securitate C1 – Managementul detecției 87
2.4.1 Categoria de activități de securitate C1 - Managementul Detecției 87
2.4.2 Categoria de activități de securitate: C2 - Managementul incidentelor de Securitate 95
2.5 Domeniul de securitate D: Reziliență 103
2.5.1 Categoria de activități de securitate D1 – Managementul continuității afacerii 103
2.5.3 Categoria de securitate D2 - Managementul crizelor 106

CAPITOLUL 3: INDICATORI DE EVALUARE A CONFORMITĂȚII 109

Anexa 1: Alinierea cerințelor de securitate cu standard internaționale 120
Anexa 2: Listă standarde 141
Anexa 3: Legislație 147

CUVÂNT ÎNAINTE

Acest ghid a fost conceput ca un instrument de lucru care să ofere suport operatorilor de servicii esențiale în vederea implementării cerințelor minime de asigurare a securității rețelelor și sistemelor informatice așa cum sunt acestea publicate în Normele tehnice din 09.11.2020, **Text publicat în Monitorul Oficial, Partea I nr. 1142 din 26 noiembrie 2020.** Prin Ordonanța 104/2021 publicată în Monitorul Oficial din 24 septembrie 2021 a fost înființat **Directoratul Național de Securitate Cibernetică (DNSC)** instituție care înlocuiește CERT.

Autorii au conceput acest material în primul rând ca o resursă educațională pentru profesioniștii din domeniul guvernantei securității cibernetice din cadrul organizațiilor și, în mod particular, operatorilor de servicii esențiale (OSE) dar și ca un ghid ce poate fi folosit în implementarea și evaluarea nivelului maturității sistemului de guvernanță și control al acestora. În acest ghid, referințele la CERT.RO au fost înlocuite cu DNSC.

Ghidul se adresează atât responsabililor NIS dar și managerilor IT/CIO/CISO și, nu în ultimul rând, studenților de la facultățile unde se studiază securitatea cibernetică/securitatea informațiilor. Având la bază ghidurile *ENISA (European Network Information Security Agency),* suita de standarde *ISO 27000,* controalele descrise în *CIS (Center for Internet Security), CSA (Cloud Security Alliance)* și *NIST (National Institute for Standards and Technology)* materialul prezintă exemple de implementare tehnică și administrativă a cerințelor minime de securitate cibernetică și exemple de indicatori de evaluare a conformității cu normele tehnice.

În timp ce măsurile de control (cerințele minime de securitate) au fost elaborate pentru a asigura un nivel adecvat de gestionare a riscurilor de securitate cibernetică și răspunsul la incidente pentru operatorii de servicii esențiale în conformitate cu obligațiile care le revin în temeiul legislației NIS, ele pot fi utilizate de organizațiile din orice sector sau comunitate în măsura în care acestea sunt ajustate pe necesitățile specifice ale acestora. Liniile directoare permit organizațiilor - indiferent de mărime, grad de risc de securitate cibernetică sau nivel de maturitate al securității cibernetice - să aplice principiile și cele mai bune practici pentru a îmbunătăți securitatea și reziliența.

Abordările și interpretările prezentate reprezintă una din metodele pentru gestionarea riscurilor de securitate cibernetică într-un mediu care operează servicii esențiale, dar nu singura. Tipologia riscurilor diferă în funcție de sectorul/industria din care fiecare organizație face parte, având potențiale riscuri, amenințări și vulnerabilități unice, care necesită o abordare specifică. Scopul acestui ghid este de

a prezenta abordări practice în vederea implementării unui sistem de control robust, atât din punct de vedere procedural cât și din punct de vedere tehnic. De asemenea, pentru fiecare secțiune au fost identificate legături cu alte standarde, ghiduri și documente relevante din domeniul securității informației/cibernetice ca un suport pentru documentarea fiecărei arii în scop.

Ghidul este conceput de un grup de lucru format din profesioniști din cadrul ISACA Romania Chapter (Information Systems Audit and Control Association – organizația din România) cu experiență relevantă în proiectarea, implementarea și auditarea sistemelor de control IT precum și cu o bună cunoaștere a practicilor curente specifice unor industrii cu profil diferit și reprezintă interpretarea acestora cu privire la cerințele legislative locale *(lege și normă)* din perspectiva standardelor și celor mai bune practici în domeniul guvernanței și controlului sistemelor de securitate a informației și cibernetice.

Prin **urmare** acest ghid oferă doar una din căile pe care un responsabil NIS sau un responsabil cu asigurarea securității informațiilor le poate urma și nu exclude faptul că există alte informații, proceduri și teste care se pot folosi în mod rezonabil spre obținerea acelorași rezultate.

În determinarea conformității unor cerințe specifice, a unor proceduri sau teste, cititorii trebuie să integreze circumstanțele specifice organizației, securității cibernetice sau managementului riscurilor prezente în cazurile particulare ale mediului sistemelor informaționale sau tehnologiei din propria organizație

Mulțumiri domnului Dan Cîmpean, director DNSC și echipei Directoratului Național pentru Securitate Cibernetică pentru suportul asigurat în conceperea, realizarea și revizuirea acestui ghid.

Grațiela Măgdălinoiu, președinte ISACA Romania Chapter

Tiberiu Anghel, membru echipă conducere ISACA Romania Chapter

****

Cu peste 50 de ani de existență, ISACA (www.isaca.org) este o asociație globală ce ajută persoanele și organizațiile să își atingă potențialul maxim prin tehnologie. ISACA este prezentă în mai mult de 188 de țări, incluzând mai mult de 217 filiale. ISACA oferă profesioniștilor din domeniului IT accesul la cunoștințe, acreditări, educație și comunități pentru a avansa în carierele lor și pentru a susține procesul de transformare a organizațiilor pe care le reprezintă. Publicațiile ISACA au la bază expertiza membrilor săi (jumătate de milion de specialiști în securitate cibernetică, guvernanță, asigurări, risc și inovație). ISACA Romania Chapter este înființată în 2003, ajungând astăzi la peste 450 de membri.

CAPITOLUL 1: INTRODUCERE

1.1 Concepte generale

În implementarea cerințelor minime de securitate, operatorii de servicii esențiale (OSE) trebuie să ia în considerare că măsurile (controalele) de securitate menționate în Normele tehnice trebuie să fie:

- **Eficiente** în creșterea posturii de securitate cibernetică a unui OSE în raport cu peisajul amenințărilor acum și în viitorul previzibil.
- **Adaptate** pentru a asigura că efortul financiar, uman și tehnic este aplicat măsurilor care vor avea cel mai mare impact în ceea ce privește îmbunătățirea securității unui OSE.
- **Compatibile** pentru a aborda vulnerabilitățile intersectoriale și completat cu măsuri de securitate specifice sectorului.
- **Proporționale** față de riscuri, cu accent pe protejarea sistemelor și infrastructurilor care stau la baza serviciilor esențiale.
- **Concrete și ușor de înțeles**, pentru a se asigura că măsurile sunt de fapt puse în aplicare în totalitate și pentru a spori activ postura de securitate cibernetică.
- **Verificabile** pentru a se asigura că OSE poate furniza auditorilor dovezi ale implementării eficiente a măsurilor de securitate.
- **Incluzive** pentru a se asigura că sunt acoperite toate cele patru domenii de securitate: *guvernanță, protecție, apărare cibernetică, reziliență*.

Conform *COBIT (Control Objectives for Information and Related Technologies)* guvernanța asigură că sunt evaluate nevoile beneficiarilor, condițiile și opțiunile, cu scopul de a identifica:

- obiective echilibrate, asumate și care pot fi atinse;
- stabilirea priorităților și luarea deciziilor;
- monitorizarea performanței și conformitatea cu direcțiile și obiectivele asumate.

În majoritatea organizațiilor, guvernarea este responsabilitatea consiliului director sub conducerea președintelui acestuia. În cazul organizațiilor mari, complexe, responsabilitățile specifice guvernării pot fi delegate unor structuri organizatorice speciale.

Managementul planifică, creează, administrează și monitorizează activitățile/procesele în conformitate cu direcțiile stabilite de organismul de guvernanță, cu scopul de a atinge obiectivele organizației. În majoritatea organizațiilor, managementul este responsabilitatea nivelului executiv, sub conducerea directorului executiv (CEO).

Guvernanța unei organizații are în vedere 5 tipuri de active[1]:

- umane
- financiare
- proprietate intelectuală
- informații și tehnologie (IT)
- relațiile economice/de afaceri

În ceea ce privește guvernanța IT amintim cele mai cunoscute cadre de lucru, standarde și bune practici care pot fi utilizate în dezvoltarea practică a unui sistem de guvernanță a tehnologiilor informaționale:

- *Capability Maturity Model Integration (CMMI)*
- *Publicațiile ISACA din seria COBIT 2019*
- *Publicațiile International Organization for Standardization (ISO) (ISO 38500 - Corporate governance of Information Techonlogy)*
- *Infrastructure Library (ITIL) sau ISO 20000 - Service Management*
- *PRojects IN Controlled Environments (PRINCE2®)*
- *Project Management Body of Knowledge® (PMBOK®)*
- *The Open Group Architecture Framework (TOGAF®)*

În realizarea acestui ghid ne-am bazat pe 3 definiții conform ITIL și COBIT:

- **Proces** - *un set structurat de activități proiectat pentru a îndeplini un obiectiv specific.* Un proces preia una sau mai multe intrări (inputs) și le transformă în rezultate (outputs) definite. Poate include oricare dintre roluri, responsabilități, instrumente și controale de management necesare pentru a furniza rezultatele cu un grad mare de încredere. Un proces poate defini politici,

[1] **Weill, Peter; Jeanne Ross: IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, USA, 2004**

standarde, recomandări, activități și instrucțiuni de lucru dacă acestea sunt necesare.

- **Procedură** - *un document care conține pașii/etapele prin care se descrie cum se îndeplinește/realizează o activitate și rolurile implicate.* Procedurile sunt definite ca părți din procese.
- **Instrucțiune de lucru** - *un document care conține instrucțiuni detaliate care specifică exact ce pași trebuie urmați pentru a finaliza o activitate*. O instrucțiune de lucru conține mult mai multe detalii decât o procedură și este creată numai dacă sunt necesare instrucțiuni detaliate.

Pentru a satisface obiectivele de guvernanță și de management, fiecare OSE ar trebui să stabilească, să adapteze și să susțină un sistem de guvernanță construit dintr-un număr de componente[2]. Aceste componente sunt factori care, individual și colectiv, contribuie la buna funcționare a sistemului de guvernanță IT a organizației:

- **Procesele** sunt un set organizat de practici și activități pentru a atinge anumite obiective și pentru a produce un set de rezultate care sprijină atingerea obiectivelor generale legate de IT.
- **Structurile organizaționale** sunt entitățile cheie de decizie într-o organizație.
- **Principiile, politicile/procedurile și cadrele de lucru** descriu comportamentul dorit pentru managementul activităților curente.
- **Informațiile** care se regăsesc în întreaga organizație includ toate informațiile produse și utilizate, necesare pentru funcționarea eficace a sistemului de guvernanță al organizației.
- **Cultura, etica și comportamentul** angajaților sunt factorii care asigură succesul activităților de guvernanță și management.
- **Angajații, abilitățile și competențele acestora** sunt necesare pentru luarea unor decizii bune, pentru efectuarea acțiunilor corective și pentru succesul în finalizarea tuturor activităților.
- **Serviciile, infrastructura sistemele și aplicațiile** includ infrastructura, tehnologia/sistemele și aplicațiile care furnizează organizației sistemul de guvernanță pentru prelucrările din cadrul IT.

Chiar dacă COBIT 2019 și ISO 20000 (de exemplu) tratează domeniul guvernanței IT, principiile și bunele practici descrise în aceste publicații se aplică și în cazul guvernanței securității cibernetice.

[2] **Traducere și adaptare COBIT 2019 - Introduction and Methodology, pg. 19**

1.2 Domeniul de securitate Guvernanță[3]

Analiza riscurilor de securitate a sistemelor informatice

Operatorul de servicii esențiale (OSE) efectuează și actualizează periodic analiza a riscurilor de securitate, identificând sistemele/ echipamentele informatice critice (SIC) care stau la baza furnizării serviciilor esențiale ale OSE și identifică principalele riscuri pentru aceste SIC. Acest proces este esențial pentru a construi și a menține un sistem robust de gestionare a riscurilor. Rezultatele actualizărilor ar trebui implementate printr-un sistem circular de îmbunătățire continuă.

Evaluarea riscurilor ia în considerare, cel puțin:

- noile amenințări în domeniul securității cibernetice;
- punctele slabe descoperite recent;
- pierderea eficacității măsurilor de securitate;
- modificările situației de risc cauzate de modificările arhitecturii rețelelor şi sistemelor informatice;
- orice alte modificări si evoluții ale situației si nivelului de risc.

Politica de securitate a sistemului informatic

Pornind de la analiza riscurilor, OSE elaborează, menține și implementează o politică de securitate a sistemelor informatice (**PSSI**) și un sistem de management al securității informațiilor (**SMSI**) aprobat de conducerea executiva si garantând astfel asumarea acesteia..

Politica stabilește obiectivele strategice de securitate, descrie guvernanța securității (sau managementul riscului organizației) și se referă la toate politicile relevante de securitate ale sistemului informațional specific (de exemplu, privind procesul de acreditare a securității, audit de securitate, criptografie, întreținere a securității, gestionarea incidentelor etc.).

Acreditarea securității sistemului informatic[4]

Pornind de la analiza riscurilor și în conformitate cu un proces de acreditare menționat în PSSI, OSE acreditează SIC identificate în analiza riscurilor de securitate a sistemelor informatice, inclusiv, printre altele, inventarul și arhitectura

[3] **Traducere și adaptare după Reference document on security measures for Operators of Essential Services CG Publication 01/2018, NIS Cooperation Group, February 2018**

[4] **Acreditarea SIC" trebuie înțeleasă ca decizia proprie a OSE de identificare a SIC-ului său, riscurile asociate și riscurile reziduale pe care OSE alege să le accepte**

componentelor de administrare ale SIC. Scopurile procesului de acreditare pentru operator sunt de a integra SIC în cadrul managementului riscului organizației și de a accepta formal riscurile reziduale.

Ca parte a procesului de acreditare și în funcție de analiza riscurilor, este necesara efectuarea unui audit de securitate pentru verificarea aplicării și eficacității măsurilor de securitate care se aplică SIC. Decizia de acreditare va lua în considerare analiza riscurilor, măsurile de securitate aplicate SIC, rapoartele de audit și riscurile reziduale și motivele care justifică acceptarea acestora. OSE definește un program de revizuire si management al schimbării pentru a asigura actualitate SIC in contextul extern si intern al organizației

Indicatori de evaluare a conformității securității sistemului informatic

Pentru fiecare SIC și în conformitate cu o serie de indicatori și metode de evaluare, OSE evaluează conformitatea acestuia cu PSSI-ul său. Indicatorii se pot referi la performanța organizației in gestionarea riscurilor, menținerea menținerea unui nivel adecvat de securitate, drepturile de acces ale utilizatorilor, autentificarea accesului la resurse și administrarea resurselor.

Auditul de securitate al sistemului informatic

OSE stabilește și actualizează o politică și proceduri pentru efectuarea evaluărilor de securitate a sistemului informatic și a auditurilor activelor critice și a SIC, ținând cont de analiza riscurilor actualizată periodic.

Securitatea resurselor umane

OSE se asigură in primul rând că, angajații și furnizorii/ contractanții înțeleg și își asuma responsabilitățile lor și sunt potriviți pentru rolurile stabilite. Politicile de securitate stabilite pentru sistemul informatic instituie un plan de comunicare a securității SIC pentru tot personalul, precum și un program de instruire în domeniul securității pentru angajații care utilizează SIC.

Gestionarea activelor

OSE stabilește un cadru adecvat pentru identificarea, clasificarea și implementarea unui inventar al proceselor IT, sistemelor și elementelor componente ale rețelelor și sistemelor informatice, inclusiv a datelor. Această gestionare a activelor permite lansarea actualizărilor și patch-urilor și, după caz, determină ce componente sunt afectate de noi amenințări de securitate.

Cartografierea ecosistemului

OSE stabilește o cartografiere a ecosistemului său, incluzând părțile interesate interne și externe, inclusiv, dar fără a se limita la furnizori, în special cei cu acces la, sau care gestionează activele critice ale operatorului.

Scopul acestei cartografieri este de a identifica și evalua riscurile potențiale reprezentate de relațiile cu părțile interesate ale ecosistemului. Pentru a efectua această evaluare, operatorul va lua în considerare patru parametri majori:

- **Maturitate**: care sunt capacitățile tehnice ale părților interesate în ceea ce privește securitatea cibernetică?
- **Încredere**: Pot presupune că intențiile părții interesate față de mine sunt legitime?
- **Nivel de acces**: Care sunt drepturile de acces ale părților interesate la activele mele critice și SIC?
- **Dependență**: în ce măsură relația cu părțile interesate este critică pentru activitatea mea?

Relațiile ecosistemului

OSE stabilește o politică față de relațiile sale cu ecosistemul său pentru a reduce riscurile potențiale identificate. Aceasta include în special interfețele dintre SIC și terți. În general, sunt luate în considerare cerințele de securitate pentru componentele SIC operate de terți. Operatorul se asigură prin acorduri de nivel de serviciu (SLA) și/ sau mecanisme de audit că si furnizorii săi implementează măsuri adecvate de securitate.

1.3 Domeniul de securitate Protecție

Configurarea sistemelor

OSE instalează doar servicii și funcționalități sau conectează echipamente care sunt esențiale pentru funcționarea și securitatea SIC. Dacă componentele suplimentare sunt inevitabile (de exemplu, din motive economice), acestea sunt analizate în conformitate cu analiza riscurilor. Aceste componente trebuie utilizate numai când este necesar și doar cu măsuri de securitate adecvate.

De exemplu, OSE conectează la SIC doar echipamente, periferice hardware și suporturi amovibile pe care le-a înregistrat în mod corespunzător și care sunt esențiale pentru funcționarea sau securitatea SIC-ului său.

Segregarea sistemelor

OSE își separă sistemele pentru a limita propagarea incidentelor de securitate IT în sistemele sau subsistemele sale. În acest scop, OSE separă fizic sau logic fiecare SIC de celelalte sisteme informatice proprii sau de sistemul informatic al terților. În cazul în care un SIC în sine este compus din subsisteme, OSE le separă din punct de vedere fizic sau logic. OSE permite numai interconectări - între SIC și alte sisteme sau între subsistemele SIC - care sunt esențiale pentru funcționarea și securitatea unui SIC.

OSE pune în aplicare măsuri de securitate adecvate pentru interconectările ce nu pot fi evitate (de exemplu, interconectările cu sistemele IT ale furnizorilor sau clienților).

Filtrarea traficului

OSE filtrează fluxurile de trafic care circulă în sistemele sale informatice critice (SIC). Prin urmare, operatorul interzice fluxurile de trafic care nu sunt necesare pentru funcționarea sistemelor sale și care ar putea facilita un atac.

OSE definește și actualizează constant regulile de filtrare (după adresa rețelei, după numărul portului, prin protocol etc.) pentru a restrânge fluxurile de trafic la fluxurile necesare funcționării și securității SIC.

OSE filtrează fluxurile de intrare, cele existente in SIC și fluxurile între subsistemele SIC la nivelul interconectării acestora, limitând astfel fluxurile numai la cele strict necesare pentru funcționarea și securitatea SIC.

Criptografie

În PSSI, OSE stabilește și implementează o politică și proceduri legate de criptografie, în vederea asigurării utilizării adecvate și eficiente a criptografiei pentru a proteja confidențialitatea, autenticitatea și / sau integritatea informațiilor din SIC.

Conturi pentru administrare

OSE stabilește conturi specifice pentru administrare, pentru a fi utilizate numai de administratorii care desfășoară operațiuni de administrare (instalare, configurare, gestionare, întreținere etc.) la nivelul SIC-ului său. Lista acestor conturi trebuie actualizata periodic si poate include si detalii despre conturile care nu sunt de administrare.

În acest scop, permisiunile acordate administratorilor devin individuale și limitate pe cât posibil la perimetrul funcțional și tehnic al fiecăruia. Conturile de

administrator sunt utilizate numai pentru conectarea la sistemul informatic de administrare, exclusiv prin intermediul conturilor dedicate.

Administrarea sistemelor informatice

Resursele hardware și software utilizate în scopuri de administrare sunt gestionate și configurate de OSE sau, după caz, de furnizorul de servicii, intern sau extern, pe care OSE l-a autorizat să efectueze aceste operațiuni.

Sistemele informatice de administrare sunt utilizate exclusiv în scopuri de administrare și pentru a efectua astfel de operațiuni . În special, sistemul informatic dedicat nu este utilizat pentru accesul la site-uri web sau sisteme de mesagerie pe internet, iar utilizatorii nu se conectează la sistem printr-un mediu software utilizat pentru alte funcții decât operațiunile de administrare.

OSE creează o rețea fizică și/sau virtuală dedicată pentru a conecta sistemele de administrare la resursele care urmează să fie administrate. Administratorul utilizează în acest scop interfața de administrare fizică a resurselor[5]. În cazul în care măsurile de administrare nu sunt efectuate prin intermediul rețelei dedicate, fluxurile sunt protejate prin mecanisme de autentificare și criptare[6].

In nici o circumstanță, nici o parolă, sub formă de text simplu sau hash, nu este scrisă sau stocata in aceasta forma în jurnalele de înregistrare a evenimentelor produse de resursele utilizate pentru administrare.

Autentificare și identificare

Pentru identificare, OSE stabilește conturi unice pentru utilizatori sau pentru procese automatizate care trebuie să acceseze resursele din SIC[7]. Conturile neutilizate sau care nu mai sunt necesare vor fi dezactivate. Trebuie implementat un proces de revizuire permanent.

OSE protejează accesul la resursele SIC-ului său pentru utilizatori sau procesele automate utilizând un mecanism de autentificare. OSE definește regulile pentru gestionarea credențialelor de autentificare ale SIC.

---

[5] Atunci când acest lucru nu este fezabil, operatorul dezvoltă un set de măsuri de reducere a riscurilor și le descrie în dosarul de acreditare al SIC în cauză

[6] Atunci când acest lucru nu este fezabil, OSE dezvoltă un set de măsuri pentru protejarea confidențialității și integrității datelor, consolidând în același timp verificările și trasabilitatea operațiunilor de administrare menționate și le descrie în dosarul de acreditare al SIC în cauză.

[7] Atunci când acest lucru nu este fezabil din motive tehnice sau operaționale, operatorul dezvoltă un set de măsuri de trasabilitate și de reducere a riscurilor și le descrie în dosarul de acreditare al SIC în cauză

Ori de câte ori este necesar și, în cazurile în care acest lucru este fezabil, OSE trebuie să schimbe credențialele de autentificare. În mod particular, OSE trebuie să schimbe de la început credențialele implicite de autentificare instalate de producătorul / furnizorul unei resurse înainte ca aceasta să intre în funcțiune. Neglijarea acestui aspect reprezintă un risc ridicat pentru securitatea oricărei infrastructuri din care face parte o astfel de resursă sau cu care interacționează.

Drepturile de acces

Printre regulile definite în politica sa de securitate a sistemelor, OSE acordă drepturi de acces unui utilizator sau unui proces automat numai atunci când acel acces este strict necesar pentru ca utilizatorul să-și îndeplinească misiunea sau pentru ca procesul automat să își desfășoare operațiunile tehnice. Principiul *„need to know – need to do”* și *„least privileged”* trebuie aplicate in mod consistent.

OSE definește drepturile de acces la funcționalitățile multiple ale resursei și alocă aceste drepturi de acces strict utilizatorilor / proceselor automatizate in baza unor nevoi bine întemeiate. OSE examinează cel puțin o data pe an aceste drepturi de acces, identificând legăturile dintre conturi, drepturile de acces asociate și resursele sau funcționalitățile care sunt accesate cu aceste drepturi de acces și păstrează o listă actualizată a conturilor privilegiate (de exemplu, un cont de administrare). OSE verifică orice modificare potențială a unui cont privilegiat pentru a verifica dacă drepturile de acces la resurse și funcționalități sunt alocate pe baza celui mai mic privilegiu - „least privileged” (sunt acordate doar drepturile strict necesare) și sunt adecvate cu utilizarea contului.

Mentenanța securității IT

OSE dezvoltă și implementează o procedură de mentenanța a securității în conformitate cu PSSI. În acest scop, procedura definește condițiile care permit menținerea nivelului minim de securitate pentru resursele SIC. Procedura descrie politica privind instalarea oricărei versiuni noi sau măsură corectivă pentru o resursă desemnată Menționează, de asemenea, obligativitatea OSE-ului privind informarea cu privire la vulnerabilități și măsuri corective de securitate care privesc resursele SIC (hardware și software).

OSE instalează[8] și menține numai versiuni ale resurselor sale hardware și software SIC care sunt acceptate de furnizorii sau producătorii lor și actualizate din

[8] **În unele cazuri, atunci când se justifică din motive tehnice sau operaționale, OSE decide pentru anumite resurse să nu instaleze o versiune acceptată de furnizor sau producător. În aceste cazuri, OSE aplică procedura - conform politicii sale - pentru a reduce riscurile legate de utilizarea unei versiuni învechite și descrie în dosarul său de acreditare măsurile luate și motivele care au justificat neinstalarea versiunii acceptate**

punct de vedere al securității. OSE verifică originea și integritatea versiunii înainte de instalarea acesteia (conform termenelor definite în procedură) și analizează impactul tehnic și operațional al acestei versiuni asupra SIC în cauză.

OSE protejează accesul la SIC atunci când accesul se face prin rețele terțe. În acest caz, OSE protejează prin criptare și mecanisme de autentificare accesul la SIC, ţine evidenţa echipamentelor utilizate pentru accesarea SIC și, de asemenea, gestionează și configurează echipamentele menționate mai sus.

Sisteme de control industrial

Multe servicii esențiale funcționează prin sisteme de control industriale (SCI).Dacă este cazul, operatorul ia în considerare cerințele speciale de securitate pentru SCI. De exemplu, abordarea clasică a tehnologiei informației (care se concentrează pe transferul și accesul la informații) ar putea fi înlocuită cu o abordare tehnologică operațională (hardware-ul și software-ul sunt utilizate pentru a cauza sau detecta modificări într-un proces fizic).

Securitate fizică și a mediului de lucru

OSE previne accesul fizic neautorizat, deteriorarea și interferența cu informațiile organizației și locatiile in care se procesează informațiile.

1.4 Domeniul de securitate Apărare

Detectare

Operatorul instalează un sistem de detectare a incidentelor de securitate de tip „Teste/verificări de analiză pentru fișiere și protocoale”. Acest sistem analizează fluxurile de date care tranzitează aceste teste pentru a căuta evenimente care pot afecta securitatea SIC. Acestea sunt poziționate astfel încât să poată[9] analiza toate fluxurile schimbate între SIC și sistemele de informații ale terților.

Înregistrarea evenimentelor/Logare

OSE instalează un sistem de stocare pe fiecare SIC pentru a înregistra evenimente legate, cel puțin, de autentificarea utilizatorului, gestionarea conturilor și drepturile de acces, modificările regulilor de securitate și funcționarea SIC și care acoperă serverele de aplicații care acceptă activități critice, servere de infrastructură

[9] **Atunci când acest lucru nu este fezabil din motive tehnice, OSE descrie în dosarele de acreditare pentru SIC în cauză motivele tehnice care au împiedicat utilizarea testelor..**

de sistem, servere de infrastructură de rețea, echipamente de securitate, stații de inginerie și întreținere a sistemelor industriale, echipamente de rețea, stații de lucru administrative. OSE înregistrează prin sistemul de înregistrare evenimente cu marcarea orei și a datei utilizând surse de timp sincronizate și centralizează arhivele pentru cel puțin șase luni.

Corelarea și analiza jurnalelor

OSE creează un sistem de corelare și analiză a jurnalelor care cercetează evenimentele înregistrate de sistemul de jurnal instalat pe fiecare din echipamentele din SIC pentru a detecta evenimentele care afectează securitatea SIC. Sistemul de corelare și analiză a jurnalelor este instalat și operat de OSE (sau de furnizorul de servicii desemnat în acest sens) printr-un sistem de informații dedicat utilizat numai pentru detectarea evenimentelor care pot afecta securitatea sistemelor de informații.

Răspuns la incidente de securitate

OSE creează, actualizează şi pune în aplicare o procedură pentru gestionarea, răspunsul și analiza incidentelor care afectează funcționarea sau securitatea SIC, în conformitate cu PSSI.

OSE pune în aplicare un sistem informatic dedicat pentru gestionarea incidentelor, pentru a stoca, printre altele, înregistrările tehnice ale analizei incidentelor. OSE separă sistemul informatic dedicat pentru gestionarea incidentelor de SIC afectat de incident și stochează înregistrările tehnice aferente pentru o perioadă de cel puțin o șase luni. OSE ia în considerare, la proiectarea sistemului, nivelul de confidențialitate al documentelor stocate.

Raport incidente

OSE creează, actualizează și implementează proceduri pentru raportarea incidentelor.

Comunicarea cu autoritățile competente și CSIRT Naţional

OSE implementează un serviciu care îi permite să confirme primirea, fără întârzieri nejustificate, a informațiilor trimise de autoritatea sa națională competentă cu privire la incidente, vulnerabilități, amenințări și mapări relevante (inventar actualizat al SIC, interconectări ale SIC cu terțe rețele etc.). De asemenea, implementează o procedură pentru tratarea informațiilor primite și, după caz, pentru luarea măsurilor de securitate necesare pentru protejarea SIC. OSE furnizează autorității sale naționale competente detalii de contact actualizate (numele departamentului, numărul de telefon și adresa de e-mail) pentru acest serviciu. OSE

este încurajat să își conecteze sistemul de management al incidentelor cu alte Echipe de Răspuns la Incidente de Securitate Informatică (CSIRTs).

1.5 Domeniul de securitate Reziliență

Managementul continuității afacerii poate îmbrăca mai multe forme, depinzând de structura și scopurile organizației. Pentru organizațiile mai complexe este uzuală dezvoltarea unui Plan de Continuitate a Afacerii/Activității (în engleză, Business Continuity Plan) care, odată activat în situațiile de criză, să prevadă modalitatea practică de recuperare a afacerii, nu doar a sistemelor IT. Acest plan poate fi construit ca urmare a unei Analize de Impact (Business Impact Analysis) prin care se determină parametrii acceptabili pentru timpul de recuperare în caz de dezastru (Recovery Time Objective) și timpul dinaintea apariției dezastrului în care nu mai putem recupera datele pierdute (Recovery Point Objective).

Această abordare completă este descrisă în standarde dedicate precum:

- *Good Practice Guidelines,* emis de The Business Continuity Institute, sau
- *ISO 22301,* Business Continuity Management Systems

În legislația locală, la momentul publicării acestui ghid, precum și conform standardului ISO27001, în forma lui actuală, nu se prevede în mod expres obligativitatea implementării unui Plan de Continuitate a Afacerii în înțelesul larg, ci doar componentele acestora ce țin de securitatea informației. Ca atare, deși o abordare completă la nivelul organizației ar putea include un plan de continuitate a afacerii, ne vom rezuma în restul acestui ghid la a enumera recomandări cu privire la scopul strict al obligației OSE de a se conforma cerințelor curente. În cazul în care, însă, organizația deține un astfel de Plan de Continuitate a Afacerii, recomandăm actualizarea acestuia pentru a răspunde la cerințele de mai jos, și integrarea managementului continuității afacerii într-un astfel de plan disponibil la nivelul întregii organizații.

