Standard ocupațional

Specialist în proceduri şi instrumente de securitate a sistemelor informatice

În sectorul: **Tehnologia informației, comunicații, poştă**

Cod:.

Data aprobării: 16.10.2008

Denumire document electronic:

Versiunea: 0

Data de revizuire preconizată: octombrie 2010

Inițiatorul standardului: Centrul de Pregătire în Informatică – CPI-S.A.

Standardul a fost elaborat în cadrul proiectului **PHARE / 2005/ 017-553.04.02.02.01. 810 "Elaborarea de standarde ocupaționale pentru domeniul tehnologiilor informației".**

Coordonatorul echipei de redactare a standardului ocupațional: ing. **Cecilia Târâcă**, consultant în informatică, evaluator de competențe profesionale certificat de CNFPA – Centrul de Pregătire în Informatică CPI-S.A.

Echipa de redactare:
Mihaela Tudose, economist – cibernetică, formator, formator de formatori, evaluator de competențe profesionale certificat de CNFPA - Centrul de Pregătire în Informatică CPI-S.A.
Eugenia Alexandra Mihaela Aldica, matematician- informatică, formator, formator de formatori, evaluator de competențe profesionale certificat de CNFPA - Centrul de Pregătire în Informatică CPI-S.A.

Verificatorul standardului ocupațional: ing. Nica Gălbenuşi

Redactorii calificării: **Mihaela Tudose; Eugenia Alexandra Mihaela Aldica**

Denumirea analizei ocupaționale: Specialist în proceduri şi instrumente de securitate a sistemelor informatice

Data elaborării analizei ocupaționale: mai 2008

Responsabilitatea pentru conținutul acestui standard ocupațional şi al calificărilor bazate pe acest standard ocupațional revine Comitetului sectorial Tehnologia informației, Comunicații, Poştă.

Data validării: 3 octombrie 2008

Comisia de validare:

Preşedinte: Gheorghe Şerban

Membrii: Remus Tudorică

Ștefania – Carmen Dimofte

Descrierea ocupației

Specialistul în proceduri[1] şi instrumente[2] pentru securitatea sistemelor informatice[3] este persoana responsabilă cu găsirea şi implementarea celor mai potrivite măsuri şi mijloace pentru protejarea sistemelor informatice, astfel încât informația cu care operează organizația să fie sigură şi corectă. Specialistul răspunde oficial de dezvoltarea, analiza, evaluarea şi implementarea politicii de securitate a informației[4] într-o organizație. Se consideră că un sistem informatic cuprinde: calculatoare, sisteme de transmitere a datelor, alte componente hardware, sisteme de operare, aplicații şi componente software, date prelucrate precum şi personalul implicat în introducerea, păstrarea, prelucrarea şi extragerea informațiilor. Tehnologia Informației şi Comunicații (prescurtat IT&C sau TIC) cuprinde setul de instrumente tehnice ce includ echipamentele hardware, componentele software, rețelele de calculatoare, echipamentele de comunicații şi standardele asociate lor. Este cadrul folosit pentru obținerea, distribuirea, păstrarea şi folosirea informației. Specialistul în proceduri şi instrumente pentru securitatea sistemelor informatice are competențe legate de: asigurarea protecției informației, detectarea şi evaluarea vulnerabilităților şi a riscului, folosirea tehnologiilor adecvate pentru asigurarea securității rețelelor de comunicații, a celor de calculatoare, a echipamentelor şi a componentelor software de orice fel, indiferent de specificul informațional al organizație. Protecția sistemelor informatice este asigurată prin: prevenirea oricăror acțiuni îndreptate împotriva funcționarii corecte a sistemelor informatice, prin identificarea vulnerabilităților, reducerea numărului şi a pagubelor ce pot apărea ca efect al atacurilor materializate ca urmare a breşelor de securitate generate de vulnerabilități.

Specialistul in proceduri si instrumente de securitate a sistemelor informatice:

elaborează şi aplică elemente din programul de securitate, inclusiv cele referitoare la securitatea fizică a datelor, asigură confidențialitatea informațiilor şi disponibilitatea lor pentru persoanele în drept să le obțină şi să le folosească;

identifică si evaluează vulnerabilitățile sistemului informatic, identifică amenințările potențiale, evaluează şi prioritizează pierderile şi acțiunile îndreptate către reducerea amenințărilor si a pierderilor de orice fel;

găseşte răspunsurile la violările de securitate identificate şi raportate;

proiectează politici si proceduri de securitate aplicabile sistemului informatic;

elaborează ghiduri de bună practică legate de cerințele de securitate ale sistemului informatic şi de măsurile necesare pentru protejarea sistemului;

aplică standardele de securitate pentru rețele şi calculatoare şi validează din punctul de vedere al securității sistemul informatic (soluția IT&C aflată in funcțiune);

monitorizează / supraveghează aplicarea măsurilor de securitate proiectate pentru protejarea bunurilor fizice, a aplicațiilor şi a altor produse software, a datelor şi colecțiilor de date față de utilizarea neautorizată;

analizează şi revizuieşte amenințările, vulnerabilitățile, politicile, procedurile şi instrumentele legate asigurarea securității sistemului informatic;

elaborează rapoarte legate de asigurarea securității sistemului informatic, de gradul de aplicare a măsurilor de securitate stabilite, de vulnerabilitățile cunoscute şi asumate.

---

[1] Prin procedură se înțelege metoda de rezolvare a unei probleme, defalcată în etape succesive.

[2] Instrumentul este sistemul tehnic pentru cercetarea, observarea, măsurarea sau controlul unor mărimi şi este folosit pentru îndeplinirea unei acțiuni sau atingerea unui scop.

[3] Sistemul informatic este sistemul bazat pe TIC ce permite: introducerea, stocarea, prelucrarea si extragerea informațiilor.

[4] Informația = ştire, veste, comunicare, lămurire, un mesaj primit şi înțeles.

Activitatea specialistului în proceduri şi instrumente pentru securitatea sistemelor informatice poate fi considerată ca laborioasă, de mare întindere şi complexitate şi de mare răspundere. Informațiile sunt esențiale pentru organizații: informațiile sigure şi corecte permit desfăşurarea normală a activității unei organizații şi oferă încredere în relațiile cu clienții şi partenerii.

Principalele activități ale specialistului în proceduri şi instrumente pentru securitatea sistemelor informatice sunt legate de:

