AUTORITATEA NAȚIONALĂ PENTRU CALIFICĂRI

STANDARD OCUPAȚIONAL

MANAGER DE SECURITATE

Sectorul: Administrație şi Servicii publice

Versiunea: 00

Data aprobării: 10.10.2011

Data propusă pentru revizuire: octombrie 2014

Inițiator proiect:

Fundația Centrul Academic Internațional pentru Securitate și Justiție, B-dul Poligrafiei, nr 3A, etaj 1, Camera 4, sector 1, București

Echipa de redactare:

Horațiu Cătălin BARBU, coordonator de program, Fundația "Centrul Academic Internațional pentru Securitate și Justiție" - B-dul Poligrafiei, nr 3A, etaj 1, Camera 4, sector 1, București
Stelian ARION, Director general, SC Secant Security SRL, Str. Dr.Mihail Mirinescu Nr. 11, sector 5, București

Verificator sectorial:

Ioan NĂSTASE, Expert formare profesională continuă, membru al Comitetului Sectorial Administratie și Servicii Publice.

Comisia de validare:

Gabriel CHIFU Vicepreședintele Comitetului Sectorial Administrație și Servicii Publice

Ion VOIVOZEANU Expert FPC Comitetul Sectorial Administrație și Servicii Publice

Stelian ARDELEAN Expert FPC Comitetul Sectorial Administrație si Servicii Publice

Denumirea documentului electronic: SO_Manager de securitate_00

Responsabilitatea pentru conținutul standardului ocupațional revine Comitetului Sectorial *Administrație şi Servicii publice.*

Descriere:

Prezentul document a fost elaborat ca rezultat al dezvoltării analizei ocupaționale pentru aria ocupațională alți conducători de compartimente cu activități nelucrative din unitățile economico-sociale mari - grupa COR 1239.

Ocupația avută în vedere în stabilirea ariei ocupaționale este:

COR 123906 - Manager de securitate.

Managerul de securitate, sub conducerea managerului general şi în colaborare cu alți conducători , organizează activitatea compartimentului de specialitate, avizează recrutarea si formarea personalului din subordine, urmăreşte randamentul şi eficiența activităților, reprezintă organizația în relațiile cu terți.

În România, în exercitarea profesiei de manager de securitate sunt aplicabile prevederile cadrului legislativ specific: legea privind siguranța națională a României; legea privind protecția informațiilor clasificate; legea privind accesul la informațiile clasificate; hotărârii de guvern privind protecția informațiilor secrete de serviciu; hotărârii de guvern privind colectarea, transportul, distribuirea şi protecția pe teritoriul României a corespondenței clasificate; hotărârii de guvern pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România, normelor de aplicare a legii privind protecția informațiilor clasificate; ordonanța de urgență privind organizarea şi funcționarea Oficiului Registrului Național al Informațiilor Secrete de Stat; legea privind liberul acces la informațiile de interes public; legea pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date; legea privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul comunicațiilor electronice precum şi Ordinele directorului general ORNISS ca autoritate la nivel național în domeniul securității informațiilor clasificate.

Activitatea managerului de securitate este o activitate obiectivă care asigură echipei de conducere informațiile necesare şi cunoştințele suficiente despre cadrul de desfăşurare al procesului de management al securității, astfel încât obiectivele entității să fie îndeplinite. Securitatea trebuie să identifice amenințările, vulnerabilitățile și riscurile, să evidențieze măsurile care trebuiesc luate pentru a diminua riscurile la un nivel rezonabil şi să implice managementul de vârf în proces, astfel încât acesta să înțeleagă impactul şi să poată determina dacă rezultatele preconizate a fi obținute sunt acceptabile. Aceasta este mecanismul prin care activitatea managerului de securitate crează valoare adăugată pentru entitate.

Activitatea managerului de securitate cuprinde:

Securitatea Fizică – ansamblul de reglementări şi măsuri de protecție adoptate la nivelul entităților, sectoarelor, locurilor, echipamentelor, instalațiilor şi în cadrul activităților în care acestea sunt gestionate în scopul de a: interzice accesul neautorizat, clandestin sau prin forță la acestea; detecta și împiedica acțiunile subversive, inclusiv cele de spionaj; contribui la realizarea accesului la informații numai pe baza principiului "necesității de a cunoaşte"; detecta și înlătura slăbiciunile ascunse ale sistemului de securitate adoptat; preveni orice alte situații, împrejurări sau fapte de natură a periclita ori compromite securitatea entității.

Securitatea personalului – ansamblul procedurilor de protecție care se aplică persoanelor ce urmează a deține, a avea acces și a lucra cu informații clasificate.

Securitatea documentelor clasificate – ansamblul procedurilor, cerințelor și a măsurilor privind gestionarea și controlul documentelor clasificate.

Securitatea Industrială – sistemul de norme și măsuri care reglementează protecția informațiilor clasificate în cadrul activităților contractuale cu agenți economici și instituții publice.

Securitatea Sistemelor Informatice și de Comunicații - *INFOSEC* - pricipii de bază și cerințele minime de securitate în domeniul protecției Sistemelor Informatice și de Comunicații.

Instruirea și educația preventivă a personalului - Dezvoltarea educației de securitate și instruirea unitară a întregului personal pentru asigurarea securității în conformitate cu prevederile legislației naționale și procedurilor interne ale entității.

Valorile pe care managerul de securitate trebuie să le posede cuprind valori etice, valori morale şi valori personale.

Etica profesională – datorită faptului că managerul de securitate trebuie să lucreze la standarde înalte de profesionalism pentru a asigura calitatea serviciilor şi a menține încrederea publicului, este nevoie să se

conformeze standardelor etice. Acestea includ: integritatea, independența şi obiectivitatea, confidențialitatea şi competența profesională.
Valorile morale trebuie să fie cel puțin la nivelul celor etice, iar managerul de securitate să poată să discearnă între ce este bine şi ce este rău, corect sau greşit din punct de vedere moral.
Valorile personale – Valorile personale sunt unul din cei mai buni predictori pe termen lung ai potențialului profesional şi ai valorii personale adăugate. Acestea solicită managerului să fie: echilibrat, ambițios, entuziast, persuasiv, devotat, motivat, flexibil, adaptabil.
Managerul de securitate nu va divulga unor terțe persoane (fizice sau juridice) neautorizate nici un fel de date, fapte sau situații pe care le-a constatat în cursul ori în legătură cu îndeplinirea atribuțiunilor profesionale.
Managerul de securitate îşi desfăşoară activitatea atât la sediul entității, cât şi la sediile filialelor, agențiilor, reprezentanțelor, punctelor de lucru ori altor structuri din compunerea acesteia ori potrivit prevederilor contractuale şi/sau cerințe ale terților.
Principalele responsabilități ale managerului de securitate sunt:
- stabileşte concepția, obiectivele, planurile şi procesele de securitate în conformitate cu:
- legislația cu aplicabilitate în domeniul securității
- obiectivele entității sau/şi
- contractelor în care aceasta este parte
- propune echipei de management variante de proiecte de securitate cu evidențierea ierarhizării eficienței acestora din punctul de vedere al raportului efect/efort.
- conduce structura de securitate a entității în realizarea sarcinilor şi atribuțiilor curente şi pentru îndeplinirea obiectivelor:
- răspunde de efectuarea analizelor în domeniul securității pentru un imobil, locație, rută de transport, proces tehnologic, eveniment, etc. Elaborează sau după caz coordonează elaborarea şi aprobă rapoartele de audit de securitate sau revizuire a constatărilor anterioare. Elaborează recomandări în materie de securitate adresate managementului entității.
- răspunde de planificarea, dezvoltarea şi punerea în aplicare a planurilor de securitate cum ar fi: planul de prevenire a scurgerii de informații clasificate, planul de protecție fizică, planuri pentru situații de urgență, proceduri operaționale de securitate etc..
- obținerea avizelor şi acreditărilor impuse de prevederile legale.
- efectuează periodic analize de risc şi propune proiecte pe termen scurt, mediu şi lung pentru arealul în care îşi desfăşoară activitatea entitatea, cu privire la nivelul de criminalitate, terorism, delincvență la locul de muncă, amenințări de dezastre naturale şi artificiale.
- conduce desfăşurarea cercetării administrative interne în ceea ce priveşte securitatea şi sprijină personalul autorizat în investigarea incidentelor de securitate în limita mandatului încredințat şi a competențelor legale.
- monitorizează şi evaluează performanțele entității pe probleme şi programe de securitate, recomandă măsuri adecvate de corecție.
- consiliază echipa de management în scopul asigurării conformității deciziilor şi măsurilor cu prevederile legale, conținutul standardelor internaționale şi prevederile reglementărilor interne/cerințelor contractuale, în materie de securitate.
- oferă consultanță şi consiliere conducerii cu privire la alocarea şi utilizarea de resurse suplimentare pentru protecția personalului, activelor sau informațiilor entității în cazul în care compromiterea sau pierderea acestora ar implica riscuri majore cu impact semnificativ în desfăşurarea activității entității.
- stabileşte şi menține relații corecte cu clienții ori partenerii entității pentru a asigura înțelegerea completă a nevoilor acestora în materie de securitate şi a propune soluții eficiente.
- se informează şi se documentează permanent asupra evoluțiilor industriei şi tehnologiei de securitate, soluțiilor de actualitate în domeniu, amenințărilor şi riscurilor noi ce ar putea avea impact asupra activităților entității.
- organizează şi desfăşoară instruirea şi educația preventivă a personalului pe linia activității de securitate.

