STANDARD OCUPAȚIONAL

Ocupația: Administrator de rețea de calculatoare

Domeniul: **Electrotehnică, automatică, electronică, informatică / tehnologia informației**

Cod COR: 213902

2007

Inițiator revizuire standard: Centrul de Pregătire în Informatică CPI – S.A.

Standardul a fost elaborat in cadrul programului PHARE 2003 Coeziune Economică şi Socială – Dezvoltarea resurselor umane, prin cofinanțare PHARE (80%) şi CPI-SA (20%).

Titlu proiect: „Elaborarea de standarde ocupaționale pentru domeniul tehnologiilor informației, ca suport necesar şi obligatoriu pentru aplicarea reglementărilor legale privind formarea profesională a adulților"

Referința proiect: RO-200-005-551.05.03.02.147

Echipa de redactare a standardului ocupațional:

Mihaela Tudose – inginer de sistem, specialist in administrarea rețelelor de calculatoare, trainer autorizat Microsoft pentru domeniul administrării rețelelor de calculatoare - Centrul de Pregătire în Informatică - CPI – S.A

Veronica Fulga – inginer de sistem, specialist in administrarea rețelelor de calculatoare, trainer autorizat Microsoft pentru domeniul administrării rețelelor de calculatoare - Centrul de Pregătire în Informatică - CPI – S.A.

Nicoleta Caloian - specialist in administrarea rețelelor de calculatoare, expert instructor - Centrul de Pregătire în Informatică - CPI – S.A.

Echipa de validare / Referenți de specialitate:

Remus Tudorică – doctor în informatică, director general - CPI – S.A.

Dominic Bucerzan – matematician – informatician, doctor in informatica, vicepreşedinte Asociația Patronală FORTI

Dan Cismasiu, matematician-informatician, inginer de sistem, director general S.A.S. Sibiu, vicepreşedinte Asociația Patronală FORTI

Sorin Dimofte - inginer electrotehnică – manager implementare software - SIVECO S.A.

Sorin Iuga – matematician-informatician - S.C. SHARK Industries

Eugen Maftei, matematician-informatician, vicepreşedinte Asociația Națională a Experților Formatori în Informatică (ANEFI)

Florin Izvoranu - administrator de rețea – CPI-SA

Comitetul Sectorial pentru Tehnologia Informației, Comunicații si Poştă

UNITĂȚI DE COMPETENȚĂ

Domenii de competență	Nr. crt.	Titlul unității
FUNDAMENTALE	1	Comunicarea la locul de muncă
	2	Lucrul în echipă
	3	Dezvoltarea profesională
GENERALE PE DOMENIUL DE ACTIVITATE	4	Aplicarea normelor de tehnica securității muncii şi de prevenire şi stingere a incendiilor
	5	Aplicarea procedurilor de calitate
	6	Organizarea activităților
SPECIFICE OCUPAȚIEI	7	Proiectarea, instalarea şi administrarea infrastructurii de rețea
	8	Asigurarea funcționalității rețelei de calculatoare şi a echipamentelor de conectare şi de comunicații
	9	Administrarea serverelor
	10	Interconectarea rețelelor şi accesul la rețeaua globală Internet
	11	Proiectarea şi aplicarea strategiei de securitate a rețelei
	12	Instruirea şi asistarea utilizatorilor

Descrierea ocupației

Administratorul de rețea de calculatoare:

proiectează, dezvoltă, implementează, întreține în funcțiune soluții IT&C[1] ce includ lucrul în rețea şi/ sau accesul la Internet: pune cele mai convenabile soluții la dispoziția angajaților şi a conducerii organizației (firmă, instituție), în funcție de specificul activităților desfăşurate şi de rezultatele aşteptate;

cunoaşte şi este preocupat de înțelegerea în profunzime a activităților desfăşurate în organizație (firmă, instituție), de modul cum pot fi ele susținute prin soluții IT&C ce includ rețele de calculatoare[2]. Soluțiile IT&C special proiectate sau adaptate vor avea la bază cerințele de lucru ale organizației (firmă, instituție), performanțele aşteptate, în condițiile unor costuri acceptabile şi într-un timp determinat;

transpune/ participă la transpunerea fluxurilor si proceselor informaționale din organizație (firmă, instituție) in cerințe şi specificații IT&C - ce includ operarea intr-un mediu cu resurse distribuite in rețea - construite în jurul principiilor şi conceptelor ce guvernează utilizarea rețelelor de calculatoare;

alege şi implementează arhitectura de rețea şi tehnologiile de conectare şi comunicații în funcție de specificul activităților desfăşurate în organizație (firmă, instituție), de gradul de securitate aşteptat şi de bugetul alocat;

studiază, cunoaşte, înțelege şi analizează tendințele tehnologice în industria IT&C; este expert în calculatoare, rețele de calculatoare, comunicații;

lucrează în echipă cu alți experți pentru selectarea, adaptarea, proiectarea, integrarea celor mai convenabile soluții pentru distribuirea şi accesul la resursele din rețea, în condițiile respectării regulilor specifice de securitate asupra echipamentelor, componentelor software, informațiilor şi transmisiilor de date;

identifică şi încorporează modificările şi/ sau configurările ce pot fi aduse componentelor hardware şi software ale rețelei: supraveghează/ monitorizează funcționarea echipamentelor de comunicații cu scopul de a păstra mediul de operare al rețelei în limita parametrilor normali de funcționare;

stabileşte parametrii etalon de funcționare şi soluțiile ce vor fi adoptate în situația detectării anomaliilor de funcționare a componentelor rețelei;

aplică standardele tehnice în vigoare şi cerințele specifice ale organizației (firmă, instituție), aşa cum decurg ele din activitățile desfăşurate;

stabileşte soluții, proceduri, tehnici, recomandări de bună practică pentru menținerea bunei funcționări şi a corectei utilizări a calculatoarelor, echipamentelor de conectare la rețea şi a celor destinate comunicațiilor;

diagnostichează, **identifică şi soluționează** incidentele apărute în funcționarea rețelei în general, a echipamentelor de legătură şi a celor de comunicații;

decide asupra modului in care utilizatorii (angajați şi conducere) au acces şi folosesc resursele disponibile în rețea;

elaborează recomandări de buna practica pentru buna funcționare si corecta utilizare a calculatoarelor, a echipamentelor de conectare la rețea si a celor destinate comunicațiilor;

proiectează, implementează, urmăreşte aplicarea strictă a regulilor de securitate ce guvernează accesul la resursele rețelei: conturi pentru utilizatori, parole, modalități de

[1] IT&C, Information Technology and Communications, în limba română, Tehnologia informației si Comunicațiilor

[2] O rețea se compune din calculatoare interconectate şi care comunică intre ele, astfel încât utilizatorul să poată folosi atât resursele locale cât şi pe cele aflate la distanță, în limita privilegiile (restricțiilor) ce îi sunt acordate conform strategiei de securitate.

autentificare, permisiuni, restricții, drepturi, privilegii, machete de securitate, metode de configurare automată a mediului de operare al utilizatorilor, proceduri personalizate;

proiectează, implementează şi urmăreşte aplicarea măsurilor specifice obținerii transmisiilor sigure de informații;

stabileşte rolurile client – server ale componentelor din rețea, distribuția aplicațiilor şi a serviciilor, privilegiile şi restricțiile specifice;

instalează şi configurează infrastructura şi conexiunile la rețea, sisteme de operare**,** servicii, proceduri client, aplicații specifice rețelei;

colaborează cu toate compartimentele funcționale ale organizației (firmă, instituție) oferind asistență în folosirea tehnologiilor informației în activitatea curentă; este la curent cu solicitările şi necesitățile reale de acces la resursele rețelei locale, la resurse aflate în alte rețele, inclusiv în rețeaua globală Internet;

informează utilizatorii (angajați, conducere) despre noile facilitați, configurații, tehnologii de conectare şi comunicare în rețea, a căror utilizare ar putea îmbunătăți calitatea produselor şi/sau a serviciilor care fac obiectul activității organizației (firmă, instituție), inclusiv stilul de muncă şi de viață al celor care le utilizează;

organizează sesiuni de instruire a utilizatorilor, corespunzător noilor soluții tehnologice implementate, sau care urmează a fi implementate;

identifică şi eşalonează activitățile de întreținere/ up-gradare software şi hardware pentru echipamentele specifice rețelelor de calculatoare.