Managementul continuității afacerii

În conformitate cu politica de securitate a sistemelor informatice (**PSSI**), operatorul definește obiective si oferă suport strategic cu privire la managementul continuității afacerii in cazul unui incident de securitate.

Managementul recuperării in caz de dezastru

În conformitate cu politica de securitate a sistemelor informatice (**PSSI**), operatorul definește obiective si oferă suport strategic cu privire la managementul recuperării in cazul unui dezastru/ incident sever de securitate informatica.

Organizarea gestionarii crizelor

Operatorul definește in politica sa de securitate a sistemelor informatice (**PSSI**) organizarea gestionarii crizelor in cazul unui incident de securitate si continuitatea activităților organizației.

Procesul de gestionare al crizelor

Operatorul descrie in politica sa de securitate a sistemelor informatice (**PSSI**) procesul pentru managementul crizelor ce trebuie implementat de către organizație si care trebuie folosit in cazul unui incident sever de securitate, si pentru continuitatea activităților organizației.

1.6 Managementul riscurilor

1.6.1 Introducere

În timp au fost dezvoltate mai multe modele de cuantificare (calitativă sau cantitativă) a diferitelor tipuri de riscuri cărora trebuie să le facă față o organizație, de la simple la foarte complexe. Modelele calitative sunt cunoscute în literatura de specialitate ca fiind cele ce se bazează, mai ales, pe experiența personală. Modelele cantitative fac apel la formule matematice încercând să introducă mai multă rigoare.

Exista mai multe tipuri de risc cu impact diferit asupra organizației:

- **Riscul fizic** cuprinde defectarea echipamentelor precum şi condițiile nesatisfăcătoare ale mediului în care funcționează.
- **Riscul logic** provine din aplicarea greșită a anumitor proceduri, a unor instrucțiuni greșite (programare greșită, prelucrări necorespunzătoare) sau erori umane mai mult sau mai puțin intenționate.
- **Riscul economic** este cel legat de utilizarea echipamentelor informatice în viața organizației. Pentru OSE, calculatorul/infrastructura are un rol esențial și orice anomalie în funcționarea sa poate să aibă consecințe grave ducând până la întreruperea parțială sau totală a operării.

- **Riscul reputațional** provine din neîndeplinirea așteptărilor părților interesate și organizația este astfel percepută negativ.
- **Riscul de neconformitate** deși poate fi privit tot ca un risc economic vizează doar sancțiunile pe care o organizație le primește ca urmare a nerespectării obligațiilor legale și de reglementare.

Managementul riscurilor este definit ca *procesul prin care se identifică şi se controlează pierderile unei organizații.*

Primul element ce trebuie avut în vedere este identificarea tuturor elementelor din mediul sistemului informațional si reprezintă o inventariere a activelor ce se doresc a fi protejate: infrastructura rețelei, sistemul de operare, aplicațiile, informațiile procesate în sistem, dispozitive externe de stocare a informației.

Al doilea obiectiv este identificarea riscurilor asociate acestor active, aici putând fi incluse:

- pierderile financiare;
- pericole precum incendii, întreruperi în alimentarea cu energie electrică sau cataclisme naturale;
- frecvența și gravitatea erorilor (umane sau mecanice);
- furtul sau alterarea aplicațiilor sau a datelor/informațiilor procesate;
- probleme cauzate de incompetența managerială;
- istoricul incidentelor sau problemelor anterioare.

Odată identificate, riscurile trebuie evaluate în funcție de severitatea efectelor pe care le produc. Astfel se dezvolta o formula de calcul a impactului financiar pe care fiecare risc în parte îl are, precum și o determinare a costurilor implicate şi a probabilității de apariție a acestora (calcularea probabilității ratei de apariție a unei pierderi şi multiplicarea acesteia cu costul estimat al pierderii).

A treia etapă presupune selectarea unei metode adecvate prin care să poată fi eliminat sau măcar controlat efectul negativ pe care impactul fiecărui risc în parte îl are asupra organizației. Iată câteva exemple:

- *Eliminarea sau evitarea*. Cu excepția dezastrelor naturale, toate riscurile menționate anterior pot fi eliminate/evitate sau diminuate;
- *Transferul către altă organizație*. Acest lucru presupune apelarea la soluții de tip „outsourcing” sau „co-sourcing”;

- *Controale prin care să se diminueze frecvența sau gravitatea unui risc* (cu excepţia dezastrelor naturale);
- *Asigurarea.*

Metodele prin care pot fi eliminate sau reduse riscurile depind de circumstanțele particulare fiecărei organizații în parte.

Standardul ISO/IEC 31000 oferă un set de principii și orientări de gestionare a riscurilor pentru organizații. Pe de altă parte standardul ISO/IEC 27005 specifică orientări și procese pentru gestionarea riscului de securitate al sistemelor informaționale ale unei organizații, bazându-se în special pe cerințele unui sistem de management al securității informațiilor (SMSI) implementat în conformitate cu ISO/IEC 27001.

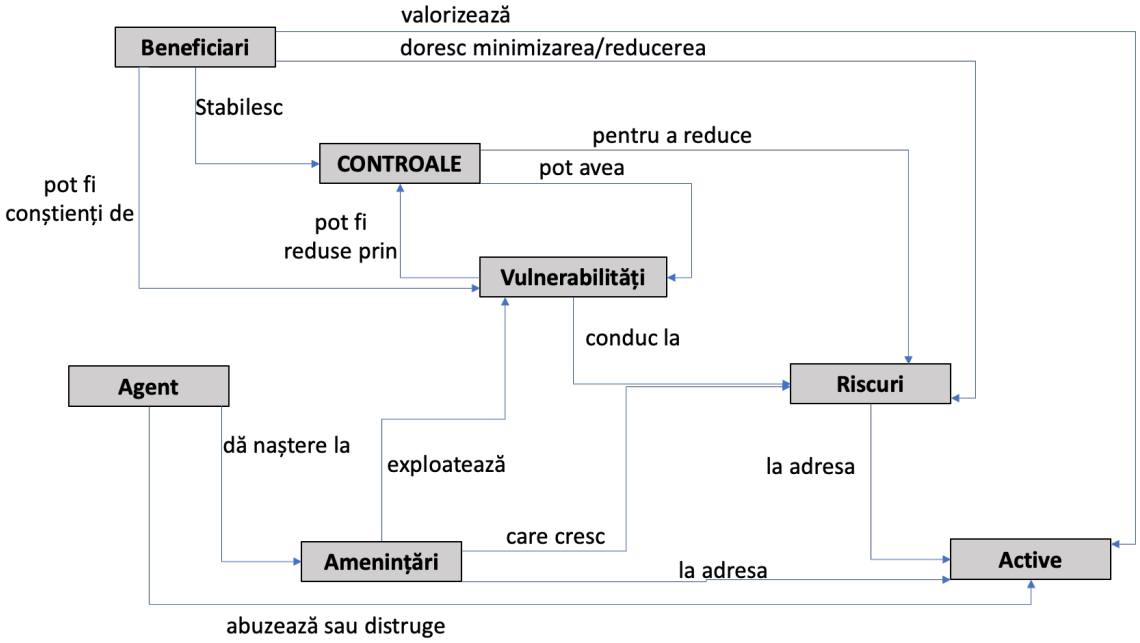
ISO/IEC 27005 nu oferă însă o metodologie specifică pentru gestionarea riscurilor de securitate a sistemelor informaționale. Este însă responsabilitatea organizației să definească abordarea sa față de gestionarea riscurilor.

1.6.2 Managementul riscurilor conform standardelor ISO

Asigurarea securității informațiilor are ca principala preocupare protejarea activelor organizației împotriva amenințărilor interne și externe, amenințări care sunt clasificate în funcție de potențialele daune pe care le pot provoca activelor protejate.

Figura de mai jos (denumită ”diagramă de context”), preluată și tradusă din ISO/IEC 27032[10], ilustrează relațiile dintre active, vulnerabilități și controale și clarifică înțelesul controalelor din Norme:

[10] ISO/IEC 27032 – Information Technology – Security techniques – Guidelines for Cybersecurity



Mai jos este un ghid orientativ, conform standardului ISO 27005[11] si Legea NIS al, managementul riscurilor la adresa securității informațiilor. Aceasta constă in următoarele etape:

1. Stabilirea contextului

Pentru aceasta prima etapa, este necesara parcurgerea următorilor pași:

- Definirea unei metodologii de gestionare a riscurilor adecvată realității OSE;
- Identificarea părților interesate interne și externe;
- Identificarea modelului de guvernanță care trebuie aplicat în gestionarea riscurilor și definirea unui proces de escaladare adecvat;
- Definirea rolurilor și responsabilităților pentru gestionarea riscurilor interne și externe și atribuirea resurselor umane corespunzătoare (De ex. manager de risc);
- Identificarea unui instrument software pentru a sprijini gestionarea și tratarea riscurilor;
- Definirea și identificarea înregistrărilor care trebuie create și întreținute (De ex. ARNISD, LIRIE, RERO etc), politicile, procesele și procedurile corespunzătoare;
- Identificarea criteriilor de evaluare a riscurilor pentru a evalua relevanța riscului în cadrul OSE;

[11] ISO/IEC 27005 - Information Technology - Security Techniques - Information security risk management

- Definirea nivelurilor de impact care ar trebui să sprijine gestionarea riscurilor (în funcție de daune, costuri sau criteriile CERT;
- Definirea criteriilor de acceptare a riscurilor (în funcție de factorii inerenți tehnologiilor, financiari, operaționali sau umani);
- Definirea sferei și limitelor sistemului de management al riscurilor.

2. Estimarea riscurilor

2.1 Identificarea riscurilor

Identificarea evenimentelor care pot provoca o posibilă pierdere pentru OSE:

- identificarea activelor (hardware, software, conectică de rețea. amplasamente fizice, resurse umane);
- identificarea amenințărilor;
- identificarea controalelor;
- identificarea amenințărilor;
- identificarea impactului.

2.2 Analiza riscurilor

În practică, analiza calitativă a riscurilor este cea mai bună metodă fiind utilizată ca o primă abordare pentru obținerea indicatorilor generali de nivel de risc și pentru identificarea celor mai relevante riscuri.

Metoda de analiză trebuie să fie în concordanță cu criteriile de evaluare a riscurilor definite în faza de stabilire a contextului (punctul 1 din tabel).

2.3 Evaluarea riscurilor

Criteriile de evaluare a riscurilor ar trebui să fie aliniate cu contextul extern și intern al managementului riscului de securitate a informațiilor.

3. Tratarea riscurilor

Tratarea riscurilor se definește ca identificarea controalelor care pot fi implementate pentru a atenua, evita, sau transfera riscul, precum și definirea unui plan de tratament pentru acestea. În baza planului de tratare a riscurilor se determină riscul rezidual (Acesta corespunde fazei de ”acceptare” a riscurilor).

4. Comunicare și consultare

Informațiile și deciziile legate de riscuri ar trebui să fie comunicate tuturor părților interesate relevante. OSE va elabora planuri de comunicare pentru a sprijini

procesul de gestionare a riscurilor.

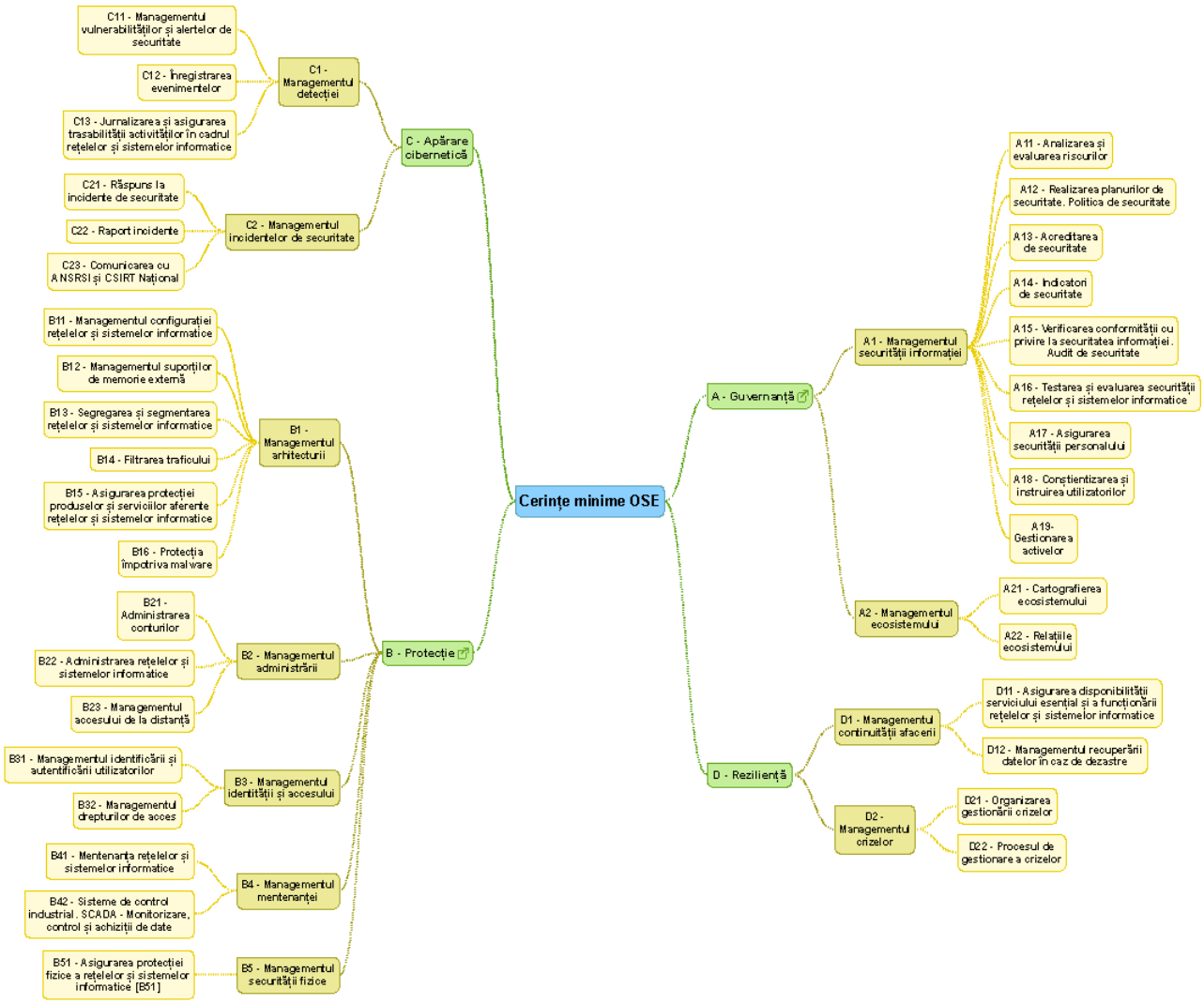
5. Monitorizare și revizuire riscuri

Riscurile și factorii care le afectează (de exemplu: valoarea activelor, impactul, vulnerabilitățile și probabilitatea unui eveniment) ar trebui să fie monitorizate și revizuite în mod regulat, astfel încât să se reflecte orice schimbare care a avut loc în contextul OSE și care ar fi putut duce la o modificare a riscului:

- au fost adăugate active noi
- modificări ale relevantei/ nivelului de importanta al activelor pentru OSE
- amenințări noi care pot fi active, atât în interiorul, cât și în afara organizației,
- posibilitatea exploatării de noi vulnerabilități prin amenințări;
- posibilă creștere a impactului, consecințelor amenințărilor, vulnerabilităților care, grupate, conduc la un nivel inacceptabil de risc;
- incidente de securitate a informațiilor care pot apărea.

CAPITOLUL 2: IMPLEMENTAREA CERINȚELOR MINIME DE SECURITATE

Pornind de la schema de mai jos ghidul prezintă exemple de implementare a cerințelor minime de securitate. Exemplele vizează atât implementarea tehnică (acolo unde este posibil) cît și implementarea administrativă (procedurală), inclusiv referințe la alte documente normative (standarde sau bune practici).



2.1 Domeniul de securitate : A - GUVERNANŢĂ

2.1.1 Categoria de activități de securitate: A 1 - Managementul securității informației

Note:

Activitățile de securitate din cadrul A1 trebuie privite în ansamblu, luând în considerare corelarea lor pentru o implementare eficientă și cronologică.

A19 (*Gestionarea activelor*) este esențială pentru a identifica activele utilizate de către OSE, precum si clasificarea acestora din perspectiva confidențialității, integrității, si disponibilității, în funcție de nevoile organizației. Acesta ar trebui sa fie primul pas realizat de către OSE.

Apoi, pasul următor ar trebui să fie realizarea analizei de risc (conform A11 – *Analiza si evaluarea riscurilor*). Odată identificate riscurile (nivelul acestora și modalitatea de tratare a riscului), politica de securitate (împreuna cu SMSI) poate fi creată și apoi implementata (A12 – *Realizarea planurilor de securitate*).

Desigur, pentru implementarea celor de mai sus este importantă implicarea personalului OSE, atât prin conștientizarea rolului acestora, cât și prin instruirea cu privire la (noi) tipuri de amenințări (A17 – *Asigurarea securității personalului* - si A18 – *Conștientizarea si instruirea utilizatorilor*).

Procesele si procedurile interne create, precum și implementarea acestora este verificată la nivel de management OSE (A13 – *Acreditarea de securitate*), prin audit (A15 – *Verificarea conformității cu privire la securitatea informației*) și prin testarea și evaluarea periodică (A16 – *Testarea si evaluarea securității rețelelor si sistemelor informatice*). Pentru aceste verificări sunt relevanți și indicatorii de securitate (A14 – *Indicatori de securitate*).

Notăm ca pentru efectuarea unei analize de risc eficiente se stabilește întâi metodologia de risc (A1.1.2.). Aceasta este ulterior aplicata in analiza ce se efectuează asupra fiecărui element din inventar (A 1.1.1) rezultatul obținut fiind registrul de riscuri (A 1.1.3.).

Măsura de securitate: A11 - Analizarea și evaluarea riscurilor

Nota:

Acest control este în relație strânsă cu controlul A19 referitor la inventarierea și gestionarea activelor, pasul prevăzut de A19 stând la baza acestui control (A11).

[A111]. Analiza riscurilor de securitate. *OSE efectuează și actualizează periodic o* ***analiză a riscurilor*** *de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale, identificând sistemele/echipamentele informatice critice care stau la baza furnizării serviciului esențial și principalele riscuri.*

Indicatori de control:

- **ARNIS** - analiza riscurilor de securitate a rețelelor și sistemelor informatice, document elaborat la nivelul OSE, prin care sunt identificate elementele critice care stau la baza furnizării serviciului esențial și sunt identificate principalele riscuri în vederea gestionării și diminuării acestora

Implementarea procesului/administrativă:

Crearea unui proces și a unei proceduri interne corespunzătoare procesului de evaluare a riscurilor de securitate cibernetică (nu este obligatoriu să fie denumită/etichetată ARNIS). Această analiză privind securitatea cibernetică poate fi de sine stătătoare sau poate fi inclusă în procedura privind analiza de risc realizată de către organizație pentru ansamblul sistemelor informatice pe care le deține. Procedura și procesul de mai sus trebuie revizuite periodic de către management pentru a asigura adecvarea continuă și eficacitatea abordării.

Procedura ar trebui să identifice etapele procesului de estimare și evaluare a riscurilor:

- modalitatea de identificare a riscului în legătură cu activele și procesele IT ale organizației.
- actualizarea scenariilor analizate în cadrul analizei de risc în funcție de noile tipologii de amenințări, precum și necesitatea actualizării măsurilor de securitate existente având în vedere riscul ca acestea să fie compromise.
- realizarea analizei de risc care să prezinte impactul și probabilitatea (care ajută la calcularea nivelului de risc) pentru fiecare risc identificat.
- modalitatea de creare și actualizare a registrului de risc (RERO) care va conține inclusiv informații detaliate privind fiecare risc identificat, alături de

impactul, probabilitatea, nivelul de risc, controalele implementate și în curs de implementare.

- Frecventa cu care pașii de mai sus vor fi repetați (cel puțin o dată pe an, precum și pentru orice activ IT sau proces de business nou/modificat în cadrul organizației).

Soluție tehnică:

Poate fi o soluție software de tip GRC - ”Governance risk and compliance” sau alte soluții software dedicate evaluării riscurilor. Pot fi folosite de asemenea machete Excel pentru automatizarea analizei și generarea registrului riscurilor.

Probe: *Procedura de identificare și evaluare a riscurilor*

Referințe:

ISO 27005, ISO31000, NIST 800-53: RA1

ISO 27001: A.8.1.1, A.12.6.1, A.18.2.1

NIST CSF: ID.GV-4, ID.RA-1, 3, 4, 5, 6, ID.RM-1, 2, 3, RS.IM-1, 2, ID.SC-1, 2, PR.IP 12, RC.IM-1, 2, ID.AM-1, 2, 4, 5, DE.CM-8, RS.MI-3, RS.AN-5

[A112]. Gestionarea riscurilor de securitate. *Pentru aplicarea procesului de analiză și evaluare a riscurilor, OSE stabilește o* ***metodologie*** *de gestionare a riscurilor furnizării serviciilor esențiale care va reflecta procesul de evaluare a riscurilor operatorului economic, criteriile de analiză, de acceptare și de reducere a riscurilor.*

Indicatori de control:

- **MEGRE** - metodologie de gestionare a riscurilor furnizării serviciilor esențiale, document prin care este prezentat procesul de evaluare a riscurilor operatorului economic, criteriile de analiză, de acceptare și de reducere a riscurilor

Implementarea procesului/administrativă:

Crearea unui proces si a unei proceduri (MEGRE) care să conțină următoarele aspecte:

- se va avea în vedere analiza de risc (ARNIS) realizată deja întrucât aceasta prezintă gravitatea și probabilitatea (care ajută la calcularea nivelului de risc) pentru fiecare risc identificat.

- selectarea unui răspuns la risc (cum ar fi: diminuarea frecvenței sau gravitatea unui risc, transferul, acceptarea riscului întrucât se regăsește în cadrul nivelul apetitului la risc al OSE, eliminarea sau evitarea prin nerealizarea activității care generează riscul), în funcție de apetitul de risc al organizației.
- descrierea controalelor care urmează a fi implementate.
- implementarea controalelor stabilite în urma analizei de risc și monitorizarea implementării acestora.
- monitorizarea implementării acestor controale și revizuirea periodică a eficacității acestora și a necesității îmbunătățirii/modificării acestora.

Procedura aceasta poate fi un document de sine stătător sau poate fi parte din procedura de analiză a riscurilor organizației.

Soluție tehnică:

Poate fi o soluție software de tip GRC - ”Governance risk and compliance” sau alte soluții software dedicate evaluării riscurilor. Pot fi folosite de asemenea machete Excel pentru automatizarea analizei și generarea registrului riscurilor

Probe: *Analiza riscurilor*

Referințe: *ISO 27005, ISO31000, NIST800-53: RA1, RA2*

[A113]. Evaluarea riscurilor de securitate. *Rezultatul evaluării riscurilor va fi documentat în* ***registrul de risc*** *organizațional.*

1. În procesul de evaluare a riscurilor, OSE va avea în vedere cel puțin:

- noile amenințări în domeniul securității cibernetice;

- punctele slabe descoperite recent;

- pierderea eficacității măsurilor de securitate;

- modificările situației de risc cauzate de modificările arhitecturii rețelelor și sistemelor informatice;

- orice alte modificări ale situației de risc.

Indicatori de control:

- **RERO** - registrul de risc organizațional

Implementarea procesului/administrativă:

Crearea și actualizarea registrului de risc (RERO) va conține inclusiv informații detaliate privind fiecare risc identificat, alături de impactul, probabilitatea, nivelul de risc, răspunsul la risc (masurile de control agreate si stadiul de implementare al

acestora, sau, după caz, orice decizie a managementului cu privire la modul de adresare a riscului).

Soluție tehnică

Poate fi o soluție software de tip GRC - ”Governance risk and compliance” sau alte soluții software dedicate evaluării riscurilor. Pot fi folosite de asemenea machete Excel pentru automatizarea analizei și generarea registrului riscurilor

Probe de audit: *registrul riscurilor (RERO)*

Referințe:

ISO 27002: A.18.2.1

NIST SP 800-53: CA-2, CA-7, CA-8, RA- 3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5

Măsura de securitate A12: Realizarea planurilor de securitate. Politica de securitate

[A121]. Politica de securitate. *Pornind de la ARNIS, OSE elaborează, menține și implementează* ***o politică de securitate a rețelelor și sistemelor informatice*** *care asigură furnizarea serviciilor esențiale și un sistem de management al securității informațiilor.*

1. PONIS stabilește obiectivele strategice de securitate, descrie guvernanța securității și reflectă toate politicile specifice de securitate ale SMSI (procesul de acreditare de securitate, audit de securitate, criptografie, întreținere securitate, manipulare incidente etc.).

Indicatori de control

- **PONIS -** politica de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale
- **SMSI -** sistemul de management al securității informației
- **RAIPOD -** raport privind implementarea politicii de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale și a documentelor de aplicare a acesteia

Implementarea procesului/administrativă:

Crearea și implementare unei politici la nivelul organizației, aprobată in prealabil de management (denumită PONIS in Normele tehnice, aprobate prin Ordinul nr. 1.323 din 9 noiembrie 2020, publicat în Monitorul Oficial, Partea I, nr. 1142

din 26 noiembrie 2020) care stabilește abordarea organizației cu privire la managementul obiectivelor de securitate a informației în cadrul organizației.

Politica va conține definiția securității informației si obiectivele și principiile referitoare la securitatea informațiilor. Această politică trebuie să aibă în vedere legislația aplicabilă, contractele încheiate de către organizație, precum și liniile generale pentru procedurile relevante din punctul de vedere al securității informației ce trebuie adoptate și menținute de către organizație, în zonele descrise în acest ghid și care includ în principiu următoarele (așa cum sunt descrise în legislație): gestionarea accesului la informații, procesul de acreditare, realizarea auditului intern și extern, realizarea periodica de teste de penetrare si de scanare a rețelei pentru detecția vulnerabilităților , configurarea dispozitivelor mobile, criptarea datelor în tranzit și stocate, anonimizarea datelor, ștergerea datelor, realizarea configurărilor, testarea securității aplicațiilor utilizate de către organizație.

Având în vedere analizele de risc de la A11 și conținutul acestei politici de la A12, se va implementa un sistem de management al securității informației (SMSI). SMSI va include cadrul de proceduri și procese privind securitatea informației (in care se vor reflecta principiile generale în acest domeniu). SMSI va cuprinde un proces ciclic: planifică, implementează, verifică, îmbunătățește, asigurând prin ciclicitate îmbunătățirea continuă a proceselor privind securitatea informației. SMSI asigură astfel guvernanța ecosistemului privind securitatea informației.

Soluție tehnică:

Crearea si publicarea documentelor în intranetul OSE sau într-un sistem de management documente, accesibile angajaților.

Probe: politica de securitate și documentarea care descriere implementarea sistemului de securitate implementat (astfel cum este ea creată în cadrul organizației: proceduri, procese, etc)

***[A122]. Implementarea politicii de securitate**. OSE întocmește în beneficiul managementului său, cel puțin anual, un raport privind implementarea PONIS și a documentelor de aplicare a acesteia.*

Raportul specifică inventarul riscurilor, nivelul securității rețelelor și sistemelor informatice și acțiunile de securitate planificate și realizate.

Implementarea procesului/administrativă:

Toți pașii luați în privința securității informației trebuie documentați. Această documentație poate fi preluată din documentația creată la momentul implementării procedurilor interne privind securitatea informației și a controalelor. De exemplu, se pot avea în vedere mapa pregătită pentru acreditare (descrisă în A13), ARNIS, precum și orice alte modalități de documentare a acestor activități. Din punct de vedere legislativ, această documentație este identificată drept RAIPOD, un raport care specifică inventarul riscurilor (preluat din RERO), nivelul securității rețelelor și sistemelor informatice și acțiunile de securitate planificate și realizate.

Soluție tehnică

Publicarea documentelor în intranetul OSE sau într-un sistem de management documente, accesibile angajaților .

Probe: raportul privind implementarea PONIS și documente aferente care reflectă această implementare.

Referințe:

ISO 27002: A5.1.1

NIST 800-53: ID.GV-1, 2, 3, 4, ID.BE-1, 2 3, 4, PR.AT-2, 3, 4, 5, DE.DP-1, ID.AM-6

Măsura de securitate A13: Acreditarea de securitate

***[A131]. Acreditarea rețelelor și sistemelor informatice.** În baza ARNIS și în conformitate cu **procesul de acreditare** stabilit în PONIS, OSE acreditează rețelele și sistemele informatice, inclusiv componentele de administrare.*

Acreditarea de securitate este o decizie formală luată de managementul de nivel înalt al OSE prin care se certifică procesul de identificare a riscurilor care afectează securitatea și modul de implementare a măsurilor necesare pentru protejare și are valabilitate de cel mult un an. Decizia certifică, de asemenea, faptul că orice risc rezidual a fost identificat și acceptat la nivel managerial.

Decizia de acreditare de securitate are la bază mapa de acreditare de securitate care cuprinde următoarele documente/mijloace:

- analiză riscuri și obiective de securitate;

- proceduri și măsuri de securitate aplicate;

- rapoarte de audit de securitate;

- rapoarte de evaluare a conformității;

- riscuri reziduale și motive care justifică acceptarea acestora.

Indicatori de control:

- **PEANIS -** procesul de acreditare stabilit în PONIS prin care OSE acreditează NIS utilizate în furnizarea serviciilor esențiale, inclusiv componentele de administrare
- **DANIS -** decizia de acreditare; decizie formală luată de managementul de nivel înalt al OSE
- **MANIS -** mapa de acreditare de securitate; document în baza căruia se emite DANIS

Implementarea procesului/administrativă:

Acest control presupune un proces de analiză (denumit PEANIS) din partea managementului cu privire la riscurile identificate în procesul de analiză de risc (așa cum este descris la A1.1.) alături de alte surse de informații menționate mai jos, precum și o decizie (denumită DANIS) cu privire la modalitatea de răspuns la riscurile identificate (conform procedurii descrise la A1.1.).

Analiza realizată de management va include informații din mai multe surse (care vor constitui MANIS), inclusiv:

- analize interne ale departamentelor relevante privind securitatea informației, inclusiv rapoarte interne de audit și rapoarte de conformitate cu cerințele legale aferente și procedurilor interne relevante cu privire la:
  - analiză riscuri și obiective de securitate;
  - proceduri și măsuri de securitate aplicate;
  - rapoarte de audit de securitate;
  - rapoarte de evaluare a conformității;

- riscuri reziduale și motive care justifică acceptarea acestora.

- rapoarte de audit extern

Soluție tehnică: informațiile puse la dispoziție pentru acreditare pot fi incluse într-o aplicație relevantă de GRC (Governance, risk, compliance).