Lista unităților de competență

Titluri şi categorii de unități de competență	Nivel de responsabilitate şi autonomie
Unități de competență cheie	
Unitatea 1: Comunicare în limba oficială	4CNC/6EQF
Unitatea 2: Comunicare în limbi străine	3CNC/5EQF
Unitatea 3: Competențe de bază în matematică, ştiință şi tehnologie	3CNC/5EQF
Unitatea 4: Competențe informatice	4CNC/6EQF
Unitatea 5: Competența de a învăța	4CNC/6EQF
Unitatea 6: Competențe sociale şi civice	3CNC/5EQF
Unitatea 7: Competențe antreprenorială	4CNC/6EQF
Unitatea 8: Competența de exprimare culturală	3CNC/5EQF
Unități de competență generale	
Unitatea 1: Organizarea sistemului de management al securității	4CNC/6EQF
Unitatea 2: Verificarea conformității cu prevederile din domeniul sănătății şi securității în muncă	4CNC/6EQF
Unitatea 3: Urmărirea conformității cu prevederile din domeniul apărării împotriva incendiilor şi de protecție a mediului	4CNC/6EQF
Unitatea 4: Dezvoltarea profesională de securitate.	4CNC/6EQF
Unități de competență specifice	
Unitatea 1: Organizarea securității fizice	4CNC/6EQF
Unitatea 2: Organizarea securității personalului	4CNC/6EQF
Unitatea 3: Asigurarea securității documentelor	4CNC/6EQF
Unitatea 4: Stabilirea securității industriale	4CNC/6EQF
Unitatea 5: Organizarea securității sistemelor informatice şi de comunicaţii	4CNC/6EQF

Organizarea sistemului de management al securității (unitate de competență generală)		**Nivelul de responsabilitate şi autonomie** 4CNC/6EQF
Elemente de competență	**Criterii de realizare asociate rezultatului activității descrise de elementul de competență**	**Criterii de realizare asociate modului de îndeplinire a activității descrise de elementul de competență**
1. Identifică cerinţele generale ale sistemului de management al securității (SMS).	1.1. Cerințele generale ale SMS sunt identificate ținând cont de nevoile, rolurile şi responsabilitățile cu privire la securitate. 1.2. Cerințele generale ale SMS sunt identificate cu definirea schemei organizatorice şi dimensionarea resurselor necesare.	Identificarea cerinţelor generale ale SMS se face cu corectitudine, creativitate.
2. Determină cerințele politicii de securitate.	2.1. Cerințele politicii de securitate sunt determinate cu definirea şi structurarea obiectivelor pornind de la cerințele identificate şi rezultatele documentarii despre situația existentă. 2.2. Cerinţele politicii de securitate sunt determinate ţinând cont de îndeplinirea obiectivelor, de asigurarea oportunităţii, disponibilităţii, corectitudinii şi nerepudierii datelor şi informaţiilor precum şi pentru asigurarea caracterului neechivoc al comunicării între componentele SMS.	Determinarea cerinţelor politicii de securitate se face cu corectitudine, creativitate, flexibilitate.
3. Stabileşte cerințele planificării securităţii.	3.1. Cerințele planificării securității sunt stabilite ținând cont de valorile şi activitățile identificate ca fiind vitale pentru entitate, de analiza amenințărilor şi vulnerabilităților şi cu întocmirea listei riscurilor de securitate. 3.2. Cerințele planificării securității sunt stabilite cu identificarea și argumentarea opțiunilor de tratare a riscurilor de securitate, cu propunerea şi argumentarea măsurilor pentru reducerea riscurilor, cu prezentarea şi evaluarea riscurilor reziduale. 3.3. Cerințele planificării securităţii sunt stabilite ţinând cont de asigurarea conformității cu prevederile legale şi cerinţele contractuale, a sustenabilităţii SMS şi cu evidenţierea rezultatelor preconizate.	Stabilirea cerinţelor planificării securității se realizează cu flexibilitate și creativitate.
4. Fundamentează cerințele pentru implementarea securităţii.	4.1. Cerințele pentru implementarea securității sunt fundamentate cu asigurarea nivelului de competență şi de instruire al personalului şi cu stabilirea procedurilor de comunicare şi documentelor SMS. 4.2. Cerinţele pentru implementarea securității sunt fundamentate ţinând cont de măsurile de conducere şi coordonare ale SMS, de planurile şi procedurile de acţiune ale componentelor SMS în situaţii speciale şi de urgenţă.	Fundamentarea cerinţelor pentru implementarea securităţii se face cu atenţie, acurateţe, responsabilitate.

5. Realizează cerințele în materie de control al securității.	5.1. Cerințele în materie de control al securității sunt realizate cu stabilirea programelor de monitorizare și control ale securității și cu stabilirea modului de tratare al incidentelor de securitate. 5.2. Cerințele în materie de control al securității sunt realizate cu evaluarea SMS.	Realizarea cerinţelor în materie de control al securităţii se face cu responsabilitate și exigenţă.
6. Elaborează cerințele pentru îmbunătăţirea securității.	6.1. Cerințele pentru îmbunătățirea securității sunt elaborate ținând cont de periodicitatea revizuirii SMS, realizarea auditului de securitate precum și de evaluarea eficacității acțiunilor corective. 6.2. Cerințele pentru îmbunătăţirea securităţii sunt elaborate cu evaluarea rezultatelor auditului de securitate și prezentarea în format standardizat a concluziilor și propunerilor de eficientizare.	Elaborarea cerinţelor pentru îmbunătăţirea securităţii se face cu adaptabilitate, creativitate, flexibilitate.

Contexte:
-cadrul legislativ și standardele aplicabile;
-Sistemul de Management al Securității (SMS) ;
-elemente specifice activității.

Gama de variabile:
-cerințe contractuale;
-tipurile și natura misiunilor;
-tipuri de organizații: societăți comerciale de stat, publice sau private, unități ale administrației centrale si locale, organizații nonprofit, etc.;
-domenii de activitate: industrial, prestări servicii, regii si companii de utilități, unități de învățământ, culturale, artistice, sportive, sanitare etc;
-mediul de lucru: spații publice, spații private, spații deschise amenajate ori neamenajate, cladiri și construcții, încăperi de securitate și încăperi tip tezaur, containere de securitate, mijloace de transport specializate etc.;
-topologii: clădiri, perimetre, instalații, infrastructuri etc.;
-documente specifice: programul de prevenire a scurgerii informațiilor clasificate, planul de pază, planul de pază și apărare al obiectivelor, sectoarelor și locurilor care prezintă importanță deosebită, planuri de contingență, planuri de evacuare și/sau distrugere pentru situații de urgență, norme și proceduri interne ;
-sisteme tehnice de supraveghere, control și semnalizare;
-echipamente individuale specifice.

Cunoştinţe:
Noțiuni despre:
-amenințări, vulnerabilități și riscuri;
-politici și sisteme de securitate;
-sisteme integrate de securitate;
-tipuri de incidente de securitate;
-colectarea, evaluarea și păstrarea elementelor cu caracter probatoriu;
-cuantificarea numărului, caracteristicilor și impactului incidentelor de securitate;
-standarde de management al securității;
-costuri, beneficii și eficiență în materie de securitate;
-metode și echipamente de testare și evaluare;
-utilizarea sistemelor informatice;
-utilizarea echipamentelor de comunicație și semnalizare;
-resurse materiale, resurse financiare, resurse umane, instituționale, legale;
-părțile interesate: clienți, personal propriu, consultanți, furnizori, autorități publice.