- Elaborarea inventarului informațiilor şi al bunurilor care au legătură cu informația, inclusiv identificarea proprietarului (deținătorului) informației, responsabil cu aplicarea strictă a măsurilor de securitate;
- Clasificarea informațiilor după gradul de protecție specifică necesară;
- Stabilirea procedurilor de copiere, păstrare, transmitere, distrugere, salvare, restaurare, prelucrare pentru fiecare categorie (clasă) de informații identificată în organizație;
- Elaborarea documentelor privitoare la strategia şi obiectivele de securitate ale organizației şi la cadrul organizațional de aplicare;
- Construirea modelului amenințărilor şi al vulnerabilităților cu care se confruntă organizația şi stabilirea criteriilor pentru evaluarea importanței riscurilor;
- Stabilirea legăturilor dintre amenințări, vulnerabilități, probabilitatea de materializare, pierderi potențiale, riscuri şi construirea pe această bază a tabelului riscurilor ce pot afecta activitatea şi dezvoltarea normală a organizației;
- Elaborarea planului de management al riscurilor, al acțiunilor de prevenire şi de reacție după materializarea amenințării / vulnerabilității, precum şi elaborarea planului măsurilor de securitate aplicabile;
- Definitivarea politicii de securitate a organizației ce va conține măsuri de securitate defalcate pentru fiecare post de lucru (rol îndeplinit în organizație). Măsurile sunt aplicabile la nivelul resurselor umane, mediului de lucru, comunicațiilor şi operațiunilor efectuate în organizație, controlului accesului, achiziționării, dezvoltării şi întreținerii componentelor hardware şi software, al managementului incidentelor de securitate şi al continuării activităților organizației.
- Proiectarea procedurilor de testare / verificare a aplicării măsurilor de securitate în organizație, respectiv evaluarea conformității rezultatelor cu obiectivele din strategia de securitate a organizației;
- Elaborarea planului de implementare a măsurilor de securitate, a celui de testare periodică a reacției la incidente previzibile; stabilirea persoanelor responsabile cu implementarea măsurilor de securitate;
- Elaborarea planului de comunicare (de alertă) şi răspuns la apariția incidentelor sau la suspiciunea apariției unui incident, inclusiv a planului de identificare a atacului, atacatorului şi de acumulare a dovezilor;
- Proiectarea machetei jurnalelor / formularelor pentru: raportarea incidentelor identificate şi a răspunsurilor, documentarea detaliată a incidentelor, identificarea erorilor şi a deficiențelor de funcționare ;
- Elaborarea codului de conduită în vederea asigurării securității informației în organizație, a ghidului de aplicare a măsurilor de securitate; organizarea sesiunilor de instruire şi antrenare a personalului pentru aplicarea procedurilor de securitate.

Principalele responsabilități ale *specialistului în proceduri*[5] *şi instrumente*[6] *pentru securitatea sistemelor informatice* sunt:

Identificarea cerințelor de securitate a informației

Proiectarea procedurilor de securitate a informației

[5] Prin procedură se înțelege metoda de rezolvare a unei probleme, defalcată în etape succesive.

[6] Instrumentul este sistemul tehnic pentru cercetarea, observarea, măsurarea sau controlul unor mărimi şi este folosit pentru îndeplinirea unei acțiuni sau atingerea unui scop.

Elaborarea programului de implementare a securității informației

Revizuirea modelului amenințărilor şi al vulnerabilităților

Instruirea personalului

Informația este considerată o resursă importantă a organizațiilor. Informația poate fi stocată pe hârtie, electronic, poate fi transmisă prin poştă, transmisă prin mijloace electronice, prezentată pe filme sau comunicată în timpul unei conversații. Securitatea informației se obține prin acțiuni de protecție față de o gamă largă de amenințări cu scopul de a asigura continuitatea activității organizației, minimizarea riscului apariției şi manifestării unor evenimente nedorite şi maximizarea investiției şi oportunităților organizației. Securitatea informației se obține prin implementarea unui set adecvat de politici şi proceduri specifice.

Informațiile şi resursele (bunurile) care au legătură cu informația pot fi: baze de date, fişiere de date, contracte, acorduri, documentații, informații rezultate din cercetare, manuale de utilizare, specificații de realizare, specificații tehnice de orice fel, materiale folosite pentru instruirea personalului, proceduri operaționale şi ajutătoare, planuri curente şi cele legate de continuarea activității (afacerii), arhive şi informații arhivate, dovezi de audit, resurse software (programe / aplicații, sisteme de operare, programe utilitare, instrumente pentru dezvoltarea şi testarea aplicațiilor, jurnale de evenimente, jurnale de erori, registrele care consemnează operații efectuate şi stări constatate), resurse hardware (echipamente, inclusiv echipamentele mobile, mijloace / medii de comunicații).

Securitatea informației înseamnă protecția în fața amenințărilor identificate şi pentru care a fost evaluat riscul materializării, manifestării acestora.

Față de complexitatea atribuțiilor ce îi revin specialistului în proceduri şi instrumente pentru securitatea sistemelor informatice, considerăm că practicarea cu succes a acestei ocupații necesită vaste cunoştințe teoretice şi deprinderi practice, după cum urmează:

- solide cunoştințe de hardware si software: arhitecturi de calculatoare, sisteme de operare, sisteme de fişiere, permisiuni de acces, privilegii, restricții, baze de date, aplicații diverse;
- rețele de calculatoare: topologii LAN, WAN, topologii VLAN, principii de securitate a rețelelor, servere, proceduri şi instrumente de autentificare, conectarea în rețea, managementul serviciilor director de resurse, interconectarea rețelelor, echipamente de interconectare, segmentarea rețelelor, firewall, conectivitatea la Internet, protocoale, infrastructură specifică, servicii de rețea, comunicații sigure;
- managementul riscului, vulnerabilități, amenințări; politici, proceduri, instrumente pentru: detectarea intruşilor şi intruziunilor, protecția față de atacurile asupra sistemului informatic, păstrarea integrității şi confidențialității datelor.

În plus, specialistul are nevoie de: gândire logică, abilități de analiză, interpretare, prezentare de informații, uşurință ţn scrierea de rapoarte, corespondență comercială, manuale, ghiduri, uşurință in rezolvarea problemelor, atenție distributivă, posibilitatea de a lucra sub presiune, abilități de comunicare şi persuasiune, capacitatea de a lucra in condiții de stres.

Unitățile de competențe cheie	**Cod de referință:**
Unitatea 1: **Comunicare în limba oficială** Unitatea 2: **Comunicare în limbi străine** Unitatea 3: **Competențe de bază în matematică, ştiință, tehnologie** Unitatea 4: **Competențe informatice** Unitatea 5: **Competența de a învăța** Unitatea 6: **Competențe sociale şi civice**	
Unitățile de competențe generale	**Cod de referință:**
Unitatea 1: **Aplicarea prevederilor legale referitoare la sănătatea şi securitatea în muncă şi în domeniul situațiilor de urgență** Unitatea 2: **Aplicarea normelor de protecție a mediului** Unitatea 3: **Aplicarea procedurilor de calitate**	
Unitățile de competenta specifice	**Cod de referință:**
Unitatea 1:**Identificarea cerințelor de securitate a informației** Unitatea 2:**Proiectarea procedurilor de securitate** Unitatea 3:**Elaborarea programului de implementare a securității informației** Unitatea 4: **Revizuirea modelului amenințărilor şi al vulnerabilităților** Unitatea 5: **Instruirea personalului**	

Unitatea 1 - Aplicarea prevederilor legale referitoare la securitatea şi sănătatea în muncă şi în domeniul situațiilor de urgență **(unitate generală)**			Coduri de referință
Descrierea unității de competență: Unitatea cuprinde cunoştințele şi deprinderile necesare practicantului în vederea aplicării corecte a prevederilor legale referitoare la sănătatea, securitatea în muncă şi situațiile de urgență în scopul evitării producerii accidentelor, acordării de prim ajutor şi intervenției în cazul situațiilor de urgență.			**NIVELUL UNITĂȚII: 2**
Elemente de competență	**Criteriile de realizare din punctul de vedere al deprinderilor practice necesare**	**Criteriile de realizare din punctul de vedere al cunoştințelor necesare**	**Criteriile de realizare din punctul de vedere al atitudinilor necesare**
1. Transpune în practică prevederile legale referitoare la sănătatea şi securitatea în muncă	1.1. Însuşirea normelor referitoare la sănătatea şi securitatea în muncă este realizată prin participarea la instruiri periodice, pe teme specifice locului de muncă. 1.2. Echipamentul de lucru şi protecție specific activităților de la locul de muncă este asigurat conform prevederilor legale. 1.3. Mijloacele de protecție şi de intervenție sunt verificate, în ceea ce priveşte starea lor tehnică şi modul de păstrare, conform cu recomandările producătorului şi adecvat procedurilor de lucru specifice. 1.4. Situațiile de pericol sunt identificate şi analizate în scopul eliminării imediate. 1.5. Situațiile de pericol care nu pot fi eliminate imediat sunt raportate persoanelor abilitate în luarea deciziilor.	Persoana supusă evaluării demonstrează că ştie şi înțelege: • NSSM şi pentru situații de urgență. • Legislație şi proceduri de lucru specifice locului de muncă. • Specificul locului de muncă.	• Situațiile de pericol sunt identificate şi analizate cu atenție; • Situațiile de pericol, care nu pot fi eliminate imediat, sunt raportate cu promptitudine persoanelor abilitate; • Raportarea factorilor de risc este făcută pe cale orală sau scrisă; • Înlăturarea factorilor de risc este făcută cu responsabilitate; • În caz de accident este contactat imediat personalul specializat şi serviciile de urgență; • Măsurile de prim ajutor sunt aplicate cu promptitudine şi responsabilitate, cu antrenarea întregii echipe.