Cunoştințe necesare practicării ocupației:

sisteme de operare, sisteme de fişiere, strategii şi reguli de securitate;

privilegii şi restricții ale utilizatorilor, conturile utilizatorilor, resurse şi administrarea resurselor rețelei, relații client / server, comenzi de la tastatură, fişiere cu comenzi, fişiere script, instrumente de administrare;

instrumente de administrare adecvate;

evenimente, jurnale, mesaje de eroare şi de avertizare şi interpretarea lor, măsuri şi criterii de performanță, instrumente de urmărire şi evaluare a performanțelor;

concepte şi arhitecturi de rețea (Ethernet, Token Ring, FDDI, ATM, Frame Relay, etc), tehnologii specifice, standarde de conectare şi de comunicații;

funcționarea rețelelor, tipuri de rețele, medii de comunicații, topologii specifice, construirea şi întreținerea infrastructurii de rețea, transmisii de date, protocoale, supravegherea traficului de informații şi a încărcării rețelei, instrumente de urmărire şi control;

conexiuni în rețea, adaptoare de rețea, drivere specifice, proceduri client, servere şi servicii, protocoale, reguli de adresare şi de acces, conexiuni LAN,WAN, VPN, acces de la distantă (remote), instrumente de administrare, SNMP;

securitatea accesului în rețea, securitatea datelor accesibile în rețea, autentificarea utilizatorilor, transmisii sigure în rețea, criptarea şi decriptarea datelor, salvarea / restaurarea informațiilor folosite în rețea;

servicii director de resurse, publicarea şi accesul la resursele din director, reguli de securitate asociate şi modalități de implementare, instrumente de administrare;

rețele LAN, bridge-uri, rutere, tabele de rutare, protocoale de rutare şi protocoale rutabile, concentratoare, niveluri OSI, protocolul TCP/IP, interconectarea rețelelor, conectarea la Internet, servicii Intranet;

securitatea rețelelor, detectarea intruşilor, proceduri de supraveghere şi apărare față de atacurile externe şi interne, produse şi servicii de tip „firewall”;

rețele WAN, comutare de pachete, X25., VPN, conexiuni „dial-up”, ISDN, ADSL, rețele „wireless”, standarde de conectare în rețea, etc.;

Internet: servere Web, servere de poştă electronică, "firewall", servicii (DNS, DHCP), protocoale specifice, instrumente de administrare;
aplicații: "e-commerce", "e-business", "office", produse antivirus, alte aplicații;;
asigurarea calității: respectarea standardelor industriale în privința calității produselor şi serviciilor;
tendințe ale dezvoltării tehnologiilor hardware şi software, tendințe ale dezvoltării comunicațiilor.

Deprinderi practice:

spirit analitic: identifică informațiile lipsă, analizează logic o situație (problemă) tehnică şi o rezolvă prin soluții noi, inovatoare;
atenție la detalii: obține unui rezultat corect chiar atunci când se află sub presiune, verifică acuratețea (corectitudinea) informațiilor înainte de a le folosi;
pasiune şi entuziasm pentru succesul propriilor acțiuni, dispus către excelentă;
responsabilitate, adaptează timpul de lucru la cerințele activităților;
comunicare eficientă: față în față, la telefon, în scris, prin prezentări, foloseşte noile instrumente ale tehnologiei comunicațiilor: telefoane mobile, SMS-uri, MMS-uri, e-mail, forum-uri, blog-uri, etc.;
orientat către client: alege ceea ce este mai bun pentru utilizatorul final, pentru confortul si profitul lui;
putere de concentrare în situații de stres, hotărâre în luarea deciziilor în timp util;
flexibilitate, învață singur;
inițiativă – nu aşteptă să i se spună ce are de făcut;
caracteristici de conducător: evaluează consecințele posibile ale acțiunilor care vor urma (ale lipsei de acțiune) şi face în aşa fel încât să minimizeze consecințele negative;
tehnici de negociere;
persuasiune – putere de convingere;
spirit organizatoric.

UNITATEA 1

Comunicarea la locul de muncă

Descriere

Unitatea se referă la competența necesară comunicării eficiente, în vederea desfăşurării activităților la nivelul de performanță solicitat de locul de muncă. Administratorul de rețea de calculatoare inițiază şi participă la discuții în vederea găsirii şi folosirii celor mai convenabile soluții de proiectare, implementare, monitorizare, dezvoltare, securizare a rețelelor de calculatoare.

Elemente de competență	Criterii de realizare
1. Colaborează cu toate compartimentele funcționale ale organizației	1.1. Colaborarea pentru stabilirea cererii de echipamente, componente hardware şi/sau software necesare funcționarii rețelei de calculatoare se bazează pe aspectele strategice şi de calitate cerute de organizație. 1.2. Colaborarea pentru stabilirea cererii de echipamente hardware necesare conectării calculatoarelor în rețea şi interconectării rețelelor are la bază soluția IT&C adoptată de organizație. 1.3. Colaborarea cu utilizatorii resurselor rețelei se face pornind de la aplicațiile pe care ei le folosesc şi în conformitate cu nivelul cerut pentru securitatea accesului la informații şi securitatea transmisiilor în rețea..
2. Informează personalul asupra noutăților tehnice din domeniu	2.1. Noile soluții de conectare şi acces la rețea sunt comunicate personalului respectând regulile de securitate impuse pentru lucrul în rețea, cerințele de lucru ale organizației, specificul activităților desfăşurate, performanțele aşteptate în condiții bine stabilite. 2.2. Eventualele modificări / adaptări ale soluției curente de lucru în rețea ca şi implementarea soluțiilor noi sunt din timp aduse la cunoştința personalului. 2.3. Personalul este informat din timp asupra noutăților tehnice care ar putea îmbunătăți performanțele proprii, stilul de viață şi de muncă.
3. Comunică cu utilizatorii	3.1. Comunicarea cu utilizatorii are la bază aplicațiile folosite şi de regulile de securitate ce operează în rețea. 3.2. Fiecare utilizator (angajat, personal de conducere) **ştie** că i-au fost acordate numai privilegiile sau permisiunile de acces necesare şi suficiente pentru efectuarea sarcinilor de serviciu. 3.3 Regulile de securitate ce operează în rețea sunt aduse periodic la cunoştința personalului organizației. 3.4. Incidentele de funcționare a rețelei şi cele de aplicare a regulilor de securitate sunt aduse la cunoştința administratorului de rețea imediat ce au fost detectate. 3.5. În urma primirii unei notificări de apariție a unui incident, transmite către utilizatori operațiile răspuns ce vor fi efectuate. 3.6. Remedierile efectuate vor fi anunțate imediat.

Gama de variabile

Comunicarea poate avea diferite forme:
- orală
- prezentare
- discuții (cu unul sau a mai mulți interlocutori)
- în scris - inclusiv prin mijloace de comunicații moderne (e-mail, forum-uri, blog-uri, site-uri web dedicate, SMS, telefonie fixă sau mobilă, sisteme de semnalizare de orice fel, avertizări, alerte, etc.).

Aspecte strategice şi de calitate:
- strategia de dezvoltare a organizației
- creşterea calității produselor/serviciilor
- creşterea productivității muncii
- îmbunătățirea condițiilor de muncă.

Soluția IT&C implică:
- echipamentele hardware
- produsele, componentelor, aplicațiile software
- regulile de lucru impuse personalului.

Soluția de lucru în rețea implică:
- adaptoare de rețea
- conectori
- medii de comunicații
- echipamente de transmisie şi retransmisie
- reguli de securitate.
- aplicații
- proceduri de acces şi de control

Personalul poate fi:
- angajați
- cadre de conducere

Interlocutori pot fi:
- inginerul de sistem
- programatori - dezvoltatori de aplicații
- operatori calculator şi rețea
- personalul de conducere a organizației
- utilizatori de aplicații
- alți angajați care folosesc echipamente IT&C şi care au acces la resursele rețelei, inclusiv la rețeaua globală Internet
- etc.

Comunicarea va fi adecvată:
- problemei în discuție
- mediului de lucru şi
- experienței interlocutorului
- interesului interlocutorului.

Exprimarea este clară, concisă, corectă şi va folosi termenii tehnici cei mai adecvați, în raport cu gradul de cunoştințe şi de educație ale interlocutorului.

Noutățile tehnice din domeniu se referă la:
- facilitați
- configurații
- tehnologii
- echipamente, componente hardware şi software apărute
- condiții: timp şi costuri

Ghid pentru evaluare

Cunoştinţele necesare se referă la:
- însuşirea şi înţelegerea terminologiei de lucru şi a termenilor tehnici folosiți în vorbirea tehnică, în manuale, documentații de specialitate, ghiduri de utilizare, în ceea ce priveşte atât activitățile şi operațiile din domeniul de activitate al organizației cât şi cele folosite in domeniul IT&C în general şi în domeniul rețelelor de calculatoare în special.
- comunicare şi informare: exprimarea trebuie să fie clară, concisă, corectă şi să folosească termenii tehnici cei mai adecvați, în funcție de cunoştințele şi abilitățile de lucru în rețea dovedite de interlocutor..
- dialogul cu interlocutorul trebuie sa fie deschis, prietenos şi fără ambiguități.