Verificarea conformității cu prevederile din domeniul sănătății şi securității în muncă (unitate de competență generală)		**Nivelul de responsabilitate şi autonomie** 4CNC/6EQF
Elemente de competență	**Criterii de realizare asociate rezultatului activității descrise de elementul de competență**	**Criterii de realizare asociate modului de îndeplinire a activității descrise de elementul de competență**
1. Verifică respectarea prevederilor din domeniul sănătății şi securităţii în muncă.	1.1. Respectarea prevederilor din domeniul securității şi sănătății în muncă este verificată ținând cont de riscurile identificate şi de activitățile şi documentele specifice prevăzute de reglementările în vigoare. 1.2. Respectarea prevederilor din domeniul securității şi sănătății în muncă este verificată ținând cont de procedurile de acțiune în caz de pericol grav și iminent și de modul de acțiune al personalului.	Verificarea respectării prevederilor din domeniul sănătății şi securităţii în muncă se realizează cu responsabilitate, atenţie, exigenţă.
2. Controlează starea şi modul de utilizare al mijloacelor tehnice şi al echipamentului individual de lucru şi protecţie.	2.1. Starea şi modul de utilizare al mijloacelor tehnice este controlată împreună cu personalul desemnat ținând cont de criteriile funcționale şi caracteristicile tehnice ale acestora. 2.2. Starea şi modul de utilizare al echipamentului individual de protecție și de lucru este controlată ținând cont de cerinţele de securitate şi sănatate în muncă şi pentru asigurarea desfăşurării activităţilor în condiţii de siguranţă.	Controlul stării şi modului de utilizare al mijloacelor tehnice şi al echipamentului individual de lucru şi protecţie se face cu acurateţe, corectitudine şi exigenţă.
Contexte: -cadrul legislativ și normele aplicabile; -proceduri de acțiune în caz de pericol grav și iminent; -responsabilități și mod de acțiune al personalului aflat în zona de competență.		
Gama de variabile: -riscuri privind mediul de muncă: factori fizico-chimici, biologici, substanţe ori materiale periculoase, microclimat, etc.; -riscuri privind securitatea muncii: cădere, alunecare, împiedicare, coliziune, electrocutare etc.; -situații cu potențial de risc: pericol de incendiu, avarii la instalații, conducte sau rezervoare, la rețele electrice, de transmitere a datelor, telefonice, calamități naturale, elemente de siguranță deteriorate. -mijloacele de avertizare şi semnalizare: panouri, culori de securitate, etichete, semnale luminoase, semnale acustice, atenționare verbală etc. -particularitățile obiectivului: topologie, gradul de încărcare a obiectivului cu persoane, diverse bunuri şi valori etc.;		
Cunoştinţe: Noțiuni despre: -legislația aplicabilă; -standarde de securitate a muncii; -managementul riscurilor de natura sănătății și securității în muncă; -echipamente de protecție, de lucru și materiale igienico-sanitare.		

Urmărirea conformității cu prevederile din domeniul apărării împotriva incendiilor și de protecție a mediului (unitate de competență generală)		**Nivelul de responsabilitate şi autonomie** 4CNC/6EQF
Elemente de competență	**Criterii de realizare asociate rezultatului activității descrise de elementul de competență**	**Criterii de realizare asociate modului de îndeplinire a activității descrise de elementul de competență**
1. Verifică respectarea prevederilor din domeniul apărării împotriva incendiilor .	1.1. Respectarea prevederilor din domeniul apărării împotriva incendiilor este verificată ținând cont de corelarea măsurilor de apărare împotriva incendiilor cu riscurile identificate şi de avizele, autorizațiile şi documentele prevăzute în reglementările incidente. 1.2. Respectarea prevederilor din domeniul apărării împotriva incendiilor este verificată împreună cu personalul de specialitate, ținând cont de criteriile funcționale și de caracteristicile mijloacelor tehnice corespunzător activităților de apărare împotriva incendiilor.	Verificarea respectării prevederilor din domeniul apărării împotriva incendiilor se face cu responsabilitate, acurateţe, exigenţă.
2. Controlează respectarea prevederilor din domeniul protecției mediului.	2.1. Respectarea prevederilor din domeniul protecției mediului este controlată ținând cont de avizele, autorizările şi documentațiile aferente şi de măsurile de protecție a mediului. 2.2. Respectarea prevederilor din domeniul protecției mediului este controlată având în vedere gestionarea eficientă a deşeurilor, în special a celor toxice şi periculoase. 2.3. Respectarea prevederilor din domeniul protecției mediului este controlată cu testarea şi evaluarea planurilor pentru situații de urgență şi capacitate de răspuns și cu verificarea instruirii personalului.	Controlarea respectării prevederilor din domeniul protecției mediului se face cu responsabilitate, acurateţe, exigenţă.

Contexte:
-cadrul legislativ şi standardele aplicabile;
-modul de acțiune în situații de incendiu sau urgență;
-responsabilități și mod de acțiune al personalului aflat în zona de competență.

Gama de variabile:
-factori de mediu: apa, aerul, solul şi subsolul, habitate naturale, ființele vii etc.
-factori de risc: chimici; mecanici-mişcări funcționale ale echipamentelor, deplasările mijloacelor de producție sub efectul gravitației; termici; electrici; biologici; radiații; gaze ori amestecuri de materiale inflamabile sau explozive etc.
-tipuri de obiective: uzine, secții, instalații tehnologice, clădiri sociale şi/sau administrative, depozite, centrale termice, gospodării de apă, etc.
-riscuri de incendiu ori poluare specifice specificului locurilor de muncă: birouri, ateliere, stații, instalații, centre de calcul, cabinete, laboratoare etc.
-caracteristicile mediului în zonele de desfășurare a activităților: condiții generale de mediu, climă, calitatea apei, solului și aerului, resurse naturale, floră și faună.
-poluanți: orice substanță solidă, lichidă sau sub formă gazoasă/vapori sau energie -termică, fonică, vibrații, radiații etc. care modifică mediul şi poate aduce daune organismelor vii şi

bunurilor materiale. -particularitățile obiectivului: topologie, gradul de încărcare a obiectivului cu persoane, diverse bunuri şi valori etc.
Cunoştinţe: -cadrul legislativ specific ce reglementează activitățile de apărare împotriva incendiilor şi de protecţie a mediului. -conservarea calității factorilor de mediu. -protecția resurselor naturale şi conservarea biodiversității. -conținutul activităților de apărare împotriva incendiilor. -tipuri de mijloace tehnice de apărare împotriva incendiilor. -caracteristici tehnice şi funcționale ale mijloacelor de apărare împotriva incendiilor. -manipularea şi gestiunea deşeurilor.

Dezvoltarea profesională de securitate (unitate de competență generală)		**Nivelul de responsabilitate şi autonomie** 4CNC/6EQF
Elemente de competență	**Criterii de realizare asociate rezultatului activității descrise de elementul de competență**	**Criterii de realizare asociate modului de îndeplinire a activității descrise de elementul de competență**
1. Evaluează nivelul de instruire profesională.	1.1. Nivelul de instruire profesională de securitate este evaluat ținând cont de obiectivele si politica de securitate, de responsabilitățile angajatului şi de istoricul incidentelor de securitate pe o perioadă relevantă. 1.2. Nivelul de instruire profesională de securitate este evaluat ținând cont de procesul organizațional de dezvoltare profesională.	Evaluarea nivelului de instruire profesională al personalului de securitate este realizată cu atenție și exigență.
2. Identifică necesitățile de instruire şi de perfecționare profesională.	2.1. Necesitățile de instruire şi perfecționare profesională sunt identificate în funcție de rezultatele evaluarii şi de noutățile din domeniul de activitate. 2.2. Necesitățile de instruire şi perfecționare profesională sunt identificate cu respectarea cerințelor legale privind pregătirea profesională.	Identificarea necesităților de instruire şi perfecționare profesională de este realizată cu corectitudine și responsabilitate.
3. Stabileşte modalitățile de instruire şi de perfecționare profesională.	3.1. Modalitățile de instruire şi de perfecționare profesională de securitate sunt stabilite în funcție de necesitățile identificate şi de posibilitățile existente. 3.2. Modalitățile de instruire şi de perfecționare profesională de securitate sunt stabilite astfel încât să asigure o eficiență maximă a pregătirii.	Stabilirea modalităților de instruire şi perfecționare profesională de securitate este realizată cu acuratețe și realism.
Contexte: -tehnici de evaluare a cunoştintelor de: securitate fizică; securitatea personalului; securitatea documentelor; securitatea industrială; securitatea sistemelor informatice și de comunicații; sănătate şi securitate în muncă; securitate la incendiu; protecția mediului. -transformarea modelelor comportamentale, structurilor cognitive şi atitudinale sub influența mediului şi a propriilor acțiuni. -managementul formării profesionale continue a adulților.		
Gama de variabile: -obiectivele si politica de securitate a entității. -responsabilitățile angajatului sau categoriei de angajați. -istoricul incidentelor de securitate pe o perioadă relevantă. -evoluția cerințelor profesionale. -procesul organizațional de dezvoltare profesională.		
Cunoştințe: Noțiuni despre: -legislația generală şi specifică în domeniul securității. -managementul organizațiilor. -structura entității și cultura organizațională. -performanța organizațională și factori care o afectează. -tehnici şi metode pentru educarea eficientă a persoanelor adulte. -modalități de instruire: autoinstruirea, studiul legislației, schimburi de experiență cu specialişti, studierea literaturii de specialitate, participarea la cursuri de instruire, de perfecționare profesională şi de specializare. -surse de informare: legislație specifică, publicații de specialitate, Internet, bune practici în domeniu, schimburi de informații şi de experiență cu specialişti, participări la conferințe, simpozioane, târguri de specialitate etc. -tehnici şi metode de comunicare.		