2. Reduce factorii de risc	2.1. Identificarea factorilor de risc este realizată în funcție de particularitățile locului de muncă. 2.2. Raportarea factorilor de risc este făcută conform procedurilor interne. 2.3. Înlăturarea factorilor de risc este făcută conform reglementărilor în vigoare.		
3. Respectă procedurile de urgență şi de evacuare	3.1. Accidentul este semnalat cu promptitudine personalului specializat şi serviciilor de urgență. 3.2. Măsurile de evacuare în situații de urgență sunt aplicate corect, respectând procedurile specifice. 3.3. Măsurile de prim ajutor sunt aplicate, în funcție de tipul accidentului.		

Gama de variabile

Documentație de referință: legislație specifică securității şi sănătății în muncă, NSSM şi în domeniul situațiilor de urgență, regulament de ordine interioară (ROI), fişa postului, plan prevenire şi protecție, proceduri interne specifice locului de muncă, tematică pentru instruiri etc.
Riscuri: pericol de lovire pe căi de circulație, cădere de obiecte şi materiale de la înălțime, în timpul manevrării, proiectare de particule în special în ochi, risc de alunecare, pericol de tăiere cu scule şi unelte conținând părți metalice/ ascuțite, arsuri etc.
Factori de risc: referitori la sarcina de muncă, executant, mediul de muncă, procesul tehnologic.
Particularitățile locului de muncă: în interiorul unor clădiri, manevrări de piese cu risc, condiții de luminozitate, etc.
Situații de urgență: accidente, cutremure, incendii, explozii, inundații, etc.
Aspecte relevante: fronturi de lucru existente şi tipurile activităților desfăşurate, modalitatea de organizare a activităților, existența şi repartizarea căilor de acces, numărul de participanți în procesul de muncă şi distribuirea pe posturi de lucru, condițiile de iluminare, etc.
Mijloace de semnalizare: ***utilizate permanent*** - panouri (indicatoare, plăci), culori de securitate; etichete (pictograme, simbol de culoare pe fond); ***utilizate ocazional*** - semnale luminoase, acustice, comunicare verbală (pentru atenționare asupra unor evenimente periculoase, chemare sau apel al persoanelor pentru o acțiune specifică sau evacuare de urgență), etc.
Echipamentul individual de protecție a muncii: halat, mănuşi diverse, etc.
Persoane abilitate: inginer, şef de echipă, responsabili NSSM şi situații de urgență, medici, pompieri,etc.
Servicii abilitate: servicii de ambulanță, pompieri, protecție civilă, etc.
Modalități de intervenție: îndepărtarea accidentaților din zona periculoasă, degajarea locului pentru eliberarea accidentaților, anunțarea operativă a persoanelor abilitate, etc.
Tipuri de accidente: traumatisme mecanice produse prin cădere, lovire, compresiune, tăiere, alunecare, pătrunderea corpurilor străine în ochi, etc.

Tehnici de evaluare recomandate
- Teoretice - test oral, test scris
- Practice - observarea directă în condiţii de muncă reale
- Rapoarte din partea altor persoane.

Unitatea 2 - Aplicarea normelor de protecție a mediului **(unitate generală)**			Coduri de referință
Descrierea unității de competență Unitatea cuprinde cunoştinţele şi deprinderile necesare practicantului în vederea aplicării corecte a normelor de protecție a mediului, în scopul diminuării riscurilor de mediu precum şi a consumului de resurse naturale.			**NIVELUL UNITĂȚII: 2**
Elemente de competență	**Criteriile de realizare din punctul de vedere al deprinderilor practice**	**Criteriile de realizare din punctul de vedere al cunoştinţelor necesare**	**Criteriile de realizare din punctul de vedere al atitudinilor necesare**
1. Transpune în practică norme de protecție a mediului	1.1. Problemele de mediu asociate activităților desfăşurate sunt identificate corect în vederea aplicării normelor de protecție. 1.2. Normele de protecție a mediului sunt însuşite prin instructaje periodice pe tot parcursul executării lucrărilor. 1.3. Normele de protecție a mediului sunt aplicate corect evitându-se impactul nociv asupra mediului înconjurător zonei de lucru.	Persoana supusă evaluării demonstrează că ştie şi înțelege: • Norme specifice de protecție a mediului. • Legislație şi proceduri interne de urgență, specifice. • Particularitățile locului de muncă.	• Problemele de mediu, asociate activităților desfăşurate sunt identificate cu atenție. • Normele de protecție a mediului sunt însuşite cu responsabilitate. • Eventualele riscuri ce pot afecta factorii de mediu de la locul de muncă şi vecinătăți sunt anunțate cu promptitudine personalului abilitat şi serviciilor de urgență. • Intervenția pentru aplicarea de măsuri reparatorii se desfăşoară cu promptitudine. • Identificarea situațiilor în care se pot produce pierderi necontrolate de resurse naturale se face cu responsabilitate.
2. Acționează pentru diminuarea riscurilor de mediu	2.1. Aplicarea procedurilor de recuperare a materialelor refolosibile se face adecvat specificului activităților derulate. 2.2. Reziduurile rezultate din activitățile de pe locul de muncă sunt manipulate şi depozitate conform procedurilor interne, fără afectarea mediului înconjurător. 2.3. Intervenția pentru aplicarea de măsuri reparatorii asupra mediului înconjurător se face în conformitate cu procedurile de urgență şi legislația în vigoare. 2.4. Intervenția pentru aplicarea de măsuri reparatorii se desfăşoară evitând agravarea situației deja create.		

3. Acționează pentru diminuarea consumului de resurse naturale**.** 3.1. Utilizarea resurselor naturale se face judicios. 3.2. Acțiunea pentru diminuarea pierderilor de resurse naturale se face permanent, conform procedurilor specifice.		

Gama de variabile

Documentație de referință: legislație privind protecția mediului, norme de protecția mediului, regulament de ordine interioară (ROI), fișa postului, plan prevenire și protecție, proceduri interne specifice locului de muncă, tematică instruiri etc.
Factori de mediu: apă, aer, sol, specii și habitate naturale.
Riscuri: poluarea apei, aerului, solului, degradarea biodiversității, etc.
Factori de risc ce acționează asupra mediului:
- chimici: substanțe toxice, corozive, inflamabile;
- mecanici: mișcări funcționale ale echipamentelor etc;
- termici;
- electrici;
- biologici;
- radiații;
- gaze (inflamabile, explozive);
- alți factori de risc ai mediului.

Instructaje periodice: zilnice, săptămânale, lunare sau la intervale stabilite prin instrucțiuni proprii, în funcție de specificul condițiilor de lucru.
Persoane abilitate: inginer, șef de echipă, responsabili de mediu, pompieri, etc.
Servicii abilitate: servicii de ambulanță, pompieri, protecție civilă, etc.
Resurse naturale: apă, gaze, sol, resurse energetice, etc.