La evaluare se va urmări:
- capacitatea de sintetizare şi redare a evenimentelor importante pentru buna funcționarea a componentelor hardware / software;
- capacitatea de comunicare corectă, concisă şi eficientă cu diferiți interlocutori;
- capacitatea de a asculta cu atenție şi răbdare partenerii de dialog şi de a preîntâmpina eventuale divergențe;
- demonstrarea unor atitudini precum atenție, rigoare, fermitate în luarea deciziilor, aplicarea promptă a deciziilor ierarhic superioare;

UNITATEA 2

Lucrul în echipă

Descriere

Unitatea se referă la competența necesară lucrului în echipă: administratorul de rețea va participa în calitate de responsabil cu proiectarea, implementarea, dezvoltarea şi menținerea în funcțiune în deplină siguranță a rețelei / rețelelor de calculatoare, ca parte a soluției IT&C.

Elemente de competență	Criterii de realizare
1. Identifică rolurile specifice muncii în echipă	1.1. Rolurile îndeplinite de fiecare membru sunt stabilite în funcție de sarcina specifică ce este realizată de echipă. 1.2. Atribuțiile specifice fiecărui membru al echipei sunt stabilite de comun acord în funcție de sarcina specifică indicată de şeful direct. 1.3. Propunerile de îmbunătățire a activității echipei sunt discutate şi agreate în comun.
2. Efectuează lucrul în echipă	2.1. Condițiile de lucru pentru desfăşurarea normală a activității sunt asigurate prin participarea tuturor membrilor echipei. 2.2. Sarcinile echipei sunt rezolvate prin implicarea tuturor membrilor. 2.3. Lucrul în echipă este efectuat cu respectarea drepturilor la opinie ale celorlalți membri şi a regulilor de comunicare inter-umană stabilite. 2.4. Încadrarea activităților echipei în termenele stabilite se face prin respectarea rolurilor specifice şi a responsabilităților individuale ale membrilor echipei.
3. Coordonează tehnic personalul din subordine	3.1. Sarcinile şi atribuțiile personalului din subordine sunt stabilite şi planificate strict în funcție de competențele şi abilitățile dovedite. 3.2. Îndeplinirea sarcinilor individuale ale personalului din subordine este periodic verificată. 3.3. Procedurile de răspuns la incidente petrecute în rețea sunt periodic analizate, corectate şi transmise personalului din subordine.

Gama de variabile

Activități/ sarcini specifice echipei:

- întruniri pentru crearea echipei
- stabilirea activităților, sarcinilor şi termenelor pentru fiecare membru din echipă
- întruniri organizate ad-hoc în urma apariției unui incident în rețea: membrii echipei identifică şi evaluează pierderile de orice fel ce pot apărea, stabilesc măsurile ce vor fi luate ca răspuns la apariția incidentului.
- întruniri pentru prezentarea stadiul la care a ajuns realizarea lucrării, propunerea de îmbunătățiri etc.

Membrii echipei: programatori, inginer de sistem, utilizatori, manageri, responsabili ai diferitelor compartimente funcționale ale organizației, etc.

Membrii echipei de lucru extinse pot fi: şef ierarhic**,** colegi din echipa care efectuează lucrarea, colegi din alte compartimente, furnizori, clienți, consultanți, specialişti în rețele de calculatoare, specialişti în marketing, consilieri juridici, consilieri pe probleme de resurse umane, etc.

Structura echipelor, numărul membrilor, sarcinile principale ale echipelor vor diferi în funcție de domeniul principal de activitate al organizației: instituții bancare, de servicii financiare, de asigurări, producție de maşini şi utilaje, bunuri de consum îndelungat, bunuri şi servicii domestice, transport de marfă şi de persoane, construcții şi instalații pentru construcții, comerț, servicii legate de instruire şi educație, etc.

Ghid pentru evaluare

Cunoştințele necesare se referă la:
- teoria grupurilor, conducerea echipelor, gestionarea şi prevenirea conflictelor, rolul membrilor unei echipe, dinamica grupurilor şi a echipelor.
- modalități de stabilire a obiectivelor şi evaluarea gradului lor de îndeplinire

La evaluare se va urmări:
- capacitatea de analiză, sinteză,
- hotărâre
- fermitate în luarea şi aplicarea deciziilor
- obiectivitatea, operativitatea
- capacitatea de a integra în practică cunoştințele teoretice
- capacitatea de a rezolva probleme şi conflicte
- capacitatea de a negocia şi de a găsi alternative.
- spiritul de prevedere, evaluarea şi asumarea riscurilor, evaluarea consecințelor unor acțiuni (a lipsei de acțiune).
- calități de conducător şi de organizator, puterea de a-i asculta cu atenție pe ceilalți, gândirea creatoare, inovația.

UNITATEA 3

Dezvoltarea profesională

Descriere

Unitatea se referă la competența necesară administratorului de rețea de calculatoare de a se autoevalua permanent în vederea îmbunătățirii propriilor performanțe profesionale; va trebui să facă față evoluției tehnologice atât domeniul rețelelor de calculatoare cât şi în domeniul IT&C şi al activităților specifice organizației (companie, firmă, consorțiu, instituție). Administratorul de rețea de calculatoare este (şi trebuie sa se mențină) expert în rețele de calculatoare şi comunicații.

Elemente de competență	Criterii de realizare
1. Identifică necesarul de cunoştințe specifice activităților din organizație	1.1. Necesarul de cunoştințe de perfecționare este stabilit prin autoevaluare obiectivă şi pe baza observațiilor venite din partea echipei de lucru. 1.2. Materialele de specialitate sunt consultate periodic sau ori de cate ori este necesar în vederea identificării, structurării şi aprofundării informațiilor noi. 1.3. Identificarea de noi surse de informare şi structurarea informațiilor se realizează prin consultarea periodică sau ori de câte ori este nevoie a materialelor de specialitate
2. Îşi însuşeşte cunoştințe noi	2.1. Cunoştințele sunt însuşite corect în urma participării la cursurile de instruire şi prin studiu individual aprofundat. 2.2. Autoinstruirea şi instruirea profesională se desfăşoară periodic, după un plan bine stabilit. 2.3. Cunoştințele dobândite în urma participării la cursuri, seminarii şi prin studiu individual sunt valorificate şi aplicate corect în activitatea curentă, în scopul creşterii calității muncii. 2.4. Manualele, specificațiile tehnice, documentațiile de specialitate sunt folosite pentru optimizarea soluției de rețea curente şi pentru proiectarea soluțiilor viitoare.

Gama de variabile

Organizație poate fi:
- firmă
- instituție
- companie

Materialele documentare de specialitate pot fi:
- publicații de specialitate, studii, lucrări de cercetare
- manuale de prezentare şi exploatare, specificații tehnice
- ghiduri de utilizare ale echipamentelor şi componentelor hardware şi ale produselor software
- materiale prezentate la expoziții, târguri, simpozioane
- documentație electronică, site-uri Internet, forumuri de discuții
- documente primite/ puse la dispoziție/ consultate la stagii de pregătire profesională /de specializare (la care a participat), seminarii, comunități de practică, organizații profesionale.

Ghid pentru evaluare

Cunoștințele necesare se referă la: publicații de specialitate, manuale, site-uri Internet specializate, a altor surse de informare, cunoaşterea diferitelor stiluri de învățare, folosirea programelor specifice de instruire / autoinstruire.

La evaluare se va urmări:
- dorința de autoinstruire şi de dobândire de cunoştințe şi deprinderi noi
- capacitatea de autoinstruire şi de organizare a propriei munci
- obiectivitate în autoevaluarea nivelului de cunoştințe
- capacitatea de analiză şi sinteză a informațiilor
- disponibilitatea pentru achiziționarea de noi cunoştințe
- preocuparea pentru instruirea /autoinstruirea continuă
- consecvența şi aplecarea spre excelență în domeniul de interes
- puterea de muncă şi de concentrare
- capacitatea de a selecta informațiile utile, de a primi şi împărtăşi cunoştințele dobândite
- capacitatea de a relaționa şi de a dezvolta cunoştințe noi.