Organizarea securității fizice (unitate de competență specifică)		**Nivelul de responsabilitate şi autonomie** 4CNC/6EQF
Elemente de competență	**Criterii de realizare asociate rezultatului activității descrise de elementul de competență**	**Criterii de realizare asociate modului de îndeplinire a activității descrise de elementul de competență**
1. Planifică securitatea fizică.	1.1. Securitatea fizică este planificată ținând cont de obiectivele de afaceri ale entității, de transpunerea cu acuratețe în norme interne de securitate fizică a prevederilor legale și cerințelor părților interesate. 1.2. Securitatea fizică este planificată cu elaborarea unui ansamblu coerent de planuri, proceduri și măsuri și cu integrarea acestora în cadrul Sistemului de Management al Securităţii 1.3. Securitatea fizică este planificată cu asigurarea fezabilității, sustenabilității și eficienței.	Planificarea securității fizice este realizată cu atenție, acuratețe, corectitudine, responsabilitate.
2. Implementează securitatea fizică.	2.1. Securitatea fizică este implementată cu stabilirea explicită a responsabilităților individuale şi a termenelor de execuție. 2.2 Securitatea fizică este implementată cu asigurarea înțelegerii corecte a planurilor, procedurilor şi măsurilor de către persoanele desemnate. 2.3 Securitatea fizică este implementată cu stabilirea explicită a protocoalelor de evaluare şi a documentelor relevante. 2.4. Securitatea fizică este implementată ținând cont de neconformităţile identificate și măsurile corective adoptate cu informarea oportună asupra desfăşurării procesului.	Implementarea securității fizice este realizată cu acuratețe, exigenţă, responsabilitate.
3. Evaluează securitatea fizică.	3.1. Securitatea fizică este evaluată cu compararea capabilităţilor SMS existent cu scopurile şi obiectivele entității. 3.2. Securitatea fizică este evaluată ținând cont de procedurile standardizate pentru obținerea informațiilor relevante. 3.2. Securitatea fizică este evaluată cu elaborarea imediată de măsuri pentru remedierea unor posibile slăbiciuni critice a SMS. 3.3. Securitatea fizică este evaluată cu analiza unui volum suficient de date pentru stabilirea eficienței planurilor, procedurilor și măsurilor existente. 3.4. Securitatea fizică este evaluată cu prezentarea în format standardizat a rezultatelor și măsurilor propuse pentru remedierea deficiențelor.	Evaluarea securității fizice este realizată cu atenție, exigență; corectitudine, responsabilitate.

Contexte: -activitatea se desfăşoară într-un cadru legislativ specific; -standarde de specialitate aplicabile; -SMS – sistemul de management al securității.
Gama de variabile: -tipuri de organizatii: societăți comerciale de stat, publice sau private, unități ale administrației centrale si locale, organizații nonprofit, etc.; -domenii de activitate: industrial, prestari servicii, regii si companii de utilități, unități de învățământ, culturale, artistice, sportive, sanitare etc. ; -amenințări, vulnerabilități și riscuri; -topologii: clădiri, perimetre, instalații, infrastructuri etc. ; -resurse materiale, financiare, umane, instituționale, legale, timpul la dispoziție etc.; -părțile interesate: clienți, personal propriu, consultanți, furnizori, contractori, autorități publice. -mediul de lucru: spații deschise amenajate ori neamenajate, cladiri și construcții, încăperi de securitate și încăperi tip tezaur, containere de securitate, spații publice, spații private, mijloace de transport specializate; -produse ale procesului de planificare: programul de prevenire a scurgerii de informații clasificate, planul de pază și apărare a obiectivelor, sectoarelor și locurilor care prezintă importanță deosebită, planuri de contingență, planuri de evacuare și/sau distrugere pentru situații de urgență; -documente relevante: planul și fișele cu obiectivele de control, raportul de audit al securității fizice; -proceduri și metode de testare și evaluare a încăperilor și sistemelor mecanice, electronice sau de altă natură folosite; -sisteme tehnice de semnalizare, supraveghere și alarmare. -echipamente individuale specifice; -sisteme informatice și de comunicații.
Cunoştinţe: Noțiuni despre: -legislația aplicabilă; -programul de prevenire a scurgerii de informații clasificate; -planul de pază și apărare a obiectivelor, sectoarelor și locurilor care prezintă importanță deosebită; -planuri de contingență; -planuri de evacuare și/sau distrugere pentru situații de urgență; -costuri, beneficii și eficiență în materie de securitate fizică; -structura entității și cultura organizațională; -performanța organizațională și factori care o afectează; -procesarea informațiilor; -managementul riscurilor; -identificarea și evaluarea valorilor și componentelor critice ale unei organizații; -identificarea și evaluarea amenințărilor și vulnerabilităților; -sisteme integrate de securitate; -managementul neconformităților; -metode și echipamente de testare și evaluare; -tipuri și forme de contracte, documentații tehnice și de execuție, rapoarte; -gestiunea economico-financiară a bunurilor și serviciilor.

Organizarea securității personalului (unitate de competență specifică)		**Nivelul de responsabilitate şi autonomie** 4CNC/6EQF
Elemente de competență	**Criterii de realizare asociate rezultatului activității descrise de elementul de competență**	**Criterii de realizare asociate modului de îndeplinire a activității descrise de elementul de competență**
1. Implementează securitatea personalului.	1.1. Securitatea personalului este implementată cu transpunerea în norme interne a prevederilor legale şi contractuale, cu stabilirea responsabilităților, cadrului conceptual, organizațional şi a modului de acțiune al componentelor SMS. 1.2. Securitatea personalului este implementată ținând cont de procedurile operaționale pentru avizarea şi atestarea personalului, de asigurarea unui răspuns oportun şi eficient la incidentele de securitate a personalului şi de stabilirea de obiective explicite pentru activitățile de educare de securitatea personalului.	Implementarea securității personalului este realizată cu creativitate, flexibilitate, acurateţe, responsabilitate.
2. Evaluează securitatea personalului.	2.1. Securitatea personalului este evaluată ținând cont de organizarea controalelor. 2.2. Securitatea personalului este evaluată cu consemnarea informațiilor şi constatărilor rezultate, analizarea datelor astfel obținute şi redactarea raportului de control. 2.3. Securitatea personalului este evaluată cu prezentarea în format standardizat a rezultatelor şi măsurilor propuse pentru remedierea deficiențelor.	Evaluarea securității personalului este realizată cu atenție acurateţe, corectitudine, exigență, responsabilitate.
Contexte: -cadrul legislativ şi standardele de specialitate aplicabile; -SMS – sistemul de management al securității.		
Gama de variabile: -tipuri de organizatii: societăți comerciale de stat, publice sau private, unități ale administrației centrale si locale, organizații nonprofit; -domenii de activitate: industrial, prestări servicii, regii si companii de utilități, unități de învățământ, culturale, artistice, sportive, sanitare etc. ; -resurse materiale, resurse financiare, resurse umane, instituționale, legale; -cuantificarea numărului, caracteristicilor şi impactului incidentelor de securitate; -informații: interne sau externe entității, clasificate şi/sau neclasificate; -proceduri de verificare a personalului, înainte de angajare, pe timpul şi după terminarea contractului; -amenințări, vulnerabilități şi riscuri la adresa personalului entității; -produse ale procesului de planificare: proceduri de vetting, planul de pregătire a personalului, autorizații de acces la informații clasificate şi certificate de securitate, proceduri şi instrucțiuni de lucru; -metode, materiale şi suporturi educaționale specifice; -documente relevante: planul de control şi fişele cu obiectivele de control, raport de audit al		

securității personalului; -proceduri, metode și mijloace de testare și evaluare a personalului.
Cunoştinţe: Noțiuni despre: -legislația aplicabilă; -programul de prevenire a scurgerii de informații clasificate ; -planul de protecție fizică; -procesarea informațiilor, algoritmi și baze de date; -analiza de risc, a vulnerabilităților, analiză de impact; -clasificarea incidentelor de securitate; -colectarea, evaluarea și păstrarea elementelor cu caracter probatoriu; -organizarea securității și protecției personalului; -metode și procedee pentru educarea eficientă a persoanelor adulte; -costuri, beneficii și eficiență în materie de securitatea personalului; -utilizarea documentelor specifice pentru analiza și evaluarea îndeplinirii cerințelor de securitate a personalului.