Probe: documentația pregătită pentru evaluarea de către management în vederea acreditării (analize interne, documentarea implementării procedurilor, etc), procesul și procedură de acreditare, decizia de acreditare

[A132]. Revizuirea validării acreditării de securitate*. Anual și ori de câte ori se identifică un eveniment/proces de dezvoltare care modifică contextul descris în procesul de acreditare sau de fiecare dată când se modifică în mod semnificativ configurația rețelelor și sistemelor informatice sau a aplicațiilor, OSE va revizui validarea acreditării de securitate. OSE are obligația reînnoirii aprobării imediat ce nu mai este valabilă.*

Implementarea procesului/administrativă:

Ciclicitatea pentru acest control poate fi stabilită în concordanță cu ciclicitatea de la A11(cel mult un an), precum și la apariția unor procese de business noi sau modificarea unor procese de business existente. La momentul revizuirii va fi actualizată întreaga documentație aferentă aspectelor noi/modificate, inclusiv dosarul pregătit pentru acreditare.

Soluție tehnică:

Informațiile puse la dispoziție pentru acreditare pot fi incluse într-o aplicație relevantă de GRC (Governance, risk, compliance).

Probe: *proces și procedură stabilită pentru revizuirea periodică a acreditării (aceasta procedură poate fi parte din PONIS)*

Referințe:

ISO 27002: A.12.1.1, A.12.7.1

NIST 800-53: ID.RA-1, 3, 4, 6, ID.RM-1, 2, 3, ID.SC -1, RS.IM-1, 2, PR.IP-7, 12, PR.PT-1, DE.CM-8, RS.MI-3

Măsura de securitate A14: Indicatori de securitate

[A141]. Indicatori de securitate. *OSE stabilește o serie de indicatori de evaluare, pe baza cărora își evaluează conformitatea cu PONIS.*

Indicatorii de securitate se pot referi la: performanțele gestionării riscurilor; menținerea resurselor în condiții sigure; drepturile de acces ale utilizatorilor; autentificarea accesului la resurse; administrarea resurselor.

Indicatori de control:

- **IEC -** indicatori de evaluare, pe baza cărora OSE își evaluează conformitatea cu PONIS
- **MEIEC -** metoda de evaluare a indicatorilor de conformitate

Implementarea procesului/administrativă:

Indicatorii de securitate (IEC) și metoda de evaluare (MEIEC) trebuie creați de către organizație pentru fiecare măsură de securitate din legislație/ aspect relevant din procedurile interne în parte. Exemple de astfel de indicatori și metode de evaluare se regăsesc în acest ghid în Capitolul 3. În acest context, PONIS, deși este politica generală privind securitatea informațiilor, implicit se referă la toate procedurile interne care adresează controalele din acest ghid.

Indicatorii trebuie creați pentru a putea fi calculați în baza informațiilor pe care OSE le are/le poate obține și trebuie să fie relevanți pentru acțiunile/elementele care trebuie măsurate, în funcție de specificul OSE și al acțiunii ce trebuie realizată pentru asigurarea securității conform cerințelor legale.

Soluție tehnică:

Indicatorii de securitate și evaluarea acestora poate fi inclusă într-un sistem electronic, în special pentru generarea rapoartelor și graficelor privind statusul indicatorilor.

Probe: Documentarea IEC

[A142]. Metode de evaluare a securității. *OSE specifică pentru fiecare indicator metoda de evaluare folosită și, dacă este cazul, marja de incertitudine în evaluarea sa.*

Dacă un indicator se schimbă semnificativ în comparație cu evaluarea anterioară, operatorul identifică și specifică motivele.

Implementarea procesului/administrativă:

Pentru fiecare IEC se va documenta și metoda de evaluare (MEIEC). Exemple de astfel de metode de evaluare pentru indicatori se regăsesc în acest ghid în Capitolul 3.

Soluție tehnică: Neaplicabil

Probe: documentarea MEIEC

Referințe:

ISO 27002: A.12.1.3

NIST 800-5: ID.AM-5, ID.RM-2, 3, PR.IP-7,8, PR.DS-4, ID.BE-5

Măsura de securitate A15: Verificarea conformității cu privire la securitatea informației. Audit de securitate

[A151]. Evaluarea conformității. *În baza ARNIS, OSE stabilește și actualizează periodic* ***procedura privind evaluarea conformității SNIS*** *și efectuarea* ***auditului de securitate*** *a rețelelor și sistemelor informatice.*

Activitatea se efectuează anual la nivelul OSE de către structura de securitate sau de o echipă complexă stabilită de managementul de cel mai înalt nivel. Ea se finalizează cu un raport de evaluare a conformității.

Indicatori de control:

- **PRECAS -** procedură privind evaluarea conformității NIS și efectuarea auditului de securitate a rețelelor și sistemelor informatice
- **RAEC -** raport de evaluare a conformității
- **RASNIS -** raport de audit de securitate a rețelelor și sistemelor informatice

Implementarea procesului/administrativă:

Cerința face referire la o procedură cu privire la evaluarea internă de către organizație a conformității NIS, cu o frecventa anuala. Această procedură se poate

regăsi sub numele de PRECAS sau poate fi inclusă în PONIS sau în alte proceduri interne, în funcție de organizarea internă a OSE. Astfel, spre deosebite de PEANIS, care descrie acreditarea de către managementul OSE a modului de implementare PONIS în cadrul OSE, PRECAS analizează conformitatea OSE cu cerințele NIS. Pentru aceasta se pot utiliza indicatorii stabiliți de către organizație conform A14.

De asemenea, procedura trebuie să includă și detalii privind realizarea auditului de către un auditor extern (și atestat) cel puțin o dată la 2 ani.

Evaluarea trebuie să presupună o metodologie de evaluare corespunzătoare pentru a identifica îndeplinirea cerințelor legale. În principiu, nu ar trebui să se limiteze doar la analiza indicatorilor de securitate menționați la A14.

Ca abordare, organizația poate avea ca punct de pornire o lista detaliată a cerințelor legale și maparea cu procedurile, procesele și controalele interne implementate, precum și un tabel cu indicatorii de control din legislație și modul în care au fost implementați în cadrul organizației. De asemenea, poate fi utilă mapa pregătită pentru acreditare.

În urma realizării activității de evaluare a conformității NIS de către departamentele menționate în cadrul PRECAS va rezulta raportul de evaluare a conformității, denumit RAEC.

Soluție tehnică: Procesul de evaluare internă poate fi inclus într-o aplicație GRC (Governance, risk and compliance).

Probe: Procedura privind evaluarea internă a conformității NIS; rapoartele de evaluare a conformității NIS, împreună cu documentația care a stat la baza acestei evaluări

[A152]. Auditul de securitate. OSE *va efectua* ***audit de securitate****, cel puțin o dată la 2 ani, și are ca rezultat un* ***raport de audit de securitate*** *a rețelelor și sistemelor informatice.*

Auditul se efectuează numai de auditori de securitate informatică pentru auditarea rețelelor și sistemelor informatice, atestați de ANSRSI și cu atestat valabil la data finalizării RASNIS.

RASNIS va cuprinde auditarea cerințelor minime specificate la [A16].

Implementarea procesului/administrativă:

Procedurile interne ale organizației (denumite în legislație PRECAS) includ detalii precum momentul realizării auditului, rolurile și responsabilitățile din cadrul OSE referitor la audit, modalitatea de furnizare informații/documente către auditori.

Auditorul va aplica standardele de audit relevante conform legislației și practicilor în domeniu, iar rezultatul auditului este un raport de audit (denumit în legislație RASNIS).

Soluție tehnică: *Neaplicabil*

Probe: rapoartele externe de audit de securitate

Referințe:

ISO 27002: A.5.1.2, A.12.7.1, A.18.2.

NIST 800-5: ID.GV-3, 4, ID.RA-1, 3, 4, 5, 6, ID.RM-1, 2, 3, DE.CM-8, DE.DP-5, ID.SC-4, PR.AC-1, PR.PT-1, PR.IP-7, 12, RS.IM-1, 2, RC.IM-1, 2

Măsura de securitate A16: Testarea și evaluarea securității rețelelor și sistemelor informatice

[A161]. Testare și evaluare securitate. *Procesul de testare și evaluare va implica verificarea sistemelor operaționale pe baza unei planificări atente astfel încât riscul întreruperii furnizării serviciului esențial să fie minim și se finalizează cu un raport de testare și evaluare a securității rețelelor și sistemelor informatice.*

Testarea și evaluarea rețelelor și sistemelor informatice presupun identificarea și prevenirea vulnerabilităților software și hardware, respectiv:

- testarea securității aplicațiilor;

- testarea securității infrastructurii rețelelor și sistemelor informatice.

Testarea și evaluarea securității rețelelor și sistemelor informatice vor fi efectuate numai de personal specializat, atestat de către ANSRSI.

Rezultatele analizelor tehnice cu privire la compromiterea securității efectuate pe parcursul auditărilor pot fi prezentate numai persoanelor care au nevoie de aceste informații pentru a-și îndeplini atribuțiile ce le revin.

Indicatori de control:

- **RATES -** raport de testare și evaluare a securității rețelelor și sistemelor informatice
- **ATECNIS -** analiză tehnică cu privire la compromiterea securității rețelelor și sistemelor informatice
- **RASNIS -** raport de audit de securitate a rețelelor și sistemelor informatice

Implementarea procesului/administrativă:

Testarea și evaluarea securității va avea în vedere două domenii:

- aplicațiile;
- infrastructura rețelelor și sistemelor informatice

Aceasta presupune o analiză tehnică care poate fi realizată doar de un evaluator atestat în acest sens. Pentru a realiza testarea, trebuie realizat un plan de testare, luând în considerare aplicațiile și infrastructura, împreună cu specificul acesteia. Planul poate fi gândit împreună cu evaluatorul pentru a identifica scenariile ce vor fi testate și stabilirea priorităților de testare în funcție de sensibilitatea procesului și/sau activului IT. De asemenea, trebuie să se aibă în vedere limitarea afectării serviciilor OSE pe perioada evaluării. Testarea trebuie realizată periodic, cel puțin anual.

În urma testării vor fi pregătite trei documente: RATES (raport de testare și evaluare a securității rețelelor și sistemelor informatice), ATECNIS (analiză tehnică cu privire la compromiterea securității rețelelor și sistemelor informatice) și RASNIS (raportul de audit menționat la A14).

Riscurile identificate în urma testării și evaluării vor fi tratate conform oricăror riscuri în timpul procesului de gestionare a riscului, urmând să fie identificat un răspuns la risc, și, dacă este necesar, controale relevante pentru reducerea riscului. Acestea vor fi aprobate de către management conform A13.

Soluție tehnică: Neaplicabil

Probe: Raport de testare și evaluare a securității rețelelor și sistemelor informatice, analiză tehnică cu privire la compromiterea securității rețelelor și sistemelor informatice, raport de audit de securitate a rețelelor și sistemelor informatice

Măsura de securitate A17: Asigurarea securității personalului

[A171]. Asigurarea securității personalului. *OSE elaborează un program de asigurare a securității personalului prin care identifică obiective și stabilește cerințe de securitate pentru fiecare etapă a relației avute de către angajați.*

PGASP se materializează prin: fișa postului (FP); contract individual de muncă (CIM); contract colectiv de muncă (CCM).

Indicatori de control:

- **PGASP** - program de asigurare a securității personalului; document prin care OSE identifică obiective și stabilește cerințe de securitate pentru fiecare etapă a relației avute de către angajați
- **COSE** - contractele de servicii sau furnizare servicii externe
- **FP** - fișa postului;
- **CIM** - contract individual de muncă
- **CCM** - contract colectiv de muncă.

Implementarea procesului/administrativă:

Un program de asigurare a securității personalului (PGASP) va avea în vedere rolul fiecărui tip de angajat, în funcție de activitatea prestată (și în special tipul de acces la date/active IT). Acest program presupune stabilirea rolului si responsabilităților personalului (de exemplu, în cadrul unor proceduri interne, așa cum este detaliat mai jos), precum și instruirea personalului în legătură cu acestea. De asemenea, PGASP trebuie corelat cu conținutul și acțiunile din SMSI.

OSE va stabili rolul și responsabilitatea angajaților în cadrul activităților de securitate a informației. Procedurile interne ale OSE în această privință pot include, fără a se limita la, aspecte precum următoarele:

- procesul de acordare a drepturilor de acces la informații care trebuie sa conțină cel puțin următoarele: aprobare pentru creare de utilizatori noi si a drepturilor de acces ale utilizatorului, , drepturi acordate conform informațiilor la care urmează să aibă acces utilizatorul conform fisei postului, durata accesului(mai ales atunci când utilizatorul este din afara organizației).
- Arhitectura sistemului cat si modul de implementare a procesului vor asigura limitarea accesului la informație doar pentru angajații care au nevoie de acest acces pentru desfășurarea activităților conform fișei postului si in baza regulilor de acces aprobate

- identificarea și raportarea incidentelor;
- clasificarea informațiilor conform procedurii interne a organizației și gestionarea informației conform acestei clasificări;
- răspunderea și consecințele în cazul nerespectării responsabilităților privind securitatea informației;
- asigurarea realizării evaluărilor necesare din punct de vedere a securității informației;
- asigurarea implementării controalelor aprobate ca răspuns la risc pentru procesul de business aferent activității respectivului angajat;
- păstrarea confidențialității informațiilor de autentificare și nedivulgarea acestora altor persoane.
- angajatul va modifica detaliile de autentificare atunci când suspectează că au fost compromise, precum și la un interval de timp prestabilit.;
- crearea unui proces în care sunt separate sarcinile și domeniile de responsabilitate care pot intra în conflict astfel încât să se reducă posibilitățile de accesare neautorizată, modificare neautorizată sau neintenționată, indisponibilitatea informației;
- alocarea persoanei (e.g. departament/angajat) responsabilă pentru fiecare activ IT, precum și pentru procesele pentru securitatea informației;
- stabilirea și documentarea coordonării relației cu furnizorii din perspectiva securității informației, precum și monitorizarea acestor furnizori

Aceste aspecte pot fi aduse la cunoștința angajaților, în cadrul fișei postului (FP), contractului individual de muncă (CIM), contractului colectiv de muncă (CCM, dacă este cazul). CIM va conține din punct de vedere juridic și clauze de confidențialitate, în sensul păstrării confidențialității de către angajat. Documentul în care se menționează aceste aspecte și modalitatea în care acestea sunt aduse la cunoștința angajaților și devin obligatorii pentru aceștia se realizează în conformitate cu legislația în domeniul dreptului muncii.

O abordare practică, în funcție de organizarea OSE și legislația muncii poate presupune includerea aspectelor menționate mai sus în proceduri interne ale OSE (care sunt aduse la cunoștința angajaților și persoanelor care au acces la date), urmând ca CIM/CCM/FP/regulamentul de ordine interioară să conțină referințe la aceste proceduri și obligații privind respectarea procedurilor.

Soluție tehnică: neaplicabil

Probe: în funcție de organizarea internă a OSE, fișa postului (FP); contract individual de muncă (CIM); contract colectiv de muncă (CCM), alte documente care conțin

rolurile și responsabilitățile (e.g. proceduri, regulament de ordine interioară), documentarea instruirii personalului, documentația privind implementarea PGASP.

[A172]. Verificarea înțelegerii responsabilităților. *OSE se asigură că angajații înțeleg responsabilitățile și sunt potriviți pentru rolurile stabilite, iar contractanții și furnizorii își asumă și angajează întreaga responsabilitate.*

Materializat prin: instructaje de securitate pentru angajați (ISA); verificări privind cunoștințele de securitate ale angajaților (VCSA).

În contractele de servicii sau furnizare servicii externe, OSE se asigură că au fost prevăzute clauze privind asigurarea securității personalului.

Indicatori de control:

- **VCSA** – Verificări privind cunoștințele de securitate ale angajaților
- **ISA** – Instructaje de securitate pentru angajați;

Implementarea procesului/administrativă:

În cadrul contractelor cu furnizori externi, organizația se asigură că există clauze privind un nivel corespunzător al securității informației (confidențialitate, integritate, disponibilitate) de către angajații furnizorului pentru activitatea prestată de aceștia (e.g. găzduirea de date ale organizației, accesarea prin VPN a unor date ale organizației).

Periodic (cel puțin o dată pe an) se va realiza un instructaj al angajaților privind aceste responsabilități și roluri (ISA), urmat de o verificare a înțelegerii acestora (VCSA). Acestea vor fi documentate, pentru a putea demonstra data la care au avut loc, persoanele care au participat, materialul prezentat, testarea cunoștințelor care a avut loc.

Soluție tehnică: Aceste instruiri pot fi realizate online, prin intermediul unei aplicații specifice în acest sens.

Probe: instructajul angajaților(ISA) și verificarea înțelegerii acestora(VCSA), contractele cu furnizorii externi.

Referințe:

ISO 27002: A.6.1.1

NIST 800-5: ID.AM-6, ID.GV-2, 3, RS.CO-1, PR.IP-7, 11, DE.DP-1, PR.AT-1, 2, 3, 4, 5

Măsura de securitate A18: Conștientizarea și instruirea utilizatorilor

Nota:

Acțiunile de conștientizare pot fi realizate în practică pentru A17 și A17.

[A181]. Instrumente de conștientizare. *OSE pune la dispoziția angajaților instrumente necesare pentru conștientizarea și educarea acestora cu privire la tipurile de amenințări de securitate informatică și măsurile de protecție corespunzătoare.*

Indicatori de control:

- **INCEA -** instrumente necesare pentru conștientizarea și educarea angajaților cu privire la tipurile de amenințări de securitate informatică și măsurile de protecție corespunzătoare în vederea limitării incidentelor

Implementarea procesului/administrativă:

Elementele menționate la A1.7. se referă preponderent la cunoașterea regulilor interne ale organizației privind securitatea informației și rolul angajaților pentru asigurarea acesteia.

Astfel, A1.8. pune accent mai mult pe zona de prezentare a unor tipuri de amenințări de securitate informatică și modalitatea de protecție aferentă (INCEA). Această prezentare poate fi realizată în mod interactiv, prin prezentarea de către un formator intern sau extern sau printr-un curs online. Există prezentări predefinite create de către firme dedicate în acest sens sau poate fi creată o prezentare dedicată conform specificului organizației sau, dupa caz, al departamentului.

Prezentarea trebuie să aibă o periodicitate, în funcție de mai multe criterii (e.g. numărul de angajați noi pe lună, elemente noi în tipologia de atac, identificarea unor noi vulnerabilități).

Conținutul prezentării, momentul când aceasta este efectuată și prezența angajaților trebuie documentate.

Soluție tehnică: Aceste instruiri pot fi realizate și online, prin intermediul unei aplicații specifice în acest sens.

Probe: instrumente (e.g. platforma online de instruire, comunicările către personal) necesare pentru conștientizarea și educarea angajaților cu privire la tipurile de amenințări de securitate informatică și măsurile de protecție corespunzătoare în vederea limitării incidentelor. De asemenea, sunt relevante aspectele incluse în programul menționat la A182.

[A182]. Instruirea și prezentarea securității. *OSE instituie un program de prezentare a securității pentru tot personalul, precum și un program de instruire în domeniul securității pentru angajații care utilizează rețelele și sisteme informatice.*

Indicatori de control:

- **PRASA -** program de prezentare a securității pentru tot personalul
- **PRISA -** program de instruire în domeniul securității pentru angajații care utilizează rețelele și sistemele informatice care stau la baza furnizării serviciilor esențiale

Implementarea procesului/administrativă:

Pentru toți angajații trebuie realizat un program de prezentare a securității (PRASA).

Pentru angajații implicați în utilizarea rețelele și sistemele informatice care stau la baza furnizării serviciilor esențiale trebuie realizate instruiri specifice în funcție de modalitatea de utilizare a acestora – e.g. utilizator, administrator (PRISA).

Periodicitatea și documentarea trebuie realizate conform celor detaliate la A1.8.1.

Soluție tehnică: Aceste instruiri pot fi realizate si online, prin intermediul unei aplicații specifice în acest sens.

Probe: program de prezentare a securității pentru tot personalul, program de instruire în domeniul securității pentru angajații care utilizează rețelele și sistemele informatice care stau la baza furnizării serviciilor esențiale, documentarea instruirii și evaluărilor.

Referințe:

ISO 27002: A.6.1.1, A.6.1.2, A.7, A.9.3.

NIST 800-5: ID.AM-6, ID.GV-2, 3, RS.CO-1, PR.IP-7, 11, DE.DP-1, PR.AT-1, 2, 3, 4, 5

Măsura de securitate A19: Gestionarea activelor

[A19.1.] Inventarierea și gestionarea activelor. *OSE stabilește un cadru adecvat pentru identificarea, clasificarea și implementarea unui inventar al proceselor IT, sistemelor și elementelor componente ale rețelelor și sistemelor informatice. În baza gestionării activelor, OSE lansează actualizări și patch-uri și, după caz, stabilește ce elemente din componența rețelelor și sistemelor informatice sunt afectate de noi probleme de securitate.*

1. Pentru identificarea amenințărilor, vulnerabilităților și riscurilor sunt identificate activele, sistemele și procesele organizației, care se materializează printr-o ***listă****.*

2. OSE elaborează o ***procedură*** *pentru etichetarea și clasificarea datelor și informațiilor pentru a reflecta sensibilitatea acestora și, în consecință, se asigură că aceasta este respectată, iar datele/informațiile sunt gestionate corespunzător..*

Indicatori de control:

- **LASPO** - lista activelor, sistemelor şi proceselor organizației
- **PRECDI** - procedură privind etichetarea și clasificarea datelor și informațiilor

Implementarea procesului/administrativă:

OSE trebuie să identifice resursele relevante din ciclul de viață al informației și să documenteze sensibilitatea lor. Se recomandă ca Ciclul de viață al informației va include cel puțin crearea, prelucrarea, stocarea, transmiterea, ștergerea și distrugerea acesteia. Documentația aferentă pentru cerințele legale din A19. trebuie păstrată în inventare dedicate (create specific pentru A191) sau existente deja (create anterior conform procedurilor interne ale organizației), după caz.

Acest inventar trebuie să reflecte situația curenta, sa fie actualizat frecvent, consistent și corelat cu alte inventare.

Pentru fiecare din resursele identificate, se recomandă alocarea unui proprietar al resursei din punct de vedere business și unul din punct de vedere tehnic.

Procesul de creare si menținere a unui inventar care să conțină procesele IT, sistemele și elementele componente ale rețelelor și sistemelor informatice trebuie formalizat într-o procedura. LASPO trebuie sa conțină cel puțin următoarele elemente:

- detalii pentru identificarea echipamentului/sistemului informatic – precum serie (sau identificator din contabilitate, alt tip de identificator intern), denumire, versiune software/OS;
- detalii privind responsabilul de business și cel tehnic aferent – precum nume, departament, număr de telefon, adresă de email (se vor include si cazurile in care responsabilii sunt furnizori externi care oferă servicii de mentenanță, în cazul externalizării complete a unei/ acestei activități).
- Detalii de amplasament al echipamentului/sistemului informatic – precum IP, MAC, server unde rulează aplicația;
- furnizori relevanți pentru funcționarea și mentenanța echipamentului/sistemului informatic;
- clasificarea din punct de vedere a sensibilității, conform celor detaliate mai jos;
- tipul de analize de securitate realizate de-a lungul timpului asupra echipamentului/sistemului informatic – precum teste de penetrare, analize de risc;

Procesul de clasificare a documentelor/informațiilor conform sensibilității acestora (fie manual, fie automat) trebuie descris formal într-o procedura (PRECDI). Această clasificare determină accesul persoanelor din cadrul organizației sau din afara acesteia la documente/informații. De obicei, această sensibilitate poate fi calculată în funcție de trei arii: nivelul de confidențialitate al informațiilor din sistemul informatic/ document/ proces, nivelul de integritate al acestor informații și nivelul de disponibilitate a informațiilor necesar departamentelor care utilizează aceste informații. Nivelurile pentru fiecare dintre aceste trei arii pot fi stabilite de OSE în cadrul procedurii, urmând ca departamentele care utilizează informațiile, împreună cu persoanele din zona tehnică aferente acestora să identifice in detaliu sensibilitatea informațiilor.

Procesul de identificare a vulnerabilităților si procesul de remediere, denumit si managementul vulnerabilităților,) poate fi automatizat parțial sau total, în cazul în care este posibil, pentru asigurarea unei rezoluții într-un timp rezonabil, precum și pentru acuratețea în identificarea și aplicarea acestora. Rezoluția poate fi: aplicarea cu succes patch-ului, actualizarea sistemului software afectat, înlocuirea sistemului cu unul care nu este vulnerabil, instituirea unei excepții pe o perioada determinata aprobata de management in baza unei analize de risc si a documentarii necesității.

Soluție tehnică:

- implementarea unei soluții de scanare care sa aiba baza de date actualizata cu cele mai recente vulnerabilități;
- implementarea unui mecanism de gestionare a patch-urilor: identificarea patch-urilor necesare, aplicarea acestora și menținerea evidenței patch-urilor de aplicat/aplicate (manual sau automatizat);
- implementarea măsurilor necesare pentru remedierea vulnerabilităților identificate în procesul de identificare a vulnerabilităților;
- utilizarea unor soluții IT care să permită clasificarea electronică a documentelor/ informațiilor conform PRECDI, dacă este oportun;
- instrument/ soluție software pentru managementul activelor/ asset management/ procese IT – asset inventory. Poate fi de sine stătătoare sau, pentru anumite aspecte, poate fi componenta unei soluții de tip ”service management” cu CMDB la bază. Pentru o organizație cu mai puțin de o sută de active un astfel de inventar realizat în Word sau Excel poate fi aplicat în practică.

Probe:

- lista activelor, sistemelor și proceselor organizației;
- procedura privind identificarea vulnerabilităților (inclusiv patch-urilor necesare) și modalitatea de remediere a acestora;
- procedură privind etichetarea și clasificarea datelor și informațiilor.

Referințe:

ISO 27002: A.8.1.1, A.12.6.1, A.18.2.1, 8.2

2.1.2 Categoria de activități de securitate: A 2 - Managementul ecosistemului

Măsura de securitate: A21 - Cartografierea ecosistemului

Note:

Procesul de cartografiere se va concretiza sub forma unui document (nu trebuie să fie obligatoriu etichetat SICAE, denumire conform Normelor Tehnice) în care vor fi prezentate schemele/ diagramele de flux însoțite de descrieri succinte ale părților implicate: interne și externe.

Pe baza cartografierii se vor identifica riscurile asociate relațiilor cu părțile implicate ale ecosistemului (denumita in Normele tehnice LIRIE). LIRIE poate fi inclusă în analiza globală a riscurilor (denumita in Normele tehnice ARNIS).

Pentru OSE care dețin certificarea ISO 27001, această cartografiere poate fi asimilată cu secțiunea Contextul Organizației a standardului ISO 27001:2018.

[A211]. Descrierea ecosistemului. *OSE stabilește o cartografiere a ecosistemului, inclusiv a părților implicate interne și externe, incluzând, dar fără a se limita la furnizori, în special a celor care au acces sau gestionează activele critice ale operatorului.*

*Cartografierea ecosistemului este materializată printr-***o situație cartografică a ecosistemului***.*

Scopul cartografierii este identificarea și evaluarea riscurilor potențiale reprezentate de relațiile cu părțile din ecosistem. Acestea sunt documentate printr-o listă a riscurilor potențiale identificate care conține evaluarea efectului acestora asupra furnizării serviciilor esențiale.

Pentru elaborarea LIRIE, OSE va avea în vedere 4 parametri majori:

*- **maturitatea**. Care sunt capacitățile tehnice ale părților interesate cu privire la securitatea cibernetică?*

*- **încrederea**. Pot presupune că intențiile părților interesate față de mine sunt fiabile?*

*- **nivelul de acces**. Care sunt drepturile de acces ale părților interesate la rețelele și sistemele informatice?*

*- **dependența**. În ce măsură relația cu părțile interesate este critică pentru activitatea mea?*

Indicatori de control:

- **SICAE** - situația cartografică a ecosistemului; document prin care se realizează stabilirea și identificarea ecosistemului care stă la baza furnizării serviciului esențial atât NIS, cât și alte componente. De asemenea include, dar fără a se limita la acestea, părți implicate, interne și externe, și furnizori, în special cei cu acces la NIS sau la gestionarea activelor esențiale ale operatorului economic.

  LIRIE - lista riscurilor potențiale identificate și evaluarea acestora în furnizarea serviciilor esențiale. Riscurile sunt reprezentate de relațiile cu părțile interesate ale ecosistemului

Implementarea procesului/administrativă:

OSE va elabora un document care va conține elementele următoare:

- Scurta descriere a organizației (departamentele OSE, serviciile oferite, locațiile fizice unde organizația își desfășoară activitatea, si a alte elemente de identificare relevante). Vor fi descrișii succint și factorii aferenți contextului extern ce afectează organizația (cerințe legale sau de reglementare; cerințe de securitate cibernetică specifice părților interesate etc). Dependențele și funcțiile critice care ajută/sprijină furnizarea serviciului esențial pot fi reprezentate vizual/grafic.
- Înțelegerea nevoilor si așteptărilor părților implicate:
  - Identificarea si definirea părților implicate: clienți, angajați, furnizori, acționari, management;
  - Identificarea nevoilor si așteptărilor părților implicate identificate.
- Determinarea scopului implementării NIS:
  - Poziția OSE la nivel sectorial si din punct de vedere al infrastructurilor critice;
  - Angajații, procesele și tehnologia folosite de către OSE pentru a dezvolta, menține, opera, întreține si monitoriza serviciile esențiale oferite;
  - Entitățile OSE supuse NIS (daca sunt produse/servicii esențiale multiple);
  - Locațiile (adrese fizice) OSE supuse NIS;
  - Cartografierea elementelor de comunicații la nivelul organizației precum si fluxurile de date.

Lista riscurilor potențiale identificate (denumita in Normele tehnice LIRIE) va conține următoarele elemente :

- riscurile potențiale sau pericolele asociate cu operațiunile și produsele furnizorilor respectiv părților interesate și impactul potențial al acestora asupra OSE;
- riscurile potențiale care includ, dar nu se limitează la, acuratețea și fiabilitatea informațiilor operaționale și financiare, încălcări ale securității, eficacitatea operațiunilor și conformitatea legală și de reglementare.

Implementare tehnică: Se vor folosi instrumente software adecvate pentru reprezentarea vizuala a ecosistemului.

Probe:

Documentul reprezentând situația cartografica a sistemului/ SICAE,

Lista riscurilor potențiale identificate aplicabile exclusiv serviciilor critice/ LIRIE (in cazul in care acestea nu sunt deja incluse in ARNIS)**,**

Analiza riscurilor organizației ARNIS daca aceasta cuprinde si evaluarea furnizorilor.

Referințe:

ISO 27001:4.1 ,4.2 4.3, 5.2, 8.1

NIST CSF: ID.AM-3, ID.AM-4, ID.AM-6, ID.BE-1, ID.BE-2, ID.BE-4

Măsura de securitate: A 22 – Relațiile Ecosistemului

Note:

Interconexiunile dintre SIC și terți pot fi documentate (si) la A21. OSE implementează o procedură de verificare a furnizorilor respectiv a terților privind cerințele de securitate impuse de către OSE (nu este obligatoriu ca documentul sa fie etichetat PROSRE, conform denumirii din Normele Tehnice). Evidenta acordurilor la nivel de serviciu și/ sau mecanisme de audit (denumita in Normele tehnice LASMA), poate fi inclusă in procedura de mai sus.