UNITATEA 4

Aplicarea normelor de tehnica securității muncii şi de prevenire şi stingere a incendiilor

Descriere

Unitatea se referă la competența administratorului de rețea de calculatoare în vederea cunoaşterii şi aplicării normelor de securitate a muncii şi de prevenire şi stingere a incendiilor.

Elemente de competență	Criterii de realizare
1. Aplică normele de protecția muncii	1.1. Legislația şi normele de protecția muncii sunt însuşite şi aplicate în conformitate cu specificul locului de muncă. 1.2. Însuşirea corectă a procedurilor în vigoare este asigurată de participarea la instructajul periodic de protecția muncii. 1.3. Măsurile de prim ajutor sunt însuşite corect.
2. Aplică normele de prevenire şi stingere a incendiilor	2.1. Legislația şi normele de prevenire şi stingerea incendiilor sunt însuşite şi aplicate în conformitate cu specificul locului de muncă. 2.2. Însuşirea corectă a procedurilor în vigoare este asigurată de participarea la instructajul periodic de prevenire şi stingere a incendiilor. 2.3. Echipamentele şi materialele de stingere a incendiilor sunt identificate corect şi rapid conform normativelor.
3. Identifică pericolele	3.1. Pericolele sunt identificate şi raportate imediat persoanei în măsură să le înlăture. 3.2. Pericolele sunt înregistrate în registrul de evenimente şi raportate prompt persoanelor abilitate, conform procedurile specifice. 3.3. Pericolele sunt corect localizate in timp si spațiu.
4. Aplică procedurile de urgență	4.1. Măsurile de urgență şi de evacuare sunt aplicate în conformitate cu specificul locului de muncă. 4.2. Accidentul apărut este semnalat prin contactarea cu promptitudine a persoanelor abilitate, conform procedurile specifice. 4.3. Primul ajutor este acordat rapid şi corect în conformitate cu tipul de accident produs. 4.4. Echipamentul de intervenție este utilizat conform normelor PSI, a celor de protecție şi igienă a muncii.

Gama de variabile

Activitatea se desfăşoară acolo unde există echipamente de conectare la rețea şi/sau de interconectare a rețelelor. Normele de protecție a muncii şi de prevenire şi stingere a incendiilor se aplică oriunde există componente (echipamente) IT&C.

Sisteme de avertizare: sonore, luminoase.

Echipamente de stingere a incendiilor: hidranți, extinctoare, lopeți, nisip, târnăcoape, găleți, etc.

Ghid pentru evaluare

Cunoştinţele necesare se referă la:
- norme de protecția muncii,
- norme de prevenire şi stingere a incendiilor specifice locului de muncă
- plan de evacuare în caz de accidente majore sau incendii
- sistemele de siguranță şi protecție ale echipamentelor
- sistemele de avertizare, de amplasare a hidranților
- etc.

La evaluare se va urmări:
- corectitudinea şi promptitudinea cu care acționează în caz de accident;
- aplicarea normelor de protecția muncii şi de prevenire şi stingere a incendiilor în cadrul activității de rutină; cunoaşterea sistemelor de siguranță şi protecție ale echipamentelor; cunoaşterea sistemelor de avertizare, amplasarea hidranților, etc.
- capacitatea de prevedere, operativitatea în luarea deciziilor

UNITATEA 5
Aplicarea procedurilor de calitate

Descriere
Unitatea se referă la competența necesară aplicării de către administratorul de rețea de calculatoare a procedurilor de calitate, a instrucțiunilor de lucru precum şi aplicării de măsuri preventive şi corective referitoare la îndeplinirea sarcinilor proprii.

Elemente de competență	Criterii de realizare
1. Aplică procedurile de calitate	1.1. Toate activitățile sunt desfăşurate respectând cerințele de calitate cuprinse în documentele de calitate, atât pentru domeniul IT&C cât şi pentru domeniul de activitate al organizației. 1.2. Pentru realizarea exigențelor de calitate sunt utilizate acțiuni preventive şi corective. 1.3. Procedurile de calitate se aplica corespunzător criteriului de calitate aferent.
2. Verifică rezultatele şi remediază neconformitățile	2.1. Deficiențele de calitate sunt constatate prin comparație cu cerințele de calitate. 2.2. Deficiențele de calitate constatate sunt raportate în timp util persoanelor în măsură să stabilească măsurile de remediere. 2.3. Neconformitățile constatate sunt remediate conform procedurilor specifice.
3. Propune actualizări / modificări ale normelor de calitate	3.1. Actualizările/modificările propuse la normele de calitate sunt elaborate conform standardelor aplicabile organizației. 3.2. Normele de calitate propuse sunt comunicate membrilor echipei, precum şi personalului implicat. 3.3. Actualizările propuse sunt înaintate spre aprobare persoanelor îndreptățite.

Gama de variabile
Documente de calitate:
- instrucțiuni de lucru
- proceduri de lucru
- standarde specifice
- etc.

Acțiuni preventive şi corective:
- proceduri reparatorii
- decizii de echipă
- decizii de management
- alocare de resurse în zonele critice
- etc.

Ghid pentru evaluare
Cunoştințele necesare se referă la:
- instrucțiuni de lucru, proceduri, standarde de calitate
- planuri de asigurarea calității
- acțiuni preventive sau corective

La evaluare se va urmări si:
- capacitatea de a lua decizii în conformitate cu procedurile de calitate în vigoare, atenția şi rigurozitatea căutării defectelor
- cunoaşterea standardelor de calitate aplicabile organizației

UNITATEA 6

Organizarea activităților

Descriere
Unitatea se referă la competența necesară administratorului de rețea de calculatoare de a organiza şi planifica activitățile specifice echipei responsabile cu proiectarea, implementarea, menținerea în funcțiune şi dezvoltarea rețelei de calculatoare, componentă a soluției IT&C implementată de organizație.

Elemente de competență	Criterii de realizare
1. Identifică activitățile echipei	1.1. Activitățile sunt identificate conform fluxului informațional, cerințelor de acces şi prelucrare a datelor distribuite în rețea, duratei de viață a echipamentelor şi limitărilor impuse de arhitectura curentă a rețelei şi standardele de conectivitate în vigoare. 1.2. Activitățile identificate sunt plasate într-un graf cu succesiuni şi paralelisme clare. 1.3. Cerințele umane, tehnice şi informaționale ale fiecărei activitati sunt identificate corect.
2. Elaborează proiectul de alocare a resurselor materiale şi umane pentru rețeaua aflată în funcțiune	2.1. Resursele materiale necesare pentru urmărirea performanțelor şi menținerea în funcțiune a rețelei de calculatoare sunt precizate detaliat pentru fiecare componentă: client, server, echipament de conectare în rețea, de interconectare a rețelelor. 2.2. Resursele umane necesare sunt precizate atât numeric, cât şi în raport de competențele cerute. 2.3. Programul operațiilor de control şi întreținere, împreună cu resursele umane şi materiale necesare sunt eşalonate corect în timp.
3. Planifică desfăşurarea activităților necesare întreținerii şi menținerii în funcțiune a rețelei de calculatoare existente	3.1. Activitatea membrilor echipei tehnice responsabile cu menținerea în funcțiune şi dezvoltarea rețelei de calculatoare este planificată, cu periodicitate şi conținut complet stabilite. 3.2. Sarcinile şi responsabilitățile fiecărui membru al echipei sunt precise, concrete, cu termene şi obiective de îndeplinit. 3.3 Pentru fiecare echipament de rețea există un singur responsabil. 3.4. Fiecărui echipament din rețea îi sunt asociate procedurile, operațiile şi termenele de efectuare. 3.5. Activitățile sunt executate conform graficului.

Gama de variabile

Activități care sunt organizate:
- verificarea funcționării conexiunilor la rețea şi a echipamentelor de comunicații,
- monitorizarea performanțelor curente ale rețelei
- monitorizarea funcționării serviciilor de rețea
- monitorizarea încărcării rețelei
- verificarea respectării de către utilizatori a regulilor de securitate
- verificări şi revizii tehnice,

- asigurarea stocului de componente şi materiale
- urmărirea aplicării şi funcționării regulilor de securitate impuse prin strategia de securitate a rețelei
- identificarea vulnerabilităților rețelei, evaluarea riscului de producere a unui incident în rețea
- operarea modificărilor, reconfigurărilor hardware şi software
- etc.

