

CURS 1 - Introducere in functionarea unui sistem informational

(notiuni teoretice, definitii, exemple teoretice si practice)

- Cursul “**Introducere in functionarea unui sistem informational** “ se adreseaza tuturor angajatilor unei organizatii : “de la femeia de servicii pana la Directorul General” si trateaza Informatia in toate formele sale, circuitele informatiei, vulnerabilitati, exploatarea vulnerabilitatilor, metode de securizare si redundanta a Sistemului Informational precum si politici de administrare si securizare a Sistemelor Infomationale.
- Nu sunt necesare cunostiinte de operare calculator si retea de date.
- Are o durata de aproximativ 16 ore pe parcursul carora se abordeaza notiuni teoretice, definitii, exemple teoretice si practice.
- Grupa minim 8 persoane pana la maxim 15 persoane.

Tematica CURS 1 pe capitole :

- Sisteme Informationale - Notiuni Introductive, Definitia Sistemului Informational, Exemple de sisteme informationale
- Informatia - Tipuri, Caracteristici, Scop, Formate, Surse, Credibilitate
- Fluxul informatiei – Definitie, Circuite, Intrare, Prelucrare – Filtre si Algoritmi, Salvare, lesire
- Infrastructura Sistemelor Informationale – Definitie, Exemple
- Comunicatie, Prelucrare, Securitate, Redundanta
- Vulnerabilitati – Definitie, Notiuni generale, Exemple, Tipologii
- Vulnerabilitati Interne, Vulnerabilitati Externe
- Exploatarea Vulnerabilitatilor, Implicatiile vulnerabilitatilor
- Securizarea sistemului – definitie, tipologie, exemple
- Securizarea Interna, Securizarea Externa
- Planul de raspuns si actiune in cazul incidentelor – definitie, exemple
- Necesitatea implementarii Planurilor de raspuns si actiune in cazul incidentelor
- Politici de administrare a sistemelor informationale – politica de gestiune, politica de securitate

CURS 2 - Securitatea sistemelor informatice

(notiuni teoretice, implicatii practice directe pentru sistemele de calcul utilizate in activitatea zilnica, exemple practice)

- Cursul 2 : “**Securitatea sistemelor informatice** “ se adreseaza tuturor angajatilor ce utilizeaza in activitatea desfasurata sisteme de calcul, acces la Internet, comunicatii electronice (eMail), periferice (imprimante, copiatoare, faxuri, etc.).
- Prezinta metode specifice practice de protectie informatica la nivelul utilizatorilor.
- Sunt necesare cunostiinte minime de operare calculator si retea de date.
- Are o durata de aproximativ 16 ore pe parcursul carora se abordeaza notiuni teoretice, implicatii practice directe pentru sistemele de calcul utilizate in activitatea zilnica, exemple practice.
- Grupa minim 8 persoane pana la maxim 15 persoane.

Tematica CURS 2 pe capitole :

- Securitatea sistemelor informatice – definitie, exemple, alcatuire/elemente constitutive
- Colaborarea intre sistemele informationale si sistemele informatice
- Probleme de securitate (Brese de securitate) – Definitie, tipologii, exemple (teoretice si practice)
- Implicatiile breselor de securitate – tipologii, exemple (teoretice si practice)
- Vulnerabilitati – Definitie, tipologii, exemple (teoretice si practice)
- Vulnerabilitati – Analiza desfasurata pe categorii – (interne, externe) fizice, logice, factor uman
- Probleme comune de securitate – la nivel sistem de calcul (PC), sisteme mobile (laptop), server, retea (Referinte si exemple practice pentru S.O. Windows)
- Sisteme de securitate informatica - securitatea sistemelor, securitatea datelor (aplicatiilor), Securitatea comunicatiilor/retelelor, Securitatea perifericelor, Managementul sistemelor de securitate IT - nivelul utilizator - (Referinte si exemple practice pentru S.O. Windows)
- Planul de raspuns si actiune in cazul incidentelor – Implementare, Executie, Exemplantic
- Politica IT – Definitie, Utilitate, Implicatii (tehnice, legale si factor uman)
- Politica IT – Implementare, Executie, Exemplantic

CURS 3 - Masuri de prevenire si combatere a incidentelor informatice

(notiuni practice, exemple teoretice si practice, hands-on)

- Cursul “**Masuri de prevenire si combatere a incidentelor informatice** “ se adreseaza angajatilor ce utilizeaza in mod frecvent sisteme de calcul, acces la Internet, comunicatii electronice (eMail), periferice (imprimante, copiatoare, faxuri, etc.), au functii de administrare a acestora, administratori de retea.
- Se Prezinta metode specifice practice de protectie informatica la nivel avansat.
- Sunt necesare cunostiinte avansate de operare calculator si experienta practica.
- Are o durata de aproximativ 16 ore pe parcursul carora se abordeaza notiuni teoretice, notiuni practice, exemple teoretice si practice, simulari de laborator, hands-on.
- Grupa minim 5 persoane pana la maxim 10 persoane.

Tematica CURS 3 pe capitole :

- Securitatea informatica - sistemelor individuale, grupului de calculatoare (retea, lan, intranet), sistemului informatic, securitate perimetrala, acces fizic, acces logic, securitate hardware - UPS, HVAC, alarma, video (schema sistem informatic - cercuri concentrice - niveluri de securitate)
- Atacuri informatice hack, crack, phishing, human error, social engineering, reverse engineering, rea-vointa - acces ilegal, furt, alterare, exploit-uri
- Exemple detaliate de atacuri practice - Romania - raifeissen phishing (mail), bancpost, sectorul privat
- Incidente – interne, externe – hard, soft, human error
- Testarea vulnerabilitatilor - scanere de vulnerabilitate, teste de penetrare, teste decriptare word/excel
- Criptare date - arhivare criptata - parole/nume de fisier, algoritmi de criptare, volume criptate (discuri virtuale)
- Recuperare date sterse/formatate - Aplicatii de recuperare de date
- Autentificare utilizatori – clasice (parole), moderne (card, USB, token), biometrie (amprenta, voce)
- Parole - tipuri de parole - complexitate, valabilitate, rotatie, periodicitate rotatie, managementul parolelor
- Accesare resurse remote – Webmail, Aplicatii si programe, SSL, VPN
- administrare avansata a sistemelor informatice - management hardware, management software, verificare periodica licente, verificare periodica actualizare soft + AV
- Politica IT – definitie, utilitate, implicatii, ramforsare / implementare, inculparea si exonerarea de responsabilitati, exemplu de politica IT