[A221]. Stabilirea relațiilor ecosistemului. *OSE elaborează și implementează o* ***procedură de stabilire a relațiilor ecosistemului****, care include interconexiunile (relațiile externe) între rețelele și sisteme informatice și terți.*

În general, cerințele de securitate trebuie luate în considerare pentru componentele rețelelor și sistemelor informatice operate de terți.

Indicatori de control:

- **PROSRE** - procedură de stabilire a relațiilor ecosistemului; documentul include interconexiunile (relațiile externe) între rețelele și sistemele informatice și terți

Implementarea procesului/administrativă:

Se va implementa procedura care va conține elementele următoare :

- interfețele dintre sistemele informatice și terți,
- cerințele de securitate pentru componentele sistemelor informatice operate de terți.

Prin intermediul acestei proceduri OSE va verifica că:

- Contractele cu furnizorii și partenerii terți sunt utilizate pentru a implementa măsuri adecvate concepute pentru a îndeplini obiectivele programului de securitate cibernetică al OSE și a planului de gestionare a riscului în lanțul de aprovizionare;
- Exista un nivel optim de coordonare cu părțile interesate si ca se desfășoară în concordanță cu planurile de răspuns la incidente de securitate;
- Schimbul voluntar de informații are loc cu părțile implicate externe pentru a realiza o conștientizare situațională mai largă a securității cibernetice;
- Furnizorii și partenerii terți sunt evaluați periodic, prin mecanisme de audit (fie efectuat de OSE, intern sau cu ajutorul unui terț, fie rezultatele unor astfel de teste sunt puse la dispoziție de către furnizori conform unor obligații contractuale) sau alte forme de evaluare, pentru a confirma că își îndeplinesc obligațiile contractuale.
- Relațiile publice sunt gestionate în coordonare cu furnizorii, subcontractorii si partenerii terți.

Implementare tehnică: Crearea si publicarea documentelor în intranetul OSE sau într-un sistem de management de documente, accesibile angajaților in conformitate cu nivelul de autoritate si responsabilitate al acestora.

Probe: *PROSRE*

Referințe

ISO 27001: 4.2, 5.2, 7.4, 7.5, 8.1, 9.3 , A.5.1.1 , A.7.1.2, A.7.2, A.7.3, A.12.7, A.13.2, A.14.2.7, A.15, A.18.1.1

NIST CSF: RS.CO-4, RS.CO-5, ID.RM-1, ID.GV-2, ID.SC-1, ID.SC-5, RC.CO-3

[A222]. Acorduri la nivel de serviciu. *OSE se asigură, prin acorduri la nivel de serviciu și/ sau mecanisme de audit, că furnizorii săi stabilesc, de asemenea, măsuri de securitate adecvate. În acest sens elaborează și păstrează o listă cu acorduri la nivel de serviciu și/ sau mecanisme de audit.*

Indicatori de control:

- **LASMA** - listă cu acorduri la nivel de serviciu și/ sau mecanisme de audit a rețelelor și sistemelor informatice.

Implementarea procesului/administrativă:

Se va crea o lista care va conține elementele următoare :

- Acordurile la nivel de serviciu cu furnizorii și partenerii terți utilizate pentru a asigura măsuri adecvate concepute pentru a îndeplini obiectivele programului de securitate cibernetică al OSE și a planului de gestionare a riscului în lanțul de aprovizionare cibernetică;
- Mecanismele OSE de audit a rețelelor și sistemelor informatice ale furnizorilor și partenerilor terți utilizate pentru a asigura măsuri adecvate concepute pentru a îndeplini obiectivele programului de securitate cibernetică al OSE și a planului de gestionare a riscului în lanțul de aprovizionare cibernetică.

Pentru fiecare se vor detalia cel puțin următoarele: data la care aceste acorduri respectiv mecanisme au fost semnate, perioada de valabilitate a acestora, data ultimei revizuiri. Acordurile si mecanismele de audit vor fi revizuite la o perioada stabilita de către OSE (cel puțin o dată la doi ani) sau ori de cate ori este necesar (de exemplu atunci când survin modificări ale organizației, in relațiilor cu furnizorii, al contextului de securitate cibernetic, etc.)

Implementarea tehnică:

Dacă se folosește o soluție de tip ”IT service management” (ITSM), aceste informați vor fi documentate în secțiunea aferentă SLA (Service level agreement). Altfel, documentarea poate fi făcută prin intermediul unei liste care sa conțină elementele descris mai sus.

Probe: listă cu acorduri la nivel de serviciu și/ sau mecanisme de audit a rețelelor și sistemelor informatice/ LASMA (sau vizualizare listă în ITSM)

Referințe:

ISO 27001: A.14.2.7, A.15, A.18.1.1

NIST CSF: ID.RM-1, ID.GV-2, ID.SC-2, ID.SC-3, ID.SC-4

2.3 Domeniul de securitate : B - PROTECŢIE

2.3.1 Categoria de activități de securitate: B 1 - Managementul arhitecturii

Măsura de securitate: B11 - Managementul configurației rețelelor și sistemelor informatice

[B111]. Arhitectura NIS*. OSE elaborează și actualizează permanent o schemă a arhitecturii rețelelor și sistemelor informatice*

Indicatori de control:

- **SANIS -** schema arhitecturii rețelelor și sistemelor informatice folosite pentru furnizarea serviciilor esențiale
- **MANIS** - mapa de acreditare de securitate; document în baza căruia se emite DANIS
- **ARNIS -** analiza riscurilor de securitate a rețelelor și sistemelor informatice, document elaborat la nivelul OSE, prin care sunt identificate elementele critice care stau la baza furnizării serviciului esențial și sunt identificate principalele riscuri în vederea gestionării și diminuării acestora

Implementarea procesului/administrativă:

Schema arhitecturii rețelelor si sistemelor informatice care asigura furnizarea serviciilor esențiale (SANIS) poate sa includă diagramele arhitecturale de nivel 2 si 3 corespunzătoare Modelului OSI (interconectarea sistemelor deschise/ Open Systems Interconnections). De asemenea poate sa includă aspecte legate de conectivitate, operaționale și de comunicații ale sistemelor, informații despre componentele sistemului, topologia rețelei și plasarea logică a componentelor în arhitectura sistemului. Componentele sistemului informatic care asigură furnizarea serviciilor esențiale se regăsesc la A19, Inventarierea si gestionarea activelor.

Arhitectura unei rețele mai mari și mai complexe ar putea împărți rețeaua într-un număr de domenii de rețea logice, cu fiecare domeniu reprezentând diferite niveluri de încredere (de exemplu, acces la desktop, finanțe, marketing, etc), fiecare protejat de un perimetru de securitate logic definit.

Domeniile și relațiile lor trebuie documentate în mod specific, atât pe harta de rețea, cât și într-o lista care identifică resursele și sistemele din rețea și domeniile în care sunt incluse. Diferite părți ale unui singur sistem (de exemplu, un sistem ERP) ar putea fi în domenii diferite; acest lucru poate fi securizat dacă arhitectura de securitate păstrează diferitele părți separat logic.

Soluție tehnică

Poate fi utilizata orice aplicație software pentru desenarea schemei arhitecturii rețelelor si sistemelor informatice precum si orice aplicație software pentru controlul instalării software-ului în sistemele operaționale (software-ul aplicațiilor sau al sistemului de operare).

Probe: Schema arhitecturii rețelelor și sistemelor informatice/ SANIS

Referințe: NIST PR.IP-1

*[B112]. **Instalarea echipamentelor și serviciilor**. OSE instalează numai servicii și funcționalități sau conectează echipamente care sunt esențiale pentru funcționarea și securitatea rețelelor și sistemelor informatice. Evidența serviciilor, funcționalităților și echipamentelor este evidențiată în ARNIS.*

1. Dacă componentele suplimentare sunt inevitabile (de exemplu, din motive economice), acestea trebuie evaluate în funcție de analiza riscurilor. Va fi materializat în MANIS.

2. ARNIS va fi actualizată permanent în funcție de componentele suplimentare implementate la nivelul securității rețelelor și sistemelor informatice.

3. Elementele componente ale rețelelor și sistemelor informatice trebuie utilizate numai atunci când este nevoie și cu măsuri de securitate adecvate.

Indicatori de control:

- **MANIS -** mapa de acreditare de securitate;
- **ARNIS -** analiza riscurilor de securitate a rețelelor și sistemelor informatice, document elaborat la nivelul OSE, prin care sunt identificate elementele critice

care stau la baza furnizării serviciului esențial și sunt identificate principalele riscuri în vederea gestionării și diminuării acestora.

Implementarea procesului/administrativă:

Instalarea unor servicii si funcționalități sau conectarea unor echipamente noi se face doar după o analiza prealabila si a confirmării ca acestea sunt esențiale pentru funcționarea și securitatea rețelelor și sistemelor informatice. Această analiza este evidențiată in ARNIS, document descris in secțiunea A11, ce conține analiza riscurilor de securitate a rețelelor și sistemelor informatice.

Daca in urma analizei necesității componentelor noi (nevoia de instalare a acestora apare in urma unui proiect nou sau pentru înlocuirea/ upgrade-ul unora deja existente) se constata ca acestea sunt inevitabile (de exemplu, din motive economice) si este necesara implementarea lor in cadrul rețelelor și sistemelor informatice, acestea vor fi evaluate in funcție de analiza riscurilor de securitate, actualizându-se analiza riscurilor de securitate a rețelelor și sistemelor informatice (ARNIS). Modificările trebuie reflectate si in mapa de acreditare de securitate (MANIS, evidențiata in cadrul secțiunea A13).

Utilizarea elementelor componente ale rețelelor și sistemelor informatice se face numai atunci când este nevoie și numai după implementarea unor măsuri de securitate adecvate.

Soluție tehnică

Stocarea dovezilor care atesta efectuarea analizei in cadrul sistemului de management al documentelor al organizației

Probe de audit:

Politica și / sau procedura de configurare a sistemelor

Tabelele de configurare ale sistemelor

Programul și planul periodic de revizuire a configurației sistemelor

Exerciții / teste anterioare documentate ale sistemelor de informații critice existente

Programare și plan de revizuire a configurației de securitate

Referințe:

ISO 27002: A.12.1, 12.5.1, A.12.5

NIST PR.IP-1,2,3

Măsura de securitate: B12 - Managementul suporților de memorie externă

***[B121]. Suporți de memorie externă**. OSE va adopta o procedură privind utilizarea suporților de memorie externă. Aceasta va cuprinde modul de utilizare, principii și măsuri de securitate atât pentru dispozitive mobile, cât și pentru suporți de memorie externă.*

1. Suporții de scris amovibili conectați la rețelele și sistemele informatice sunt utilizate exclusiv pentru operațiuni legate de furnizarea serviciului esențial și/sau funcționarea rețelelor și sistemelor informatice, inclusiv pentru întreținerea, administrarea și asigurarea securității rețelelor și sistemelor informatice.

2. La NIS vor fi conectați numai suporți amovibili înregistrați, în registre de evidență a suporților de memorie externă, fiind monitorizat accesul în rețelele și sistemele informatice.

Indicatori de control:

- **PRUSME -** procedură privind utilizarea suporților de memorie externă
- **RESME -** registre de evidență a suporților de memorie externă

Implementarea procesului/administrativă:

Pentru a preveni divulgarea, modificarea sau ștergerea neautorizată a informațiilor stocate pe suporți de memorie externa sau pe alte dispozitive mobile, OSE implementează o procedura privind utilizarea suporți de memorie externă (denumita PRUSME in Normele tehnice) în conformitate cu schema de clasificare adoptată de OSE si care cuprinde modul de utilizare (de exemplu: criptarea datelor in cazul in care confidențialitatea și integritatea sunt considerate importante, ștergerea (nerecuperabila) in cazul reutilizării dispozitivului, limitarea timpului de utilizare a dispozitivelor pentru evitarea riscului de degradarea acestuia), principii si masuri de securitate pentru dispozitive mobile și pentru suporți de memorie externă.

Procedura trebuie dezvoltata și implementata pentru a se asigura că suporții de memorie externă sunt utilizate, întreținute și transportate într-un mod sigur și controlat, pe baza clasificării informațiilor stocate pe aceste dispozitive.

Acești suporți de memorie externa, conectate la rețelele și sistemele informatice sunt utilizate exclusiv pentru operațiuni legate de furnizarea serviciului esențial și/ sau funcționarea rețelelor și sistemelor informatice, inclusiv pentru

întreținerea, administrarea și asigurarea securității rețelelor și sistemelor informatice. Accesul acestor dispozitive in rețele și sistemele informatice trebuie monitorizat.

OSE elaborează si menține actualizate registre de evidență a suporților de memorie externă (denumita RESME in Normele tehnice) in care se vor înregistra toți suporții externe/ amovibile.

Soluție tehnică

Se poate implementa o soluție software dedicata sau se poate folosi o soluție software existenta (de exemplu o soluție de securitate la nivel endpoint) prin care se poate face managementul suporților de memorie externă, fiind acceptate pentru conectarea la rețelele și sistemele informatice doar echipamentele (device-urile) înregistrate.

Probe:

Procedura privind utilizarea suporților de memorie externă documentata incluzând descrierea procesului, a rolurilor si responsabilităților precum si a tipuri de echipamente (device-uri) care sunt subiectul procedurii împreuna cu obiectivele acesteia/ PRUSME

Registrele de evidență a suporților de memorie externă actualizate la zi/ RESME

Referințe: ISO 27002 - A.8.3.1

Măsura de securitate: B13 - Segregarea și segmentarea rețelelor și sistemelor informatice

[B131]. Segregarea și segmentarea*. În vederea limitării propagării incidentelor de securitate cibernetică, OSE aplică o procedură privind segregarea și segmentarea NIS.*

1. OSE separă fizic sau logic rețelele și sistemele informatice de alte sisteme informatice proprii sau de la terți. În cazul în care rețelele și sistemele informatice sunt compuse din subsisteme, OSE le separă din punct de vedere fizic sau logic.

2. OSE stabilește și pune în aplicare măsuri de securitate adecvate pentru interconectări ale rețelelor și sistemelor informatice.

Indicatori de control:

- **PROSES -** procedură privind segregarea și segmentarea rețelelor și sistemelor informatice utilizate pentru furnizarea serviciilor esențiale
- **SANIS -** schema arhitecturii rețelelor și sistemelor informatice folosite la furnizarea serviciilor esențiale

Implementarea procesului/administrativă:

Se va crea o procedura privind segregarea și segmentarea rețelelor și sistemelor informatice utilizate pentru furnizarea serviciilor esențiale (denumita in Normele tehnice PROSES) si va include detalii despre:

- separarea fizică sau logică a rețelelor și sistemelor informatice utilizate pentru furnizarea serviciilor esențiale de alte sisteme informatice proprii sau de la terți; daca rețelele și sistemele informatice sunt compuse din subsisteme, acestea sunt separate la fel din punct de vedere fizic sau logic;
- punerea in aplicare a unor măsuri de securitate adecvate pentru interconectări ale rețelelor și sistemelor informatice;

Securitatea poate fi mai ușor de gestionat dacă rețeaua este împărțită în domenii fizice si/sau logice.

Schema arhitecturii rețelelor si sistemelor informatice care asigură furnizarea serviciilor (denumita in norme SANIS) (așa cum apare la B11), stă la baza deciziilor privind implementarea măsurilor de securitate adecvate pentru interconectarea acestor rețele in vederea respectării cerințelor de separare a rețelelor și sistemelor informatice utilizate pentru furnizarea serviciilor **es**ențiale de alte sisteme informatice proprii.

Soluție tehnică

Implementarea segmentării și segregării rețelei poate fi realizată folosind o serie de tehnici și tehnologii, incluzând: implementarea zonelor (demilitarised zones) și gateway-urilor între rețele cu cerințe de securitate diferite (domenii de securitate) utilizând tehnologii pe diferite niveluri: segmentarea rețelei in mai multe subrețele, rețele virtuale si protocoale de routere incluzând VLAN-uri si routere virtuale, mașini virtuale, firewall-uri de rețea si dispozitive de securitate pentru filtrarea traficului etc.

Probe:

Existenta unei proceduri privind segregarea și segmentarea rețelelor și sistemelor informatice utilizate pentru furnizarea serviciilor esențiale/ PROSES

Documentații despre cum este implementata separarea sistemului SIC de celelalte sisteme existente/ SANIS

Referințe:

ISO 27002 - A.12.1.4, A.13.1

Măsura de securitate: B14 - Filtrarea traficului

[B141]. Filtrarea fluxurilor*. OSE definește, implementează și actualizează permanent procedura privind filtrarea traficului, prin care stabilește reguli de filtrare a traficului (pe baza adresei de rețea, după numărul portului, pe bază de protocoale de comunicații etc.) pentru restrângea fluxurilor de trafic.*

1. OSE interzice fluxurile de trafic care nu sunt necesare pentru funcționarea rețelelor și sistemelor informatice și care ar putea facilita un atac cibernetic.

2. OSE filtrează fluxurile de intrare, cele existente și fluxurile între subsistemele rețelelor și sistemelor informatice la nivelul interconectării lor, limitând astfel fluxurile numai la cele strict necesare funcționării și asigurării securității rețelelor și sistemelor informatice.

Indicatori de control:

- **PROFIT -** procedură privind filtrarea traficului
- **ARNIS -** analiza riscurilor de securitate a rețelelor și sistemelor informatice, document elaborat la nivelul OSE, prin care sunt identificate elementele critice care stau la baza furnizării serviciului esențial și principalele riscuri în vederea gestionării și diminuării acestora

Implementarea procesului/administrativă:

Se va dezvolta o procedură privind filtrarea traficului (denumita in Normele tehnice PROFIT), care este actualizată permanent si care stabilește reguli de filtrare a traficului (pe baza adresei de rețea, după numărul portului, pe bază de protocoale de comunicații etc.) pentru restrângea fluxurilor de trafic.

OSE interzice traficul de comunicații în rețea în mod implicit și permite traficul de comunicații în rețea prin excepție (deny all, permit by exception). Această cerință se aplică traficului de comunicații de rețea de intrare și de ieșire între subsistemele rețelelor și sistemelor informatice la nivelul interconectării lor. Regulile de filtrare a traficului de comunicații în rețea permit blocarea tuturor conexiunilor si permisiunile prin excepție si astfel asigură faptul că sunt permise numai acele conexiuni esențiale și aprobate pentru funcționarea sigură a rețelelor și sistemelor informatice.

Aceste filtrări ale traficului de comunicații se pot face cu un sistem de tip firewall configurat in așa fel încât filtrarea sa fie făcută si in conformitate cu ARNIS (analiza a riscurilor făcută pentru fiecare subsistem al rețelelor și sistemelor informatice) si pentru a bloca accesul neautorizat în conformitate cu politica de control acces.

Soluție tehnică

Un sistem de tip firewall necesar monitorizării si filtrării transmisiilor de date existente la nivelul rețelelor și sistemelor informatice

Probe:

Rapoartele de monitorizare a rețelelor critice și ale SIC

Politica documentată pentru procedurile de monitorizare, inclusiv cerințele minime de monitorizare/ Procedurile de monitorizare a traficului/ PROFIT

Dovada existentei instrumentelor de monitorizare a SIC

Referințe:

NIST PR.PT-4, PR.AC-3, 5, ISO 27002 - A.13.1, A.13.2.1

Măsura de securitate: B15 - Asigurarea protecției produselor și serviciilor aferente rețelelor și sistemelor informatice

[B151]. Asigurarea protecției criptografice. *Pentru a asigura confidențialitatea, integritatea și autenticitatea datelor procesate, stocate sau tranzitate prin rețelele și sistemele informatice, OSE va stabili, implementa și menține o procedură pentru asigurarea protecției criptografice pentru informații și resurse.*

1. Măsurile criptografice se aplică în toate etapele ciclului de viață a informației și au ca obiect de aplicare aplicațiile, sistemele informatice, echipamentele de rețea și canalele de comunicare.

Indicatori de control:

- **PRAPC -** procedură pentru asigurarea protecției criptografice pentru informații și resurse

Implementarea procesului/administrativă:

OSE dezvolta si implementa o procedură privind utilizarea controalelor criptografice pentru protecția informațiilor si resurselor (denumita in Normele tehnice PRAPC), fie stocate, fie transmise, atât in cadrul sistemelor OSE cat si in comunicațiile cu terții.

Evaluarea a riscurilor pregătită anterior trebuie să stabilească nivelul necesar de protecție a informațiilor, să determine cerințele privind confidențialitatea, integritatea, autenticitatea și non-repudierea și cele mai potrivite soluții criptografice ce trebuie implementate pe întreg ciclul de viață al informației și care au ca obiect de aplicare aplicațiile, sistemele informatice, echipamentele de rețea și canalele de comunicare.

Procedura trebuie sa includă si o descriere a abordării managementului cu privire la utilizarea mijloacelor de control criptografice și principiile generale în baza cărora informațiile ar trebui protejate.

Soluție tehnică

Stocarea documentelor care dovedesc existenta politicii si implementării PRAPC in cadrul sistemului de management al documentelor

Probe:

Procedura privind utilizarea controalelor criptografice pentru protecția informațiilor si resurselor implementata si actualizata/ PRAPC

Exista procese criptografice adecvate

Referințe:

ISO 27002 - A.10.1, A.18.1.5

[B152]. Managementul cheilor de criptare. *OSE va avea în vedere utilizarea, protejarea și gestionarea cheilor criptografice de-a lungul întregului ciclu de viață a acestora.*

Indicatori de control:

- **MACC -** managementul cheilor de criptare; proces prin care se asigură producerea, utilizarea și evidența materialului criptografic, inclusiv cheile de criptare

Implementarea procesului/administrativă:

OSE va asigura un management al cheilor de criptare (de numita in Normele tehnice MACC), care sa facă referire la utilizarea, protecția și durata de viață a acestora, pe întregul lor ciclu de viață.

Procedura pentru asigurarea protecției criptografice pentru informații și resurse (denumita in Normele tehnice PRAPC) va include cerințe pentru managementul cheilor de criptare pe întregul lor ciclu de viață, inclusiv generarea, stocarea, arhivarea, recuperarea, distribuirea, retragerea şi distrugerea cheilor

Soluție tehnică

Sistem software de gestionare a cheilor de criptare sau stocarea documentelor care dovedesc existenta sistemului de management al cheilor de criptare MACC in cadrul sistemului de management al documentelor

Probe:

Sunt prevăzute măsuri de protecție pentru a proteja secretul cheilor (private) secrete

Referințe:

ISO 27002 - A.10.1, A.18.1.5

Măsura de securitate: B16 - Protecția împotriva malware

[B161]. Protecție malware*. OSE va stabili măsuri de protecție malware și va implementa mijloace de control pentru detecția, prevenirea și recuperarea informației în scopul protecției împotriva atacurilor malware.*

1. În acest sens va elabora și implementa o procedură pentru asigurarea protecției malware, în conformitate cu PONIS.

2. Echipamentele hardware, sistemele de operare, aplicațiile software și subsistemele rețelelor și sistemelor informatice trebuie configurate și protejate corespunzător atât împotriva atacurilor fizice, cât și logice

Indicatori de control:

- **PRAPMA -** procedură pentru asigurarea protecției malware

Implementarea procesului/administrativă:

OSE elaborează si implementează o procedură pentru asigurarea protecției împotriva malware-ului care va stabili mijloacele de control de detectare, prevenire și recuperare, pentru protecția împotriva malware-ului, atât la nivelul aplicațiilor hardware, sistemelor de operare, aplicațiilor software cat si a subsistemelor rețelelor și sistemelor informatice.

OSE va defini o politică de comunicare către angajați prin care utilizarea oricărui software neautorizat este interzisă.

OSE va instala o aplicație software de detectare a programelor malware pentru a preveni și bloca programele malware si o va menține actualizata la zi pentru a putea detecta cele mai recente amenințări malware.

Pentru prevenirea accesului fizic la sistemele informatice, se poate tine cont de procedura privind accesul și securitatea resurselor și informațiilor de la măsura de securitate B51 si, de asemenea, se poate tine cont de procedura elaborata la B12 care prevede, printre altele, blocarea automata a suporturilor de memorie externa neînregistrate.

Responsabilii OSE vor planifica și efectua revizii periodice ale sistemelor pentru a verifica dacă există fișiere/ software neautorizate sau interzise, ceea ce ar putea reprezenta o amenințare malware si vor planifica sesiuni regulate de instruire pentru angajați, astfel încât să poată preveni atacurile malware.

Soluție tehnică

Instalarea unui aplicații software anti-malware, centralizat si la nivel endpoint.

Probe:

Existența si implementarea procedurii pentru asigurarea protecției malware

Sunt prevăzute măsuri de protecție pentru a proteja împotriva malware-ului (software-ul malware/ antivirus instalat este actualizat si funcțional)

Înregistrări de scanare rezultate / actualizări regulate de patch-uri

Dovezi de instruire a angajaților

Referințe:

ISO 27002 - A.12.2.1

2.3.2 Categoria de activități de securitate: B 2 - Managementul administrării

Măsura de securitate: B21 - Administrarea conturilor

[B211]. Conturi de administrare. *OSE stabilește conturi de administrare destinate numai persoanelor responsabile de efectuarea operațiunilor precum instalare, configurare, întreținere, supraveghere, necesare pentru gestionarea resurselor rețelelor și sistemelor informatice.* ***Lista conturilor de administrare*** *va fi actualizată permanent.*

1. Permisiunile administratorilor sunt individualizate și restricționate la perimetrul funcțional și tehnic al fiecărui administrator.

2. Conturile de administrator sunt utilizate numai pentru conectarea la SIA.

3. Operațiunile de administrare a rețelelor și sistemelor informatice sunt realizate exclusiv de pe conturile de administrator.

Indicatori de control:

- **LICA -** lista conturilor de administrare

Implementarea procesului/administrativă:

In vederea efectuării operațiunilor de administrare, OSE restricționează și controlează alocarea și utilizarea conturilor dedicate în conformitate cu politica sa de control al accesului.

Operațiunile de administrare (instalare, configurare, întreținere, supraveghere etc.) a resurselor rețelelor și sistemelor informatice, se vor efectua doar prin intermediul unui cont dedicat (asociat unei persoane/ utilizator in baza unei aprobări) care ar trebui sa fie disponibil printr-un ID de utilizator separat, diferit de ID-ul utilizatorului folosit pentru activitățile zilnice.

Lista conturilor de administrare(denumita in Normele tehnice LICA) se va actualiza după fiecare aprobare de acest tip.

Principii de acordare a drepturilor de administrare:

- conturile de administrator ar trebui alocate pe baza „nevoii de utilizare” și, acolo unde este posibil, eveniment cu eveniment, astfel încât utilizatorii să aibă doar cerința minimă pentru rolul lor funcțional și numai atât timp cât este necesar;
- Este necesara verificarea in prealabil a competentelor utilizatorilor cu drept de administrare.

Principii de administrare pentru aceste tipuri de conturi:

- este necesara implementarea unui proces de eliminare a conturilor de administrare atunci când acestea nu mai sunt necesare;
- Când o persoana căreia i s-a alocat un cont de administrator părăsește OSE ar trebui să existe o revizuire imediată de ID-uri de utilizator și o actualizare a LICA;
- Activitățile efectuate cu conturile de administrare vor fi înregistrate și jurnalele protejate (stocate in așa fel încât sa nu poată fi modificate nici de către administratorii de sistem) și revizuite periodic.

Soluție tehnică

Stocarea documentelor in sistemul de gestionare a documentelor sau utilizarea unui software de securitate al identității (IAM – Identity and Access Management)

Probe:

Conturi de administrare personalizate și documentate cu drepturi de acces specifice acordate personalului relevant.

Lista conturilor de administrator si documentarea procesului de acordate a acestor drepturi

Referințe:

ISO 27002 A.9.2.3, A.9.2.5, A.9.2.6, A.12.4.3

Măsura de securitate: B22 - Administrarea rețelelor și sistemelor informatice

***[B221]. Utilizarea sistemelor de administrare**. OSE stabilește și aplică procedura privind utilizarea sistemelor informatice de administrare utilizate pentru operațiuni de administrare a NIS, respectând cel puțin regulile:*

1. Resursele hardware și software ale SIA sunt utilizate exclusiv pentru efectuarea operațiunilor de administrare.

– Când motivele tehnice sau organizaționale o justifică, SIA poate fi utilizată pentru a efectua alte operațiuni decât cele administrative. În acest caz, trebuie să fie puse în aplicare mecanismele de protecție a sistemului de operare și a compartimentării mediilor de lucru, pentru a permite izolarea mediului „utilizator" față de „administrator".

2. Mediul de lucru „administrator" folosit pentru operațiuni de administrare nu trebuie utilizat și în alte scopuri, cum ar fi accesarea site-urilor web sau a serverelor de e-mail.

3. Un utilizator nu trebuie să se conecteze la SIA prin intermediul unui mediu de lucru „utilizator" pentru alte funcții decât operațiuni de administrare a rețelelor și sistemelor informatice.

4. Fluxurile de date asociate cu alte operațiuni și fluxurile de administrare trebuie să fie separate prin mecanisme de criptare și autentificare, în conformitate cu MS-B15.

5. SIA sunt conectate la resursele rețelelor și sistemelor informatice printr-o legătură de rețea fizică folosită exclusiv pentru operațiunile de administrare. Resursele rețelelor și sistemelor informatice sunt administrate prin interfața lor de administrare fizică.

– Când motivele tehnice împiedică administrarea unei resurse a rețelelor și sistemelor informatice printr-o legătură de rețea fizică sau prin interfața de administrare fizică, operatorul pune în aplicare măsuri de reducere a riscurilor, cum ar fi măsuri logice de securitate. În acest caz, descrie aceste măsuri și justificările acestora în MANIS.

6. Fluxurile de administrare a rețelelor și sistemelor informatice sunt protejate de mecanisme de criptare și autentificare, în conformitate cu MS-B15.

– Dacă criptarea și autentificarea acestor fluxuri nu sunt posibile din motive tehnice, operatorul pune în aplicare măsuri pentru a proteja confidențialitatea și integritatea acestor fluxuri și pentru a consolida controlul și trasabilitatea operațiunilor de administrare. În acest caz, descrie aceste măsuri și justificările acestora în MANIS.

7. Jurnalele care înregistrează evenimentele generate de resursele SIA nu conțin nicio parolă sau alt element secret de autentificare în text simplu sau sub forma unei amprente criptografice.