Standardele de conectivitate (IEEE 802.3, 10Base-2, 10Base-5, 10Base-T, 802.11, etc.) se referă la:

- adaptoare de rețea
- topologii
- tipuri de cabluri, lungimi minime şi maxime
- tipuri de conectori
- echipamente de legătură

Arhitectura rețelei poate fi:

- Ethernet, FDDI, Token Ring, ATM, Frame Relay, etc

Ghid pentru evaluare

Cunoştințele necesare se referă la:

- instrumente, tehnici pentru organizarea activităților,
- instrumente, tehnici specifice pentru monitorizare şi supraveghere
- criterii pentru stabilirea parametrilor normali de funcționare a rețelei,
- măsuri, tehnici şi instrumente pentru măsurarea performanțelor componentelor hardware şi a celor software
- tehnici şi instrumente de configurare hardware şi software
- arhitecturi de rețea, topologii, standarde, protocoale, conexiuni la rețea, interconectarea rețelelor, acces la/din rețeaua Internet
- servicii, servere, proceduri client.

La evaluare se va urmări:

- capacitatea de organizare şi planificare
- rigurozitate în îndeplinirea sarcinilor
- respectarea termenelor
- delegarea competențelor de supraveghere, monitorizare, configurare şi administrare
- capacitatea de a conduce şi a controla îndeplinirea sarcinilor.

UNITATEA 7

Proiectarea, instalarea şi administrarea infrastructurii de rețea

Descriere

Unitatea se referă la competența necesară administratorului de rețea de calculatoare pentru proiectarea, instalarea şi întreținerea infrastructurii de rețea de calculatoare care va deservi activități din organizație.

Elemente de competență	Criterii de realizare
1. Stabileşte elementele rețelei	1.1. Sistemele/subsistemele existente în organizație care se bazează pe funcționarea rețelei sunt identificate cu rigurozitate. 1.2. Sistemele/subsistemele identificate pot fi configurate şi supravegheate individual, folosind proceduri specifice. 1.3. Sistemele/subsistemele identificate sunt utilizate conform specificațiilor tehnice ale producătorilor. 1.4. Arhitectura de rețea aleasă, conectarea componentelor în rețea, distribuirea şi configurarea serviciilor conduc la creşterea productivității muncii în organizație, la creşterea atractivității locului de muncă. 1.5. Numărul componentelor de tip server şi al celor de tip client se stabileşte în conformitate cu activitățile desfăşurate în organizație şi cu soluțiile IT&C folosite. 1.6. Serverele şi stațiile client sunt plasate în rețea şi configurate conform regulilor impuse prin strategia de securitate implementată in organizație.
2. Asigură buna funcționare a sistemelor / subsistemelor IT&C bazate pe existența şi funcționarea rețelei de calculatoare	2.1. Soluțiile alese respectă standardele în vigoare şi specificațiile tehnice ale producătorilor. 2.2. Soluțiile alese sunt atent verificate şi corectate, astfel încât aplicarea lor conduce întotdeauna la obținerea de rezultate corecte şi sigure. 2.3. Regulile, soluțiile tehnice şi procedurile stabilite şi folosite pentru replicarea/duplicarea componentelor hardware, a serviciilor, aplicațiilor critice ale sistemelor/subsistemelor asigură funcționarea corectă, sigură şi fără riscuri a sistemelor/subsistemelor IT&C. 2.4. Riscul apariției erorilor previzibile este corect evaluat. 2.5. Soluțiile ce vizează eliminarea sau atenuarea riscurilor, eliminarea erorilor previzibile sunt riguros aplicate. 2.6. La apariția incidentelor neprevăzute, sunt puse în practică proceduri de răspuns special construite.

Elemente de competență	Criterii de realizare
3. Asigură şi verifică utilizarea corectă şi sigură a componentelor rețelei de către personalul organizației	3.1. Regulile stabilite şi implementate asigură accesul controlat şi sigur al utilizatorilor numai la acele resurse de care au nevoie pentru îndeplinirea sarcinilor de serviciu conform fişei postului. 3.2. Datele/informațiile disponibile şi folosite în rețea sunt întotdeauna corecte, sigure şi sunt obținute la timp. 3.3. Regulile stabilite şi implementate pentru urmărirea traficului de informații în rețea, a încărcării rețelei, a performanțelor serverelor şi serviciilor sunt folosite numai pentru evaluarea corectă a stării de funcționare a rețelei şi a componentelor ei. 3.4. Dezvoltarea, adaptarea sau reconfigurarea rețelei se fac pe baza evaluării modului de funcționare si au drept scop creşterea performanțelor serviciilor, diminuarea încărcării rețelei, respectiv diminuarea traficului de date în rețea.

Gama de variabile

Infrastructura de rețea cuprinde:
- componentele hardware folosite pentru conectarea in rețea: adaptoare de rețea, conectori, mediul de comunicații (ex. cabluri), concentratoare (hub-uri), repetoare, bridge-uri, switch-uri, rutere;
- componentele software pentru realizarea conexiunii la rețea: drivere, protocoale de comunicații, proceduri client, aplicații de tip client, reguli de adresare, adrese;
- servicii instalate şi configurate, resurse disponibile în rețea în limita privilegiilor / permisiunilor / restricțiilor definite şi implementate prin regula de securitate.

Serviciile instalate pot fi:
- DNS
- DHCP,
- Serviciul de poştă electronică,
- Serviciul pentru publicarea paginilor web,
- Servicii director de resurse,
- Etc.

Soluțiile IT&C sunt diferite în funcție de:
- tipurile de calculatoare
- arhitectura de rețea, tehnologiile de transmitere de date, echipamente de comunicații
- tipurile de sisteme de operare, serviciile instalate şi modul în care sunt configurate
- sistemele de gestiune a colecțiilor de date
- tipurile de aplicații folosite
- reguli de securitate impuse pentru activități specifice anumitor tipuri de organizații
- etc.

Soluțiile alese se refera la:
- reguli
- soluții tehnice
- proceduri

stabilite şi implementate pentru:
- instalarea

- configurarea
- adaptarea
- depanarea

componentelor hardware şi software ale sistemelor / subsistemelor, precum şi ale aplicațiilor.
Soluțiile tehnice şi procedurile se referă la:

- instalarea componentelor hardware şi software ale sistemelor / subsistemelor / aplicațiilor / componentelor de rețea şi a conexiunilor la rețea;
- configurarea componentelor hardware şi software ale sistemelor / subsistemelor /aplicațiilor / componentelor de rețea şi a conexiunilor la rețea
- adaptarea componentelor hardware şi software ale sistemelor / subsistemelor / aplicațiilor / componentelor de rețea şi a conexiunilor la rețea;
- depanarea componentelor hardware şi software ale sistemelor / subsistemelor / aplicațiilor / componentelor de rețea şi a conexiunilor la rețea;

Resursele la care au acces utilizatorii pot fi: fişiere, aplicații, echipamente, componente

Ghid pentru evaluare

Cunoştințele necesare se referă la:

- calculatoare şi subsisteme hardware,
- sisteme de operare şi componente software, sisteme de fişiere, permisiuni, drepturi, privilegii şi restricții, machete şi reguli de securitate predefinite
- servicii de rețea şi aplicații folosite în rețea, concepte şi arhitecturi de rețea, funcționarea rețelelor,topologii, standarde de comunicații, adrese şi adresarea calculatoarelor din rețea,
- distribuirea şi folosirea serviciilor în rețea,
- medii de comunicații, rețele LAN, WAN, wireless, conexiuni la rețea, conectarea calculatoarelor in rețea, interconectarea rețelelor, rutere, tabele de rutare, servicii de rutare, protocoale de rutare şi protocoale rutabile
- securitatea rețelelor şi a datelor folosite în rețea, resurse distribuite în rețea şi accesul concurent, audit-ul asupra resurselor
- fişiere cu comenzi, fişiere script
- proceduri automate pentru instalarea şi configurarea sistemelor de operare şi a aplicațiilor,
- proceduri şi tehnici pentru instalarea, întreținerea, configurarea hardware şi software a calculatoarelor, rețelelor de calculatoare, a echipamente de comunicații
- proceduri de configurare / reconfigurare hardware şi software
- gestiunea riscurilor

La evaluare se va urmări:

- capacitatea de organizare, spiritul analitic, atenția la detalii, disponibilitatea de a rezolva probleme tehnice prin oferirea de alternative, inițiativa, capacitatea de inovare;
- capacitatea de a sesiza riscurile, asumarea riscurilor;
- capacitatea de a evalua consecințele diferitelor acțiuni, inclusiv consecințele lipsei de acțiune, spiritul de prevedere, hotărârea;
- capacitatea de a lua rapid decizii, concentrarea, capacitatea de asumare a rolului de conducător, obiectivitatea, rigurozitatea în aplicarea regulilor şi a hotărârilor, consecvența, operativitate în selectarea şi atingerea obiectivelor.