Tehnici de evaluare recomandate
- Teoretice - test oral, test scris
- Practice - observarea directă in condiții de muncă reale
- Rapoarte din partea altor persoane.

Unitatea 3 - Aplicarea procedurilor de calitate **(unitate generală)**			Coduri de referință
Descrierea unității de competență Unitatea cuprinde cunoştinţe şi deprinderi necesare pentru îndeplinirea cu succes a activităților privind aplicarea procedurilor de calitate.			**NIVELUL UNITĂȚII: 2**
Elemente de competență	**Criteriile de realizare din punctul de vedere al deprinderilor practice**	**Criteriile de realizare din punctul de vedere al cunoştinţelor necesare**	**Criteriile de realizare din punctul de vedere al atitudinilor necesare**
1. Identifică cerințele de calitate specifice	1.1. Cerințele de calitate sunt identificate corect, prin studierea prevederilor referitoare la calitatea lucrărilor, din documentația tehnică. 1.2. Cerințele de calitate sunt identificate pe baza indicațiilor din fişele tehnologice, procedurile / planurile de control. 1.3. Cerințele de calitate sunt identificate conform Sistemului de Management al Calității implementat în unitate sau Normelor interne de calitate.	Persoana supusă evaluării demonstrează că ştie şi înțelege: • Criterii şi reglementări naționale privind asigurarea calității; • Prevederile din Procedurile Sistemului de Management al Calității (SMC) implementat în unitate sau ale Normelor interne calitate; • Proceduri de lucru, proceduri de control, tehnologie de lucru etc.; • Proceduri tehnice de asigurare a calității; • Acțiunile preventive şi corective specifice locului de muncă, prevăzute în SMC sau în Normele interne de calitate.	• Cerințele de calitate sunt identificate cu atenție şi responsabilitate. • Procedurile tehnice de calitate sunt aplicate cu responsabilitate. • Verificarea calității lucrărilor executate se realizează cu responsabilitate. • Verificarea calității lucrărilor se realizează cu exigență şi atenție. • Eventualele neconformități constatate sunt remediate cu promptitudine şi responsabilitate.
2. Transpune în practică procedurile tehnice de asigurare a calității	2.1. Procedurile tehnice de asigurare a calității sunt aplicate în funcție de tipul lucrării de executat. 2.2. Procedurile tehnice de asigurare a calității sunt aplicate permanent, pe întreaga derulare a lucrărilor, în vederea asigurării cerințelor de calitate specifice acestora. 2.3. Procedurile tehnice de asigurare a calității lucrărilor sunt aplicate respectând precizările din documentația tehnică specifică.		

3. Controlează calitatea lucrărilor executate	3.1. Verificarea calității lucrărilor executate se realizează pentru toate operațiile. 3.2. Caracteristicile tehnice ale lucrărilor realizate sunt verificate prin compararea calității execuției cu cerințele de calitate impuse de tehnologia de execuție şi normele de calitate specifice. 3.3. Verificarea se realizează, prin aplicarea metodelor adecvate tipului de lucrare executată şi caracteristicilor tehnice urmărite. 3.4. Verificarea calității lucrărilor executate se realizează, utilizând corect tehnicile specifice IT.		
4. Remediază neconformitățile constatate	4.1. Neconformitățile constatate sunt remediate permanent, pe parcursul derulării lucrărilor. 4.2. Neconformitățile sunt eliminate prin înlăturarea cauzelor care le generează. 4.3. Lucrările executate îndeplinesc condițiile de calitate impuse de normele de calitate specifice.		

Gama de variabile

Cerințe de calitate: caiete de sarcini, norme interne, criterii şi reglementări interne, criterii şi reglementări naționale, standarde tehnice, alte specificații.
Tipul lucrării de executat: identificarea cerințelor de calitate, aplicarea procedurilor tehnice de asigurare a calității, verificarea calității lucrărilor executate, remedierea neconformităților constatate.
Documentația tehnică specifică: proceduri de lucru, proceduri de control, tehnologie de lucru, specificații tehnice, etc.
Calitatea execuției se referă la*:* funcționarea echipamentelor IT&C la parametrii specificați în fişele tehnice ale acestora
Metode de verificare a calității execuției: prin teste asupra parametrilor de funcționare a echipamentelor IT&C.
Dispozitive / verificatoare pentru controlul şi verificarea calității lucrărilor efectuate*:* aparate de măsură şi control specifice activităților din domeniul IT&C, produse software pentru testare şi benchmark etc.
Cauze care generează defecte: componente şi subansambluri electronice necorespunzătoare, nerespectarea tehnologiei de lucru, documentație incompletă, scule necorespunzătoare, diverse erori umane, etc.

Tehnici de evaluare recomandate

- Teoretice - test oral, test scris
- Practice - observarea directă în condiţii de muncă reale
- Rapoarte din partea altor persoane.

Unitatea 1. Identificarea cerințelor de securitate a informației **(unitate specifică)**			Coduri de referință
Descrierea unității de competență Unitatea cuprinde cunoştinţele şi deprinderile necesare pentru: • Identificarea şi inventarierea informațiilor, bunurilor, valorilor şi resurselor IT folosite în organizație şi care au legătură cu informația. Inventarul conține obiecte clasificate şi etichetate după gradul de protecție aplicat. Rezultatul identificării şi inventarierii informațiilor şi a bunurilor care au legătură cu informația este formularea *declarației de intenție* referitoare la *strategia şi obiectivele de securitate a informației*, la cadrul organizațional de aplicare a strategiei. • Identificarea amenințărilor şi a vulnerabilităților legate de siguranța informației şi a bunurilor aflate în legătură cu informațiile; identificarea pierderilor (pagube) potențiale provocate în situația materializării amenințărilor şi probabilitatea de manifestare a amenințărilor. *Rezultatul este modelul amenințărilor (vulnerabilităților).* • Analiza riscurilor, respectiv identificarea riscului (probabilitatea de apariție a unui incident), evaluarea impactului (pierdere, pagubă) şi asigurarea unui echilibru între impact şi costurile implementării măsurilor de protecție. *Rezultatul acestei activități este planul de management al riscurilor*, unde, pentru fiecare risc identificat sunt stabilite acțiunile preventive şi reactive (răspunsul în situația materializării amenințării / vulnerabilității). Operațiile corespunzătoare acestei unități de competență au drept rezultat final documentul care stabileşte strategia şi obiectivele de securitate a informației în organizație.			**NIVELUL UNITĂȚII: 5**
Elemente de competență	**Criteriile de realizare din punctul de vedere al deprinderilor practice**	**Criteriile de realizare din punctul de vedere al cunoştințelor necesare**	**Criterii de realizare din punctul de vedere al atitudinilor necesare**
1. Identifică resursele şi informațiile de protejat	1.1. Obiectele cuprinse în inventarul informațiilor, al bunurilor, valorilor şi resurselor IT care au legătură cu informația sunt etichetate conform criteriilor de importanță proprii organizației. 1.2. Clasificarea informațiilor şi a bunurilor se face conform gradului de protecție necesară. 1.3. Procedurile speciale de prelucrare, copiere, păstrare, transmitere, distrugere, salvare, restaurare respectă gradul de protecție necesară fiecărei clase de informații.	Persoana supusă evaluării demonstrează că ştie şi înțelege: • Particularitățile soluțiilor IT&C integrate, • Sistemele informatice şi modalități de analiză a sistemelor informatice, • Arhitecturi de calculatoare, sisteme de operare, sisteme de fişiere, permisiuni la resurse, privilegii şi restricții de acces, baze de date, aplicații diverse, • Tipuri de date, proceduri de păstrare, prelucrare, transmitere, securitatea datelor, confidențialitate, integritate,	• Resursele şi informațiile ce vor fi protejate prin proceduri de securitate sunt identificate cu atenție şi rigurozitate. • Declarația de intenție pentru strategia şi obiectivele referitoare la securitatea informației au la bază gândirea logică, argumentarea solidă şi denotă abilități de prezentare şi comunicare eficientă a informațiilor. • Amenințările şi vulnerabilitățile sunt identificate cu atenție la detalii şi denotă abilități de organizare,