Asigurarea securității documentelor (unitate de competență specifică)		**Nivelul de responsabilitate şi autonomie** 4CNC/6EQF
Elemente de competență	**Criterii de realizare asociate rezultatului activității descrise de elementul de competență**	**Criterii de realizare asociate modului de îndeplinire a activității descrise de elementul de competență**
1. Implementează securitatea documentelor.	1.1 Securitatea documentelor este implementată cu transpunerea cu acuratețe în norme interne a prevederilor legale și cerințelor contractuale referitoare la protecția informațiilor clasificate și cu organizarea funcționării compartimentului documente clasificate. 1.2. Securitatea documentelor este implementată cu stabilirea responsabilităților și modului de acțiune al componentelor SMS la incidente de securitatea documentelor și cu identificarea obiectivelor pentru educarea personalului pe linia protecției informațiilor clasificate.	Implementarea securității documentelor este realizată cu creativitate, flexibilitate, acuratețe, responsabilitate.
2. Verifică securitatea documentelor.	2.1. Securitatea documentelor este verificată ținând cont de modul în care este organizat controlul securității documentelor. 2.2. Securitatea documentelor este evaluată cu consemnarea informațiilor și constatărilor rezultate, analizarea datelor astfel obținute și redactarea raportului de control. 2.3. Securitatea documentelor este evaluată cu prezentarea în format standardizat a rezultatelor și măsurilor propuse pentru remedierea deficiențelor .	Verificarea securității documentelor este realizată cu atenție acuratețe, corectitudine, exigență, responsabilitate.
Contexte: -cadrul legislativ și standardele de specialitate aplicabile; -SMS-sistemul de management al securității; -proceduri standardizate de testare și evaluare a lucrului cu documente. -planuri pentru verificarea anuală a existenței documentelor, proceduri de lucru cu documentele clasificate și neclasificate;		
Gama de variabile: -tipuri de organizatii: societăți comerciale de stat, publice sau private, unități ale administrației centrale si locale, organizații nonprofit; -domenii de activitate: industrial, prestari servicii, regii si companii de utilități, unități de învățământ, culturale, artistice, sportive, sanitare etc. ; -amenințări, vulnerabilități și riscuri; -topologii: clădiri, perimetre, instalații, infrastructuri etc. ; -resurse materiale, resurse financiare, resurse umane, instituționale, legale; -părțile interesate: clienți, personal propriu, consultanți, furnizori, contractori, autorități publice. -limitări ale resurselor: materiale, financiare, umane, ale timpului la dispoziție; instituționale, legale. -sisteme electronice și de altă natură specifice întocmirii, procesării, multiplicării, manipulării, transportului și transmiterii documentelor;		

-mijloace de protecție, de păstrare, aparatură de măsură control și reglare a microclimatului. -metode, materiale și suporturi educaționale specifice;
Cunoştinţe: Noțiuni despre: -legislația aplicabilă; -liste cu informații clasificate; -programul de prevenire a scurgerii de informații clasificate; -planul de protecție fizică; -redactarea, dactilografierea/procesarea, evidența, multiplicarea, manipularea, păstrarea, transmiterea, împachetarea, transportul și distrugerea documentelor clasificate; -redactarea și aprobarea nomenclatorului unităților arhivistice; -amenințări, vulnerabilități și riscuri în materie de securitate a documentelor; -coordonarea activității de protecție a informațiilor clasificate.

Stabilirea securității industriale (unitate de competență specifică)		**Nivelul de responsabilitate şi autonomie** 4CNC/6EQF
Elemente de competență	**Criterii de realizare asociate rezultatului activității descrise de elementul de competență**	**Criterii de realizare asociate modului de îndeplinire a activității descrise de elementul de competență**
1. Asigură securitatea industrială .	1.1 Securitatea industrială este asigurată cu transpunerea în norme interne de securitate industrială a prevederilor legale referitoare la protecția informațiilor clasificate, cu stipularea în anexa de securitate a contractelor clasificate a clauzelor de protecție a informațiilor și cu precizarea protocoalelor de verificare de către autoritatea desemnată de securitate. 1.2. Securitatea industrială este asigurată cu stabilirea competențelor, responsabilităților și atribuțiunilor specifice în domeniul securității industriale şi cu stabilirea cadrului organizațional, atribuțiunilor şi modului de acțiune ale componentelor SMS la incidentele de securitate industrială.	Asigurarea securității industriale este realizată cu corectitudine, flexibilitate, acuratețe, responsabilitate.
2. Evaluează securitatea industrială.	2.1. Securitatea industrială este evaluată cu monitorizarea în condițiile legii, a modului de utilizare a informațiilor clasificate în procesul de negociere şi derulare a contractelor și cu verificarea periodică potrivit clauzelor şi procedurilor de protecție. 2.2. Securitatea industrială este evaluată ținând cont de modul în care este organizat controlul. 2.2. Securitatea documentelor este evaluată cu consemnarea informațiilor și constatărilor rezultate, analiza datelor astfel obținute și redactarea raportului de control. 2.3. Securitatea industrială este evaluată cu prezentarea în format standardizat a rezultatelor și măsurilor propuse pentru remedierea deficiențelor .	Evaluarea securității industriale este realizată cu atenție acuratețe, corectitudine, exigență, responsabilitate.
Contexte: -cadrul legislativ şi standardele de specialitate aplicabile; -SMS-sistemul de management al securității; -autoritatea desemnată de securitate; -proceduri, metode de control și evaluare a implementării prevederilor anexei de securitate.		
Gama de variabile: -tipuri de organizații: societăți comerciale de stat, publice sau private, unități ale administrației centrale si locale, organizații nonprofit; -domenii de activitate: industrial, prestări servicii, regii si companii de utilități etc. ; -topologii: clădiri, perimetre, instalații, infrastructuri etc.; -resurse materiale, resurse financiare, resurse umane, instituționale, legale; -părțile interesate: clienți, personal propriu, consultanți, furnizori, contractori, autorități publice. -limitări ale resurselor: materiale, financiare, umane, ale timpului la dispoziție, instituționale, legale.		

-mediul de lucru: spaţii deschise amenajate ori neamenajate; cladiri şi construcţii: uzine, secţii, instalaţii tehnologice, etc.; obiective speciale; elemente critice de infrastructură; -informaţii: interne sau externe entităţii, clasificate şi/sau neclasificate;
Cunoştinţe: Noţiuni despre: -legislaţia aplicabilă; -principiul necesităţii de a cunoaşte; -liste cu informaţii clasificate; -programul de prevenire a scurgerii de informaţii clasificate; -redactarea, dactilografierea/procesarea, evidenţa, multiplicarea, manipularea, păstrarea, transmiterea, împachetarea, transportul şi distrugerea documentelor clasificate; -compromiteri, divulgări, distrugeri, sustrageri, sabotaje, activităţi subversive ori alte riscuri la adresa securităţii industriale.

Organizarea securității sistemelor informatice și de comunicații (unitate de competență specifică)		**Nivelul de responsabilitate și autonomie** 4CNC/6EQF
Elemente de competență	**Criterii de realizare asociate rezultatului activității descrise de elementul de competență**	**Criterii de realizare asociate modului de îndeplinire a activității descrise de elementul de competență**
1. Implementează securitatea sistemelor informatice și de comunicații.	1.1. INFOSEC este implementată cu transpunerea în norme interne a prevederilor legale incidente și cu elaborarea unui ansamblu coerent de măsuri tehnice și politici de securitate în scopul protecției sistemelor informatice, de comunicații, altor mijloace electronice precum și a datelor și informațiilor prelucrate, stocate ori transmise cu ajutorul acestora. 1.2. Măsurile tehnice şi politicile de securitate în domeniul INFOSEC sunt implementate cu corelarea cu obiectivele entității, cu asigurarea unui nivel rezonabil al protecției împotriva amenințărilor, vulnerabilităților și riscurilor și cu asigurarea posibilității de a fi actualizate, completate, îmbunătățite și dezvoltate.	Implementarea INFOSEC este realizată cu creativitate, flexibilitate, acuratețe, responsabilitate.
2. Asigură disponibilitatea sistemelor informatice și de comunicații ulterior producerii unui dezastru.	2.1. Disponibilitatea SIC ulterior producerii unui dezastru este asigurată cu identificarea nevoilor de SIC pentru continuarea activităților, cu stabilirea pe criterii de eficiență a procedurilor operaționale și măsurilor tehnice și cu asigurarea concordanței cu obiectivele entității. 2.2. Disponibilitatea SIC ulterior producerii unui dezastru este asigurată ținând cont de etapele de implementare, de responsabilitățile privind punerea în funcțiune, de graficul de asigurare a disponibilității, precum și de integrarea procedurilor operaționale și măsurilor tehnice în planul de activitate al entității.	Asigurarea disponibilității SIC ulterior producerii unui dezastru este realizată cu atenție, acuratețe, corectitudine, responsabilitate.
3. Evaluează INFOSEC	3.1. INFOSEC este evaluată ținând cont de compararea capabilităților existente cu obiectivele în materie de INFOSEC și cu monitorizarea, testarea și controlul în condițiile legii a modului de utilizare a SPAD, RTD și SIC pe întreaga durată a activităților desfășurate de către personalul entității. 3.2. INFOSEC este evaluată cu desfășurarea de proceduri standardizate, cu înregistrarea datelor, informațiilor și constatărilor, cu analiza datelor astfel obținute și cu redactarea raportului de control. 3.3. INFOSEC este evaluată cu prezentarea în format standardizat a rezultatelor și măsurilor propuse pentru remedierea deficiențelor.	Evaluarea INFOSEC este realizată cu atenție acuratețe, corectitudine, exigență, responsabilitate.

Contexte:
-cadrul legislativ incident şi standardele aplicabile;
-SMS-sistemul de management al securităţii;
-proceduri standardizate de testare şi evaluare a SIC, RTD şi paginilor web.