Indicatori de control:

- **PRUSIA -** procedură privind utilizarea sistemelor informatice de administrare
- **PONIS -** politica de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale
- **JIERUA -** jurnalele de înregistrare a evenimentelor produse de resursele utilizate pentru administrare. Jurnalele sunt constituite și ținute sub formă electronică sau pe format fizic..
- **PPSIA -** plicul cu parole utilizate pentru sisteme informatice de administrare a rețelelor și sistemelor informatice

Implementarea procesului/ administrativă:

OSE dezvolta si implementa o procedură privind utilizarea sistemelor informatice necesare pentru operațiuni de administrare a NIS, denumita in Normele tehnice PRUSIA in care sa regăsim:

- existența unor sisteme informatice de administrare a rețelelor și sistemelor informatice SIA, ale căror resurse software si hardware sunt utilizate doar pentru efectuarea operațiunilor de administrare a NIS;
- resursele software si hardware care compun SIA sunt inventariate si documentate corespunzător, gestionarea si configurarea lor trebuie făcute de un personal specializat;
- doar in anumite condiții speciale, SIA pot fi utilizate si pentru alte operațiuni decât cele administrative, doar cu aplicarea unor mecanisme de protecție a sistemului de operare si separării mediilor de lucru pentru izolarea mediului „utilizator“ de cel „administrator”;
- mediul de lucru „administrator” poate fi folosit doar pentru activități de administrare (instalare, configurare, întreținere, supraveghere etc);
- SIA se conectează la resursele rețelelor și sistemelor informatice prin intermediul unei legături de rețea fizica si administrarea acestor resurse se face doar prin interfața lor de administrare fizică. Daca administrarea nu se poate face prin intermediul celor doua legături (rețeaua fizica sau prin interfața lor de administrare fizica) OSE pune in aplicare măsuri de reducere a riscurilor, de exemplu masuri logice de securitate, descriindu-le in MANIS

(mapa de acreditare de securitate), in documentul ce evidențiază procedurile si masurile de securitate aplicate.

- fluxurile de administrare a rețelelor și sistemelor informatice sunt protejate de mecanisme de criptare si autentificare, conform Masurilor de securitate stabilite la B15. Daca din motive tehnice nu este posibila implementarea acestor mecanisme, OSE pune în aplicare măsuri pentru a proteja confidențialitatea și integritatea acestor fluxuri și pentru a consolida controlul și trasabilitatea operațiunilor de administrare, descriind aceste măsuri și justificările acestora în MANIS, in documentul ce evidențiază procedurile si masurile de securitate aplicate;
- jurnalele, denumite in Normele tehnice JIERUA, utilizate pentru înregistrarea evenimentelor generate de SIA nu trebuie sa conțină parole sau alte elemente de autentificare scrise in clar;

Soluție tehnică

Utilizarea unor resurse hardware si software doar pentru activitățile de administrare, complet separate ca si utilizare de celelalte resurse ale rețelelor și sistemelor informatice.

Probe:

Inventar detaliat cu resurse hardware și software utilizate în scopuri de administrare.

Sisteme informaționale de administrare izolate și separate de restul infrastructurii pentru o rezistență sporită.

Referințe:

ISO 27002 A.9.3.1, A.9.4, A.12.1.4, A.12.4.3

Note:

In practica, referințele legate de parolele folosite de utilizatori sau parolele de administrare, cerințele minime de creare ale parolei, perioada de viată etc. sunt menționate într-un document formalizat numit *Politica de parole.*

[B222]. Parole administrare. *Nicio parolă, sub formă de text simplu sau hash, nu este scrisă în jurnalele de înregistrare a evenimentelor produse de resursele utilizate pentru administrare și nu este stocată sub această formă în niciun moment.*

1. Evidența parolelor de administrare se păstrează, în plic închis și sigilat [PPSIA], la componenta de securitate sau administrare a rețelelor și sistemelor informatice.

Implementarea procesului/ administrativă:

Jurnalele, denumite in Normele tehnice JIERUA, utilizate pentru înregistrarea evenimentelor generate de SIA nu trebuie sa conțină parole sau alte elemente de autentificare scrise in clar.

Parolele de administrare, trebuie păstrate in plic închis si sigilat (denumit in Normele tehnice PPSIA) si nu apar înregistrate in niciun jurnal JIERUA.

Soluție tehnică

Neaplicabila.

Probe:

Existenta unui document formalizat in care sa se regăsesc cerințele privind parolele de administrare împreuna cu modul de păstrare și comunicare a acestora.

Referințe:

ISO 27002 A.9.3.1, A.9.4, A.12.1.4, A.12.4.3

Măsura de securitate: B23 - Managementul accesului de la distanță

***[B231]. Lucrul la distanță**. OSE adoptă **o procedură privind lucrul la distanță**, în baza PONIS.*

1. PROLD va cuprinde modurile de realizare, măsurile de securitate aferente pentru protejarea resurselor și a informațiilor accesate, prelucrate și stocate din și în locațiile în care se lucrează la distanță.

2. Când furnizarea serviciului esențial necesită ca rețelele și sistemele informatice să fie accesibile printr-o rețea publică, operatorul protejează accesul prin intermediul unor mecanisme criptografice, în conformitate cu MS-B15.

Indicatori de control:

- **PROLD -** procedură privind lucrul la distanță
- **PRAPC -** procedură pentru asigurarea protecției criptografice pentru informații și resurse

Implementarea procesului/administrativă:

OSE dezvolta o procedură privind lucrul la distanță, denumita in Normele tehnice PROLD, prin care se definesc condițiile și restricțiile pentru lucrul la distanță si se pun in aplicare măsuri de securitate aferente pentru protecția informațiilor accesate, prelucrate sau stocate în locații de lucru aflate la distanță.

În mod normal, locuința angajatului nu are același nivel fizic securitate, iar zona de lucru este adesea ușor accesibilă de către membrii familiei și vizitatori. Pentru a reduce aceste riscuri, lucrul la distanță ar trebui să fie implementat după ce OSE a dezvoltat politici adecvate și proceduri, a instituit controale fizice pentru securizarea zonei de lucru și a instruit angajații care lucrează de la distanță suficient pentru a controla accesul fizic și logic la informație si la facilitățile de procesare utilizate pentru activitățile de lucru la distanță.

Conexiunile dintre locațiile OSE și facilitățile unde se desfășoară lucrul la distanță ar trebui să fie securizate prin mecanisme criptografice conform normelor stabilite la măsura de securitate B15, pentru a se asigura că informațiile nu pot fi distruse, deteriorate, compromise sau modificate iar informațiile care sunt accesibile de la distanță sunt limitate la minimum.

Soluție tehnică

Utilizare unor conexiuni securizate de tip VPN pentru accesul la resursele OSE

Probe:

Procedura privind lucrul la distanță/ PROLD

Lista conturilor VPN in relație cu lista utilizatorilor care folosesc lucrul la distanță.

Lista incidentelor si acțiunilor care au fost luate pentru adresarea acestora

Referințe:

ISO 27002 6.2.2

2.3.3 Categoria de activități de securitate B3 - Managementul identității și accesului

Măsura de securitate: B31 - Managementul identificării și autentificării utilizatorilor

Note:

Toate cerințele de securitate descrise in cadrul masurilor de mai jos sunt mai ușor de gestionat daca se utilizează un document formalizat care sa conțină referințe către: identificarea, autentificarea si acordarea drepturilor de acces utilizatorilor sau proceselor automatizate care trebuie să acceseze resursele rețelelor și sistemelor informatice. Documentul poate fi *Politica de control al accesului* care definește drepturile de acces ale utilizatorilor pe baza cerințelor de business, luând în considerare cerințele de securitate a informațiilor, a rețelelor și sistemelor informatice si orice cerințe legale sau de conformitate interna, chiar daca nu este specificata expres in Normele tehnice.

***[B311]. Identificarea utilizatorilor**. Pentru identificare, OSE stabilește și ține **evidența conturilor unice** pentru utilizatori sau pentru procesele automatizate care trebuie să acceseze resursele rețelelor și sistemelor informatice.*

1. Conturile neutilizate sau care nu mai sunt necesare trebuie să fie dezactivate.

*2. Se instituie un **proces permanent de revizuire și actualizare** a evidenței conturilor pentru utilizatori și pentru procesele automatizate.*

3. Atunci când acest lucru nu este posibil din motive tehnice sau operaționale, OSE dezvoltă un set de măsuri de trasabilitate și reducere a riscurilor și le descrie în MANIS.

Indicatori de control:

- **ECUPA -** evidența conturilor pentru utilizatori și pentru procesele automatizate
- **MANIS -** mapa de acreditare de securitate; document în baza căruia se emite DANIS
- **ARNIS -** analiza riscurilor de securitate a rețelelor și sistemelor informatice, document elaborat la nivelul OSE, prin care sunt identificate elementele critice care stau la baza furnizării serviciului esențial și sunt identificate principalele riscuri în vederea gestionării și diminuării acestora

- **MEAUP -** mecanism de autentificare pentru utilizatori și procese automatizate la resursele rețelelor și sistemelor informatice

Implementarea procesului/administrativă:

OSE dezvolta si implementează un document formalizat care sa cuprindă pașii necesari ce asigura faptul ca utilizatorii si procesele automatizate au acces doar la resursele rețelelor și sistemelor informatice pentru care au fost autorizați sa le utilizeze.

Fiecare utilizator sau proces automatizat care accesează resursele rețelelor și sistemelor informatice trebuie sa aibă alocat un identificator unic si OSE tine evidenta acestora in vederea asigurării trasabilității accesului si a acțiunilor întreprinse. Identificarea fiecărui utilizator pentru a oferi accesul la resurse conform drepturilor alocate asigura protejarea confidențialității, integrității si disponibilității informațiilor.

Toți utilizatorii sunt responsabili pentru toate acțiunile pe care le fac si acest lucru este posibil numai cu un identificator de utilizator unic.

Pe baza evidentei conturilor unice si a acțiunilor întreprinse de fiecare utilizator, OSE identifica si dezactivează sau șterge, după caz, conturile ce nu mai sunt utilizate sau nu mai sunt necesare.

OSE implementează un proces de revizuire periodica, si actualizare la notificarea departamentului HR, a evidentei conturilor unice pentru utilizatori și pentru procesele automatizate in vederea eliminării eventualelor conturi neutilizate sau a conturilor utilizatorilor care nu mai colaborează cu OSE (angajați sau contractori care au primit acces restricționat in sistem).

În acele cazuri în care nu este posibila alocarea unor conturi unice individuale (de ex. deoarece sistemul nu are funcționalitatea necesară, folosind conturi generice) lista acestora trebuie formalizata pentru a asigura o transparenta cu privire la persoanele autorizate sa folosească acele conturi, si o actualizare rapida a credentialelor acestora, in cazul unor schimbări de personal. Toate aceste masuri pentru reducerea riscurilor se detaliază in mapa de acreditare de securitate (denumita in Normele Tehnice MANIS) de la măsura de securitate A13.

Soluție tehnică

Se poate utiliza un tool IAM - Identity and Acces Management sau se poate utiliza serviciu de tip Directory Service in vederea gestionarii si păstrării evidentei conturilor unice.

Probe:

Documentele formale care descriu procesele de gestionare pentru utilizatori unici individuali si a celor generici precum si procesul de revizuire ale acestora

Evidenta formala a conturilor generice

Existenta proceselor de revizuire a conturilor (individuale si generice)

Referințe:

NIST PR.AC-1,4,6,7, ISO 27002 A.9.1, A.9.3, A.9.4.1

[B312]. Autentificarea utilizatorilor. *Pentru autentificare, OSE protejează accesul la resursele NIS pentru utilizatori sau procese automatizate, folosind un* ***mecanism de autentificare****. OSE definește regulile de gestionare a certificatelor de autentificare la rețelele și sistemele informatice.*

1. Pentru procesele critice, OSE va stabili un mecanism de autentificare în cel puțin doi pași.

2. OSE trebuie să schimbe datele de autentificare implicite instalate de producătorul/furnizorul unei resurse înainte ca acea resursă să intre în funcțiune. Neglijarea acestui aspect prezintă un risc ridicat pentru securitatea oricărei infrastructuri din care face parte o astfel de resursă sau cu care interacționează.

Implementarea procesului/administrativă:

Pentru oferirea accesului la resursele rețelelor și sistemelor informatice OSE implementează un proces de autentificare a utilizatorilor prin care se stabilește autenticitatea utilizatorilor sau proceselor automatizate. Astfel se permite accesul la resurse utilizatorilor si proceselor automatizate identificați in cadrul cerinței de securitate anterioare, B311, si, in același timp, sunt împiedicați utilizatorii necunoscuți sa aibă acces la resurse.

Pentru autentificare se pot folosi următoarele metode:

- Autentificarea prin parola, cunoscuta ca „ceva ce userul știe”;
- Autentificarea printr-un smartcard sau token un software special de autentificare sau un certificat digital, cunoscuta ca „ceva ce userul are”;

- Autentificarea biometrică, prin care se testează o caracteristica biologica a utilizatorului, utilizează amprente digitale, amprente vocale și scanări faciale sau retiniene, cunoscuta ca „ceva ce userul este”.

O metoda care asigura un nivel ridicat de securitate este aceea prin care se combina cel puțin doua din metodele menționate anterior, cum ar fi o parolă cu un autentificator sau biometrie. Această abordare, cunoscută ca „autentificare cu doi factori sau cel puțin doi factori”, oferă un nivel de securitate superior.

Pentru procesele critice identificate in urma analizei si evaluării riscurilor de la măsura de securitate A11, OSE trebuie sa stabilească un mecanism de autentificare în cel puțin doi pași.

În momentul in care se implementează procesul de instalare a unei resurse noi, OSE trebuie sa se asigure ca datelor de autentificare implicite configurate de producătorul/ furnizorul acelei resurse sunt modificate in așa fel încât sa se elimine riscul ridicat de securitate al accesului la resursa respectiva a utilizatorilor neautorizați.

Soluție tehnică

Autentificarea se poate face printr-un tool IAM - Identity and Acces Management sau se poate utiliza un serviciu de tip Directory Service. Se pot folosi aplicatii mobile pentru autentificarea cu token sau autentificarea biometrica.

Probe de audit:

Existenta mecanismului de autentificare pentru utilizatori și procese automatizate la resursele rețelelor și sistemelor informatice

Verificarea existentei autentificării in cel puțin doi pași pentru procesele critice

Referințe:

NIST PR.AC-1,4,6,7, ISO 27002 A.9.4.2, A.9.4.3

Măsura de securitate: B32 - Managementul drepturilor de acces

[B321]. Acordarea drepturilor de acces. *În baza regulilor stabilite în PONIS, OSE acordă drepturi de acces unui utilizator sau unui proces automat doar atunci când accesul este strict necesar pentru ca utilizatorul să își îndeplinească atribuțiile, iar procesul automatizat să își desfășoare operațiunile tehnice.*

1. În acordarea drepturilor de acces, OSE aplică principiul necesității de a cunoaște și principiul celui mai mic privilegiu.

2. OSE definește drepturile de acces la multiplele funcționalități ale rețelelor și sistemelor informatice și alocă aceste drepturi de acces strict utilizatorilor/proceselor automatizate care au o necesitate clară.

3. Cel puțin o dată pe an, OSE examinează atribuirea drepturilor de acces, identificând legăturile dintre conturi, drepturile de acces asociate și resursele sau funcționalitățile care sunt accesate prin drepturile de acces, și păstrează actualizată o listă a conturilor privilegiate pe nivele de acces și funcționalități accesabile.

[B322]. Verificarea conturilor privilegiate. *OSE implementează un sistem de verificare a potențialelor modificări ale unui cont privilegiat, pentru a identifica dacă drepturile de acces la resurse și funcționalități sunt alocate pe baza principiului celui mai mic privilegiu (sunt acordate doar drepturile strict necesare) și sunt adecvate cu utilizarea contului.*

Indicatori de control:

- **PONIS -** politica de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale
- **LICPA -** lista conturilor privilegiate pe nivele de acces și funcționalități accesabile
- **LICA -** lista conturilor de administrare
- **SIVMOC -** sistem de verificare a potențialelor modificări ale unui cont privilegiat

Implementarea procesului/ administrativă:

OSE aloca drepturi de acces la resurse utilizatorilor si proceselor automatizate pe baza unui proces formalizat in care se regăsesc pașii de acordare, modificare si retragere drepturi de acces, resursele rețelelor și sistemelor informatice la care utilizatorul sau procesul automatizat vor avea acces precum si acordurile proprietarului resurselor si al managerului superior al utilizatorului.

Procesul de acordare a drepturilor de acces unui utilizator sau unui proces automatizat poate fi formalizat fie conform propunerii ce se regăsește la măsura B31 sau in orice alta forma, incluzând principiile enunțate mai jos.

Alocarea nejustificată a drepturilor de acces crește vulnerabilitatea OSE la încălcarea confidențialității, pierderea integrității datelor și indisponibilitate prin utilizarea abuzivă a drepturilor alocate.

De aceea, pornind regulile de alocare a drepturilor stabilite in politica de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale (denumita in Normele Tehnice PONIS) detaliata la măsura de securitate A12, OSE aloca drepturi de acces la resurse doar utilizatorilor si proceselor automatizate care au nevoie de aceste drepturi pentru a-si îndeplini atribuțiile sau, in cazul proceselor automate, pentru a-si desfășura operațiunile tehnice.

Drepturile de acces ale utilizatorilor si ale resurselor automate trebuie să fie documentate și să descrie rețelele și sistemele informatice pe care utilizatorul sau procesele automatizate au voie să le acceseze. Astfel, drepturile de acces la multiplele funcționalități ale rețelelor și sistemelor informatice trebuie sa fie alocate doar utilizatorilor/ proceselor automatizate care au nevoie de acces pentru îndeplinirea sarcinilor pe care le au sau pentru operațiunile tehnice, in cazul proceselor.

Utilizatorii si procesele automate trebuie sa aibă acces doar la informațiile de care au nevoie conform activității pe care o desfășoară in cadrul OSE sau, in cazul proceselor automate, pentru ce operațiuni tehnice sunt implementate (principiul necesității de a cunoaște). De asemenea, utilizatorii si procesele automate vor avea alocate drepturi la un nivel minim al accesului sau permisiunilor in așa fel încât sa-si poată îndeplinii sarcinile sau sa se poată efectua operațiunile tehnice, in cazul proceselor (principiul celui mai mic privilegiu).

Pentru a menține un control eficient asupra accesului la rețelele si sistemele informatice, pentru a evita orice acces neautorizat, OSE realizează cel puțin o data pe an o revizuire a drepturilor de acces ale utilizatorilor si proceselor automatizate, verificând utilizatorii care sunt promovați, sau rolurile lor sunt schimbate sau când utilizatorii care pleacă din OSE, identificând legăturile dintre conturi, drepturile de acces asociate și resursele sau funcționalitățile care sunt accesate prin drepturile de acces, și păstrează actualizată o listă a conturilor privilegiate pe nivele de acces și funcționalități accesabile.

Conturile privilegiate pot fi verificate cu o frecventa mai mare, utilizatorii care au alocate conturi privilegiate putând modifica sau șterge informații mai ușor decât orice utilizator normal.

OSE implementează un sistem de verificare a potențialelor modificări ale unui cont privilegiat pentru a identifica daca se păstrează principiul celui mai mic privilegiu, definit mai sus, in alocarea drepturilor de acces la resurse.

Jurnalele conturilor de utilizator privilegiate (automate acolo unde se poate) trebuie păstrate pentru a se identifica acțiunile întreprinse de utilizator precum si orice modificare a drepturilor de acces aplicat acestora.

Soluție tehnică

Si in cazul controlului accesului o soluție IAM - Identity and Acces Management poate fi folosita sau se poate utiliza serviciu de tip Directory Service.

Probe:

Documentele formalizate ce descriu managementul drepturilor de acces al utilizatorilor

Lista conturilor privilegiate pe nivele de acces și funcționalități accesabile, actualizata/ LICPA.

Procesul formal de verificare a potențialelor modificări ale unui cont privilegiat implementat.

Referințe:

ISO 27002 A.9.2, A.9.4.4, A.9.4.5

2.3.4 Categoria de activități de securitateB4 - Managementul mentenanței

Măsura de securitate: B41 - Mentenanța rețelelor și sistemelor informatice

*[B411]. **Menținere securitate.** OSE elaborează și implementează o procedură pentru menținerea securității rețelelor și sistemelor informatice, în conformitate cu PONIS.*

1. În acest scop, procedura:

– definește condițiile care permit menținerea unui nivel minim de securitate a resurselor;

– descrie politica de instalare a oricărei noi versiuni sau măsuri corective pentru o resursă desemnată;

– obligă informarea cu privire la informații despre vulnerabilități și măsuri corective de securitate care privesc resursele rețelelor și sistemelor informatice (hardware și software).

Indicatori de control:

- **PROMNIS -** procedură pentru menținerea securității rețelelor și sistemelor informatice
- **PRORUVI -** procedură pentru reducea riscurilor legate de utilizarea unei versiuni învechite
- **PONIS -** politica de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale
- **MANIS -** mapa de acreditare de securitate; document în baza căruia se emite DANIS
- **PRAPC -** procedură pentru asigurarea protecției criptografice pentru informații și resurse

Implementarea procesului/administrativă:

Pornind de la politica de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale(PONIS) si in urma implementării cerințelor de securitate specificate in aceste Norme tehnice, OSE elaborează si implementează o procedura pentru menținerea securității rețelelor și sistemelor informatice.

Aceasta procedura are ca scop:

- definirea condițiilor care permit menținerea nivelului minim de securitate pentru resursele hardware si software si care acoperă in principiu cam toate masurile de securitate enunțate in acest ghid
- descrierea politicii de instalare a versiunilor noi software: firmware, patch-uri securitate etc., in conformitate cu recomandările producătorilor sau masuri de corective recomandate de aceștia.
- asigurarea informării obligatorii a OSE cu privire la vulnerabilitățile si masurile corective corective de securitate care privesc resursele rețelelor și sistemelor informatice (hardware și software) identificate si publicate de către producătorii/furnizorii resurselor respective

Soluție tehnică

Folosirea unei soluții software pentru managementul si monitorizarea resurselor software si hardware din rețelele și sistemele informatice.

Probe:

Procedura pentru menținerea securității rețelelor și sistemelor informatice

Referințe:

ISO 27002 10.1, A.11.2.4, A.12.6.1, A.14.1.1

[B412]. Actualizare resurse. *OSE instalează și menține doar versiuni ale resurselor hardware și software care sunt acceptate de furnizorii sau producătorii lor și sunt actualizate din punctul de vedere al securității.*

1. OSE verifică originea și integritatea versiunii înainte de instalarea acesteia (conform calendarului definit în PROMNIS) și analizează impactul tehnic și operațional al versiunii respective asupra securității rețelelor și sistemelor informatice.

2. În unele cazuri justificate, din motive tehnice sau operaționale, OSE decide ca pentru anumite resurse să nu instaleze o versiune acceptată de furnizor sau producător. În aceste cazuri, OSE aplică procedura pentru reducerea riscurilor legate de utilizarea unei versiuni învechite, elaborată conform PONIS, și descrie în MANIS măsurile luate, precum și motivele care au justificat să nu instaleze versiunea acceptată.

Implementarea procesului/administrativă:

Pe baza procedurii pentru reducerea riscurilor legate de utilizarea unei versiuni învechite, descrisa la măsura de securitate B411, OSE actualizează continuu versiunile resurselor hardware si software conform recomandărilor producătorilor;

Înainte de instalarea actualizărilor, OSE verifica originea si integritatea acestora, analizează impactul tehnic si operațional rezultat in urma actualizării asupra securității rețelelor și sistemelor informatice si decide instalarea sau nu a acestor actualizări.

Dacă, in unele cazuri justificate, OSE decide sa nu actualizeze versiunile conform recomandărilor producătorilor, din motive tehnice sau operaționale, de exemplu incompatibilități cu alte aplicații software/resurse instalate, trebuie aplicata procedura pentru reducea riscurilor legate de utilizarea unei versiuni învechite si descrie in MANIS, (mapa de acreditare de securitate), in documentul ce evidențiază

procedurile si masurile de securitate aplicate, ce masuri au fost luate si motivele pentru care nu s-au instalat versiunile recomandate de producător.

Soluție tehnică

Folosirea unei soluții software pentru managementul si monitorizarea resurselor software si hardware din rețelele și sistemele informatice.

Probe:

Procedură pentru reducea riscurilor legate de utilizarea unei versiuni învechite

Referințe:

ISO 27002 10.1, A.11.2.4, A.12.6.1, A.14.1.1

[B413]. Protejare resurse*. OSE protejează accesul la resursele rețelelor și sistemelor informatice atunci când accesul se face din rețele terțe.*

1. În acest caz, OSE protejează prin criptare și mecanisme de autentificare accesul la rețelele și sistemele informatice, ține evidența echipamentelor utilizate pentru accesarea rețelelor și sistemelor informatice și, de asemenea, gestionează și configurează aceste echipamente.

Implementarea procesului/administrativă:

Pentru asigurarea securității resursele rețelelor și sistemelor informatice din perspectiva accesului din rețele terțe, OSE instituie:

- mecanisme de criptate si autentificare a accesului la resurse
- păstrează o evidenta a echipamentelor utilizate pentru accesarea rețelelor;
- gestionează si configurează aceste echipamente

Mecanismele de criptare folosite sunt cele specificate la măsura de securitate B15, conform procedurii pentru asigurarea protecției criptografice pentru informații și resurse.

Mecanismele de autentificare folosite sunt cele specificate la măsura de securitate B31 si se regăsesc in documentul formalizat ce reglementează mecanismul de autentificare pentru utilizatori și procese automatizate la resursele rețelelor și sistemelor informatice

Soluție tehnică

Neaplicabila

Probe:

Procedură pentru asigurarea protecției criptografice pentru informații și resurse

Referințe:

ISO 27002 A.10.1, ISO 27002 A.9.4.2, A.9.4.3

Măsura de securitate – B42 - Sisteme de control industrial. SCADA - Monitorizare, control și achiziții de date

[B421]. Sisteme de control industriale. *Multe servicii esențiale depind de sisteme de control industriale, funcționale și sigure. Dacă este cazul, OSE ia în considerare cerințele de securitate specifice pentru ISC.*

Abordarea clasică a tehnologiei informației (axată pe transferul și accesul de/la informații) ar putea fi înlocuită cu o abordare tehnologică operațională (hardware și software - utilizate pentru detectarea modificării unui proces fizic).

Indicatori de control:

- **CEISC –** cerințe de securitate specifice pentru sistemele de control industrial
- **ANISMS –** analiza riscurilor de securitate și implementarea măsurilor de securitate pentru limitarea accesului neautorizat

Note *:*

Prin ISC înțelegem sistemele de control industriale (Industrial Control Systems - ICS), iar prin SCADA (Supervisory Control and Data Acquisition) înțelegem în mod normal un subset al sistemelor ISC care are rolul de comanda-control centralizat pentru echipamentele si procesele industriale. Sistemul SCADA este critic in functionarea oricarui ISC. În cele ce urmează vom considera acești doi termeni identici pentru scopul controalelor din această secțiune, aplicabilitatea generală a recomandărilor din acest ghid aplicându-se ambelor în aceeași măsură, și sistemelor de tip OT (Operational Technology) în general.

În general aceste sisteme sunt folosite pentru procese industriale complexe și critice. Pierderile în cazul nefuncționării pot fi foarte mari, indiferent dacă nefuncționarea este cauzată de probleme operaționale sau atacuri cibernetice.

Pentru aceste sisteme de control metodele consacrate de apărare nu se aplică în același mod. Spre exemplu, actualizarea imaginilor software comporta riscuri

operationale mari, iar antivirus sau mecanisme anti-malware nu pot fi instalate deloc în unele cazuri.

În același timp, aceste sisteme au fost în trecut țintite de actori statali, care au investit sume mari de bani în a le infiltra.

Implementarea procesului/ administrativă:

Pentru infrastructurile de acest tip procesele instituției trebuie adaptate în funcție de capabilitățile sistemelor. Accentul trebuie pus pe monitorizarea sistemelor, astfel încât comportamente anormale sau trafic anormal să fie investigate și din punct de vedere a securității cibernetice. De cele mai multe ori, cele mai importante capacități de detecție și intervenție se află la granița dintre sistemul IT și sistemul ISC, întrucât sistemele ISC vor fi separate cel puțin logic de restul rețelei OSE (având în vedere nevoia de continuitate a proceselor industriale). Astfel, controlul accesului și drepturile de acces la aceste resurse devin foarte importante și ar trebui, în general, să fie alocate și controlate la fel de restrictiv precum drepturile unui administrator de rețea, chiar si la nivel de utilizator.

Soluție tehnică

Măsurile tehnologice de protecție diferă în funcție de tehnologia operațională folosită și de modalitățile de interconectare la nivel de rețea. În funcție de nivelul de risc și de tehnologie, operatorul poate implementa sisteme de detectare sau prevenire a intruziunilor (IDS/ IPS) la nivel de rețea (bazate pe semnături, pe reguli sau pe detecția anomaliilor), tehnologii de whitelisting care să permită doar anumitor programe să ruleze pe sistemele operaționale, tehnologii de tip SIEM care să agrege informațiile de la senzori operaționali și de la aceste soluții și să identifice potențialele atacuri. Tehnologiile folosite trebuie sa fie capabile sa analizeze seria de protocoale de comunicație industrială folosite in cadrul ISC al OSE.

Probe:

Lista tehnologiilor si a protocoalelor de comunicație OT (SCADA, ICS) relevante pentru serviciile esențiale,

Referințe:

ISF SoGP PA1.3 Industrial Control Systems

Note:

Prin acest control înțelegem că accentul se pune pe restricționarea accesului la sistemele SCADA, si aceasta abordare este coerentă cu limitările inerente platformelor OT (Operational Technology) în general.

[B422]. Limitarea accesului. *Sistemele SCADA folosesc diferite conexiuni combinate, radio, seriale sau modem în funcție de necesități. Pentru amplasamente mari sunt folosite, de asemenea, conexiuni Ethernet și IP/Sonet.*

1. În aceste condiții, OSE trebuie să identifice și analizeze ***riscurile de securitate*** *și să implementeze* ***măsuri de securitate*** *pentru limitarea accesului neautorizat.*

Implementarea procesului/administrativă:

Limitarea accesului poate fi făcută la mai multe niveluri:

- Limitarea interconectărilor la nivel de rețea, care pot îmbrăca și alte forme în afară de conexiuni clasice ethernet. Aceasta poate fi făcută prin închiderea unor conexiuni (air gap) sau prin filtrarea acestora cu firewall-uri sau diode de date;
- Limitarea accesului personalului operațional, printr-o combinație de acces fizic si acces logic;
- Limitare accesului administrativ, în special a accesului de la distanță, prin aplicarea unor controale de management al accesului administrativ.

Măsurile tehnice și organizatorice trebuie să aibă la bază o analiză a riscurilor de securitate pentru platformele SCADA (numită aici ANISMS) care va fi probabil, pentru majoritatea OSE, inclusă în analiza principală de risc (LIRIE).

Soluție tehnică

Soluții tehnice de tip firewall (sau, pentru protecții hardware, tehnologii de tipul diode de date) pot permite informației să circule restricționat, permițând transferul controlat de informație. Astfel din zona IT înspre zona OT, se poate permite transferul de patch-uri și actualizări. În sensul celălalt, se poate limita cantitatea de date exfiltrată din rețelele OT, în general permițând date legate de măsurători și buna funcționare a echipamentelor.

Filtrele la nivelul IP configurate pe routere și firewall-uri pot reduce suprafața inițială de atac.

Soluții de tip servere intermediare (jump host) sau managementul identităților privilegiate (privileged identity management) combinate cu monitorizarea sesiunilor pot controla accesul administrativ în astfel de sisteme și rețele.