2. Formulează declarația de intenție privind strategia şi obiectivele de securitate a informației.	2.1.Securitatea informației, domeniul de aplicare, obiectivele generale, importanța securității informației pentru organizație sunt conforme cu viziunea şi obiectivele generale ale organizației. 2.2. Cadrul general de aplicare şi obiectivele măsurilor de securitate ce urmează a fi implementate sunt stabilite şi însuşite de managementul organizației	criptare, decriptare, semnătură electronică, salvare, restaurarea datelor, • Rețele de calculatoare, topologii, LAN, WAN, VLAN, VPN, servere, conectarea la rețea, managementul serviciului director de resurse, interconectarea rețelelor, echipamente de interconectare, segmentarea rețelelor, firewall, conectivitatea la Internet, protocoale, infrastructura specifică, servicii de rețea, standarde aplicabile rețelelor de calculatoare şi pentru accesul la Internet, • Echipamentele electronice, erori în funcționarea echipamentelor, jurnale de erori, operații de corecție şi întreținere, • Erorile în funcționarea componentelor software, a sistemelor de operare, configurări corective, jurnale de erori şi de evenimente, • Resursele informatice, atacul asupra resurselor, accesul autorizat şi cel neautorizat, atacuri din interior şi din exterior, detectarea intruşilor şi a intruziunilor, acumularea dovezilor, • Măsuri specifice de prevenire şi diminuare a pagubelor, • Standarde pentru managementul securității informației, • Analiza calitativă şi cantitativă a	planificare şi de rezolvare rapidă a problemelor. • Analiza riscurilor se face cu discernământ, dovedind abilități de prioritizare, capacitatea de a lua decizii, identificarea de alternative, creativitate în descoperirea soluțiilor noi, creativitate şi inovare. • Planul de management al riscului este elaborat cu atenție la detalii şi hotărâre. • Standardele aplicabile sunt implementate cu rigurozitate şi promptitudine. • Strategia de securitate este formulată cu claritate, conciziune, logic şi simplu.
3. Identifică amenințări şi vulnerabilități	3.1. Amenințările şi vulnerabilitățile identificate reflectă inventarul informațiilor şi al bunurilor care au legătură cu informația 3.2. Criteriile pentru evaluarea vulnerabilităților sunt conforme cu viziunea, strategia şi obiectivele organizației şi sunt acceptate şi însuşite de managementul organizației. 3.3. Amenințările şi vulnerabilitățile identificate vizează următoarele niveluri: personalul angajat, securitatea fizică, accesul la informații, achiziționarea, întreținerea şi menținerea în funcțiune a echipamentelor hardware şi a componentelor software. 3.4. Managementul vulnerabilităților şi acțiunile pentru continuarea activităților organizației folosesc criterii acceptate şi însuşite de managementul organizației..		

4.Analizează riscuri	4.1. Tabelul riscurilor ordonează amenințările /vulnerabilități conform criteriilor de importanță acceptate şi însuşite de managementul organizației. 4.2.Fiecărui risc identificat în tabelul riscurilor îi corespunde un plan pentru diminuarea riscului şi reducerea pierderilor. 4.3. Există un plan de management pentru fiecare risc unde sunt stipulate măsurile preventive şi reactive. 4.4.Există un responsabil desemnat pentru aplicarea fiecărei măsuri din planul de management.	riscurilor, managementul riscurilor, evaluarea / cuantificarea pagubelor / pierderilor, evaluarea costurilor pentru implementarea măsurilor de securitate, evaluarea rezultatelor implementării măsurilor de securitate, • Organigrama organizației, fişele posturilor, planul clădirii şi al dependințelor, manualele şi ghidurile de utilizare ale calculatoarelor, aplicațiilor, serviciilor, echipamentelor de comunicații şi telecomunicații.	
5. Elaborează strategia de securitate privind informația	5.1. Strategia privind securitatea informației pentru organizație este conformă cu riscurile identificate şi respectă declarația de intenție. 5.2. Strategia de securitate privind securitatea informației este aprobată de managementul organizației şi este publicată spre a fi cunoscută conducerii, angajaților, partenerilor, clienților, furnizorilor. 5.3. Înaintea angajării / colaborării personalul organizației şi părțile interesate cunosc şi înțeleg rolul ce le revine în aplicarea strategiei de securitate a informației la nivelul organizației. 5.4. Strategia de securitate definește: obiective clare, responsabilități individuale, consecințele încălcării măsurilor de securitate, cerințele privind instruirea personalului pentru înțelegerea şi aplicarea măsurilor de securitate .		

Gama de variabile

În general, pentru informații diferite şi organizații diferite sunt cerute grade de protecție diferite.
Bunurile, valorile, resursele IT inventariate pot fi: informații – indiferent de suport -, componente software, resurse hardware, alte bunuri şi servicii asociate.
Gradul (nivelul) de protecție asociat obiectelor inventariate poate fi: indiferent, sensibil, confidențial, critic, secret, ultra secret, etc.
În funcție de specificul organizației, de tipul activităților desfăşurate, de soluția IT&C implementată, de pregătirea şi motivarea personalului vor fi identificate amenințări şi vulnerabilități din cele mai diverse, legate de informațiile păstrate, prelucrate, transmise, expuse. Profesioniştii IT&C sunt responsabili atât pentru securitatea informației cât şi pentru breşele de securitate care folosite pot provoca pagube.
Amenințarea se referă la un pericol sau la o vulnerabilitate. Amenințările au probabilități diferite de a se materializa în evenimente nedorite (incidente). Materializarea unei amenințări poate produce pagube diferite în condiții diferite.
Amenințările (vulnerabilitățile) corespunzătoare diferitelor niveluri pot fi: erori umane, neglijență, furt, fraudă, folosirea incorectă a echipamentelor; **securitatea fizică** se poate referi la: securitatea clădirilor, a căilor de acces, a echipamentelor electronice şi de comunicații, a personalului; **accesul la informații** se poate referi la: încercarea (reuşită sau nu) de a citi, vedea (vizualiza), modifica, transfera orice fel de date (texte, grafice, date audio, video, fotografii, desene,etc.);
Riscul este posibilitatea de a suferi o pierdere, o pagubă. **Evaluarea şi analiza riscurilor** sunt legate de probabilitatea ca o amenințare să se materializeze şi de pagubele cuantificabile pe care le poate produce. Analiza riscurilor evidențiază pericole, evaluează impactul (pierdere, pagubă) şi identifică măsurile de protecție, anihilare, remediere, atenuare, transferare a riscului şi costurile aferente.
Planul de management al riscului se referă la acțiunile ce pot conduce la reducerea, eliminarea, transferarea sau asumarea completă a riscului. Responsabilul cu aplicarea măsurilor din planul de management al riscului poate fi deținătorul sau proprietarul informației sau al bunului care are legătură cu informația. Planul de management al riscului este instrumentul central pe care se bazează strategia de securitate privind informația şi va fi folosit în vederea implementării măsurilor de securitate.

Tehnici de evaluare recomandate

- Teoretice - test oral, proiect,
- Practice - observarea directă in condiții de muncă reale, demonstrație structurată
- Rapoarte din partea altor persoane.
- portofoliu de lucrări anterioare.