Gama de variabile:
-tipuri de organizaţii: societăţi comerciale de stat, publice sau private, unităţi ale administraţiei centrale si locale, organizaţii nonprofit, etc.;
-domenii de activitate: industrial, prestari servicii, regii si companii de utilităţi, unităţi de învăţământ, culturale, artistice, sportive, sanitare, etc.;
-ameninţări, vulnerabilităţi şi riscuri;
-topologii: clădiri, perimetre, instalaţii, infrastructuri etc.;
-resurse materiale, financiare, umane, instituţionale, legale, timpul la dispoziţie etc.;
-părţile interesate: clienţi, personal propriu, consultanţi, furnizori, contractori, autorităţi publice.
-mediul de lucru: spaţii publice, spaţii private, spaţii deschise amenajate ori neamenajate, cladiri şi construcţii, încăperi de securitate, mijloace de transport;
-documente relevante: programul de prevenire a scurgerii de informaţii clasificate, planuri pentru implementarea reţelelor de transmisii de date şi aparaturii aferente, cerinţe de securitate globale şi specifice, proceduri operaţionale de securitate, rapoarte de analiză, de risc şi de zonare, buletine pentru măsurători TEMPEST, planuri de control, proceduri şi fişe cu obiective de control;
-sisteme electronice şi de comunicaţii: reţelele de transmisii de voce şi date, servere şi echipamente de reţea aferente; dispozitive auxiliare specifice întocmirii, procesării, multiplicării şi transmiterii informaţiilor; echipamente de criptare/decriptare; surse principale şi de rezervă pentru alimentarea cu energie electrică;
-aparatură de măsură, control şi reglare a microclimatului;

Cunoştinţe:
Noţiuni despre:
-legislaţia aplicabilă;
-analiza de risc, a vulnerabilităţilor,
-analiză de impact;
-liste cu informaţii clasificate;
-programul de prevenire a scurgerii de informaţii clasificate;
-planul de protecţie fizică;
-managementul riscului în sisteme informatice şi de comunicaţii;
-medii de stocare;
-sisteme de prelucrare automată a datelor (SPAD);
-reţele de transmisii de date (RTD);
-sistem informatic şi de comunicaţii (SIC);
-securitatea calculatoarelor (COMPUSEC);
-securitatea comunicaţiilor (COMSEC);
-securitatea SPAD, RTD şi SIC;
-costuri, beneficii şi eficienţă în materie de asigurare a disponibilităţii SIC pentru continuarea activităţilor entităţii ulterior producerii unui dezastru.

AUTORITATEA NAȚIONALĂ PENTRU CALIFICĂRI

CALIFICAREA
MANAGER DE SECURITATE

COD RNC al calificării:

Nivelul calificării: 4 CNC / 6 EQF

Sectorul: Administrație şi Servicii Publice

Versiunea: 00

Data aprobării: 10 octombrie 2011

Data propusă pentru revizuire: 15 iulie 2014

Echipa de redactare: Horațiu Cătălin BARBU, Coordonator proiect, Fundația Centrul Academic Internațional pentru Securitate și Justiție, B-dul Poligrafiei, nr 3A, etaj 1, Camera 4, sector 1, București
Stelian ARION, Director general, S.C. Secant Security SRL, Str. Dr. Mihail Mirinescu Nr. 11, sector 5, București

Verificator sectorial: Ioan NĂSTASE, Expert formare profesională continuă, Comitetul Sectorial Administrație și Servicii Publice

Comisia de validare: Gabriel CHIFU, Vicepreşedintele Comitetului Sectorial Administrație și Servicii Publice
Ion VOIVOZEANU, Expert formare profesională continuă, Comitetul Sectorial Administrație și Servicii Publice
Stelian ARDELEAN, Expert formare profesională continuă, Comitetul Sectorial Administrație și Servicii Publice

Denumire document electronic: Q_Manager de securitate_00

Responsabilitatea pentru conținutul acestei calificări revine Comitetului Sectorial Administrație și Servicii Publice.

Titlul Calificării: Manager de securitate

Descriere:
Activitatea managerului de securitate este o activitate obiectivă care asigură echipei de conducere cunoştinţe suficiente şi informaţiile necesare despre contextul de securitate, astfel încât obiectivele entităţii să fie îndeplinite.

Motivație:
Ocupația de "Manager de securitate" este solicitată pe piața muncii în condițiile creșterii cererii de servicii de securitate pentru toate tipurile de organizații.
În condițiile actuale, când expunerea la risc devine tot mai complexă, diversă și dinamică, aspectele de management al riscului și în particular al riscului de securitate, devin la fel de importante ca și cele de eficiență economică.
Extinderea gamei de amenințări, fenomene precum globalizarea, creşterea integrării şi a complexității sistemelor, creșterea alarmantă a posibilității de producere a unor atacuri teroriste, furtul cu potențial de afectare a instalațiilor şi sistemelor complexe, fac ca gestionarea aspectelor de securitate să fie avute în vedere de conducerea organizațiilor încă de la stabilirea obiectivelor, iar performanța în securitate să facă parte din portofoliul brand-ului.
Una dintre strategiile tot mai frecvent adopatate pentru asigurarea stabilității şi dezvoltării durabile este reziliența. Reziliența permite organizației să se adapteze şi să se dezvolte indiferent de exigențele, evenimentele şi riscurile din mediul de operare.
Managerul de securitate este persoana desemnată să îmbunătățească reziliența organizațională prin planificarea, implementarea, evaluarea și îmbunătățirea Sistemului de Management al Securității.
Sistemul de Management al Securității identifică amenințările, vulnerabilitățile și riscul de securitate, evidențiază măsurile care trebuiesc luate pentru a reduce riscul de securitate la un nivel acceptat şi asigură suportul decizional necesar managementului de vârf.
Acesta este mecanismul prin care activitatea managerului de securitate crează valoare adăugată pentru entitate.

Condiții de acces:
Persoana care doreşte să devină "Manager de securitate" trebuie să facă dovada unei experiențe profesionale relevante, să fi absolvit cel puțin un program specializare / perfecționare autorizat și organizat în conformitate cu standardul ocupațional în vigoare, să nu aibă cazier judiciar, să fie clinic sănătoasă și aptă din punct de vedere psihic.

Nivelul de studii minim necesar:
Studii superioare de lungă durată.

Rute de progres:
Nu sunt aplicabile.

Cerințe legislative specifice:
Nu există.

Titlul calificării: Manager de Securitate
Codul calificării:
Nivelul calificării: 4 CNC / 6 EQF

Lista competențelor profesionale

Cod	Denumirea competenței profesionale	Nivel	Credite
	C1.Comunicare în limba oficială.	4CNC/6EQF	
	C2.Comunicare în limbi străine.	3CNC/5EQF	
	C3.Competențe de bază în matematică, știință și tehnologie.	3CNC/5EQF	
	C4.Competențe informatice.	4CNC/6EQF	
	C5.Competența de a învăța.	4CNC/6EQF	
	C6.Competențe sociale și civice.	3CNC/5EQF	
	C7.Competențe antreprenoriale.	4CNC/6EQF	
	C8.Competența de exprimare culturală.	3CNC/5EQF	
	G1.Organizarea sistemului de management al securității.	4CNC/6EQF	
	G2. Verificarea conformității cu prevederile din domeniul sănătății și securității în muncă.	4CNC/6EQF	
	G3.Urmărirea conformității cu prevederile din domeniul apărării împotriva incendiilor și de protecție a mediului.	4CNC/6EQF	
	G4.Dezvoltarea profesională de securitate.	4CNC/6EQF	
	S1.Organizarea securității fizice.	4CNC/6EQF	
	S2.Organizarea securității personalului.	4CNC/6EQF	
	S3.Asigurarea securității documentelor.	4CNC/6EQF	
	S4.Stabilirea securității industriale.	4CNC/6EQF	
	S5.Organizarea securității sistemelor informatice și de comunicații.	4CNC/6EQF	

Competența: Organizarea sistemului de management al securității.
Cod:
Nivel: 4CNC/6EQF
Credite:

