Proceduri de securizare a componentelor aplicaţiilor.

I. Baza de date.

1. Definire categorii de utilizatori:
    a. Utilizatori cu drepturi de scriere de informatii in tabelele bazei de date (administratori).
    b. Utilizatori cu drepturi restrictionate de scriere a informatiilor in anumite tabele ale bazei de date (servicii).
    c. Utilizatori cu drepturi de citire a informatiilor din tabelele bazei de date (studenti).
2. Acces utilizatori: toate categoriile sus mentionate se conecteaza la baza de date folosind nume de utilizator si parola asociata.
3. Monitorizare: se efectueaza prin crearea/ consultarea fisierelor de log ale sistemului de operare.

II. Aplicaţii

1. Categorii de utilizatori
    a. Administratori aplicatii: drepturi depline
    b. Utilizatori aplicatie: drepturi restrictionate, specifice atributiilor locului de munca si functiei
2. Acces: prin selectie categorie, nume de utilizator si parola proprie (aplicatia cere schimbarea parolei o data pe luna).
3. Monitorizare acces: se face prin completarea informatiilor aferente in tabelele dedicate.

III. Aplicaţie web

1. Categorii de utilizatori:
    a. Administratori aplicatii: drepturi depline
    b. Utilizatori aplicatie: drepturi restrictionate, specifice atributiilor activitatii desfasurate in cadrul U.Cv (angajat, student)
2. Acces:
    a. Studenti: acces pe baza de CNP si parola (parola este furnizata studentului de secretariat).
    b. Cadre didactice: acces pe baza de cod utilizator si parola.
    c. Servicii: acces pe baza de cod utilizator si parola.
3. Monitorizare: prin fisierele de log ale sistemului de operare.

IV. Creare si monitorizare parole de administrare

1. Parolele de acces la serverele de comunicatie sunt schimbate periodic sau in caz de necesitate si sunt pastrate in nodurile de comunicatie.
2. Parolele de acces la aplicatiile (de retea sau web) sunt pastrate in format electronic pe servere securizate. Accesul la ele este permis doar persoanelor care asigura administrarea serverelor in cauza si au atributii directe in securizarea datelor.

V. Blocare acces

1. In cazul accesarilor eronate (evidentiate in loguri ca actiuni nepermise), personalul IT al nodurilor de comunicatie poate recurge la blocarea accesului si/sau poate cere masuri administrative.