<table>
<tr><td colspan="3">Unitatea 2. Proiectarea procedurilor de securitate

(unitate specifică)</td><td>Coduri de referință</td></tr>
<tr><td colspan="3">Descrierea unității de competență
Unitatea cuprinde cunoştinţele, deprinderile, atitudinile legate de:
• Stabilirea gradului în care sistemul de securitate existent în organizație răspunde strategiei de securitate privind informația, amenințărilor şi riscurilor identificate. Rezultatul acestei activități este tabloul măsurilor aplicate în vederea asigurării securității informației şi evidențierea riscurilor pentru care nu se aplică (încă) măsuri de protecție şi de securitate.
• Elaborarea noilor proceduri de securitate şi modificarea celor existente pentru a se conforma strategiei de securitate a organizației. Rezultatul se materializează în procedurile şi măsurile de securitate pentru asigurarea securității informației
• Identificarea modalităților de control al gradului de aplicare în practică a măsurilor de securitate şi evaluarea efectelor pe care le produc. Rezultatele acestei activități sunt: proceduri de testare / verificare a conformității cu obiectivele din strategia de securitate privind informația, criterii de evaluare a gradului de îndeplinire a obiectivelor din strategia de securitate, machete / şabloane etalon pentru monitorizarea aplicării măsurilor de securitate.</td><td>NIVELUL UNITĂȚII: 5</td></tr>
<tr><td>Elemente de competență</td><td>Criteriile de realizare din punctul de vedere al deprinderilor practice</td><td>Criteriile de realizare din punctul de vedere al cunoştințelor necesare</td><td>Criterii de realizare din punctul de vedere al atitudinilor necesare</td></tr>
</table>

1.Proiectează tabloul măsurilor de securitate privind informația aplicabile organizației.	1.1. Tabloul măsurilor de securitate aplicabile organizației reflectă planul de management al riscurilor şi măsurile de securitate aplicabile organizației. 1.2. Tabloul măsurilor de securitate cuprinde secțiuni distincte pentru: securitatea resurselor umane, securitatea fizică şi a mediului de lucru, securitatea comunicațiilor şi a operațiunilor, controlul accesului, achiziționarea, dezvoltarea şi mentenanța componentelor hardware şi software ale sistemului informatic, managementul incidentelor de securitate şi al continuării activității organizației. 1.3. Măsurile de securitate aplicabile organizației corespund strategiei de securitate a organizației şi obiectivelor de securitate. 1.4. Tabloul măsurilor de securitate evidențiază clar riscurile pentru care nu se aplică măsuri adecvate de securitate.	Persoana supusă evaluării demonstrează că ştie şi înțelege: • Principiile generale de securitate şi aplicarea regulilor de securitate la nivelul componentelor sistemului informatic, • Standarde de securitate a informației şi aplicarea lor (BS 7799 / ISO 177799), • Securitatea serverelor şi a clienților, segmentarea rețelelor, • Securitatea aplicațiilor, controlul modificărilor, • Accesul şi securitatea accesului in Internet şi Intranet, • Securitatea sistemelor de operare şi a serviciilor, • Criptografie şi tehnici de criptare a datelor şi a transmisiilor de date, • Controlul securității accesului, controlul accesului la resurse, securitatea prin parole, drepturi,	• Tabloul măsurilor de securitate privind informația aplicabile organizației este construit cu răbdare şi atenție la detalii şi demonstrează abilități de organizare şi planificare a activităților. • Procedurile de securitate, măsurile de securitate aferente sunt elaborate prin gândire logică, cercetare şi dovedesc curiozitate ştiințifică. • Procedurile şi măsurile de securitate aferente sunt elaborate cu răbdare, atenție la detalii şi rigurozitate. • Testele etalon probează abilități de cercetare /inovare, investigare,curiozitate ştiințifică, gândire logică.

2.Elaborează proceduri noi de securitate şi le îmbunătăţeşte pe cele existente	2.1. Fiecare procedură de securitate cuprinde un set bine determinat de măsuri de securitate. 2.2. Fiecărui compartiment, post de lucru, rol în organizație îi sunt aplicabile proceduri de securitate strict stabilite. 2.3. Neîndeplinirea procedurilor de securitate antrenează aplicarea sancțiunilor specifice. 2.4. Proprietarul sau deținătorul informației sau al bunurilor aflate în legătură cu informația este responsabil de aplicarea strictă a procedurilor şi măsurilor de securitate. 2.5. Procedurile de securitate sunt clare, simple, concise, uşor de aplicat şi de urmărit şi se bazează pe tehnologii.	restricții, privilegii, autentificarea utilizatorilor, metode de autentificare, certificate, • Securitatea bazelor de date, securitatea în fața viruşilor informatici, smart card-uri, • Securitatea resurselor umane, • Securitatea fizică şi a mediului de lucru, • Securitatea comunicațiilor, a operațiunilor, expunerea informației, • Achiziționarea, dezvoltarea şi întreținerea componentelor hardware şi software ale sistemului informatic, • Managementul incidentelor de securitate şi al continuării activității organizației, • Sisteme de detectare a intruşilor şi intruziunilor, utilitare pentru analiza traficului de date în rețea, • Utilitare pentru auditul accesului utilizatorilor la resurse şi servicii, utilitare pentru analiza evenimentelor, • Criminalitatea informatică, investigare şi colectarea probelor	
3.Elaborează teste etalon pentru controlul aplicării măsurilor de securitate şi pentru evaluarea rezultatelor	3.1. Testele etalon sunt construite pentru fiecare risc identificat. 3.2. Criteriile de conformitate respectă strategia şi obiectivele de securitate ale organizației. 3.3. Testele etalon respectă tabloul măsurilor de securitate privind informația.		

Gama de variabile

Se presupune că în fiecare organizație funcționează **măsuri de securitate**, în formă incipientă sau bine structurate: porți de acces păzite sau supravegheate de la distanță, încăperi / incinte încuiate, calculatoare protejate prin folosirea conturilor de utilizator si a parolelor, blocarea accesului la ecranul desktop în cazul în care calculatorul nu este folosit un timp ceva mai îndelungat. Aceste măsuri minime de securitate vor fi completate cu măsuri şi proceduri specifice, adecvate obiectivelor de securitate privind informația ale organizației.

Obiectivele privind securitatea informației diferă de la o organizație la alta şi se pot referi la: credibilitatea organizației, asigurarea informațiilor sigure, corecte şi la timp, creşterea în timp a eficienței, deschiderea perspectivelor noi pentru organizație, motivarea personalului, etc.

Elaborarea / adaptarea măsurilor de securitate nu va afecta activitatea curentă a organizației şi nici a personalului.

Tehnici de evaluare recomandate - Teoretice - test oral, proiect, - Practice - observarea directă in condiții de muncă reale, demonstrație structurată - Rapoarte din partea altor persoane. - portofoliu de lucrări anterioare.	