Deprinderi	Cunoștințe
1. Identifică cerințele generale ale Sistemului de Management al Securității cu corectitudine și creativitate ținând cont de nevoile, rolurile și responsabilitățile cu privire la securitate, cu definirea schemei organizatorice și dimensionarea resurselor necesare. 2. Determină cerințele politicii de securitate cu corectitudine, creativitate și flexibilitate, cu structurarea obiectivelor pornind de la rezultatele documentarii despre situația existentă și cerințele identificate ținând cont de asigurarea oportunității, disponibilității, corectitudinii și nerepudierii datelor și informațiilor, precum și de caracterul neechivoc al comunicării între componentele SMS. 3. Stabilește cerințele planificării securității cu flexibilitate și creativitate, ținând cont de valorile și activitățile vitale pentru entitate, de analiza amenințărilor, vulnerabilităților și riscurilor, cu întocmirea listei riscurilor de securitate, identificarea și argumentarea opțiunilor și măsurilor pentru reducerea riscurilor, cu evaluarea riscurilor reziduale și evidențierea rezultatelor preconizate. 4. Fundamentează cerințele pentru implementarea securității cu atenție, acuratețe și responsabilitate, ținând cont de documentele SMS, măsurile de conducere și coordonare, planurile și procedurile de acțiune în situații speciale și de urgență, precum și cu asigurarea nivelului de competență al personalului. 5. Realizează cerințele în materie de control al securității cu responsabilitate și exigență, cu evaluarea SMS ținând cont de programele de monitorizare și control ale securității și de modul de tratare al incidentelor de securitate. 6. Elaborează cerințele pentru îmbunătățirea securității cu adaptabilitate și flexibilitate ținând cont de de rezultatele auditului de securitate, de evaluarea eficacității acțiunilor corective, de periodicitatea revizuirii SMS și cu prezentarea către părțile interesate în format standardizat a concluziilor și propunerilor de eficientizare.	-cadrul legislativ și standardele aplicabile; -amenințări, vulnerabilități și riscuri; -standarde de management al securității; -sisteme integrate de securitate; -tipuri de incidente de securitate; -colectarea, evaluarea și păstrarea elementelor cu caracter probatoriu; -cuantificarea numărului, caracteristicilor și impactului incidentelor de securitate; -metode și echipamente de testare și evaluare; -mediul de lucru: spații publice, spații private, spații deschise amenajate ori neamenajate, cladiri și construcții, încăperi de securitate și încăperi tip tezaur, containere de securitate, mijloace de transport specializate etc.; -topologii: clădiri, perimetre, instalații, infrastructuri etc.; -resurse materiale, financiare, umane, instituționale, legale; -părți interesate: clienți, personal propriu, consultanți, furnizori, autorități publice. -documente specifice: programul de prevenire a scurgerii informațiilor clasificate, planul de pază, planul de pază și apărare al obiectivelor, sectoarelor și locurilor care prezintă importanță deosebită, planuri de contingență, planuri de evacuare și/sau distrugere pentru situații de urgență, norme și proceduri interne;
Metode de evaluare	
• observarea candidaților îndeplinind cerințele de la locul de muncă. • simulare/demonstrație structurată, rapoarte de calitate, asupra procesului și/sau produselor realizate.	• test scris • întrebări orale
• proiect.	
• portofoliu.	

Competența: Verificarea respectării prevederilor din domeniul sănătății şi securității în muncă.
Cod:
Nivel: 4CNC/6EQF
Credite:

Deprinderi	Cunoştințe
1. Verifică respectarea prevederilor din domeniul sănătății și securității în muncă cu responsabilitate, atenție și exigență, ținând cont de activitățile şi documentele specifice prevăzute de reglementările în vigoare, de riscurile identificate, de procedurile de acțiune în caz de pericol grav și iminent și de modul de acțiune al personalului. 2. Controlează împreună cu personalul desemnat starea și modul de utilizare al mijloacelor materiale și tehnice cu acuratețe, corectitudine și exigență, ținând cont de cerințele de securitate și sănatate în muncă, de asigurarea desfășurării activităților în condiții de siguranță, de criteriile funcționale și caracteristicile tehnice ale acestora.	-standarde de securitate a muncii; -riscuri privind mediul de muncă; -riscuri privind securitatea muncii; -managementul riscurilor de natura sănătății și securității în muncă; -întocmirea și completarea corectă a documentelor de organizare și conducere a activității de securitate și sănătate în muncă. -organizarea acțiunilor personalului în caz de pericol grav și iminent. -proceduri de acțiune în caz de pericol grav și iminent. -materiale și mijloace de semnalizare și avertizare; -criterii funcționale și caracteristici ale mijloacelor tehnice; -echipamente de protecție, de lucru și materiale igienico-sanitare.
Metode de evaluare	
• observarea candidaților îndeplinind cerințele de la locul de muncă • simulare/demonstrație structurată • rapoarte de calitate, asupra procesului şi/sau produselor realizate de candidați	• test scris • întrebări orale
• proiect	
• portofoliu	

Competența: Urmărirea conformității cu prevederile din domeniul apărării împotriva incendiilor și de protecție a mediului.
Cod:
Nivel: 4CNC/6EQF
Credite:

Deprinderi	Cunoştințe
1. Verifică împreună cu personalul de specialitate respectarea prevederilor din domeniul apărării împotriva incendiilor cu responsabilitate, acuratețe și exigență, ținând cont de corelarea măsurilor de apărare împotriva incendiilor cu riscurile identificate, de avizele, autorizațiile şi documentele prevăzute în reglementările incidente, de criteriile funcționale și de caracteristicile mijloacelor tehnice existente. 2. Controlează respectarea prevederilor din domeniul protecției mediului cu responsabilitate, acuratețe și exigență, ținând cont de avizele, autorizările și documentațiile aferente, de măsurile de protecție a mediului, de gestionarea eficientă a deşeurilor, în special a celor toxice şi periculoase, cu testarea și evaluarea planurilor pentru situații de urgență și capacitate de răspuns și al modului de acțiune a personalului.	-factori de mediu -factori de risc -poluanți -riscuri de incendiu ori poluare specifice -tipuri de mijloace tehnice de apărare împotriva incendiilor. -caracteristici tehnice şi funcționale ale mijloacelor de apărare împotriva incendiilor. -conținutul activităților de apărare împotriva incendiilor. -caracteristicile mediului în zonele de desfășurare a activităților. -conservarea calității factorilor de mediu. -protecția resurselor naturale și conservarea biodiversității. -manipularea și gestiunea deșeurilor.
Metode de evaluare	
• observarea candidaților îndeplinind cerințele de la locul de muncă • simulare/demonstrație structurată • rapoarte de calitate, asupra procesului şi/sau produselor realizate de candidați	• test scris • întrebări orale
• proiect	
• portofoliu	

Competența: Dezvoltarea profesională de securitate.
Cod:
Nivel: 4CNC/6EQF
Credite:

Deprinderi	**Cunoştințe**
1. Evaluează nivelul de instruire profesională cu atenție și exigență ținând cont de obiectivele si politica de securitate, de responsabilitățile angajatului, de istoricul incidentelor de securitate pe o perioadă relevantă și de procesul organizațional de dezvoltare profesională. 2. Identifică necesitățile de instruire şi de perfecționare profesională cu corectitudine și responsabilitate, cu respectarea cerințelor legale privind pregătirea profesională, în funcție de rezultatele evaluării și de noutățile din domeniul de activitate. 3. Stabilește modalitățile de instruire şi de perfecționare profesională cu acuratețe și realism în funcție de necesitățile identificate și de posibilitățile existente astfel încât să asigure o eficiență maximă a pregătirii.	-legislația generală şi specifică în domeniul securității; -managementul formării profesionale continue a adulților; -structura entității și cultura organizațională; -performanța organizațională și factori care o afectează; -tehnici de evaluare a cunoștintelor; -tehnici pentru educarea eficientă a persoanelor adulte; -modalități de instruire; -surse de informare; -tehnici și metode de comunicare.
Metode de evaluare	
• observarea candidaților îndeplinind cerințele de la locul de muncă; • simulare/demonstrație structurată; • rapoarte de calitate, asupra procesului şi/sau produselor realizate de candidați.	• test scris; • întrebări orale.
• proiect.	
• Portofoliu.	

Competența: Organizarea securității fizice.
Cod:
Nivel: 4CNC/6EQF
Credite:

Deprinderi	Cunoştințe
1. Planifică securitatea fizică cu acuratețe și responsabilitate, ținând cont de obiectivele entității, de transpunerea cu acuratețe în norme interne de securitate fizică a prevederilor legale, a cerințelor părților interesate, cu elaborarea unui ansamblu coerent de planuri, proceduri și măsuri, integrarea acestora în Sistemul de Management al Securității, cu asigurarea fezabilității, sustenabilității și eficienței. 2. Implementează securitatea fizică cu responsabilitate şi exigență, cu stabilirea explicită a responsabilităților individuale şi termenelor de execuție, cu asigurarea înțelegerii corecte a planurilor, procedurilor şi măsurilor de către persoanele desemnate, cu stabilirea explicită a protocoalelor de evaluare şi a documentelor relevante, ținând cont de neconformitățile identificate, de măsurile corective adoptate precum și cu informarea oportună a părților interesate asupra desfășurării procesului. 3. Evaluează securitatea fizică cu atenție și corectitudine ținând cont de capabilitățile existente procedurile standardizate, cu compararea cu scopurile și obiectivele entității, cu analiza unui volum suficient de date pentru stabilirea eficienței planurilor, procedurilor și măsurilor existente, cu elaborarea imediată de măsuri pentru remedierea unor eventuale slăbiciuni critice, precum și cu prezentarea în format standardizat a rezultatelor și măsurilor propuse pentru remedierea deficiențelor.	-legislația aplicabilă; -amenințări, vulnerabilități și riscuri; -identificarea și evaluarea valorilor și componentelor critice ale unei organizații; -identificarea și evaluarea amenințărilor, vulnerabilităților și riscurilor; -managementul riscurilor; -sisteme integrate de securitate; -produse ale procesului de planificare: programul de prevenire a scurgerii de informații clasificate, planul de pază și apărare a obiectivelor, sectoarelor și locurilor care prezintă importanță deosebită, planuri de contingență, planuri de evacuare și/sau distrugere pentru situații de urgență -managementul neconformităților; -proceduri de evaluare; -echipamente de testare; -tipuri și forme de contracte, documentații tehnice și de execuție, rapoarte; -părți interesate: clienți, personal propriu, consultanți, furnizori, contractori, autorități publice
Metode de evaluare	
• observarea candidaților îndeplinind cerințele de la locul de muncă; • simulare/demonstrație structurată; • rapoarte de calitate, asupra procesului şi/sau produselor realizate de candidați.	• test scris • întrebări orale
• proiect.	
• portofoliu.	