UNITATEA 8
Asigurarea funcționalității rețelei de calculatoare şi a echipamentelor de conectare şi de comunicații

Descriere

Unitatea se referă la competența necesară administratorului de rețea de calculatoare pentru: stabilirea de soluții, proceduri, tehnici pentru buna funcționare şi corecta utilizare a echipamentelor de comunicații. Se includ aici procedurile şi tehnicile de monitorizare şi supraveghere împreună cu cele de răspuns la apariția unui incident.. Urmărirea pe termen lung a performanțelor va fi văzută ca un instrument pentru optimizarea funcționării sistemelor, subsistemelor şi aplicațiilor, ca un mijloc de preîntâmpinare şi/ sau detectare din timp a erorilor de funcționare.

Elemente de competență	Criterii de realizare
1. Monitorizează funcționarea rețelei	1.1. Lista parametrilor de referință/control şi valorile etalon folosite pentru evaluarea performanțelor performanțele echipamentelor hardware şi ale componentelor software respectă specificațiile producătorilor şi se încadrează în standarde. 1.2. Fiecare echipament şi fiecare resursă monitorizată sunt caracterizate prin setul propriu de parametri şi valori acceptate, conform standardelor de funcționare şi specificațiilor producătorului. 1.3 Momentele de timp, regulile şi procedurile stabilite pentru supravegherea şi colectarea valorilor parametrilor de referință nu afectează lucrul utilizatorilor şi nici funcționarea sigură a sistemelor/ subsistemelor/ serviciilor / aplicațiilor. 1.4. Regulile, procedurile şi criteriile folosite pentru evaluarea performanțelor nu conduc la ambiguități şi identifică din timp posibilitatea apariției unor erori de funcționare. 1.5. Jurnalele cu valorile măsurate ale parametrilor de referință/control vor fi păstrate şi analizate periodic, în vederea stabilirii corecțiilor suplimentare pentru preîntâmpinarea apariției erorilor de funcționare. 1.6. Jurnalele de evenimente sunt analizate periodic din punct de vedere statistic şi tehnic pentru evaluarea punctelor slabe. 1.7. Punctele slabe, critice, limitările curente sunt eliminate prin folosirea remediilor stabilite conform specificațiilor tehnice ale producătorilor, echipamentelor hardware şi ale produselor software. 1.8. Auditul resurselor folosite de utilizatori este folosit numai în scopul identificării şi preîntâmpinării breşelor de securitate şi respectă legile în vigoare.
2. Detectează nefuncționalitățile hardware şi software	2.1. Pentru evenimentele semnificative, erori, nefuncționalități hard şi soft există proceduri bine stabilite executate de membrii specializați ai echipei tehnice IT&C. 2.2. Evenimentele, erorile, nefuncționalitățile pentru care nu există proceduri standard de remediere sunt evaluate şi se elaborează soluții de remediere. 2.3. Pentru evenimentele şi incidentele pentru care există proceduri standard de remediere se aplică aceste proceduri. 2.4. Vulnerabilitățile identificate sunt corectate cu promptitudine.

Elemente de competență	Criterii de realizare
3.Stabileşte parametrii etalon	3.1. Fiecare componentă monitorizată este evaluată conform etalonului propriu. 3.2. Fiecare etalon este revizuit riguros în cazul reconfigurării infrastructurii de rețea. 3.3. Fiecare etalon este revizuit cu atenție în cazul modificării soluției generale IT&C. 3.4. La baza stabilirii parametrilor etalon stau caracteristicile tehnice şi de funcționare ale echipamentelor.

Gama de variabile

Caracteristici hardware:
- tipul de calculator
- arhitectura calculatorului
- arhitectura rețelei, tipul conexiunilor la rețea, echipamentele de comunicații folosite, gradul de securitate acceptat pentru transmiterea datelor
- etc.

Caracteristici software:
- sistem de operare
- sistem de fişiere
- SGDB
- Sisteme gestiune a colecțiilor de date,
- Servicii de rețea
- Protocoale
- etc.

Soluția IT&C implementata: ansamblul sistemelor, subsistemelor hardware şi software, a serviciilor şi aplicațiilor, a procedurilor, a regulilor de administrare, control si utilizare care formează sistemul informatic al organizației.

Lista de parametrii de referință pentru:
- evaluarea performanțelor de funcționare
- tehnicile şi instrumentele folosite pentru colectarea şi măsurarea valorilor parametrilor
- periodicitatea colectării acestor informații
- criteriile de apreciere
- valorile admisibile

se va stabili pe baza:
- caracteristicilor hardware
- caracteristicilor software
- numărul de utilizatori
- tipul de aplicații folosite
- caracteristicile mediului de comunicații în rețea
- performanțele aşteptate
- etc.

Procedurile şi mijloacele de corectare depind de:
- sistemul de operare
- arhitectura calculatorului
- arhitectura şi caracteristicile rețelei de calculatoare
- aplicațiile şi serviciile folosite
- platformele hardware şi software care funcționează
- etc.

Ghid pentru evaluare

Cunoştinţele necesare se referă la:
- parametrii de stare ai sistemelor / subsistemelor, serviciilor, aplicațiilor şi proceduri de colectare, păstrare, interpretare ale valorilor parametrilor
- instrumente, tehnici pentru monitorizarea, supravegherea funcționării componentelor hardware şi a celor software
- instrumente, tehnici pentru monitorizarea (audit) accesului utilizatorilor la resurse
- sisteme de fişiere şi reguli de securitate
- resurse distribuite în rețea şi acces concurent

La evaluare se va urmări:
- capacitatea de organizare, spiritul analitic, atenția la detalii, disponibilitatea de a rezolva probleme tehnice prin oferirea de alternative, inițiativa;
- capacitatea de a sesiza riscurile, asumarea riscurilor;
- capacitatea de a evalua consecințele diferitelor acțiuni, inclusiv consecințele lipsei de acțiune, spiritul de prevedere, hotărârea;
- capacitatea de a lua rapid decizii, concentrarea, capacitatea de asumare a rolului de conducător, obiectivitatea, rigurozitatea în aplicarea regulilor şi a hotărârilor, consecvența, operativitate în selectarea şi atingerea obiectivelor

UNITATEA 9

Administrarea serverelor

Descriere

Unitatea se referă la competența necesară administratorului de rețea de calculatoare pentru: instalarea, configurarea şi întreținerea hardware şi software a serverelor[3].

Elemente de competență	Criterii de realizare
1. Instalează, configurează şi ~~a~~dministrează echipamentele hardware ale serverului	1.1. Resursele hardware instalate respectă indicațiile fabricantului. 1.2. Resursele hardware instalate şi configurate respectă cerințele soluției IT&C implementate în organizație. 1.3. Accesul şi utilizarea resurselor serverului respectă strategia de securitate a rețelei. 1.4. Pentru resursele hardware critice este asigurată redundanța sau replicarea.
2. Instalează, configurează si administrează serviciile[4]	2.1. Serviciile sunt instalate şi configurate conform specificațiilor elaboratorilor. 2.2. Permisiunile de administrare sunt acordate numai personalului calificat şi cu respectarea strategiei de securitate a rețelei. 2.3. Administrarea serviciilor se face de la distanță folosind instrumente specifice. 2.4. Soluțiile de salvare / restaurare şi / sau redundanță a informațiilor sunt corecte şi eficiente.
3. Supraveghează utilizarea serviciilor	3.1. Jurnalele obținute prin monitorizarea serviciilor sunt păstrate pentru a fi periodic consultate. 3.2. Jurnalele identifică utilizatorii care au avut acces la serviciu, în limita permisiunilor ce le-au fost acordate. 3.3. Jurnalele identifică tentativele nereuşite ale utilizatorilor de a avea acces la servicii. 3.4. Intruşii şi atacatorii din interior şi exterior pot fi identificați prin informațiile păstrate în jurnale.

Gama de variabile

Resurse hardware:
- tipul de calculator
- numărul de procesoare
- tipul şi numărul de hard discuri
- dimensiunea memoriei
- numărul şi tipul adaptoarelor de rețea
- etc.

Resurse software:
- sistemul de operare

[3] Server = care serveşte; un calculator sau un program care oferă servicii altor programe sau unor utilizatori, fie local (la același calculator) fie prin rețea.
[4] Serviciu = funcție oferită (pusă la dispoziție) pentru altcineva (client) de un program sau de un calculator (server).

- serviciul / serviciile instalat / instalate
- protocoalele folosite
- procedurile de filtrare a accesului folosite,
- etc.

