Ministerul Educaţiei și Cercetării

al Republicii Moldova   
Universitatea Tehnică a Moldovei

Faculatea Calculatoare, Infromatică și Microelectronică   
  
  
  
  
  
  
  
RAPORT

# LUCRARE DE LABORATOR NR. 3

# la Tehnologii ale securității informaționale

**Tema:** Configurarea drepturilor de acces în Windows și Linux.

A efectuat:

st. gr. TI-211 Popa Cătălin

A verificat: Octavian Răducanu

UTM, Chișinău 2023

**Tema:**

Configurarea drepturilor de acces în Windows și Linux.

**Scopul lucrării:**

* Tipuri de conturi de utilizator (Administrator, Guest, Standart)
* Drepturi de acces la fișiere și dosare
* Metodele de autentificare ale utilizatorilor. Autentificare Multi-Factor (TwoFactorAuth.org)
* Information rights management (IRC)

**1. Tipuri de conturi de utilizator (Administrator, Guest, Standart)**

**Există mai multe tipuri de conturi de utilizator în sistemele de operare și programele software. Iată câteva dintre cele mai comune tipuri:**

**- Administrator - Acest tip de cont are drepturi depline și control complet asupra sistemului sau aplicației. Utilizatorii cu un cont de administrator pot instala, dezinstala, configura și modifica setările sistemului sau aplicației, precum și pot gestiona alte conturi de utilizator.**

**- Utilizator standard - Acest tip de cont are permisiuni limitate în comparație cu un cont de administrator. Utilizatorii standard pot utiliza majoritatea funcțiilor și aplicațiilor, dar nu pot face modificări majore la nivelul sistemului sau aplicației, precum instalarea de software sau modificarea setărilor de securitate.**

**- Guest - Acest tip de cont este conceput pentru utilizatorii temporari care nu au nevoie de acces la funcționalitățile complete ale sistemului sau aplicației. Utilizatorii cu un cont de oaspete pot utiliza doar funcțiile și aplicațiile de bază, iar modificările făcute de ei sunt șterse la închiderea sesiunii.**

**- Alte tipuri de conturi - Există și alte tipuri de conturi, cum ar fi conturile de serviciu sau de sistem, care sunt utilizate pentru a executa diferite procese și sarcini de pe sistem sau aplicație. Aceste conturi sunt configurate în mod specific pentru a îndeplini anumite sarcini și au, de obicei, permisiuni limitate.**

**Este important să utilizați un tip de cont de utilizator potrivit în funcție de nevoile și cerințele dvs. De exemplu, pentru a evita pierderea datelor importante sau instalarea de software neautorizat, este recomandat să utilizați un cont de utilizator standard în loc de un cont de administrator pentru utilizarea zilnică a sistemului sau aplicației.**

Mai jos, voi arăta cum am creat un nou utilizator pe sistema Windows 7.

Mai întâi apăsăm pe bara de start și introducem User și tastăm ENTER. După care se va afișa fereastra pentru utilizatori, cum este reprezentat în figura 1 de mai jos.

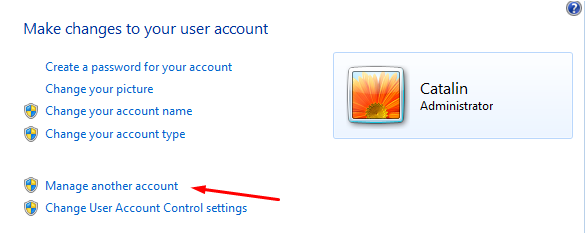


Figura 1. Creare utilizator nou

Mai departe tastăm pe *manage another account* și se va afișa următoarea fereastră, asemenea celei din figura 2 și tastăm *create a new account*.

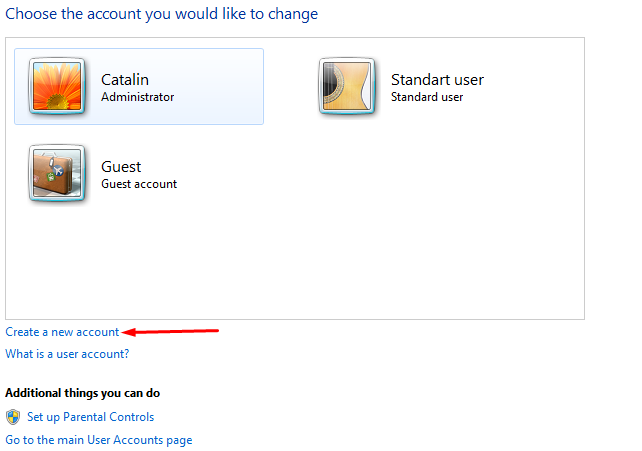


Figura 2. Manage account

În continuare este necesar de a introduce numele utilizatorului și nivelul de permisiune, ca în figura 3, și tastăm *create account*.

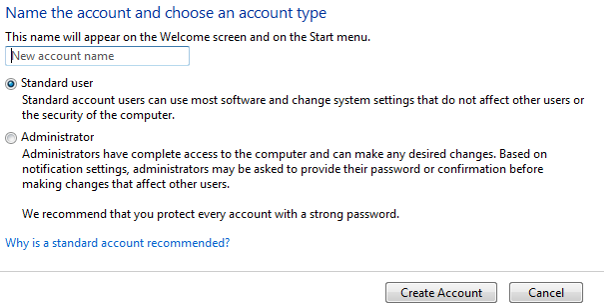


Figura 3. Configure account

Astfel am creat foarte rapid și ușor un nou utilizator, mai departe voi arăta cum putem schimba între ei utilizatorii. Pentru aceasta vom urma mai întâi pasul, reprezentat în figura 4.