Probe:

Identificarea si documentarea tehnologiilor OT (SCADA, ICS) relevante pentru serviciile esențiale (poate fi de asemenea inclusă în cartografierea sistemului),

Documentarea regulilor de acceptare a traficului prin firewall/diode de date

Documentarea drepturilor de acces si a listei utilizatorilor cu acces la sistemul ISC

Identificarea si documentarea riscurilor legate de acestea (ANISMS),

Măsuri de securitate specifice cu privire cel puțin la limitarea accesului (CEISC).

Referințe:

ISF SoGP PA1.3 Industrial Control Systems

Măsura de securitate – B51 - Managementul securităţii fizice. Asigurarea protecţiei fizice a reţelelor şi sistemelor informatice

[B511]. Acces la resurse. *OSE previne* ***accesul fizic neautorizat****, deteriorarea și interferența la informațiile şi facilitățile de procesare a informațiilor în rețelele și sistemele informatice.*

În acest sens, OSE elaborează şi aplică o ***procedură privind accesul şi securitatea resurselor şi informațiilor****.*

Indicatori de control:

- **PRASI –** procedură privind accesul și securitatea resurselor și informațiilor

Notă:

Suplimentar, trebuie avută în vedere legea 333/2003 în forma ei actuală, care reglementează printre altele obligațiile societăților comerciale și a organizațiilor care dețin bunuri ori valori.

Implementarea procesului/administrativă:

Pornind de la inventarul activelor (LASPO, prevăzut în A19), operatorul de servicii esențiale trebuie să asigure protejarea fizică a acestor active. Asigurarea protecției fizice are trei mari componente:

1. restricționarea accesului fizic
2. protejarea mediului în care acestea funcționează (parametrii de temperatură, umiditate, etc.);
3. asigurarea utilităților suport (disponibilitatea curentului, conexiunilor de rețea).

Pentru asigurarea acestei protecții, operatorul trebuie să aibă în vedere nu doar echipamentele care susțin sistemele informatice, ci și conexiunile de rețea (inclusiv locurile pe unde trec cablurile, și diverse cabinete în care se află echipamente de comunicații în afara centrului de date) și mediile de lucru de unde pot fi accesate aceste sisteme informatice.

Trebuie în primul rând definite zonele sau perimetrele de securitate, și stabilite reguli de acces și de protecție a mediului pentru acestea. În cazul companiilor cu multe locații, pentru asigurarea unui nivel de control centralizat, conformitatea cu aceste reguli poate fi verificată periodic (prin rotație).

Zonele pot include centre de date, medii de lucru (birouri), zone cu acces public, zone de livrare sau încărcare.

Restricționarea accesului pe zone se face în funcție de importanța acestora. În zonele mai puțin importante se poate permite accesul vizitatorilor, cu înregistrarea acestora, iar în zonele critice accesul este strict restricționat, și înregistrat momentul intrării și ieșirii.

Asimilăm cerința de a preveni interferența la facilitățile de procesare cu ecranarea față de exterior. Totuși, în practică sunt rare situațiile în care este necesar un sistem de ecranare suplimentar.

Soluție tehnică

Restricțiile fizice pot îmbrăca diverse forme:

- clădiri solide, fără breșe, și cu uși solide;
- mecanisme de control fizic (bare, alarme, lacăte, turnicheți);
- mecanisme de control acces (cu cheie, sau electronice, cele electronice având în general avantajul de a permite identificarea în log-uri a persoanelor cărora le-a fost permis accesul);
- camere video și de supraveghere;
- zone de recepție și pază.

Următorii factori sunt importanți pentru protecția mediului în care funcționează echipamentele: focul, fumul, exploziile, apa, praful, vibrațiile, efecte ale substanțelor chimice, radiații electromagnetice, furtul, vandalismul. În practică, accentul se pune pe protecția contra incendiului și inundațiilor, acestea fiind pericolele cele mai comune. Centrele de date sunt echipate în general cu mecanisme de detecție a incendiilor și inundațiilor, și mecanisme de stingere a incendiilor. Mecanismele de stingere automată a incendiilor (sprinklere cu apă, gaz inert) trebuie evaluate cu atenție, deoarece pot pune în pericol viețile omenești și pot deteriora echipamentele (cu apă, în cazul sprinklerelor, sau prin vibrații puternice, în cazul buteliilor cu gaz inert).

Probe:

Proceduri care asigură securitatea fizică

Măsuri pentru prevenția accesului neautorizat

Măsuri pentru prevenirea deteriorării (protecția mediului în care operează sistemele informatice)

Măsuri pentru prevenirea interferențelor (dacă e cazul)

Referințe:

ISO27001, anexa 1, cap. 11. - Securitatea fizică şi a mediului de lucru

2.4 Domeniul de securitate C1 – Managementul detecției

2.4.1 Categoria de activități de securitate C1 - Managementul Detecției

Măsura de securitate: C11 - Managementul vulnerabilităților și alertelor de securitate

Note:

Implementarea procedurii PRODAIS poate fi preluată din modul de configurare și operare a sistemelor de detecție/management vulnerabilității existente.

[C111]. Fluxul alertelor de securitate. *OSE elaborează, actualizează și implementează, în conformitate cu PONIS, o* ***procedură pentru detectarea alertelor și incidentelor de securitate*** *care afectează rețelele și sistemele informatice.*

1. PRODAIS prevede măsuri organizatorice și tehnice destinate detectării alertelor și incidentelor de securitate care afectează rețelele și sistemele informatice.

*- Măsurile organizatorice includ **procedurile de operare** pentru dispozitivele de detectare și descriu lanțul de procesare pentru evenimentele de securitate identificate de aceste dispozitive.*

- Măsurile tehnice specifică natura și poziționarea dispozitivelor de detectare.

*2. OSE instituie un **sistem de detectare a incidentelor și alertelor de securitate**.*

- Dispozitivele de detecție analizează fluxurile de date care tranzitează rețelele și sistemele informatice pentru a identifica evenimente care ar putea afecta rețelele și sistemele informatice.

- Atunci când acest lucru nu este posibil din motive tehnice, operatorul descrie în MANIS motivele tehnice care au împiedicat utilizarea dispozitivelor de detecție.

Indicatori de control:

- **PRODAIS** - procedură pentru detectarea incidentelor de securitate care afectează rețelele și sistemele informatice
- **SIENIS** - sistem de înregistrare evenimente la nivelul rețelelor și sistemelor informatice
- **MANIS** - mapa de acreditare de securitate; document în baza căruia se emite DANIS

Implementarea procesului/administrativă:

In mediile IT complexe si interconectate, exista multiple surse de alertare in cadrul sistemelor de detecție a alertelor de securitate. Alertele la rândul lor vor fi monitorizate si investigate de personal dedicat, fie din interiorul companiei, fie contractat.

Alertele pot fi generate de sisteme dedicate de detecție sau de sisteme dedicate altor scopuri IT, dar care au implementate anumite alerte. Sistemele de detecție pot fi, fără a se limita la: EDR (Endpoint Detection and Response), firewall, IDS(Intrusion Detection System), IPS (Intrusion Protection System), antivirus, IAM (Identity and Access Management), DLP (Data Loss Prevention), cloud security (securitatea sistemelor virtuale).

OSE va implementa o procedură care va conține elementele următoare :

a) Măsuri organizatorice:

- Rolurile și responsabilitățile pentru operarea sistemelor si proceselor de detecție
- Pragurile de alertă pentru evenimente si incidente stabilite (se urmărește pagina web a DNSC pentru a include ultimele actualizări);
- Modul de raportare al evenimentelor în conformitate cu criteriile și fluxul de lucru stabilite;
- Pașii prin care are loc schimbul voluntar de informații cu părțile interesate externe pentru a realiza o conștientizare situațională mai largă a securității cibernetice;
- Se va completa MANIS cu informațiile corespunzătoare (inclusiv motivele tehnice care au împiedicat utilizarea dispozitivelor de detecție);

b) Măsuri tehnice:

- diagramă de rețea care exemplifică tipul și poziționarea echipamentelor de detecție si detaliază fluxurile alertelor de la generare pana la stocarea in sistem
- Se va implementa sistemul de înregistrare a evenimente la nivelul rețelelor și sistemelor informatice / SIENIS

Implementarea tehnică:

O soluție (N)IDS (Network - Intrusion Detection System) si orice alta sursa de generare de alerte din cadrul sistemului integrată cu SIEM (precum antivirus, firewall, DLP, EDR, etc). Este recomandata implementarea unui produs de tip EDR/SIEM pentru gestionarea, investigarea si stocarea alertelor de securitate.

Crearea si publicarea documentelor formale/ procedurilor în intranetul OSE sau într-un sistem de management de documente

Probe:

Procedură pentru detectarea incidentelor de securitate/ PRODAIS

Dovada implementării unui sistem de înregistrare evenimente la nivelul rețelelor și sistemelor informatice/ SIENIS

Justificarea motivelor tehnice care au împiedicat utilizarea dispozitivelor de detecție, document inclus in mapa de acreditare de securitate/ MANIS

Soluția tehnică implementată (IDS)

Referințe:

ISO 27001: 9.1, A.12.4, A.12.6.1, A.15.2.1

NIST CSF: PR.DS-6, PR.DS-8, DE.AE-1, DE.AE-5, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3

[C112]. Evaluarea și monitorizarea vulnerabilităților. *OSE dezvoltă* ***un proces de identificare, clasificare, remediere și eliminare a vulnerabilităților****, în special în software și firmware.*

1. Pentru limitarea riscurilor de securitate și corectarea vulnerabilităților, OSE va implementa un ***program pentru managementul vulnerabilităților****, care poate include, fără a se limita la acestea:*

- instalarea unui patch;

- modificări în PONIS;

- reconfigurarea unui software (de exemplu, Firewall);

- educarea utilizatorilor despre social engineering.

Indicatori de control:

- **PEIREV** - proces de identificare, clasificare, remediere și eliminare a vulnerabilităților, în special în software și firmware, la nivelul rețelelor și sistemelor informatice
- **PGMAVU -** program pentru managementul vulnerabilităților în rețelele și sistemele informatice
- **ARNIS -** analiza riscurilor de securitate a rețelelor și sistemelor informatice, document elaborat la nivelul OSE, prin care sunt identificate elementele critice care stau la baza furnizării serviciului esențial și sunt identificate principalele riscuri în vederea gestionării și diminuării acestora

Implementarea procesului/administrativă:

Programul de management al vulnerabilităților presupune definirea un proces de identificare, clasificare, urmărire si remediere a acestora. Astfel, OSE va identifica vulnerabilitățile cu ajutorul unui software specializat pentru scanarea si detectarea vulnerabilităților. Ulterior, vulnerabilitățile vor fi clasificate in baza criticalitatii.

Criticalitatea este rezultatul unei formule dintre riscul calculat in ARNIS al activului vulnerabil si criticalitatea vulnerabilității așa cum este definita in industrie. In funcție de criticalitatea vulnerabilității, OSE va defini intervale de remediere de la data identificării (de exemplu nivel critic – 7 zile, nivel ridicat -14 zile, nivel mediul – 30 de zile). După clasificarea acestora, vulnerabilitățile vor fi alocate către proprietarii activelor pentru remediere. OSE va urmări remedierea acestora in intervalul stabilit si va asigura coordonarea echipei de securitate cu cea a echipelor de remediere in această perioadă pentru a asigura conformitatea.

OSE va dezvolta si implementa un set de proceduri pentru managementul vulnerabilităților (denumita in Normele tehnice PEIREV) cuprinzând in mod minimal următoarele detalii:

- legătura cu lista activelor, sistemelor și proceselor organizației (denumita in Normele tehnice LASPO);
- soluția tehnica folosita pentru identificarea vulnerabilităților si programul de identificare (intervale de scanare, intervale de raportare);
- soluția tehnica folosita pentru urmărirea remedierii si eliminării vulnerabilităților;
- procesul de scanare, analiza si raportare a vulnerabilităților către proprietarii activelor;
- procesul de stabilire a criticalității unei vulnerabilități si a intervalelor de timp de remediere;
- procesul de urmărire a remedierii si raportare către management;
- responsabilii pentru identificarea vulnerabilităților si coordonarea programului de remediere.

OSE va actualiza documentul ARNIS pe baza vulnerabilităților identificate si a statusului acestora. In baza unei evaluări de risc, OSE va implementa un sistem de management al excepțiilor. Excepțiile sunt vulnerabilități care nu pot fi remediate datorita configurației sistemului sau a vechimii sistemului care nu mai permite actualizări. Excepțiile sunt documentate in baza unei analize de risc efectuate in prealabil si trebuie sa conțină o data la care se așteaptă actualizarea sau înlocuirea sistemului.

Implementarea tehnică: configurarea unor soluții de tip ”vulnerability scanning” si de tip ticketing pentru urmărirea remedierii.

Probe:

Politici si proceduri formalizate cu privire la procesul de management al vulnerabilităților/ PEIREV

Dovezi privind funcționalitatea si implementarea PGMAVU

Analiza de risc a organizației din punct de vedere al riscurilor de securitate/ ARNIS

Referințe:

ISO 27001: 8.1, A.11.2.4, A.12.1.2, A.12.6, A.14.1.1, A 14, A.15.2.

NIST CSF: PR.MA-1, PR.MA-2, PR.IP-1, PR.IP-2, PR.IP-3, PR.IP-4, PR.IP-7, PR.DS-3, PR.DS-4, ID.SC-4:

Măsura de securitate: C12 - Înregistrarea evenimentelor

[C121]. Monitorizare evenimente. *OSE pune în aplicare un* ***sistem de înregistrare evenimente*** *la nivelul rețelelor și sistemelor informatice pentru evenimente legate de autentificarea utilizatorului, conturilor și gestionării drepturilor de acces, accesului la resurse, modificărilor regulilor NIS și funcționării rețelelor și sistemelor informatice.*

SIENIS ajută la detectarea incidentelor de securitate prin colectarea datelor de înregistrare.

Evenimentele înregistrate de SIENIS sunt ***timbrate*** *cu ajutorul surselor de timp sincronizate, centralizate și* ***arhivate*** *pentru o perioadă de cel puțin șase luni.*

Formatul de arhivare a evenimentelor permite ***cercetarea automată*** *a acestor evenimente.*

Indicator de control:

- **SIENIS** - sistem de înregistrare evenimente la nivelul rețelelor și sistemelor informatice
- **SIEM** - managementul monitorizării, cercetării și identificării rapide a principalelor cauze de afectare a securității, precum și ale încălcării politicilor de securitate
- **SCAJ** - sistem de corelație și analiză de jurnal

Implementarea procesului/administrativă:

Monitorizarea evenimentelor sta la baza managementului alertelor de securitate. Toate alertele de securitate sunt generate de reguli de alertare rezultate din analiza evenimentelor stocate in mediul IT al OSE. Astfel, dezvoltarea, operarea si întreținerea acestui sistem sunt vitale pentru a asigura detecția si intervenția in cazul unui incident de securitate cibernetica. Evenimentele sunt generate de către programele folosite de OSE si pot fi: date de autentificare, modificări ale

documentelor, modificări de software, erori de funcționare, etc. Aceste evenimente sunt centralizate într-o soluție de tip SIEM sau similar. Majoritatea sistemelor conțin funcționalitatea de a trimite aceste evenimente către o terța parte (SIEM sau similar) in mod automat.

OSE va asigura buna funcționare a fluxurilor de evenimente către SIEM. Întreruperea acestor fluxuri creează goluri in procesele de detecție. Daca nu sunt înregistrate evenimente nu pot fi generate alerte de securitate. Astfel, OSE va documenta procesul de mentenanța si intervenție in caz de întrerupere a fluxurilor, cat si timpii dedicați (SLA) de remediere in caz de întrerupere a acestora.

***Implementarea tehnică**:* o soluție de tip SIEM si soluții de gestionarea a fluxurilor de comunicare a evenimentelor dintre software-generator si SIEM.

Probe:

Evidenta implementării unui sistem de înregistrare a evenimentelor/ SIENIS

Evidenta implementării unei soluții tehnice de tip SIEM

Referințe:

ISO 27001: 7.5, A.12.1.1, A.16.1.1, A.16.1.2, A.16.1.3

NIST CSF: RS.CO-2, RS.CO-3, RS.CO-4, RS.CO-5, DE.DP-4:

[C122]. Sisteme de management. *În vederea apărării cibernetice a securității rețelelor și sistemelor informatice, OSE dezvoltă și implementează un* ***SIEM*** *(Security Information and Event Management) ca un set de instrumente care combină* ***SEM*** *(gestionarea evenimentelor de securitate) și* ***SIM*** *(gestionarea informațiilor de securitate).*

Indicator de control:

- **SIENIS** - sistem de înregistrare evenimente la nivelul rețelelor și sistemelor informatice
- **SMMEIS** - sistem de monitorizare și management al evenimentelor și incidentelor de securitate.
- **SIEM** - managementul monitorizării, cercetării și identificării rapide a principalelor cauze de afectare a securității, precum și ale încălcării politicilor de securitate

Implementarea procesului/administrativă:

Sistemul de management al evenimentelor si alertelor de securitate presupune procese de configurare si de mentenanța ale sistemului (SMMEIS). Procesele de mentenanța presupun monitorizarea fluxurilor de informații si a funcționalităților sistemului in parametri normali de funcționare. In cadrul procedurii pentru detectarea incidentelor de securitate (PRODAIS), OSE va documenta responsabilii cu administrarea, responsabilitățile acestora si timpii de remediere in caz de funcționare sub parametrii stabiliți. De asemenea, in cadrul aceleiași proceduri OSE definește perioade de revizuire a sistemului pentru a se asigura ca fluxurile de date sunt relevante si la zi in raport cu noile amenințări de securitate cibernetica. Administrarea presupune inclusiv mentenanța regulilor de alertare si a fluxurilor de alerte

Implementarea tehnică*:* o soluție de tip SIEM (de tip licența comercială, open source sau dezvoltată cu resurse propriii)

Probe:

Harta cartografica a sistemului si a fluxurilor de evenimente/ SICAE,

Evidenta implementării unor soluții tehnice de tip SIENIS & SIEM

Referințe:

ISO 27001: A.16.1.1, A.16.1.4, A.16.1, A.16.1.6, A.16.1.7

NIST CSF: ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, ID.SC-5, PR.IP-9, PR.IP-10, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.AN-5, RS.MI-1, RS.MI-2, RS.MI-3, RS.IM-1:, RS.IM-2, RS.CO-1, RS.CO-3, RS.CO-4, RS.CO-5, RS.RP-1, RC.RP-1, RS.CO-2:

Măsura de securitate: C 13 - Jurnalizarea și asigurarea trasabilității activităților în cadrul rețelelor și sistemelor de comunicații

[C131]. Jurnalizare și trasabilitate. *OSE pune în aplicare un* ***sistem de corelație și analiză de jurnal*** *care exploatează evenimentele înregistrate de SIENIS, pentru a detecta* ***evenimente susceptibile*** *care afectează securitatea rețelelor și sistemelor informatice. SCAJ ajută la detectarea incidentelor de securitate prin analizarea datelor de jurnal.*

SCAJ este instalat și funcționează pe un sistem informatic dedicat exclusiv în scopul detectării evenimentelor care ar putea afecta securitatea rețelelor și sistemelor informatice.

Indicator de control:

- **SIENIS** - sistem de înregistrare evenimente la nivelul rețelelor și sistemelor informatice
- **SCAJ** - sistem de corelație și analiză de jurnal

Implementarea procesului/administrativă:

OSE va dezvolta un proces de mentenanța si revizie a sistemului de corelație si analiza. Acest sistem este parte din sistemul de management al alertelor de securitate cibernetica agregat in sisteme de tip SIEM sau XDR. OSE desemnează un responsabil al procesului care verifica starea de funcționare a sistemului si îl actualizează ori de cate ori necesar.

Implementarea tehnică*:* o soluție de tip SIEM (de tip licența comerciala, open source sau dezvoltată cu resurse propriii)

Probe:

Evidenta implementării unui sistem de corelație si analiza de jurnal/ SCAJ

Evidenta implementării unei soluții tehnice de tip SIEM

Documente privind formalizarea si implementarea procesului de mentenanța si revizie a sistemului

Referințe:

ISO 27001: 9.1, 9.3, A.16.1.4, A.16.1.7

NIST CSF: ID.RA-4, ID.RA-5, PR.PT-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, DE.DP-3, DE.DP-4, DE.DP-5, PR.IP-7, RS.AN-1, RS.AN-5

2.4.2 Categoria de activități de securitate: C2 - Managementul incidentelor de Securitate

Măsura de securitate: C21 - Răspuns la incidente de securitate

[C211]. Fluxul incidentelor. *OSE creează, actualizează și pune în aplicare o* ***procedură pentru gestionarea, răspunsul și analiza incidentelor*** *care afectează funcționarea sau securitatea rețelelor și sistemelor informatice, în conformitate cu PONIS.*

Indicator de control:

- **PRORAI** - procedură pentru gestionarea, răspunsul și analiza incidentelor care afectează funcționarea sau securitatea rețelelor și sistemelor informatice

Implementarea procesului/administrativă:

OSE dezvolta si implementează o procedura pentru gestionarea, răspunsul si analiza incidentelor, denumita in Normele tehnice PRORAI, în care se va descrie procesul de management a incidentelor, împărțite pe etape:

- Planificare și pregătire - politici, planuri, proceduri, angajament la conducerea superioară;
- Detecție si sistem de raportare - monitorizează, detectează și raportează;
- Evaluare și decizie - analiză și decizie privind cursul acțiunii;
- Răspuns - izolare, eradicare, recuperare, rezolvare, închidere;
- Lecția învățată - îmbunătățiri.

In etapa de planificare, OSE definește rolurile si responsabilitățile de implementare si mentenanța a sistemului de detecție si răspuns. De asemenea, definește rolurile si responsabilitățile in monitorizarea si investigarea alertelor de securitate pentru a confirma daca alerta este de tip *false positive (incident neconfirmat)* sau *true positive (incident confirmat)*. Mai departe, OSE stabilește roluri si responsabilități in cazul unui incident confirmat de securitate cibernetica, procedura care va seta pașii de răspuns si persoanele implicate. După ce incidentul a fost rezolvat, părțile implicate vor organiza o sesiune de lecții învățate pentru a asigura creșterea rezilienței rețelei.

Implementarea tehnică*:*

O soluție de tip SIEM pentru sistemul de înregistrare al evenimentelor

O soluție de tip SIEM sau XDR pentru managementul alertelor de securitate cibernetica

Crearea si publicarea documentelor formale cu privire la managementul incidentelor, în intranetul OSE sau într-un sistem de management de documente

Probe:

Procedură pentru gestionarea, răspunsul și analiza incidentelor/ PRORAI,

Evidenta implementării unei soluții tehnice de tip SIEM si/sau soluția de tip XDR

Referințe:

ISO 27001: A.16.1.1, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7

NIST CSF: ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, ID.SC-5, PR.IP-9, PR.IP-10, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.AN-5, RS.MI-1,RS.MI-2, RS.MI-3, RS.IM-1, RS.IM-2, RS.CO-1, RS.CO-3, RS.CO-4, RS.CO-5, RS.RP-1, RC.RP-1, RS.CO-2:

[C212]. Monitorizarea incidentelor. *OSE trebuie să implementeze un* ***sistem de monitorizare și management al evenimentelor și incidentelor de securitate****, bazat cel puțin pe un senzor de detectare a intruziunilor la nivel de rețea care beneficiază de o sursă perpetuă de indicatori de compromitere și pe analiza logurilor de pe echipamentele sau stațiile de lucru critice pentru desfășurarea activității, în vederea identificării abaterilor de la* ***politicile de securitate și a intruziunilor****.*

Indicator de control:

- **SIDGI** - sistem informatic dedicat pentru gestionarea incidentelor

Implementarea procesului/administrativă:

Procesul de implementare din aceasta etapa se bazează pe implementarea adecvata a proceselor de la masurile C11- C212. Daca vreunul dintre elementele sistemului, precum fluxurile de evenimente si alerte, sistemul de corelare, sistemul de jurnalizarea sau sistemul de management al alertelor nu funcționează conform, OSE ar putea sa rateze evenimente de securitate importante si sa compromită rețeaua OSE.

Incidentele sunt gestionate in baza alertelor de securitate generate de echipamente (câteva exemple: NIDS, IAM, antivirus, firewall, etc) sau in baza raportărilor făcute de utilizatori (raportări de tip SPAM, phishing sau alte potențiale incidente detectate de utilizatori). OSE se asigura ca toate alertele de securitate sunt monitorizate si rezolvate in timp real de o echipa dedicata. Echipa poate fi proprie sau contractată printr-o terța parte.

Implementarea tehnică*:*

O soluție de tip SIEM/XDR.

Crearea si publicarea documentelor formale cu privire la managementul incidentelor, în intranetul OSE sau într-un sistem de management de documente

Probe:

Evidenta implementării unei soluții tehnice de tip SIEM sau XRD

Evidenta gestionarii alertelor de securitate conform procedurii pentru gestionarea, răspunsul și analiza incidentelor/ PRORAI

Evidenta fiabilității sistemului in privința gestionarii evenimentelor si alertelor

Referințe:

ISO 27001: A.16.1.1, A.16.1.4, A.16.1.5, A.16.1, A.16.1.7

NIST CSF: ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, ID.SC-5, PR.IP-9, PR.IP-10, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.AN-5, RS.MI-1,RS.MI-2, RS.MI-3, RS.IM-1, RS.IM-2, RS.CO-1, RS.CO-3, RS.CO-4, RS.CO-5, RS.RP-1

[C213]. Gestionarea incidentelor. *OSE pune în aplicare un* ***sistem informatic dedicat pentru gestionarea incidentelor****, pentru a depozita, printre altele,* ***evidența tehnică a analizei incidentelor****.*

OSE separă SIDGI de rețelele și sistemele informatice afectate de incident și păstrează ***registrele tehnice*** *aferente pentru o perioadă de cel puțin o jumătate de an.*

OSE ia în considerare, la proiectarea sistemului, ***nivelul de confidențialitate*** *al documentelor stocate.*

Indicator de control:

- **PRORAI** - procedură pentru gestionarea, răspunsul și analiza incidentelor care afectează funcționarea sau securitatea rețelelor și sistemelor informatice
- **SMMEIS** - sistem de monitorizare și management al evenimentelor și incidentelor de securitate.
- **SIDGI** - sistem informatic dedicat pentru gestionarea incidentelor

Implementarea procesului/administrativă:

Pentru a asigura integritatea si non repudierea datelor colectate in scopuri de securitate (evenimente si alerte) OSE va dezvolta sistemul de monitorizare si management (SMEIS) cat si sistemul de gestionare a incidentelor (SIDGI) într-o rețea separata logic de restul rețelei OSE, asigurând auditarea accesului la aceste resurse. OSE va documenta arhitectura in harta cartografica a sistemului si in cadrul procedurii de acces la documente si sisteme. Nu in ultimul rând, OSE va asigura ca

arhitectura sistemului permite analiștilor de securitate sa acceseze resurse pentru a izola un activ sau o porțiune de rețea in caz de incident.

***Implementarea tehnică**:*

Dezvoltarea unei subretele, separata logic de restul rețelei IT al OSE, unde vor fi instalate si configurate soluțiile de monitorizare, detecție si răspuns al incidentelor de securitate cibernetica. In aceasta subrețea vor fi configurate uneltele de tip SIEM/XDR sau sistemul de ticketing folosit pentru gestionarea alertelor si al incidentelor.

Probe:

Harta cartografica a sistemului

Dovezi privind implementarea soluțiilor tehnice de tip SIEM/XDR si/sau dovezi privind implementarea unei soluții tehnice de ticketing. Pentru ambele soluții tipuri de soluții si pentru orice alta soluție tehnica aleasă, se va face dovada documentarii incidentelor conform politicilor in vigoare.

Referințe:

ISO 27001: A.16.1.1, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7

NIST CSF: ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, ID.SC-5, PR.IP-9, PR.IP-10, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.AN-5, RS.MI-1,RS.MI-2, RS.MI-3, RS.IM-1, RS.IM-2, RS.CO-1, RS.CO-3, RS.CO-4, RS.CO-5, RS.RP-1, RC.RP-1, RS.CO-2:

Măsura de securitate: C22 Raport incidente de securitate

***[C221]. Raportarea incidentelor.** OSE creează, actualizează și implementează **o procedură pentru raportarea incidentelor de securitate**.*

Indicator de securitate:

- **PRORIS** - procedură pentru raportarea incidentelor de securitate

Implementarea procesului/administrativă:

OSE dezvolta un mecanism de raportare a incidentelor de securitate cibernetica. Volumul alertelor analizate, detalii privind fiabilitatea sistemului si fluxurile de evenimente si alerte, cat si detalii privind remedierea vor fi detaliate intr-un raport lunar prezentat către managerii de departament si/ sau conducerea executiva. Incidentele de securitate cibernetica confirmate vor fi documentate si raportate

către conducerea companiei si către DNSC. OSE va dezvolta o procedura pentru raportarea incidentelor (nu este obligatoriu să fie etichetată PRORIS) care va conține cel puțin:

- Pașii ce trebuie parcurși pentru raportarea unui incident;
- Părțile implicate pentru fiecare tip de raportare in parte;
- Rolurile și responsabilitățile părților implicate.

***Implementarea tehnică**:*

Documentarea incidentelor se poate efectua cu ajutorul SIEM/ XDR sau in cadrul aplicației de ticketing. Raportarea se va face respectând pașii din procedura pentru raportarea incidentelor de securitate/ PRORIS.

Crearea si publicarea documentelor formale cu privire la raportarea incidentelor de securitate, în intranetul OSE sau într-un sistem de management de documente

Probe:

Procedură pentru raportarea incidentelor de securitate/ PRORIS,

Documentarea incidentelor in cadrul SMMEIS.

Referințe:

ISO 27001: 7.5, A.12.1., A.16.1.1 , A.16.1.2, A.16.1.3

NIST CSF: RS.CO-2, RS.CO-3, RS.CO-4, RS.CO-5, DE.DP-4

Măsura de securitate: C23 Comunicarea cu ANRSI și CSIRT Național

***[C231]. Interconectare națională.** OSE se interconectează la serviciul de alertare și cooperare al DNSC care îi permite să ia notă, fără întârziere, de informațiile transmise de DNSC, ca CSIRT National, cu privire la incidente, vulnerabilități, amenințări și informări relevante.*

*OSE elaborează și implementează o **procedură de interconectare la serviciul de alertare și cooperare al DNSC**.*

OSE asigură monitorizarea permanentă a alertelor și solicitărilor primite prin acest serviciu ori prin celelalte modalități de contact.

Indicatori de securitate:

- **PRISAC** - procedură de interconectare la serviciul de alertare și cooperare al DNSC

Implementarea procesului/administrativă:

OSE va realiza procedura pentru interconectarea la serviciul de alertare și cooperare al DNSC (nu este obligatoriu să fie etichetată PRISAC) în conformitatea cu instrucțiunile DNSC (se va urmări situl DNSC). Procedura va conține, fără a se limita la, descrierea tehnica a soluției de interconectare, procesele de comunicare si transfer de informații si drepturile de acces la sistem.

Implementarea tehnică:

Sistemul de tip SIEM/XDR sau sistemul de ticketing va fi interconectat cu sistemul de raportare al incidentelor la nivel național. La data publicării ghidului, aceste specificații tehnice nu sunt disponibile.