Competența: Organizarea securității personalului
Cod:
Nivel: 4CNC/6EQF
Credite:

Deprinderi	Cunoştinţe
1. Implementează securitatea personalului cu acuratețe și responsabilitate, cu transpunerea în norme interne a prevederilor legale și contractuale, cu stabilirea responsabilităților, cadrului conceptual, organizațional şi modului de acțiune al componentelor SMS pentru asigurarea unui răspuns oportun şi eficient la incidentele de securitate a personalului, ținând cont de procedurile operaționale pentru avizarea și atestarea personalului și de stabilirea de obiective explicite pentru activitățile de educare de securitate a personalului. 2. Evaluează securitatea personalului cu corectitudine și exigență, ținând cont de organizarea controalelor, consemnarea informațiilor și constatărilor, analizarea datelor, redactarea raportului de control și prezentarea în format standardizat către părțile interesate a rezultatelor și măsurilor pentru remedierea deficiențelor.	-cadrul legislativ și standardele de specialitate aplicabile; -programul de prevenire a scurgerii de informaţii clasificate ; -planul de protecție fizică; -procesarea informațiilor, algoritmi și baze de date; -analiza de risc, a vulnerabilităților, analiză de impact; -clasificarea incidentelor de securitate; -colectarea, evaluarea și păstrarea elementelor cu caracter probatoriu; -costuri, beneficii și eficiență în materie de securitatea personalului; -utilizarea documentelor specifice pentru analiza și evaluarea îndeplinirii cerințelor de securitate a personalului.
Metode de evaluare	
• observarea candidaților îndeplinind cerințele de la locul de muncă; • simulare/demonstrație structurată; • rapoarte de calitate, asupra procesului şi/sau produselor realizate de candidați.	• test scris; • întrebări orale.
• proiect.	
• portofoliu.	

Competența: Asigurarea securității documentelor
Cod:
Nivel: 4CNC/6EQF
Credite:

Deprinderi	Cunoştințe
1. Implementează securitatea documentelor cu flexibilitate și responsabilitate, ținând cont de transpunerea cu acuratețe în norme interne a prevederilor legale și cerințelor contractuale referitoare la protecția informațiilor clasificate, cu organizarea funcționării compartimentului documente clasificate, cu stabilirea responsabilităților și modului de acțiune al componentelor SMS la incidentele de securitate a documentelor și cu identificarea obiectivelor pentru educarea personalului pe linia protecției informațiilor clasificate. 2. Verifică securitatea documentelor cu corectitudine și exigență ținând cont de modul în care este organizat controlul securității documentelor, cu consemnarea informațiilor și constatărilor, analizarea datelor, redactarea raportului de control și prezentarea în format standardizat către părțile interesate a rezultatelor și măsurilor propuse pentru remedierea deficiențelor.	-cadrul legislativ și standardele de specialitate aplicabile; -liste cu informații clasificate; -programul de prevenire a scurgerii de informații clasificate; -planul de protecție fizică; -redactarea, dactilografierea / procesarea, evidența, multiplicarea, manipularea, păstrarea, transmiterea, împachetarea, transportul şi distrugerea documentelor clasificate; -redactarea şi aprobarea nomenclatorului unităților arhivistice; -amenințări, vulnerabilități şi riscuri în materie de securitate a documentelor; -sisteme electronice și de altă natură specifice lucrului cu documente;
Metode de evaluare	
• observarea candidaților îndeplinind cerințele de la locul de muncă; • simulare/demonstrație structurată; • rapoarte de calitate, asupra procesului şi/sau produselor realizate de candidați.	• test scris • întrebări orale
• proiect.	
• portofoliu.	

Competența: Stabilirea securității industriale
Cod:
Nivel: 4CNC/6EQF
Credite:

Deprinderi	Cunoştințe
1. Asigură securitatea industrială cu corectitudine și responsabilitate ținând cont de transpunerea în norme interne a prevederilor legale incidente, cu stabilirea competențelor, responsabilităților și atribuțiunilor specifice, cu stipularea în anexa de securitate a contractelor clasificate a clauzelor de protecție a informațiilor, cu precizarea protocoalelor de verificare de către autoritatea desemnată de securitate și cu stabilirea cadrului organizațional, atribuțiunilor şi modului de acțiune ale componentelor SMS la incidentele de securitate industrială. 2. Evaluează securitatea industrială cu exigență și corectitudine, ținând cont de modul în care este organizat controlul, de monitorizarea și verificarea periodică a modului de utilizare a informațiilor clasificate în procesul de negociere şi derulare a contractelor, cu consemnarea informațiilor și constatărilor, analizarea datelor, redactarea raportului de control și prezentarea în format standardizat către părțile interesate a rezultatelor și măsurilor propuse pentru remedierea deficiențelor.	-cadrul legislativ și standardele de specialitate aplicabile; -autoritate desemnată de securitate; -proceduri de evaluare a implementării prevederilor anexei de securitate. -tipuri de organizații; -liste cu informații clasificate; -programul de prevenire a scurgerii de informații clasificate; -redactarea, dactilografierea/procesarea, evidența, multiplicarea, manipularea, păstrarea, transmiterea, împachetarea, transportul şi distrugerea documentelor clasificate; -compromiteri, divulgări, distrugeri, sustrageri, sabotaje, activități subversive ori alte riscuri la adresa securității industriale
Metode de evaluare	
• observarea candidaților îndeplinind cerințele de la locul de muncă • simulare/demonstrație structurată • rapoarte de calitate, asupra procesului şi/sau produselor realizate de candidați	• test scris • întrebări orale
• proiect	
• portofoliu	

Competența: Organizarea securității sistemelor informatice și de comunicații.
Cod:
Nivel: 4CNC/6EQF
Credite:

Deprinderi	Cunoștințe
1. Implementează securitatea sistemelor informatice și de comunicații cu creativitate, flexibilitate și responsabilitate, cu transpunerea în norme interne a prevederilor legale incidente, elaborarea unui ansamblu coerent de politici de securitate și măsuri tehnice în scopul protecției sistemelor informatice, de comunicații, altor mijloace electronice precum și a datelor și informațiilor prelucrate, stocate ori transmise cu ajutorul acestora, ținând cont de corelarea cu obiectivele entității, asigurarea unui nivel rezonabil al protecției și a posibilității de a fi actualizate, completate, îmbunătățite și dezvoltate. 2. Asigură disponibilitatea sistemelor informatice și de comunicații pentru continuarea activităților ulterior producerii unui dezastru cu responsabilitate și acuratețe, ținând cont de obiectivele entității, de identificarea nevoilor pe criterii de eficiență, cu stabilirea procedurilor operaționale, a măsurilor tehnice și etapelor de implementare, a responsabilităților privind punerea în funcțiune și graficului de asigurare a disponibilității, precum și cu integrarea în planul de activitate al entității. 3. Evaluează INFOSEC cu acuratețe, corectitudine și exigență, ținând cont de compararea capabilităților existente cu obiectivele entității, cu desfășurarea de proceduri standardizate pentru monitorizarea, testarea și controlul modului de utilizare al SPAD, RTD și SIC, cu înregistrarea informațiilor și constatărilor, analiza datelor, redactarea raportului de control și prezentarea în format standardizat către părțile interesate a rezultatelor și măsurilor propuse pentru remedierea deficiențelor.	-cadrul legislativ incident și standardele aplicabile; -analiza de risc, a vulnerabilităților, de impact; -managementul riscului în sisteme informatice și de comunicații; -documente: programul de prevenire a scurgerii de informații clasificate, planuri pentru implementarea rețelelor de transmisii de date și aparaturii aferente, cerințe de securitate globale și specifice, proceduri operaționale de securitate, rapoarte de analiză, de risc și de zonare, buletine pentru măsurători TEMPEST, planuri de control, proceduri și fișe cu obiective de control; -proceduri standardizate de testare și evaluare a SIC, RTD și paginilor web. -sisteme informatice și de comunicații (SIC) -sisteme de prelucrare automată a datelor (SPAD); -rețele de transmisii de date (RTD); -securitatea sistemelor informatice și de comunicații (INFOSEC); -securitatea calculatoarelor (COMPUSEC); -securitatea comunicațiilor (COMSEC); -costuri, beneficii și eficiență în materie de asigurare a disponibilității SIC
Metode de evaluare	
• observarea candidaților îndeplinind cerințele de la locul de muncă • simulare/demonstrație structurată • rapoarte de calitate, asupra procesului și/sau produselor realizate de candidați	• test scris • întrebări orale
• proiect	
• portofoliu	