Soluția IT&C poate diferi în funcție de :

- tipurile de calculatoare
- arhitectura de rețea, tehnologiile de transmitere de date, echipamente de comunicații
- sistemul de operare, serviciile instalate, modul de configurare a serviciilor
- regulile de securitate impuse

Strategia de securitate include:

- reguli
- norme
- ghiduri de bună practică
- proceduri de răspuns la apariția incidentelor
- proceduri automate de configurare / reconfigurare a serviciilor, aplicațiilor, mediilor de operare ale utilizatorilor,
- etc.

Intruşi şi atacatori: persoane care folosesc o identitate falsă şi penetrează în rețea. Atacatorii preiau controlul asupra sistemului de operare, alterează datele păstrate local şi produc prejudicii organizației sau persoanelor.

Ghid pentru evaluare

Cunoştințele necesare se referă la:

- servicii, ex. DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), poşta electronică, publicarea şi accesul la site-uri web, servicii Director sau Catalog de resurse etc.;
- Protocoale ex. TCP/IP, UDP, LDAP, SMTP, POP, IMAP, HTTP, HTTPS, etc.;
- Servicii de baze de date distribuite;
- Instrumente şi tehnici de administrare a serviciilor, inclusiv administrare de la distanță;
- instrumente, tehnici pentru monitorizarea, supravegherea funcționării componentelor hardware şi a celor software;
- instrumente, tehnici pentru monitorizarea (audit) accesului utilizatorilor la resurse
- sisteme de fişiere şi reguli de securitate
- resurse distribuite în rețea şi acces concurent

La evaluare se va urmări:

- capacitatea de organizare, spiritul analitic, atenția la detalii, disponibilitatea de a rezolva probleme tehnice prin oferirea de alternative, inițiativa;
- capacitatea de a sesiza riscurile, asumarea riscurilor;
- capacitatea de a evalua consecințele diferitelor acțiuni, inclusiv consecințele lipsei de acțiune, spiritul de prevedere, hotărârea;
- capacitatea de a lua rapid decizii, concentrarea, capacitatea de asumare a rolului de conducător, obiectivitatea, rigurozitatea în aplicarea regulilor şi a hotărârilor, consecvența, operativitate în selectarea şi atingerea obiectivelor

UNITATEA 10

Interconectarea rețelelor şi accesul la rețeaua globală Internet

Descriere

Unitatea se referă la competența necesară administratorului de rețea de calculatoare pentru: asigurarea accesului personalului din organizație la resurse aflate în afara rețelei locale[5], inclusiv în rețeaua Internet[6].

Elemente de competență	Criterii de realizare
1. Proiectează soluția de interconectare a rețelelor	1.1..Conexiunile dintre rețele sunt conforme cu arhitecturile rețelelor şi respectă standardele de interconectare. 1.2. Componentele hardware şi software ale echipamentelor de legătură sunt configurate respectând regulile de securitate a transmisiilor de date din strategia de securitate a organizației. 1.3. Tabelele de rutare sunt corect configurate şi indică adresele rețelelor accesibile.
2. Implementează soluția de interconectare	2.1.Instalarea şi configurarea echipamentelor de legătură între rețele respectă instrucțiunile din documentația tehnică a fabricantului. 2.2. Instalarea şi configurarea componentelor software respectă indicațiile elaboratorilor şi sunt conforme strategiei de securitate a organizației. 2.3. Instalarea şi configurarea produselor de tip „firewall" permite accesul în deplină siguranță la resursele rețelelor interconectate. 2.4. Filtrele asociate prin procedurile de tip „firewall" respectă strategia de securitate a organizației.
3. Proiectează şi realizează conectarea la rețeaua Internet	3.1. Cerințele de conectare la Internet sunt identificate în conformitate cu fişa postului pentru fiecare categorie de personal şi respectă strategia de securitate a organizației. 3.2. Accesul permis din rețeaua Internet la serviciile şi serverele organizației este corect identificat şi respectă strategia de securitate privitoare la accesul la informațiile organizației. 3.3. Colaborează cu organizațiile specializate pentru stabilirea conexiunilor la Internet. 3.4. Realizează conectarea la Internet în conformitate cu standardele în vigoare şi cu specificațiile organizațiilor specializate. 3.5. Implementează regulile de securitate pentru accesul la şi din rețeaua Internet în conformitate cu strategia de securitate a organizației.
4. Monitorizează accesul la serviciile locale	4.1. Accesul din Internet la servicii este strict monitorizat pentru detectarea intruşilor şi identificarea „atacatorilor". 4.2. Jurnalele sunt păstrate şi analizate periodic din punct de vedere statistic. 4.3. Detectarea intruşilor şi a „atacatorilor" este urmată de executarea procedurilor predefinite conform strategiei de securitate.

[5] Rețea locală = rețea de calculatoare ce acoperă – în general – o arie locală, restrânsă, ca de ex. un birou, o clădire, un grup de clădiri alăturate.

[6] Internet = rețea globală de servicii standard, rețea de rețele, rețea publică compusă prin interconectarea rețelelor.

Gama de variabile

Arhitecturi de rețea: soluție tehnică şi tehnologică de construire ă rețelelor. Exemple de arhitecturi: Ethernet, Token Ring, FDDI, ATM, Frame Relay.

Echipamente de legătură între rețele: rutere, bridge-uri, gateway-uri.

Strategia de securitate a organizației se compune din totalitatea normelor, regulilor, îndrumarelor de bună practică ce protejează bunurile organizației.

„Firewall": serviciu de filtrare a pachetelor transferate între rețele. Asigură protecția rețelei.

Organizații specializate pentru realizarea conectării la Internet: Internet Service Provider, autoritatea locală de acordare a numelor de domenii cunoscute în Internet şi a adreselor IP;

Intruşi: persoane ce folosesc eventual o identitate falsă şi penetrează neautorizat intr-o rețea de calculatoare.

Atacatori: persoane neautorizate, eventual folosind o identitate falsă, care obțin controlul asupra sistemelor de operare cu scopul de altera informații şi de a aduce prejudicii organizațiilor sau persoanelor.

Ghid pentru evaluare

Cunoştințele necesare se referă la:
- servicii de rutare, protocoale de rutare, protocoale rutabile, tabele de rutare, adrese de rețea;
- servicii, ex. DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), poşta electronică,, publicarea şi accesul la site-uri web, servicii Director sau Catalog de resurse etc.
- Protocoale ex. TCP/IP, UDP, LDAP, SMTP, POP, IMAP, HTTP, HTTPS, FTP, PPP, PPTP, SLIP, L2TP, etc.;
- Arhitecturi de rețea, ex. Ethernet, FDDI, Token Ring, ATM, Frame Relay, etc.
- Adaptoare de rețea, modem-uri, conexiuni „wireless"
- Conexiuni: LAN, WAN, VPN, dial-up, ISDN, ADSL,, etc.
- Proceduri şi metode de autentificare, certificate, servicii tip RADIUS, etc.
- Switch-uri, bridge-uri, rutere, tabele de rutare, protocoale de rutare, VLAN, NAT, RIP, OSPF, etc.;
- Servicii tip „firewall", filtrare de pachete, proceduri de transport, porturi;
- Instrumente, proceduri pentru administrarea de la distanță, ex. SNMP, nslookup, Telnet, etc.

La evaluare se va urmări:
- capacitatea de organizare, spiritul analitic, atenția la detalii, disponibilitatea de a rezolva probleme tehnice prin oferirea de alternative, inițiativa;
- capacitatea de a sesiza riscurile, asumarea riscurilor;
- capacitatea de a evalua consecințele diferitelor acțiuni, inclusiv consecințele lipsei de acțiune, spiritul de prevedere, hotărârea;
- capacitatea de a lua rapid decizii, concentrarea, capacitatea de asumare a rolului de conducător, obiectivitatea, rigurozitatea în aplicarea regulilor şi a hotărârilor, consecvența, operativitate în selectarea şi atingerea obiectivelor

UNITATEA 11

Proiectarea si aplicarea strategiei de securitate a rețelei

Descriere

Unitatea se referă la competența necesară administratorului pentru definirea, proiectarea, implementarea şi urmărirea aplicării strategiei de securitate[7] la nivelul rețelei de calculatoare şi al informațiilor transmise în rețea[8]. Aplicarea componentelor strategiei asigură corectitudinea informațiilor transmise şi folosite in organizație.