Unitatea 3. Elaborarea programului de implementare a securității informației **(unitate specifică)**			Coduri de referință
Descrierea unității de competență Unitatea de competență se referă la cunoştinţele, deprinderile şi atitudinile necesare in vedere conducerii / coordonării programului de implementare a securității informației şi se referă la: • Elaborarea, testarea, implementarea şi revizuirea planului de implementare a măsurilor de securitate corespunzătoare amenințărilor (vulnerabilităților) cunoscute • Elaborarea şi implementarea planului de testare periodică a reacției la incidente • Elaborarea şi implementarea planului de comunicare (alertare) şi de răspuns la apariția (sau numai la suspiciunea) unui incident de securitate • Elaborarea şi implementarea procedurilor de acumulare a dovezilor şi identificarea tipului de atac şi al atacatorului. • Raportarea incidentelor şi a răspunsurilor la incidente			**NIVELUL UNITĂȚII: 5**
Elemente de competență	**Criteriile de realizare din punctul de vedere al deprinderilor practice**	**Criteriile de realizare din punctul de vedere al cunoştinţelor necesare**	**Criterii de realizare din punctul de vedere al atitudinilor necesare**
1. Elaborează planul de implementare şi testare a măsurilor de securitate a informației	1.1. Măsurile de securitate incluse în planurile de implementare şi testare respectă politica de securitate a organizației. 1.2. Măsurile de securitate incluse în planurile de implementare şi testare unt aprobate de managementul organizației care le consideră suficiente pentru protejarea sistemului informatic. 1.3. Succesiunea şi implementarea măsurilor de securitate şi a celor de testare sunt aprobate de managementul organizației care desemnează persoanele responsabile cu implementarea şi testarea măsurilor de securitate	Persoana supusă evaluării demonstrează că ştie şi înțelege: • Principiile generale de securitate şi aplicarea regulilor de securitate la nivelul componentelor sistemului informatic, • Planificarea şi organizarea activităților, • Măsuri specifice de securitate şi reguli de aplicare a lor, • Principii de certificare internă şi de omologare – auditare a sistemelor IT&C, • Standarde specifice: ISO 17799,	• Planul de implementare şi testare a măsurilor de securitate a informației este elaborat cu rigurozitate şi dovedeşte atenție la detalii, claritate în luarea deciziilor şi urmărirea atingerii obiectivelor, logică în abordarea şi rezolvarea problemelor, capacitatea de a rezolva eficient probleme. • Implementarea măsurilor de securitate se face cu obiectivitate şi denotă aptitudini de comunicare şi relaționare cu personalul organizației şi terți implicați în utilizarea resurselor • Monitorizarea sistemului informatic

2. Proiectează şi implementează măsurile de securitate a informației şi de testare a reacției la apariția de incidente	2.1. Măsurile de securitate proiectate şi implementate vizează toate nivelurile de aplicabilitate: • Resurse umane • Securitatea fizică şi a mediului de lucru • Managementul operațiilor şi al comunicațiilor • Controlul accesului • Achiziția, dezvoltarea şi mentenența sistemelor • Managementul incidentelor de securitate 2.2. Aplicarea măsurilor de securitate şi a procedurilor de testare a reacției la incidente nu afectează buna desfăşurare a activităților organizației 2.3. Planul de comunicare (alertare, raportare) a incidentelor şi a suspiciunilor de apariție a incidentelor este aprobat de managementul organizației şi respectă legile în vigoare şi strategia de securitate a informației adoptata de organizație. 2.4. Procedurile de acumulare a dovezilor privind identificarea atacatorului şi a tipului de atac respectă legile în vigoare şi declarația universală a drepturilor omului	ETSI, • Standarde de evaluare şi omologare internă a securității echipamentelor şi sistemelor ISO 15408, • Metode, proceduri şi instrumente pentru testarea securității informației, • Sisteme, utilitare pentru identificarea intruziunilor şi a intruşilor, • Machete, şabloane etalon pentru verificarea condițiilor de securitate curente, • Instrumente, programe utilitare pentru: supravegherea rețelelor, supravegherea traficului de date, monitorizarea performanțelor sistemelor şi a rețelelor, detectarea alterării performanțelor. • Instrumente, programe utilitare pentru verificarea conformității sistemelor cu machete etalon de securitate,	se face cu discernământ, cu respectarea tuturor legilor în vigoare, prin asumarea răspunderii pentru acumularea dovezilor incriminatorii
3. Monitorizează sistemul informatic cu privire la asigurarea securității informației	3.1. Incidentele de securitate şi atacurile identificate sunt raportate imediat şi sunt complet şi corect descrise. 3.2. Raportarea incidentelor se face prin canale formalizate de management. 3.3. Dovezile acumulate respectă legile în vigoare şi declarația universală a drepturilor omului		

Gama de variabile

Planul de implementare şi testare a măsurilor de securitate va fi detaliat în funcție de dezvoltarea tehnologică, obiectivele, strategia, viziunea organizației şi se va conforma politicii / obiectivelor de securitate acceptate şi asumate de managementul organizației şi cu respectarea legilor în vigoare. Planul de implementare nu va putea fi considerat niciodată perfect: s-a dovedit că apar frecvent situații neprevăzute care conduc la reevaluarea măsurilor de securitate, la reordonarea lor sau la identificarea unor condiții mai bune de aplicare. Utilitarele / machetele / şabloanele folosite pentru monitorizare se vor modifica o dată cu modificarea măsurilor de securitate aplicate şi a posibilităților de supraveghere / auditare. Nu în ultimul rând, atenuarea / diminuarea unor riscuri poate atrage apariția unor vulnerabilități noi care vor trebui la rândul lor tratate, rezolvate sau asumate.
Incidentele de securitate vor fi descrise / caracterizate prin: simptome, origine, punct de intrare , intenția atacatorului, gravitatea incidentului, expunerea şi acțiunea întreprinsă pentru limitarea pagubelor.
Incidentele de securitate pot fi: atacuri, vulnerabilități dovedite, breşe recunoscute în securitate, etc.
Masuri specifice de securitate pot fi cele legate de: resurse umane, securitatea fizică şi a mediului de lucru, managementul operațiunilor şi al comunicațiilor, controlul accesului, achiziția, dezvoltarea şi întreținerea sistemelor, managementul incidentelor, etc.

Tehnici de evaluare recomandate

- Teoretice - test oral, proiect
- Practice - observarea directă in condiții de muncă reale, demonstrație structurată
- Rapoarte din partea altor persoane.
- portofoliu de lucrări anterioare.

Unitatea 4. Revizuirea modelului amenințărilor şi al vulnerabilităților **(unitate specifică)**			Coduri de referință
Descrierea unității de competență Unitatea de competență cuprinde cunoştințele, deprinderile şi atitudinile legate de asigurarea securității informației ca activitate continuă. Politica de securitate a unei organizații, măsurile de securitate, planul de aplicare a măsurilor de securitate, măsurile de control şi aplicarea lor vor fi revizuite periodic sau ori de câte ori este nevoie. Incidentele de securitate raportate conduc la reevaluarea riscurilor şi stabilirea măsurilor de securitate corespunzătoare. Revizuirea modelului amenințărilor şi al vulnerabilităților este necesară pentru că în organizație: • apar informații şi resurse noi legate de acestea • au loc modificări ale sistemului informatic (soluția IT&C) ceea ce determină vulnerabilități şi riscuri noi • sunt identificate noi măsuri de securitate şi proceduri adecvate modificărilor survenite			**NIVELUL UNITĂȚII: 5**
Elemente de competență	**Criteriile de realizare din punctul de vedere al deprinderilor practice**	**Criteriile de realizare din punctul de vedere al cunoştințelor necesare**	**Criterii de realizare din punctul de vedere al atitudinilor necesare**