Probe:

Procedură de interconectare la serviciul de alertare și cooperare al DNSC/PRISAC

Dovada interconectării sistemului de monitorizare și management al evenimentelor și incidentelor de securitate (SMMEIS) cu platforma națională de raportare a incidentelor de securitate cibernetica.

Referințe:

ISO 27001: 7.4, 7.5, A.6.1.3, A.6.1.4, A.8.2.2,

NIST CSF: RS.CO-2, RS.CO-3, RS.CO-4, RS.CO-5, DE.DP-4

[C232]. Responsabili NIS*. OSE nominalizează responsabili cu securitatea rețelelor și sistemelor informatice însărcinați cu monitorizarea mijloacelor de contact (responsabili NIS) și furnizează către DNSC, ANSRSI, datele de contact la zi ale acestora (numele și prenumele, funcțiile și departamentele din care fac parte, numere de telefon, adrese de e-mail etc.).*

OSE elaborează și actualizează permanent ***lista responsabililor NIS****.*

Indicatori de securitate:

- **LIRNIS -** lista responsabililor NIS

Implementarea procesului/administrativă:

Se va crea o lista responsabililor NIS, (denumita in Normele LIRNIS), care va conține elementele următoare :

- Datele de identificare ale responsabililor NIS (numele și prenumele, funcția și departamentul din care face parte, numărul de telefon, adresa de e-mail)
- Data numirii acestora.

Implementarea tehnică:

Crearea si publicarea documentului privind lista responsabililor NIS în intranetul OSE sau într-un sistem de management de documente.

Probe:

Lista responsabililor NIS/ LIRNIS, formalizata

Fișa postului

Referințe: Neaplicabil

[C233]. Gestionare informații primite de la DNSC. *OSE implementează o* ***procedură pentru gestionarea informațiilor primite și, după caz, a măsurilor de securitate adoptate pentru protejarea rețelelor și sistemelor informatice****.*

Indicatori de securitate:

- **PRIMSA** - procedură pentru gestionarea informațiilor primite și, după caz, a măsurilor de securitate adoptate pentru protejarea NIS

Implementarea procesului/administrativă:

DNSC, prin intermediul interconectării OSE cu sistemul național de raportare a incidentelor, va putea primi informații privind amenințări sau indicatori de compromis care pot fi implementați in rețeaua OSE pentru a creste gradul de reziliența a rețelei.

OSE va crea si implementa o procedură (nu este obligatoriu să fie etichetata PRIMSA; generic poate fi denumita și ”plan de comunicare”) care avea în vedere:

- Modul de diseminare si implementare a informațiilor primite de la CERT;
- Beneficiarii informațiilor;
- Canalele securizate prin care vor fi comunicate informațiile (în cazul informațiilor confidențiale);

- Acțiunile tehnice sau organizatorice luate de OSE in baza informațiilor primite.

Implementarea tehnică:

Crearea si publicarea procedurii pentru gestionarea informațiilor primite și, după caz, a măsurilor de securitate adoptate pentru protejarea NIS în intranetul OSE sau într-un sistem de management de documente

Capacitatea si dovezile de implementare a informațiilor primite in cadrul OSE (ex: blocarea de indicatori de compromis la nivel de firewall)

Probe:

Procedură pentru gestionarea informațiilor primite și, după caz, a măsurilor de securitate adoptate pentru protejarea NIS/ PRIMSA

Dovada interconectării cu serviciul de alertare si cooperare al DNSC si dovezi privind funcționarea in parametrii

Referințe:

ISO/IEC 27001: A.16.1.2,

NIST CSF: CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4.

2.5 Domeniul de securitate D: Reziliență

2.5.1 Categoria de activități de securitate D1 – Managementul continuității afacerii

Măsura de securitate D11 - Asigurarea disponibilității serviciului esențial și a funcționării rețelelor și sistemelor informatice

[D111]. Asigurarea disponibilității. *În conformitate cu PONIS, OSE definește o procedură privind managementul asigurării disponibilității serviciului esențial, în caz de incident de securitate cibernetică.*

Indicatori de control:

- **PRADE -** procedură privind managementul asigurării disponibilității serviciului esențial, în caz de incident de securitate cibernetică

Implementarea procesului/administrativă:

OSE va documentează, în cadrul unei proceduri privind managementul continuității afacerii, cel puțin următoarele:

- Implementarea unei structuri de management adecvate în cazul unui incident de securitate cibernetică ce poate afecta continuitatea afacerii;
- Modalități concrete de asigurare a personalului de răspuns la incident disponibil în cazul unui astfel de incident, care să aibă autoritatea necesară pentru a răspunde la incident, să fie responsabil pentru răspunsul la incidente, și să fie capabil sa răspundă, atât ca și capabilități personale, cât și ca acces fizic și la sisteme . Menționăm că competențele de răspuns la incident pot fi în interiorul organizației, sau pot exista aranjamente cu companii specializate în asigurarea răspunsului la incidente.

Procedura nu este obligatoriu să fie etichetată PRADE, așa cum este definita in Normele tehnice. Politica poate fi un document de sine stătător, sau ca parte a unui plan de continuitate a afacerii, dacă acesta există.

Riscurile acoperite prin această procedură trebuie să se regăsească printre riscurile identificate în secțiunea A1. Mai exact, în lista de riscuri identificate vor trebui incluse și riscurile de indisponibilitate a serviciului esențial în cazul unui incident de securitate.

Modalitatea de răspuns trebuie structurată sub forma unor planuri a căror scop este să readucă sistemele la starea inițială. Pentru ca aceste planuri să fie implementabile practic, OSE asigurata resurse umane, tehnice și nu în cele din urmă financiare, adecvate, aflate la dispoziția celor responsabili în caz de răspuns la incident de securitate cibernetică.

Validarea planurilor se realizează în mod normal prin testări periodice, de cele mai multe ori parțiale (foarte rare sunt cazurile în care, în cazul unor organizații mari, se fac teste complete de recuperare). Aceste testări pot include verificări ale planurilor (“desk-top review”), asamblări ale echipelor de gestionare a crizelor (“call tree exercises”) precum și teste de recuperare parțială sau totală.

Implementarea tehnică:

Crearea si publicarea documentelor formale/ procedurilor în intranetul OSE sau într-un sistem de management de documente, on line sau offline.

Soluțiile tehnice dedicate de tip back-up, atât pentru stocarea informației, cat si pentru restaurarea sistemului in caz de dezastru.

Probe:

Planuri de continuitate a afacerii

Planuri de gestionare a crizelor

Planuri de recuperare în caz de dezastru

Proceduri de răspuns la incidente

Referințe:

The BCI Good Practice Guidelines PP5 - Response Structure

ISF Standard of Good Practices BC1.2 - Business Continuity Programme

Măsura de securitate D12 - Managementul recuperării datelor în caz de dezastre

***[D121]. Recuperarea datelor**. În conformitate cu PONIS, OSE definește o procedură privind managementul recuperării datelor în caz de dezastre, precum și în caz de incidente severe de securitate cibernetică.*

Indicatori de control:

- **PROMRE -** procedură privind managementul recuperării datelor în caz de dezastre, precum și în caz de incidente severe de securitate cibernetică

Implementarea procesului/administrativă:

Modalitatea de recuperare a datelor în caz de dezastru este dependentă de soluțiile tehnice implementate precum și de modalitățile de backup existente. Procedurile de recuperare a datelor vor fi specifice tehnologiilor folosite (mașini fizice sau virtuale, sisteme de operare, aplicații, baze de date, medii cloud, echipamente de rețea, etc.)

Procedura va trebui să documenteze atât pașii pentru recuperarea datelor și sistemelor cât și informațiile necesare identificării resurselor (medii de backup, mașini fizice/virtuale, locații, subscripții cloud, etc.) fără a păstra datele de acces în aceste proceduri. Resursele pot fi identificate in baza implementării măsurii A11.

Implementarea tehnică: Dependentă de infrastructura tehnică. În mod generic acestea pot include site-uri alternative pentru stocare, instanța separata pentru backup în cazul compromiterii unor subscripții cloud, servicii de telecomunicații de backup, servere de rezervă.

Probe:

Procedura de recuperare a datelor în caz de dezastre și de incidente severe de securitate cibernetică, care să se aplice serviciilor esențiale

Rezultatele testelor de restaurare a sistemului la starea inițiala prin intermediul mediilor de stocare de tip back-up.

Referințe:

The BCI Good Practice Guidelines PP5 - Response Structure

ISF Standard of Good Practices BC1.2 - Business Continuity Programme

2.5.3 Categoria de securitate D2 - Managementul crizelor

Măsura de securitate: D21 Organizarea gestionării crizelor

[D211]. Organizarea gestionării crizelor cibernetice. OSE definește în PONIS sau separat o procedură privind organizarea gestionării crizelor în caz de incidente de securitate cibernetică pentru asigurarea continuității activităților organizaționale.

Indicatori de control:

- **PROCIS -** procedură privind organizarea gestionării crizelor în caz de incidente de securitate cibernetică pentru asigurarea continuității activităților organizaționale
- **PEGEC -** procese de gestionare a crizelor; documente prin care OSE stabilește procesele și modurile de implementare în caz de incidente de securitate cibernetică pentru asigurarea continuității activităților organizaționale

Implementarea procesului/administrativă:

Implementarea răspunsului pentru acest tip de crize trebuie să asigure o mobilizare rapidă a managementului și personalului tehnic (intern si extern, dacă este cazul) și un răspuns punctual coordonat.

Organizarea gestionării crizelor revine conducerii organizației, chiar dacă criza este de natură tehnologică. Motivul pentru care conducerea organizației trebuie să își asume un rol activ în planificarea și executarea răspunsului pentru orice criză este

că autoritatea formală și reală pentru luarea, implementarea deciziilor și alocarea sarcinilor rezidă cu aceștia. Delegarea luării deciziilor unui eșalon de management inferior sau către un nivel de execuție duce la blocaje și întârzieri semnificative în răspunsul la situația de criză.

Gestionarea crizelor conține următoarele elemente organizatorice:

- Stabilirea obiectivelor răspunsului la criză;
- Comunicarea internă în timpul crizelor - cu personal și management;
- Comunicarea externă în timpul crizelor - autorități (inclusiv CSIRT național), și, după caz, contractori, clienți, persoane vizate (conform GDPR), media, etc.
- Coordonarea echipelor de răspuns la incidente.

Implementarea tehnică: Pentru organizarea situațiilor de criză se pot face exerciții pregătitoare și de testare ce includ simularea asamblării echipelor de gestionare a crizelor („call trees"), revizuirea procesului în cadrul unor workshop-uri („Desk-top review") și simulări propriu**-zise ale situațiilor de criză și exerciții de recuperare în caz de dezastru.**

Probe:

Procedurilor de management al situațiilor de criză

Referințe:

The BCI Good Practice Guidelines PP5 - Response Structure

ISF Standard of Good Practices BC1.2 - Business Continuity Programme

Măsura de securitate: D22 Procesul de gestionare a crizelor

[D221]. Gestionarea crizelor cibernetice. *OSE definește în PONIS sau separat procesele de gestionare a crizelor pe care le va implementa în caz de incidente de securitate cibernetică pentru asigurarea continuității activităților organizaționale.*

Indicatori de control:

- **PEGEC -** procese de gestionare a crizelor; documente prin care OSE stabilește procesele și modurile de implementare în caz de incidente de securitate cibernetică pentru asigurarea continuității activităților organizaționale

Implementarea procesului/administrativă:

OSE documentează procese punctuale de gestionare a situațiilor de criză în caz de incidente de securitate cibernetică. Acestea pot include, printre altele:

- Planuri de răspuns la nivelul organizației;
- Identificarea/nominalizarea și activarea echipelor de răspuns la criză (in mod fizic sau virtual);
- Instrucțiuni pentru comunicarea în timpul crizelor;
- Comunicarea cu contractorii implicați în aceste procese;
- Liste cu persoane și locații;
- Acces la locații de recuperare, și echipamente pregătite pentru situațiile de criză;
- Liste cu proceduri de recuperare, și locațiile unde pot fi acestea accesate.

Implementarea tehnică

Modalitățile de comunicare în timpul crizelor sunt centrate în mod tradițional pe mesagerie mobilă și conferințe pregătite și configurate în centralele telefonice. În ziua de azi se folosesc cu preponderență în mod practic sistemele de mesagerie instant, ca un compromis între operativitate și securitate. Există soluții complementare dedicate care asigură comunicarea în timpul crizelor, cu facilități legate de înregistrarea răspunsurilor si deciziilor persoanelor implicate.

Probe:

Procesele de gestionare a crizelor, documentate

Referințe:

The BCI Good Practice Guidelines PP5 - Response Structure

ISF Standard of Good Practices BC1.2 - Business Continuity Programme

CAPITOLUL 3: INDICATORI DE EVALUARE A CONFORMITĂȚII[12]

Art. 6 din Normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale, din 09.11.2020 impune:

> ***[A141].*** *Indicatori de securitate. OSE stabilește o serie de indicatori de evaluare, pe baza cărora își evaluează conformitatea cu PONIS.*
>
> ***1.*** *Indicatorii de securitate se pot referi la: performanțele gestionării riscurilor; menținerea resurselor în condiții sigure; drepturile de acces ale utilizatorilor; autentificarea accesului la resurse; administrarea resurselor.*
>
> ***[A142].*** *Metode de evaluare a securității. OSE specifică pentru fiecare indicator metoda de evaluare folosită și, dacă este cazul, marja de incertitudine în evaluarea sa.*
>
> ***1.*** *Dacă un indicator se schimbă semnificativ în comparație cu evaluarea anterioară, operatorul identifică și specifică motivele.*
>
> ***(2)*** *Indicatori de control. IEC; MEIEC.*
>
> *IEC - indicatori de evaluare, pe baza cărora OSE își evaluează conformitatea cu PONIS*
>
> *MEIEC - metoda de evaluare a indicatorilor de conformitate*

Chiar dacă textul articolului este ambiguu când face referire la ”indicatori de securitate” și ulterior la ”indicatori de evaluare”, vom înțelege prin **indicatori de conformitate** un set de date care ajută la măsurarea obiectivă, cu referire la o anumită perioadă de timp, a evoluției acțiunilor întreprinse de OSE pentru a se conforma cerințelor minime de securitate precizate în Norme.

În continuare exemplificăm o serie de indicatori de evaluare a conformității. **Acești indicatori nu trebuie să se limiteze doar la subiectele menționate în Norme ci trebuie să evalueze conformitatea cu politica de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale**

PONIS trebuie să stabilească obiectivele strategice de securitate, să descrie guvernanța securității și să reflectă toate politicile specifice de securitate ale SMSI

[12] **Exemplele sunt traduse și adaptate după ISO 27004:2016 - Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation**

(procesul de acreditare de securitate, audit de securitate, criptografie, întreținere securitate, manipulare incidente etc.).

Operatorul de servicii esențiale trebuie să facă dovada că are și o *metoda de evaluare a indicatorilor de conformitate - MEIEC*

1. Analizarea și evaluarea riscurilor [A11] - Registrul riscurilor (RERO)

Descriptor IEC	**Descriere**
IdIEC	Definit de organizație, poate fi alfanumeric (de ex. IEC_01) sau mnemonic (de ex. IEC_RiscReg)
Descriere	Evaluează expunerea OSE la riscuri de securitate cibernetică
Formula/Calcul	• Numărul total de riscuri medii și mari • Numărul de riscuri medii și mari fără actualizarea stării în ultimul an/trimestru
Valoare țintă:	1
Dovadă implementare	RERO actualizat
Frecvența	Trimestrial/anual, în funcție de complexitatea rețelei OSE
Responsabilități(RACI)	– Responsabilii de risc execută (R) – Conducerea organizației este informată (I) – CISO/Responsabil NIS este responsabil (A)
Date de intrare	RERO
Format raportare	Grafice cu prezentarea tendințelor

2. Politica de securitate [A12] - PONIS

Descriptor IEC	**Descriere**
IdIEC	Definit de organizație, poate fi alfanumeric (de ex. IEC_02) sau mnemonic (de ex. IEC_RevPol)
Descriere	Procentul de politici revizuite
Formula/Calcul	Numărul de politici de securitate revizuite/Total politici de securitate*100
Valoare țintă:	100
Dovadă implementare	Istoricul reviziilor din pagina de gardă a politicilor sau lista politicilor revizuite
Frecvența	Anual
Responsabilități(RACI)	– Responsabilul de politică execută (R) – Conducerea organizației este informată (I) – CISO/Responsabil NIS este responsabil (A)
Date de intrare	Lista politicilor, plan de revizuire, pagina de gardă cu istoricul revizuirilor
Format raportare	Grafic/numeric

3. Testarea și evaluarea securității rețelelor și sistemelor informatice [A16] - ATECNIS, RATES

Descriptor IEC	**Descriere**
IdIEC	Definit de organizație, poate fi alfanumeric (de ex. IEC_03) sau mnemonic (de ex. IEC_PenTest)
Descriere	Procentul de rețele/sisteme informatice critice pentru care s- executat un test de penetrare și o evaluare a vulnerabilităților.
Formula/Calcul	Numărul de rețele/sisteme informatice critice pentru care s-a realizat un test de penetrare și o evaluare a vulnerabilităților // Numărul de rețele/sisteme informatice critice * 100
Valoare țintă:	100
Dovadă implementare	Rapoartele testelor de penetrare și evaluare a vulnerabilităților (RATES, ATECNIS) și numărul sistemelor/rețelelor critice
Frecvența	Anual
Responsabilități(RACI)	– Expert tehnic execută testul de penentrare(R) – Conducerea organizației este informată (I) – CISO/Responsabil NIS este responsabil (A)
Date de intrare	Inventarul activelor (LASPO), RATES, ACTENIS
Format raportare	Grafic/numeric

4. Conștientizarea și instruirea utilizatorilor [A18] - PGASP

Descriptor IEC	**Descriere**
IdIEC	Definit de organizație, poate fi alfanumeric (de ex. IEC_04) sau mnemonic (de ex. IEC_Instr)
Descriere	Procentul de angajați care au beneficiat de programe de instruire și conștientizare
Formula/Calcul	Numărul de angajați care au beneficiat de instruire SMSI/numărul total de angajați implicați în furnizarea serviciilor esențiale* 100 Numărul de angajați care au beneficiat de reînoirea cunoștințelor în ultimul an/ numărul total de angajați implicați în furnizarea serviciilor esențiale* 100
Valoare țintă:	90%
Dovadă implementare	PRISA
Frecvența	Anual
Responsabilități(RACI)	– Responsabil resurse umane execută programul de instruire și conștientizare (R) – Conducerea organizației este informată (I) – CISO/Responsabil NIS este responsabil (A)
Date de intrare	PRASA, PRISA
Format raportare	Reprezentare grafică

5.Managementul configurației rețelelor și sistemelor informatice [B11] -

Descriptor IEC	**Descriere**
IdIEC	Definit de organizație, poate fi alfanumeric (de ex. IEC_05) sau mnemonic (de ex. IEC_MngConfig)
Descriere	Procentul de echipamente configurate în conformitate cu procedurile aprobate.
Formula/Calcul	Numărul de dispozitive configurate corect/număr total de dispozitive* 100
Valoare țintă:	100%
Dovadă implementare	Rezultatul scanărilor cu instrumente software
Frecvența	Lunar
Responsabilități(RACI)	– Responsabil cu administrarea resurselor (R) – Conducerea organizației este informată (I) – CISO/Responsabil NIS este responsabil (A)
Date de intrare	LASPO, PRECDI, PEIREV, PGMAVU
Format raportare	Reprezentare grafică

6.Filtrarea traficului [B14] - PROFIT

Descriptor IEC	**Descriere**
IdIEC	Definit de organizație, poate fi alfanumeric (de ex. IEC_06) sau mnemonic (de ex. IEC_Trafic)
Descriere	Reguli pentru filtrarea traficului care nu sunt aplicate.
Formula/Calcul	Numărul regulilor de filtrare neaplicate.
Valoare țintă:	0
Dovadă implementare	Reguli de filtare existente la nivel de firewall
Frecvența	Semestrial/anual
Responsabilități(RACI)	– Administrator de rețea (R) – CIO este informat (I) – CISO/Responsabil NIS este responsabil (A)
Date de intrare	PROFIT, ARNIS
Format raportare	Numărul sau lista cu reguli neutilizate

7. Protecția împotriva malware [B16] - PRAPMA

Descriptor IEC	**Descriere**
IdIEC	Definit de organizație, poate fi alfanumeric (de ex. IEC_07) sau mnemonic (de ex. IEC_Malware)
Descriere	Numărul/procentul de sisteme afectate de malware
Formula/Calcul	Numărul de echipamente afectate de malware/total număr de echipamente
Valoare țintă:	0
Dovadă implementare	Monitorizarea sistemelor antimalware
Frecvența	Zilnic/săptămânal
Responsabilități(RACI)	– Administrator rețea/CISO (R) – Conducerea organizației este informată (I) – CISO/Responsabil NIS este responsabil (A)
Date de intrare	Soluția antimalware
Format raportare	Numărul de sisteme afectate, grupate pe tipuri de active (stații de lucru, laptop, server etc).

8. Managementul identificării și autentificării utilizatorilor [B31] – ECUPA, MEAUP

Descriptor IEC	**Descriere**
IdIEC	Definit de organizație, poate fi alfanumeric (de ex. IEC_08) sau mnemonic (de ex. IEC_UtilAcc)
Descriere	Procentul de sisteme din infrastructura critică pentru care se realizează periodic revizuirea drepturilor de acces.
Formula/Calcul	Numărul de sisteme din infrastructura critică pentru care drepturile de acces se revizuiesc periodic /Total număr de sisteme din infrastructura critică * 100
Valoare țintă:	0
Dovadă implementare	Sistemul administrare conturi, PAM, IAM,mail
Frecvența	După fiecare modificare a situației unui angajat și cel puțin trimestrial
Responsabilități(RACI)	– Responsabil proces/risc execută (R) – CISO/Administrator sistem este informat (I) – CISO/Responsabil NIS este responsabil (A)
Date de intrare	LASPO, LICA, LICPA,
Format raportare	Grafic

9. *Asigurarea protecției fizice a rețelelor și sistemelor informatice [B51] - PRASI*

Descriptor IEC	**Descriere**
IdIEC	Definit de organizație, poate fi alfanumeric (de ex. IEC_09) sau mnemonic (de ex. IEC_SecFiz)
Descriere	Eficiența sistemului de control fizic al accesului.

Formula/Calcul	0 lipsă sistem control acces fizic 1 Acces fizic pe bază de cheie 2 Acces fizic pe bază de card și jurnalizare 3 Acces fizic pe bază de card, PIN și jurnalizare 4 Acces biometric
Valoare țintă:	2
Dovadă implementare	Inspectare elemente sisteme: • Existența sistemului de de control acces • Utilizare carduri de acces/coduri PIN • Funcționalități de jurnalizare • Acces biometric
Frecvența	Anual
Responsabilități(RACI)	– Responsabil proces/risc execută (R) – Audit intern este informat (I) – CISO/Responsabil NIS este responsabil (A)
Date de intrare	PRASI,
Format raportare	Grafic

10. Răspuns la incidente de securitate [C21]– PRORAI, SMMEIS, SIDGI

Descriptor IEC	**Descriere**
IdIEC	Definit de organizație, poate fi alfanumeric (de ex. IEC_10) sau mnemonic (de ex. IEC_Siem)
Descriere	Măsoară eficiența gestionării evenimentelor și informațiilor de securitate
Formula/Calcul	Se definesc categoriile de incidente de securitate și intervalele de timp țintă în care incidentele de securitate ar trebui rezolvate pentru fiecare categorie de incidente de Securitate. Se compară numărul de incidente pentru care timpul de rezolvare depășește intervalele de timp țintă ale categoriei
Valoare țintă:	0
Dovadă implementare	Rapoarte SIEM, SIENIS
Frecvența	Lunar
Responsabilități(RACI)	– Responsabil administrare SIEM (R) – Responsabil incidente de securitate/CISO (I) – CISO/Responsabil NIS este responsabil (A)
Date de intrare	SIEM, PRORAI, SMMEIS, SIDGI
Format raportare	Grafic

Anexa 1: Alinierea cerințelor de securitate cu standarde internaționale

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
Analizarea și evaluarea riscurilor	A11	Analiza riscurilor de securitate	A111	ARNIS	I01	6 Planificare 8 Funcţionare 9.3 Revizuire de către management 10 Îmbunătăţire A.8.1.1 Inventarul resurselor A.12.6.1 Managementul vulnerabilităţilor tehnice A.18.2.1 Revizuirea independentă a securităţii informaţiei	ID.GV-4 ID.RA-1, 3, 4, 5, 6 ID.RM-1, 2, 3 RS.IM-1, 2 ID.SC-1, 2 PR.IP 12 RC.IM-1, 2 ID.AM-1, 2, 4, 5 DE.CM-8 RS.MI-3 RS.AN-5	SR 7.8
		Gestionarea riscurilor de securitate	A112	MEGRE	I02			
		Evaluarea riscurilor de securita	A113	RERO	I03			

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
Realizarea planurilor de securitate. Politica de securitate	A12	Politica de securitate	A121	PONIS	I04	4.3 Determinarea domeniului de aplicare a sistemului de management al securităţii informaţiei 4.4 Sistem de management al securităţii informaţiei 5.1 Conducere şi angajament 5.2 Politică 5.3 Roluri organizaţionale, responsabilităţi şi autoritate 6.2 Obiectivele de securitate a informaţiei şi planificarea obţinerii lor 9.3 Revizuire de către management A.5.1.1 Politici de securitate a informaţiei A.5.1.2 Revizuirea politicii de securitate a informaţiei A.6.1.1 Roluri şi responsabilităţi privind securitatea informaţiei A.7.2.1 Responsabilităţile managementului	ID.GV-1, 2, 3, 4 ID.BE-1, 2 3, 4 PR.AT-2, 3, 4, 5 DE.DP-1 ID.AM-6	
				SMSI	I05			
		Implementarea politicii de securitate	A122	RAIPOD	I06			

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
						A.18.1.1 Identificarea legislaţiei aplicabile şi a cerinţelor contractuale A.18.1.2 Drepturile de proprietate intelectuală A.18.2.2 Conformitatea cu politicile şi standardele de securitate		
Acreditarea de securitate	A13	Acreditarea rețelelor și sistemelor informatice	A131	PEANIS	I07	6.1 Acţiuni referitoare la riscuri şi oportunităţi 8 Funcţionare 9.2 Audit intern 10.1 Neconformitate şi acţiune corectivă A.12.1.1 Proceduri de operare documentate A.12.7.1 Mijloacele de control al auditului sistemelor informaţionale	ID.RA-1, 3, 4, 6 ID.RM-1, 2, 3 ID.SC -1 RS.IM-1, 2 PR.IP-7, 12 PR.PT-1 DE.CM-8 RS.MI-3	SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12
				DANIS	I08			
				MANIS	I09			
		Revizuirea validării acreditării de securitate	A132	DANIS	I08			
				MANIS	I09			
Indicatori de	A14	Indicatori de securitate	A141	IEC	I10	6.2 Obiectivele de securitate a	ID.AM-5	SR 3.4

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
securitate		Metode de evaluare a securității	A142	MEIEC	I11	informaţiei şi planificarea obţinerii lor 7.1 Resurse 7.2 Competenţă 9 Evaluarea performanţei A.12.1.3 Managementul capacităţii	ID.RM-2, 3 PR.IP-7,8 PR.DS-4 ID.BE-5	SR 4.1
Verificarea conformității cu privire la securitatea informației. Audit de securitate	A15	Evaluarea conformității	A151	PRECAS	I12	6 Planificare 8 Funcţionare 9.2 Audit intern 9.3 Revizuire de către management 10 Îmbunătăţire A.5.1.2 Revizuirea politicii de securitate a informaţiei A.12.7.1 Mijloacele de control al auditului sistemelor informaţionale A.18.2 Revizuirea securităţii informaţiei	ID.GV-3, 4 ID.RA-1, 3, 4, 5, 6 ID.RM-1, 2, 3 DE.CM-8 DE.DP-5 ID.SC-4 PR.AC-1 PR.PT-1 PR.IP-7, 12 RS.IM-1, 2 RC.IM-1, 2	SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12
				RAEC	I13			
		Auditul de securitate	A152	RASNIS	I14			
Testarea și evaluarea	A16	Testare și evaluare	A161	RATES	I15			

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
securității rețelelor și sistemelor informatice		securitate		ATECNIS	I16			
Asigurarea securității personalului	A17	Asigurarea securității personalului	A171	PRASP	I17	4.1 Înţelegerea organizaţiei şi contextului ei 4.2 Înţelegerea nevoilor şi aşteptărilor părţilor interesate 5.3 Roluri organizaţionale, responsabilităţi şi autoritate 6.2 Obiectivele de securitate a informaţiei şi planificarea obţinerii lor 7 Suport 9.1 Supraveghere, măsurare, analiză şi evaluare A.6.1.1 Roluri şi responsabilităţi privind securitatea informaţiei A.6.1.2 Separarea sarcinilor A.7 Securitatea resurselor umane A.9.3 Responsabilităţile	ID.AM-6 ID.GV-2, 3 RS.CO-1, PR.IP-7, 11 DE.DP-1 PR.AT-1, 2, 3, 4, 5	SR 1.1, SR 1.2 SR 1.4, SR 1.5, SR 1.9, SR 2.1 SR 2.1 SR 5.2
				FP	I18			
				CIM	I19			
				CCM	I20			
		Verificarea înțelegerii responsabilităților	A172	ISA	I21			
				VCSA	I22			
				COSE	I23			
Conștientizarea și instruirea utilizatorilor	A18	Instrumente de conștientizare	A181	INCEA	I24			
		Instruirea și prezentarea securității	A182	PRASA	I25			
				PRISA	I26			

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
						utilizatorului		
Gestionarea activelor	A19	Inventarierea și gestionarea activelor	A191	LASPO	I27	A.8.1.1 Inventarul resurselor A.12.6.1 Managementul vulnerabilităţilor tehnice A.18.2.1 Revizuirea independentă a securităţii informaţiei 8.2 Clasificarea informaţiei		
				PRECDI	I28			
Cartografierea ecosistemului	A21	Descrierea ecosistemului	A211	SICAE	I29	4.1 Înţelegerea organizaţiei şi contextului ei 4.2 Înţelegerea nevoilor şi aşteptărilor părţilor interesate 4.3 Determinarea domeniului de aplicare a sistemului de management al securităţii informaţiei 5.2 Politică 8.1 Planificare operaţională şi control operaţional	ID.AM-3, 4, 6 ID.BE-1, 2, 4 ID.AM-6	
				LIRIE	I30			
Relațiile ecosistemului	A22	Stabilirea relațiilor ecosistemului	A221	PROSRE	I31	4.2 Înţelegerea nevoilor şi aşteptărilor părţilor interesate	RS.CO-4, 5 ID.RM-1	SR 1.13 SR 2.6