Elemente de competență	Criterii de realizare
1. Defineşte strategia de securitate a rețelei	1.1.Cerințele de asigurare a securității rețelei şi a transmisiilor de date sunt identificate pe baza activităților desfăşurate în organizație. 1.2. Vulnerabilitățile şi amenințările sunt corect identificate şi prioritizate. 1.3. Obiectivele activității de management al riscurilor[9] sunt eliminarea, atenuarea sau transferul pierderilor/ pagubelor. 1.4. Fiecărui risc identificat îi corespunde un set de proceduri a căror aplicare conduce la atenuarea sau eliminarea pagubelor.
2. Construieşte şi implementează procedurile cuprinse în strategia de securitate	2.1.Procedurile de securitate respectă principiul apărării în profunzime (stratificată), al privilegiului minim şi pe cel al minimizării suprafeței atacate. 2.2. Procedurile de securitate construite sunt centrate pe protecția datelor, aplicațiilor, sistemelor de operare, echipamentelor, mediilor de comunicații. 2.3. Procedurile de securitate ce trebuie respectate sunt aduse la cunoştința personalului periodic sau în caz de necesitate. 2.4. Sistemele de operare, aplicațiile, serviciile, transmisiile de date, comunicațiile în rețea sunt configurate să aplice automat procedurile de securitate incluse in strategie.
3. Urmăreşte aplicarea procedurilor de securitate	3.1. Jurnalele de evenimente sunt periodic analizate pentru identificarea potențialelor breşe de securitate. 3.2. Reacțiile (feedback) din partea managerilor şi a personalului sunt periodic şi atent evaluate. 3.3. Aplicarea procedurilor de securitate nu violează drepturile persoanelor şi nu împiedică desfăşurarea activităților din organizație. 3.4. Modificările aduse procedurilor de securitate vor fi aduse imediat la cunoştința personalului. 3.5. Detectarea apariției unui incident neprevăzut determină un răspuns (reacție) prestabilit.

[7] Strategia de securitate se compune din totalitatea normelor, regulilor, procedurilor, îndrumarelor de bună practică care protejează bunurile organizației: echipamente hardware de orice fel, produse, aplicații, componente software de orice fel, date şi orice alt fel de informații (desene, planuri, filme audio-video, proprietatea intelectuală de orice fel, etc.).

[8] Informații transmise în rețea pot fi date, voce, imagini grafice, fotografii, imagini video.

[9] Managementul riscurilor este procesul de identificare şi cuantificare a riscurilor împreună cu deciziile asociate ca acțiuni ce vor fi întreprinse pentru atenuarea sau diminuarea pagubelor. Riscul este probabilitatea (posibilitatea) de a suferi o pagubă, o pierdere.

Gama de variabile

Organizație: firmă, companie, instituție.

Procedurile de securitate: succesiuni de operații, acțiuni - de obicei de configurare - ce restrâng, restricționează modul de operare al aplicațiilor şi serviciilor; in alte situații sunt operații ce vor fi executate ca reacție la apariția unor evenimente deosebite. Aceste proceduri sunt descrise în manualele de utilizare sau în ghidurile de bune practici.

Informații transmise in rețea pot fi: date, imagini grafice, fotografii, imagini video, etc.

Ghid pentru evaluare

Cunoştințele necesare se referă la:

- produse antivirus, corecții, patch-uri, upgrade-uri folosite pentru creşterea siguranței rețelei de calculatoare;
- proceduri, tehnici pentru izolarea serverelor şi a serviciilor, proceduri pentru blocarea accesului la diferite resurse,
- proceduri şi tehnici de restricționare a accesului la resurse, servicii, aplicații, echipamente hardware locale sau la distanță;
- conturile utilizatorilor, politica de parole a organizației,
- drepturi, privilegii, permisiuni, restricții, machete de securitate, configurarea restrictivă a mediului de operare al utilizatorilor, inhibarea componentelor software şi hardware ce nu vor fi folosite;
- instalarea şi configurarea automată a sistemelor de operare, instalarea şi configurarea automată a aplicațiilor
- aplicații: "e-commerce", "e-business", "office", produse antivirus, upgrade-uri, alte aplicații, descărcarea automată de upgrade-uri,
- managementul proiectelor: cerințele şi strategiile lucrului în echipă, participarea în echipă, atingerea obiectivelor, conducerea echipei, gestionarea conflictelor
- managementul riscurilor, evaluarea pierderilor, prioritizarea amenințărilor şi vulnerabilităților, modele de analiză a riscurilor (ex. STRIDE) .
- asigurarea calității: respectarea standardelor industriale în privința calității produselor şi serviciilor.
- servicii şi vulnerabilitățile lor, măsuri de protecție,
- autentificarea în rețea, metode de autentificare, servicii de autentificare, certificate, chei publice – chei private, criptări şi decriptări, semnătură digitală, algoritmi de criptare/decriptare, etc.

La evaluare se va urmări:

- spiritul analitic: identifică informațiile lipsă, analizează logic o situație (problemă) tehnică şi o rezolvă prin soluții noi, inovatoare
- capacitatea de a observa detalii: obținerea unui rezultat corect chiar atunci când este sub presiune, verificarea acurateței (corectitudinii) informațiilor înainte de a le folosi
- pasiune pentru succesul propriilor acțiuni, dispus către excelență
- responsabilitate
- comunicare eficientă
- capacitatea de orientare către client, pentru confortul şi profitul acestuia
- capacitatea de a lua decizii în timp util
- flexibilitatea, capacitatea de a învăța singur
- inițiativa – nu aşteaptă să i se spună ce are de făcut
- capacitatea de evaluare a consecințelor posibile ale acțiunilor şi minimizarea acțiunilor negative
- capacitatea de negociere
- puterea de convingere
- spirit organizatoric

UNITATEA 12
Instruirea şi asistarea utilizatorilor

Descriere

Unitatea se referă la competența necesară administratorului de rețea de calculatoare pentru instruirea personalului în vederea folosirii corecte a echipamentelor şi tehnologiilor si asistarea acestuia pentru derularea aplicațiilor in rețea.

Elemente de competență	Criterii de realizare
1. Stabileşte cerințele de instruire ale utilizatorilor rețelei de calculatoare	1.1. Nevoia individuală de instruire / autoinstruire a utilizatorilor este stabilită ca diferență între cunoştințele şi deprinderile actuale şi cele necesare bunei desfăşurări a activității la locul de muncă. 1.2. Nevoia de instruire / autoinstruire a utilizatorilor respectă soluțiile tehnologice implementate sau în curs de implementare şi este în concordanță cu fişa postului. 1.3. Obiectivele instruirii / autoinstruirii - tematica individuală de instruire / autoinstruire a utilizatorilor respectă sarcinile de serviciu, aşa cum apar ele în fişa postului.
2. Organizează activitățile legate de instruirea / autoinstruirea utilizatorilor rețelei de calculatoare	2.1. Planul individual de instruire / autoinstruire al fiecărui angajat este adaptat cerințelor de instruire. 2.2. Planul individual de instruire / autoinstruire respectă tematica individuală şi nu perturbă activitățile desfăşurate în organizație. 2.3. Planul de instruire este întocmit pentru toți utilizatorii pentru o perioadă determinată cerută de conducere.
3. Verifică modul de desfăşurare a instruirii utilizatorilor	3.1. Instruirea utilizatorilor se desfăşoară conform planificării. 3.2. Cunoştințele şi deprinderile utilizatorilor sunt testate şi evaluate periodic. 3.3. Testarea, evaluarea periodică respectă planul individual de instruire / autoinstruire şi sarcinile specificate în fişa postului.
4. Asistă utilizatorii de aplicații în rețea pentru derularea acestora în condiții optime	4.1. Aplicațiile ce se derulează în rețea sunt monitorizate cu atenție. 4.2. Orice abatere de la derularea normală a aplicațiilor este sesizată şi remediată cu promptitudine. 4.3. La implementarea aplicației în rețea se efectuează o instruire detaliată a utilizatorilor aplicației.

Gama de variabile

Obiectivele instruirii / autoinstruirii se stabilesc în funcție de:
- echipamentele şi componentele software folosite
- pregătirea profesională şi experiența angajaților
- specificul de activitate al organizației

- fișa postului
- caracteristicile funcționale ale rețelei,
- competențele individuale
- aplicațiile folosite
- etc.

Elemente concrete ale planului de instruire:
- tematica de studiu
- planificarea în timp
- locul de desfăşurare
- persoana responsabilă (expert, formator, instructor etc.)

Ghid pentru evaluare

Cunoştințele necesare se referă la:
- modalitățile de stabilire a nevoilor de instruire individuală: interviu, chestionar, activități practice semnificative, observare directă, etc.
- tehnici de instruire: prezentări teoretice, demonstrații practice, simulări etc.
- sesiuni de formare continuă

La evaluare se va urmări:
- capacitatea de organizare a unui mediu de instruire sau de studiu individual sau în grup
- coordonarea echipei responsabile