1.Identifică modificările apărute în modelul amenințărilor şi al vulnerabilităților.	1.1. Informațiile şi resursele noi legate de modificarea amenințărilor sunt identificate şi inventariate cu promptitudine pe măsura apariției lor. 1.2. Inventarul informațiilor vehiculate şi prelucrate în organizație, al bunurilor, valorilor, resurselor IT care au legătură cu acestea este completat / modificat prompt cu informațiile identificate. 1.3. Modificările tehnologice şi cele curente aduse sistemului informatic (soluției IT&C) sunt identificate separat şi analizate pentru găsirea vulnerabilităților şi riscurilor noi. 1.4. Tabelul riscurilor este reordonat după includerea amenințărilor /vulnerabilităților identificate conform criteriilor de importanță acceptate şi însuşite de managementul organizației. 1.5. Fiecărui risc identificat în tabelul riscurilor îi corespunde un plan pentru diminuarea riscului şi reducerea pierderilor în conformitate cu strategia de securitate a organizației.	Persoana supusă evaluării demonstrează că ştie şi înțelege: • Principiile generale de securitate şi aplicarea regulilor de securitate la nivelul componentelor sistemului informatic, • Standarde de securitate a informației ți aplicarea lor (BS 7799 / ISO 177799) • Securitatea serverelor şi a clienților, segmentarea rețelelor, • Securitatea aplicațiilor, controlul modificărilor, • Accesul şi securitatea accesului in Internet şi Intranet, • Securitatea sistemelor de operare, a serviciilor, • Criptografie şi tehnici de criptare a datelor şi a transmisiilor de date, • Controlul securității accesului, controlul accesului la resurse, securitatea prin parole, drepturi, restricții, privilegii, autentificarea utilizatorilor, metode de autentificare,	• Resursele şi informațiile protejate prin proceduri de securitate sunt identificate cu atenție şi rigurozitate. • Amenințările şi vulnerabilitățile sunt identificate cu atenție la detalii şi denotă abilități de organizare, • Tabloul măsurilor de securitate privind informația aplicabile organizației este construit cu răbdare şi atenție la detalii şi demonstrează abilități de organizare şi planificare a activităților • Procedurile de securitate, măsurile de securitate aferente sunt elaborate prin gândire logică, cercetare şi dovedesc curiozitate ştiințifică • Procedurile şi măsurile de securitate aferente sunt elaborate cu răbdare, atenție la detalii şi rigurozitate

2. Revizuieşte tabloul măsurilor de securitate privind informația aplicabile organizației	2.1. Tabloul măsurilor de securitate aplicabile organizației reflectă planul de management al riscurilor şi măsurile de securitate aplicabile organizației. 2.2. Tabloul măsurilor de securitate evidențiază clar şi separat riscurile pentru care nu se aplică măsuri adecvate de securitate.	certificate, • Securitatea bazelor de date, securitatea în fața viruşilor informatici, smart card-uri, • Securitatea resurselor umane • Securitatea fizică şi a mediului de lucru, • Securitatea comunicațiilor, a operațiunilor, expunerea informației • Achiziționarea, dezvoltarea şi mentenanța componentelor hardware şi software ale sistemului informatic, • Managementul incidentelor de securitate ți al continuării activității organizației, • Sisteme de detectare a intruşilor şi intruziunilor, utilitare pentru analiza traficului de date în rețea, • Utilitare pentru auditul accesului utilizatorilor la resurse şi servicii, utilitare pentru analiza evenimentelor, • Criminalitatea informatică, investigare şi colectarea probelor.	

Gama de variabile

Activitatea de protejare a sistemelor informatice nu se încheie niciodată. Responsabilul cu elaborarea şi implementarea măsurilor de securitate trebuie să facă față noilor **provocări tehnologice** legate de existența, transmiterea, păstrarea, prelucrarea informației
Măsurile de securitate identificate şi aplicate vor împiedica accesul, folosirea neautorizată şi distrugerea informațiilor şi a echipamentelor legate de acestea.

Tehnici de evaluare recomandate

- Teoretice - test oral, proiect,
- Practice - observarea directă in condiții de muncă reale, demonstrație structurată
- Rapoarte din partea altor persoane.
- portofoliu de lucrări anterioare.

Unitatea 5: Instruirea personalului **(unitate specifică)**			Coduri de referință
Descrierea unității de competență Unitatea de competență cuprinde cunoştinţele, deprinderile şi atitudinile pentru instruirea şi antrenarea personalului pentru dezvoltarea în organizație a unei culturi a securității informației; codurile de conduită şi ghidurile de bune practici sunt componentele principale necesare dezvoltării unei culturi a securității informației. Existența, calitatea şi utilizarea acestora întreţin interesul pentru utilizarea şi transmiterea informațiilor corecte şi sigure. Educarea (instruirea) managementului de vârf asupra managementului securității informației şi asupra posibilelor beneficii este deosebit de importantă pentru succesul general al organizației. Gradul de securitate a unui sistem informatic depinde în mare măsură de gradul de instruire în domeniu a persoanelor implicate, de motivarea şi - nu în ultimul rând - de integritatea lor morală.			**NIVELUL UNITĂȚII:5**
Elemente de competență	**Criteriile de realizare din punctul de vedere al deprinderilor practice**	**Criteriile de realizare din punctul de vedere al cunoştinţelor necesare**	**Criterii de realizare din punctul de vedere al atitudinilor necesare**
1.Elaborează coduri de conduită, ghiduri practice şi manuale pentru aplicarea în organizație a măsurilor de securitate	1.1. Responsabilitățile şi rolurile îndeplinite în aplicarea măsurilor de securitate– componente ale codului de conduită - sunt înscrise în fişa postului pentru tot personalul organizației. 1.2. Sancțiunile disciplinare – pentru situația încălcării măsurilor de securitate - sunt formulate clar şi sunt cunoscute de personalul organizației. 1.3. Codurile de conduită, ghidurile practice, manualele sunt complete, concise, clare, fără ambiguități. 1.4. Codurile de conduită, ghidurile practice, manualele sunt permanent disponibile pentru tot personalul organizației.	Persoana supusă evaluării demonstrează că ştie şi înțelege: • Tehnici de ordonare şi prezentare adecvată a informațiilor, • Tehnici de redactare a materialelor scrise, • Tehnici de captare a atenției interlocutorilor, • Metode de instruire adecvate adulților.	• Codurile de conduită, ghidurile practice şi manualele pentru aplicarea în organizație a măsurilor de securitate sunt elaborate cu atenție şi dovedesc conlucrarea cu toate compartimentele funcționale ale organizației. • Codurile de conduită, ghidurile practice şi manualele pentru aplicarea în organizație a măsurilor de securitate sunt redactate simplu şi corect, fără ambiguități şi sunt uşor de parcurs şi de înțeles.
2.Organizează şi conduce sesiuni de instruire (antrenament)	2.1. Sesiunile de instruire sunt organizate cu periodic. 2.2.Sesiunile de instruire sunt preponderent practice. 2.3. Sesiunile de instruire testează gradul in care personalul cunoaşte şi înțelege responsabilitățile ce îi revin.		

Gama de variabile

Ghidurile practice, manualele codurile de conduită au rolul de a asigura un nivel adecvat de conştientizare, educație şi instruire în privința măsurilor de securitate şi a utilizării corecte a resurselor şi sistemelor în condițiile minimizării riscurilor de securitate.
Responsabilitățile şi rolurile au în vedere: confidențialitatea, protecția datelor, etica, utilizarea corespunzătoare a echipamentelor şi sistemelor, într-un cuvânt practicile considerate corecte în organizație. Sesiunile de instruire şi cele de exerciții practice au drept scop sensibilizarea personalului organizației față de problemele de securitate a informației, astfel încât să înțeleagă responsabilitățile ce îi revin şi să fie implicat în acțiunile de reducere a riscurilor de furt, fraudă, folosire necorespunzătoare a sistemelor.
Sancțiunile disciplinare pentru acele persoane care încalcă regulile (măsurile) de securitate trebuie considerate drept elemente de descurajare a practicilor neconforme cu politica de securitate a organizației.

Tehnici de evaluare recomandate

- Teoretice - test oral, test scris, proiect,
- Practice - observarea directă in condiții de muncă reale, demonstrație structurată
- Rapoarte din partea altor persoane.
- portofoliu de lucrări anterioare.