Măsuri de securitate [MS]		Cerințe de securitate [CS]		Indicatori de control [IC]		Corespondenta standarde ISO/NIST/ISA		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
		Acorduri la nivel de serviciu	A222	LASMA	I32	5.2 Politică 7.4 Comunicare 7.5 Informaţie documentată 8.1 Planificare operaţională şi control operaţional 9.3 Revizuire de către management A.5.1.1 Politici de securitate a informaţiei A.7.1.2 Cerinţe şi condiţii de angajare A.7.2 În timpul perioadei de angajare A.7.3 Încetarea şi schimbarea contractului de muncă A.12.7 Consideraţii privind auditul sistemelor informaţionale A.13.2 Transferul informaţiei A.14.2.7 Dezvoltare externalizată A.15 Relaţii cu furnizorii A.18.1.1 Identificarea legislaţiei aplicabile şi a	ID.GV 2 ID.SC-1, 2, 3, 4,5 RC.CO-3	SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12 SR 3.1 SR 3.5 SR 3.8 SR 4.1 SR 4.2 SR 4.3 SR 5.1 SR 5.2 SR 5.3 SR 6.1 SR 6.2 SR 7.1 SR 7.6

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
						cerinţelor contractuale		
Managementul configurației rețelelor și sistemelor informatice	B11	Arhitectura NIS	B111	SANIS	I33	4.3 Determinarea domeniului de aplicare a sistemului de management al securităţii informaţiei A.6.2.1 Politică referitoare la dispozitivele mobile A.8.3.1 Managementul suporturilor amovibile A.12.1 Proceduri operaţionale şi responsabilităţi A.12.5 Controlul software-ului operaţional A.12.6.2 Restricţii la instalarea de software A.13.1.2 Securitatea serviciilor de reţea A.14.1 Cerinţe de securitate pentru sistemele informaţionale A.14.2.1 Politica de dezvoltare securizată A.14.2.2 Proceduri de control	PR.IP-1, 2, 3 DE.AE-1 PR.PT-3	SR 1.13 SR 2.3 SR 2.4 SR 2.6 SR 3.1 SR 3.3 SR 3.4 SR 3.5 SR 3.8 SR 4.1 SR 4.2 SR 4.3 SR 5.1 SR 5.2 SR 5.3 SR 7.1 SR 7.2 SR 7.6 SR 7.8
		Instalarea echipamentelor și serviciilor	B112	ARNIS	I01			
				MANIS	I09			
Managementul suporților de memorie externă	B12	Suporți de memorie externă	B121	PRUSME	I34			
				RESME	I35			

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
						al modificării sistemelor A.14.2.3 Revizuirea tehnică a aplicaţiilor după modificări aduse platformelor operaţionale A.14.2.4 Restricţii privind modificările asupra pachetelor software A.14.2.5 Principiile ingineriei sistemelor securizate A.14.2.6 Mediul de dezvoltare securizat		
Segregarea și segmentarea rețelelor și sistemelor informatice	B13	Segregarea și segmentarea	B131	PROSES SANIS	I36 I33	A.12.1.4 Separarea mediilor de dezvoltare, testare şi funcţionare A.13.1 Managementul securităţii reţelei	PR.DS-5, 7 PR.PT-3, 4 PR.AC- 5, 6	SR 1.13 SR 2.6 SR 3.1 SR 3.5 SR 3.8 SR 4.1 SR 4.2 SR 4.3 SR 5.1 SR 5.2 SR 5.3

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
								SR 7.1 SR 7.6
Filtrarea traficului	B14	Filtrarea fluxurilor	B141	PROFIT	I37	8.1 Planificare operaţională şi control operaţional A.13.1 Managementul securităţii reţelei A.13.2.1 Politici şi proceduri pentru transferul informaţiei A.13.2.2 Acorduri de transfer al informaţiei	PR.PT-4 PR.AC-3, 5 PR.DS-2 DE.CM-6, 7	SR 1.13 SR 2.6 SR 3.1 SR 3.5 SR 3.8 SR 4.1 SR 4.2 SR 4.3 SR 5.1 SR 5.2 SR 5.3 SR 7.1 SR 7.6
				ARNIS	I01			
Asigurarea protecției produselor și serviciilor aferente rețelelor și sistemelor informatice	B15	Asigurarea protecției criptografice	B151	PRAPC	I38	A.10.1 Mijloace de control referitoare la criptografie A.18.1.5 Reglementări privind măsurile criptografice	ID.GV-3 PR.DS-1, 2, 5, 6, 8 PR.PT-4	SR 5.2
		Managementul cheilor de criptare	B152	MACC	I39			
Protecția împotriva	B16	Protecție malware	B161	PRAPMA	I40	A.12.2.1 Mijloace de control		

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
malware						împotriva malware-ului		
Administrarea conturilor	B21	Conturi de administrare	B211	LICA	I41	A.9.2.3 Managementul drepturilor de acces privilegiat A.9.2.5 Revizuirea drepturilor de acces ale utilizatorului A.9.2.6 Retragerea sau adaptarea drepturilor de acces A.12.4.3 Jurnale ale activităţilor administratorului şi operatorului	PR. AC-1, 4, 7 PR.AT-2,4	SR 1.1 SR 1.2 SR 1.3 SR 1.4 SR 1.5 SR 1.7 SR 1.8 SR 1.9 SR 2.1
Administrarea rețelelor și sistemelor informatice	B22	Utilizarea sistemelor de administrare	B221	PRUSIA	I42	A.9.3.1 Utilizarea informaţiei secrete de autentificare A.9.4 Controlul accesului la sisteme şi aplicaţii A.12.1.4 Separarea mediilor de dezvoltare, testare şi funcţionare A.12.4.3 Jurnale ale activităţilor administratorului şi operatorului	PR.AC-1, 3, 4, 6, 7 PR.DS-5,6, 7 PR.AT-2, 3, 4 PR.PT-4	SR 1.1 SR 1.2 SR 1.3 SR 1.4 SR 1.5 SR 1.7 SR 1.8 SR 1.9 SR 1.10 SR 2.1 SR 5.2 SR 6.1
				PONIS	I04			
		Parole administrare	B222	JIERU	I43			
				PPSIA	I44			

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
Managementul accesului de la distanță	B23	Lucrul la distanță	B231	PROLD	I45	6.2.2 Lucrul la distanţă		
				PRAPC	I38			
Managementul identificării și autentificării utilizatorilor	B31	Identificarea utilizatorilor	B311	ECUPA	I46	A.9.1 Cerinţe de afaceri pentru controlul accesului A.9.3 Responsabilităţile utilizatorului A.9.4.1 Restricţionarea accesului la informaţie A.9.4.2 Proceduri securizate de conectare A.9.4.3 Sistem de management al parolelor	PR.AC-1, 4,6, 7 PR.DS-5	SR 1.1 SR 1.2 SR 1.3 SR 1.4 SR 1.5 SR 1.6 SR 1.7 SR 1.8 SR 1.9 SR 1.10 SR 1.11 SR 1.12 SR 1.13 SR 2.1 SR 2.2 SR 2.3 SR 2.4 SR 2.5 SR 2.6 SR 2.7
				ARNIS	I01			
				MANIS	I09			
		Autentificarea utilizatorilor	B312	MEAUP	I47			

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
								SR 5.2
Managementul drepturilor de acces	B32	Acordarea drepturilor de acces	B321	PONIS	I04	A.9.2 Managementul accesului utilizatoruluit A.9.4.4 Utilizarea programelor utilitare privilegiate A.9.4.5 Controlul accesului la codul sursă al programelor	ID.AM-5,6 PR.AC-1, 4, 6, 7 PR.DS-5 PR.PT-3	SR 1.1 SR 1.2 SR 1.3 SR 1.4 SR 1.5 SR 1.7 SR 1.8 SR 1.9 SR 1.10 SR 2.1
				LICPA	I48			
				LICA	I41			
		Verificarea conturilor privilegiate	B322	SIVMOC	I49			
Mentenanța rețelelor și sistemelor informatice	B41	Menținere securitate	B411	PROMNIS	I50	7.5.3 Controlul informaţiei documentate 8.1 Planificare operaţională şi control operaţional 10.1 Neconformitate şi acţiune corectivă A.11.2.4 Întreţinerea echipamentelor A.12.1.2 Managementul schimbărilor A.12.6.1 Managementul	PR.MA-1, 2 PR.IP-1, 2, 3,4, 7, PR.DS-3, 4 ID.SC-4	SR 3.1 SR 3.3 SR 3.4 SR 3.8 SR 6.1 SR 7.6
		Actualizare resurse	B412	PRORUVI	I51			
				PONIS	I04			
				MANIS	I09			
		Protejare resurse	B413	PRAPC	I38			

Măsuri de securitate [MS]		Cerințe de securitate [CS]		Indicatori de control [IC]		Corespondenta standarde ISO/NIST/ISA		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
						vulnerabilităţilor tehnice A.14.1.1 Analiza şi specificarea cerinţelor de securitate a informaţiei A 14.2 Securitatea în procesele de dezvoltare şi de suport A.15.2.2 Gestionarea schimbărilor serviciilor furnizorilor		
Sisteme control industrial. SCADA - Monitorizare, control și achiziții de date	B42	Sisteme de control industriale	B421	CEISC	I52	4 Contextul organizaţiei 5.2 Politică 5.3 Roluri organizaţionale, responsabilităţi şi autoritate 7 Suport 8 Funcţionare 9.1 Supraveghere, măsurare, analiză şi evaluare A.6.1.1 Roluri şi responsabilităţi privind securitatea informaţiei A.8.1.1 Inventarul resurselor A.8.2.3 Manipularea resurselor A.9 Controlul accesului	ID.BE-1, 2, 3, 4, ID.AM-1, 2, 4, 6 ID.GV-2 ID.SC-1, 2, 3, 4, 5 PR.AC -5 PR.PT-4	SR 1.10 SR 1.13 SR 2.1 SR 2.2 SR 2.3 SR 2.4 SR 2.5 SR 2.6 SR 2.7 SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12
		Limitarea accesului	B422	ANISMS	I53			

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
						A.11 Securitatea fizică şi a mediului de lucru A.12 Securitatea operaţiunilor A.14 Achiziţia, dezvoltarea şi mentenanţa sistemelor A.15 Relaţii cu furnizorii A.17 Aspecte ale securităţii informaţiei pentru managementul continuităţii afacerii		SR 3.1 SR 3.2 SR 3.3 SR 3.4 SR 3.5 SR 3.8 SR 3.9 SR 4.1 SR 4.2 SR 4.3 SR 5.1 SR 5.2 SR 5.3 SR 5.4 SR.6.1 SR 6.2 SR 7.1 SR 7.2 SR 7.3 SR 7.4 SR 7.6 SR 7.8

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
Asigurarea protecției fizice a rețelelor și sistemelor informatice	B51	Acces la resurse	B511	PRASI	I54	A.8.1 Responsabilitatea pentru resurse A.11 Securitatea fizică şi a mediului de lucru	ID.AM-1, 4 DE.CM-2, 3, 6 PR.IP-5, 6, PR.AC-2, 3 PR.DS-3 PR.PT-2,5	SR 1.13 SR 2.6 SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12 SR 4.2 SR 5.2 SR 7.8
Managementul vulnerabilităților și alertelor de securitate	C11	Fluxul alertelor de securitate	C111	PRODIS	I55	9.1 Supraveghere, măsurare, analiză şi evaluare A.12.2 Protecţie împotriva malware-ului A.12.4 Înregistrare şi supraveghere A.12.6.1 Managementul vulnerabilităţilor tehnice A.15.2.1 Supravegherea şi revizuirea serviciilor furnizorilor	PR.DS-6, 8 DE.AE-1,5 DE.CM-1, 2, 3, 4, 5, 6 7 DE.DP – 1, 2, 3, PR.PT-1	SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12 SR 3.1 SR 3.3 SR 3.4 SR 3.8 SR 3.9 SR 5.1 SR 5.2 SR 5.4
				SIENIS	I56			
				MANIS	I09			
		Evaluarea și monitorizarea vulnerabilităților	C112	PEIREV	I57			
				PGMAVU	I58			
				ARNIS	I01			

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
								SR 6.1 SR 6.2
Înregistrarea evenimentelor	C12	Monitorizare evenimente	C121	SIENIS	I56	9.1 Supraveghere, măsurare, analiză şi evaluare A.12.4 Înregistrare şi supraveghere A.14.1.2 Securizarea serviciilor aplicaţiilor în reţelele publice A.15.2.1 Supravegherea şi revizuirea serviciilor furnizorilor A.18.1.3 Protejarea înregistrărilor	ID.RA-1 ID.SC-1 PR.MA-1, 2 DE.CM- 1, 2, 3, 6, 7 DE.AE – 3 RS.MI-3 PR.PT-1	SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12 SR 3.9 SR 6.1 SR 6.2
		Sisteme de management	C122	SIEM	I59			
Jurnalizarea și asigurarea trasabilității activităților în cadrul rețelelor și sistemelor informatice	C13	Jurnalizare și trasabilitate	C131	SCAJ	I44	9.1 Supraveghere, măsurare, analiză şi evaluare 9.3 Revizuire de către management A.16.1.4 Evaluarea şi decizia asupra evenimentelor de securitate a informaţiei A.16.1.7 Colectarea probelor	ID.RA-4, 5, PR.PT-1 DE.AE – 2,3,4, DE.DP-3,4,5 PR.IP-7 RS.AN-1, 5	SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12 SR 3.9 SR 6.1 SR 6.2

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
Răspuns la incidente de securitate	C21	Fluxul incidentelor	C211	PRORAI	I60	A.16.1.1 Responsabilităţi şi proceduri A.16.1.4 Evaluarea şi decizia asupra evenimentelor de securitate a informaţiei A.16.1.5 Răspunsul la incidente de securitate a informaţiei A.16.1.6 Învăţarea din incidentele de securitate a informaţiei A.16.1.7 Colectarea probelor	ID.RA- 3, 4, 5, 6 ID.SC-5 PR.IP-9, 10 RS.AN-1, 2, 3, 4, 5 RS.MI-1, 2, 3 RS.IM-1, 2 RS.CO-1, 3, 4, 5 RS.RP-1 RC.RP-1 RC.CO-2	SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12 SR 3.9 SR 5.1 SR 5.2 SR 5.4 SR 6.1 SR 6.2
		Monitorizarea incidentelor	C212	SMMEIS	I61			
		Gestionarea incidentelor	C213	SIDGI	I62			
Raport incidente	C22	Raportarea incidentelor	C221	PRORIS	I63	7.5 Informaţie documentată A.12.1.1 Proceduri de operare documentate A.16.1.1 Responsabilităţi şi proceduri A.16.1.2 Raportarea evenimentelor de securitate a informaţiei A.16.1.3 Reportarea slăbiciunilor de securitate a	RS.CO - 2, 3, 4, 5 DE.DP-4	SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12 SR 3.9 SR 6.1 SR 6.2

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
						informaţiei		
Comunicarea cu Autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice (ANSRSI) și CSIRT Național	C23	Interconectare națională	C231	PISAC	I64	7.4 Comunicare 7.5 Informaţie documentată A.6.1.3 Contactul cu autorităţile A.6.1.4 Contactul cu grupuri speciale de interese A.8.2.2 Etichetarea informaţiei	RS.CO - 2, 3, 4, 5 DE.DP-4	SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12 SR 3.9 SR 6.1 SR 6.2
		Responsabili NIS	C232	LIRNIS	I65			
		Gestionare informații primite de la DNSC	C233	PRIMSA	I66			
Asigurarea disponibilității serviciului esențial și a funcționării rețelelor și sistemelor informatice	D11	Asigurarea disponibilității	D111	PRADE	I67	9.3 Revizuire de către management 10.2 Îmbunătăţire continuă A.5.1.2 Revizuirea politicii de securitate a informaţiei A.11.2.4 Întreţinerea echipamentelor A.17.1 Continuitatea securităţii informaţiei A.17.2 Redundanţe	ID.RM-1, 2, 3 RP.IP-4, 7, 9, 10 RS.IM- 2 RC.IM-1, 2 RC.RP-1 RC.CO-1,2,3 PR.PT-5 PR.DS-4 ID.BE-5 ID.SC-5	SR 2.8 SR 3.3 SR 5.2 SR.6.1 SR 7.1, SR 7.2 SR 7.3 SR 7.4
Managementul recuperării datelor în	D12	Recuperarea datelor	D121	PROMRE	I68	A.17.2 Redundanţe	ID.BE-5 PR.PT-5 PR.IP-9, 10	SR 5.2 SR 7.1

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
caz de dezastre							PR.DS-4 RC.IM-1, 2 RC.RP-1	SR 7.2
Organizarea gestionării crizelor	D21	Organizarea gestionării crizelor cibernetice	D211	PROCIS	I69	5.3 Roluri organizaţionale, responsabilităţi şi autoritate A.6.1.1 Roluri şi responsabilităţi privind securitatea informaţiei A.11.2.4 Întreţinerea echipamentelor A.17.1 Continuitatea securităţii informaţiei	PR.DS-4 PR.IP-10 ID.BE-5	SR 3.3 SR 7.1 SR 7.2
Procesul de gestionare a crizelor	D22	Gestionarea crizelor cibernetice	D221	PEGEC	I70	7.4 Comunicare 9.3 Revizuire de către management 10.2 Îmbunătăţire continuă A.5.1.2 Revizuirea politicii de securitate a informaţiei A.6.1.3 Contactul cu autorităţile A.11.2.4 Întreţinerea echipamentelor	RC.CO-1, 2, 3 RC.RP-1 RS.IM-1, 2 ID.SC-5 PR.IP-4, 9, 10 PR.PT-5	SR 2.8 SR 3.3 SR.6.1 SR 7.1 SR 7.2 SR 7.3 SR 7.4

Măsuri de securitate [MS]		**Cerințe de securitate [CS]**		**Indicatori de control [IC]**		**Corespondenta standarde ISO/NIST/ISA**		
Denumire	**ID**	**Denumire**	**ID**	**Denumire**	**ID**	**ISO 27001**	**NIST CSF**	**ISA/IEC 62443**
						A.17.1 Continuitatea securităţii informaţiei		

Anexa 2: Listă standarde

ISO/IEC 27001:2013. Tehnologia informației - Tehnici de securitate - Sisteme de gestionare a securității informațiilor – Cerințe.

ISO/IEC 27002:2013. Tehnologia informației - Tehnici de securitate - Cod de practică pentru controale de securitate a informațiilor.

ISO/IEC 27003:2017. Tehnologia informației - Tehnici de securitate - Sisteme de gestionare a securității informațiilor - Ghid.

ISO/IEC 27004:2016. Tehnologia informației - Tehnici de securitate - Managementul securității informației - Monitorizare, măsurare, analiză și evaluare.

ISO/IEC 27005:2018. Tehnologia informației - Tehnici de securitate - Managementul riscului pentru securitatea informațiilor.

ISO/IEC 27010:2015. Tehnologia informației - Tehnici de securitate - Managementul securității informațiilor pentru comunicații intersectoriale și interorganizaționale.

ISO/IEC 27013:2015. Tehnologia informației - Tehnici de securitate - Ghid privind implementarea integrată a ISO/IEC 27001 și ISO/IEC 20000-1.

ISO/IEC 27014:2013. Tehnologia informației - Tehnici de securitate - Guvernarea securității informațiilor.

ISO/IEC 20000-1:2018. Tehnologia informației - Managementul serviciilor - Partea 1: Cerințe de sistem de gestionare a serviciilor.

ISO/IEC 21827:2008. Tehnologia informației - Tehnici de securitate - Ingineria securității sistemelor - Modelul maturității capabilității® (SSE-CMM®).

ISO/IEC/IEEE 12207:2017. ISO/IEC/IEEE 12207:2017. Ingineria sistemelor și a software-ului - Procese ale ciclului de viață software.

ISO/IEC 10181-2:1996. ISO/IEC 10181-2:1996. Tehnologia informației - Interconectare sisteme deschise - Cadre de securitate pentru sisteme deschise: Cadru de autentificare.

ISO/IEC 10181-3:1996. ISO/IEC 10181-3:1996. Tehnologia informației - Interconectare sisteme deschise - Cadre de securitate pentru sisteme deschise: Cadru de control al accesului.

C 19790:2012. ISO/IEC 19790:2012 Tehnologia informației - Tehnici de securitate - Cerințe de securitate pentru module criptografice.

ISO/IEC 11770-1:2010. ISO/IEC 11770-1:2010. Tehnologia informației - Tehnici de securitate - Management cheie - Partea 1: Cadru.

ISO/IEC 11770-5:2011. SO/IEC 11770-5:2011. Tehnologia informației - Tehnici de securitate - Management cheie - Partea 5: Managementul cheie de grup.

ISO/IEC 27032:2012. ISO/IEC 27032:2012. Tehnologia informației - Tehnici de securitate - Linii directoare pentru securitatea cibernetică.

ISO/IEC 27033-1:2015. SO/IEC 27033-1:2015. Tehnologia informației - Tehnici de securitate - Securitatea rețelei - Partea 1: Prezentare generală și concepte.

ISO/IEC 27033-2: 2012. ISO/IEC 27033-2:2012. Tehnologia informației - Tehnici de securitate - Securitatea rețelei - Partea 2: Linii directoare pentru proiectarea și implementarea securității rețelei.

ISO/IEC 27033-3:2010. ISO/IEC 27033-3:2010. Tehnologia informației - Tehnici de securitate - Securitatea rețelei - Partea 3: Scenarii rețea de referință - Amenințări, tehnici de proiectare și probleme de control.

ISO/IEC 27033-4: 2014. ISO/IEC 27033-4: 2014. Tehnologia informației - Tehnici de securitate - Securitate rețea - Partea 4: Securizarea comunicațiilor între rețele folosind gateway-uri de securitate.

ISO/IEC 27033-5: 2013. ISO/IEC 27033-5: 2013. Tehnologia informației - Tehnici de securitate - Securitate rețea - Partea 5: Securizarea comunicațiilor prin rețele folosind rețele virtuale private (RVP).

ISO/IEC 27033-6:2016. Tehnologia informației - Tehnici de securitate - Securitate rețea - Partea 6: Securizarea accesului la rețeaua IP wireless.

ISO/IEC 27034-1:2011. Tehnologia informației - Tehnici de securitate - Securitatea aplicațiilor - Partea 1: Prezentare generală și concepte.

ISO/IEC 27034-5:2017. Tehnologia informației - Tehnici de securitate - Securitatea aplicațiilor - Partea 5: Structura datelor de protocoale și securitatea aplicațiilor.

TR 103 305-1 V3.1.1 (2018-09). CYBER; Controale critice de securitate pentru o apărare cibernetică eficientă; Partea 1: Controalele critice de securitate.

TR 103 305-2 V2.1.1 (2018-09). CYBER; Controale critice de securitate pentru o apărare cibernetică eficientă; Partea 2: Măsurare și audit.

TR 103 305-3 V2.1.1 (2018-09). CYBER; Controale critice de securitate pentru o apărare cibernetică eficientă; Partea 3: Implementarea sectorului de servicii.

TR 103 305-4 V2.1.1 (2018-09). CYBER; Controale critice de securitate pentru o apărare cibernetică eficientă; Partea 4: Mecanisme de facilitare.

TR 103 305-5 V1.1.1 (2018-09). CYBER; Controale critice de securitate pentru o apărare cibernetică eficientă; Partea 5: Îmbunătățirea confidențialității.

TR 103 304 V1.1.1 (2016-07). CYBER; Protecția informațiilor personale (PII) în serviciile mobile și cloud.

TS 103 307 V1.3.1 (2018-04). CYBER; Aspecte de securitate pentru interfețele LI și RD.

TR 103 331 V1.2.1 (2019-09). CYBER; Schimb de informații amenințate structurate.

TR 103 369 V1.1.1 (2016-07). CYBER; Proiectare cerințe de ecosistem.

TR 103 370 V1.1.1 (2019-01). Ghid practic introductiv la standardele tehnice pentru confidențialitate.

TR 103 303 V1.1.1 (2016-04). CYBER; Măsuri de protecție pentru ICT (tehnologia informației și comunicațiilor) în contextul infrastructurii critice.

TS 103 458 V1.1.1 (2018-06). CYBER; Aplicarea criptării bazate pe atribute (ABE) pentru protecția PII și a datelor cu caracter personal pe dispozitive IoT, WLAN, cloud și servicii mobile - Cerințe la nivel înalt.

TS 103 487 V1.1.1 (2016-04). CYBER; Cerințe de securitate de bază privind funcțiile sensibile pentru NFV (virtualizarea funcției de rețea) și platformele conexe.

TR 103 308 V1.1.1 (2016-01). CYBER; Linie de bază de securitate privind interceptarea legală (LI) și datele păstrate (RD) pentru virtualizarea funcției de rețea (NFV) și platformele conexe.

TR 103 306 V1.4.1 (2020-03). CYBER; Ecosistemul securității cibernetice globale.

TR 103 309 V1.1.1 (2015-08). CYBER; Protecție implicită - tehnologie de securitate a platformei.

TR 103 305 V1.1.1 (2015-05). CYBER; Controale critice de securitate pentru o apărare cibernetică eficientă.

GS ISI 007 V1.1.1 (2018-12). Indicatori de securitate a informațiilor (ISI); Linii directoare pentru construirea și exploatarea unui centru securizat de operațiuni de securitate (SOC).

GS ISI 008 V1.1.1 (2018-06). Indicatori de securitate a informațiilor (ISI); Descrierea unei abordări generale de gestionare a informațiilor de securitate și evenimente (SIEM) la nivelul întregii organizații.

EG 203 310 V1.1.1 (2016-06). CYBER; Impactul informaticii cuantice asupra securității sistemelor de tehnologia informațiilor și comunicațiilor (ICT); Recomandări privind continuitatea activității și selectarea algoritmului.

ANSI/ISA 18.2:2016 Managementul sistemelor de alarmă pentru procesul industrial.

ISA 62443-1-1:2007 Securitate pentru sisteme de automatizare și control industrial. Partea 1-1: Terminologie, concepte și modele.

ISA 62443-2-1:2009. Securitate pentru sisteme de automatizare și control industrial. Partea 2: Stabilirea unui program de securitate a sistemelor de automatizare industrială și control.

ANSI/ISA 62443-3-3:2013 Securitate pentru sisteme de automatizare și control industrial. Partea 3-3: Cerințe de securitate a sistemului și niveluri de securitate.

FIPS PUB 140-2 Cerințe de securitate pentru modulele criptografice.

Institutul Național de Standarde și Tehnologie (NIST)

FIPS PUB 200 Cerințe minime de securitate pentru informații federale și sisteme de informații.

SP 800-30 Ghid managementul riscului pentru sistemele de tehnologie a informației.

SP 800-53, Revizia 4, Controale de securitate și confidențialitate pentru sisteme informaționale federale și organizații.

SP 800-150 Ghid pentru schimbul de informații despre amenințarea cibernetică.

SP 800-181 Inițiativa națională pentru educația în domeniul securității cibernetice (NICE). Cadrul forței de muncă pentru securitate cibernetică.

SP 1800-14 Protejarea integrității rutării pe Internet: validarea originii rutelor Protocolului BGP.

SP 1800-12 Certificate de verificare PIV derivate.

SP 1800-5 Managementul activelor IT.

SP 1800-4 Securitatea dispozitivelor mobile: platforme cloud și hibrid.

Cadru pentru îmbunătățirea securității cibernetice a infrastructurii critice, versiunea 1.1

IEC 62443-4-2:2019, Securitate pentru sisteme de automatizare și control industrial - Partea 4-2: Cerințe tehnice de securitate pentru componentele IACS.

IEC 62443-4-1:2018, Securitate pentru sisteme de automatizare și control industrial - Partea 4-1: Cerințe de securitate pentru dezvoltarea vieții produsului.

IEC 62443-2-1:2010, Rețele de comunicații industriale - Securitatea rețelelor și a sistemului - Partea 2-1: Stabilirea unui program de securitate a sistemului de automatizare și control industrial.

IEC TS 62443-1-1:2009, Rețele de comunicații industriale - Securitatea rețelei și a sistemului - Partea 11: Terminologie, concepte și modele.

IEC 62443-2-1:2010, Rețele de comunicații industriale - Securitatea rețelei și a sistemului - Partea 2-1: Stabilirea unui program de securitate a sistemului de automatizare și control industrial.

API STD 1164 Securitatea controlorului și supravegherea achiziției de date (SCADA) în domeniul conductelor.

COBIT® 2019 Cadru: Introducere și metodologie.

COBIT 5 pentru securitatea informațiilor.

Modelul de afaceri pentru securitatea informațiilor (BMIS).

CRAMM Versiunea 5.1 Ghid de utilizare.

Model de maturitate al managementului securității informațiilor (O-ISM3).

Controale CIS, Versiunea 7.1.

Centrul pentru Securitatea Internetului

Manualul de examinare al FFIEC.

Managementul serviciilor IT (ITIL) v3/v4

Cadru de evaluare a amenințărilor, a activelor și a vulnerabilității critice din punct de vedere operațional (OCTAVE)

CIP Versiunea 5

Securitatea informațiilor general acceptate.

Cele zece cele mai mari riscuri de securitate pentru aplicații web.

Anexa 3: Legislație

1) 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.

https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016L1148

2) Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică).

https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32019R0881

3) Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.

http://legislatie.just.ro/Public/DetaliiDocument/209670

4) Ordonanță de Urgență nr. 119 din 22 iulie 2020 pentru modificarea și completarea Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.

http://legislatie.just.ro/Public/DetaliiDocument/228369

5) Propunere de Directivă privind măsurile pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune, de abrogare a Directivei (UE) 2016/1148.

https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0014.02/DOC_1&format=PDF

6) Anexa la propunerea de Directivă privind măsurile pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune, de abrogare a Directivei (UE) 2016/1148.

https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0014.02/DOC_2&format=PDF

7) HG nr.963/2020 pentru aprobarea Listei serviciilor esențiale.

http://legislatie.just.ro/Public/DetaliiDocument/233193

8) HG nr. 976/2020 privind aprobarea valorilor de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor şi sistemelor informatice ale operatorilor de servicii esenţiale.

http://legislatie.just.ro/Public/DetaliiDocument/233298

9) HG nr. 1003/2020 NORME TEHNICE de stabilire a impactului incidentelor pentru categoriile de operatori de servicii esențiale și furnizori de servicii digitale.

http://legislatie.just.ro/Public/DetaliiDocument/235108

10) Ordinul nr. 600/2019 privind aprobarea Normelor metodologice de organizare și funcționare a Registrului operatorilor de servicii esențiale.

http://legislatie.just.ro/Public/DetaliiDocument/215629

11) Ordinul nr. 599/2019 privind aprobarea Normelor metodologice de identificare a operatorilor de servicii esențiale și furnizorilor de servicii digitale.

http://legislatie.just.ro/Public/DetaliiDocument/216121

12) Ordinul nr. 601/2019 pentru aprobarea Metodologiei de stabilire a efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale.

http://legislatie.just.ro/Public/DetaliiDocument/216151

12) Ordinul nr. 1323/2020 pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale.

http://legislatie.just.ro/Public/DetaliiDocument/233775

13) Ordinul nr. 559/2021 559 privind aprobarea Regulamentului pentru atestarea și verificarea auditorilor de securitate cibernetică.

http://legislatie.just.ro/Public/DetaliiDocument/240988

14) Decizia nr. 88/2020 privind aprobarea Listei standardelor și specificațiilor europene și internaționale.

http://legislatie.just.ro/Public/DetaliiDocument/226520