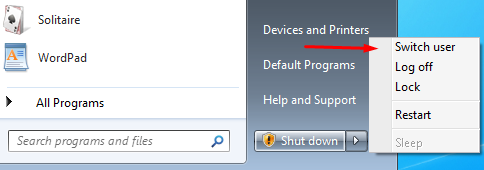


Figura 4. Schimbare utilizator

În rezultat se va afișa fereastra precum în figura 5, în care trebuie să alegem utilizatorul dorit, prin care vom realiza autentificarea. Aici sunt prezenți toți utilizatorii care au fost creați pe calculatorul respectiv.

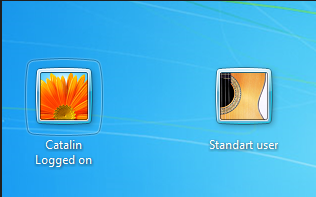


Figura 5. Utilizatori

Observăm că avem doi utlizatori la alegere. Primul este de tip administrator, iar al doilea un tilizator standart.

De asemenea, din setări se poate controlat utilizatorii, la dorință el poate fi activat sau dezactivat. Spre exemplu, în figura 6 este demonstrat un utilizator guest, care este dezactivat.

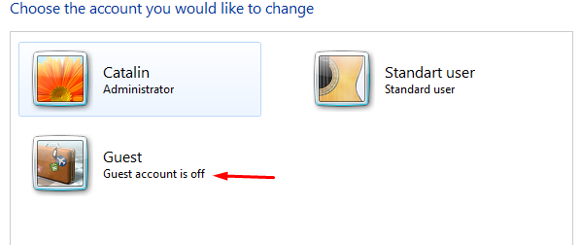


Figura 6. Utilizator dezactivat

**2. Drepturi de acces la fișiere și dosare**

Mai departe voi crea un file de pe administrator, pentru a putea observa dacă el poate fi deschis sau nu de un alt utilizator. Mai întâi este necesar de a crea un file ,după care dăm click dreapta și alegem proprietăți. Aici tastăm pe security și ne va apărea toate setările disponibile pentru a manipula cu permisiunile asupra fișierului respectiv. Aceste proprietăți le putem observa în figura 7.

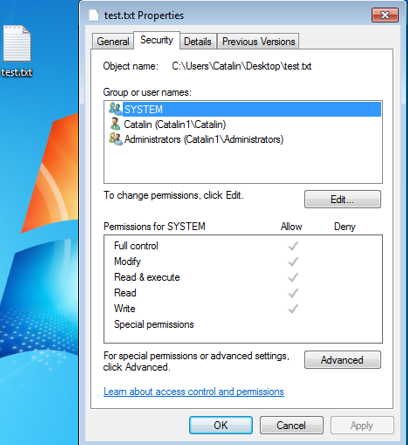


Figura 7. Proprietăți securitate

De exemplu, dacă eu doresc să deschid fișierul respectiv din numele altui utilizator, va apărea o prentâmpinare ca în figura 8, în care ne va informa că nu avem acces la acest fișier, iar pentru al accesa, este nevoie de a introduce parola de la utlizatorul care a creat acest fișier.

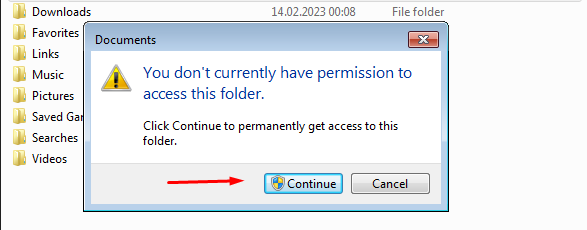


Figura 8. Acces interzis

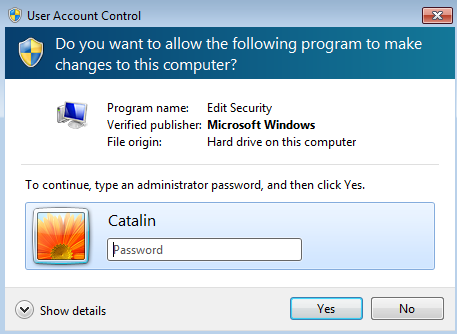


Figura 9. Introducere parolă

După introducerea parolei, observăm în figura 10, că fișierul a apărut și poate fi accesat.

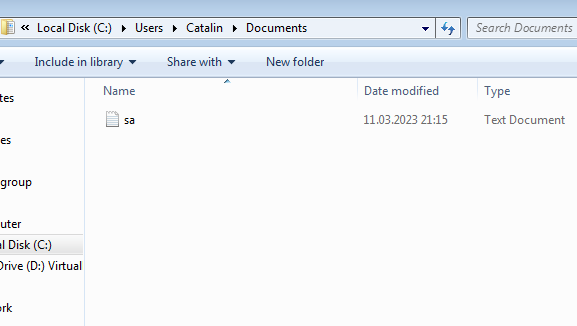


Figura 10. Accesare fișier

Acum voi crea un utilizator nou pentru sistemul linux Ubuntu. Pentru aceasta este necesar de a folosi comanda, precum este prezentat în figura 11.

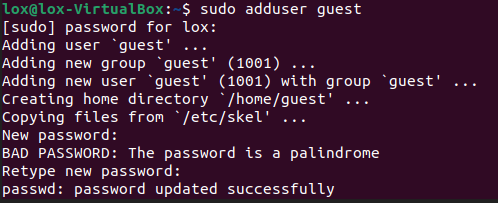


Figura 11. Creare utilizator nou pe Linux

După introducerea comenzii, este necesar de a introduce parola pentru utilizatorul nou, iar după să o confirmăm. Astfel am creat un utilizator nou, cu numele guest.

În continuare, pentru a schimba utilizatorii, urmăm pașii ca în figura 12.

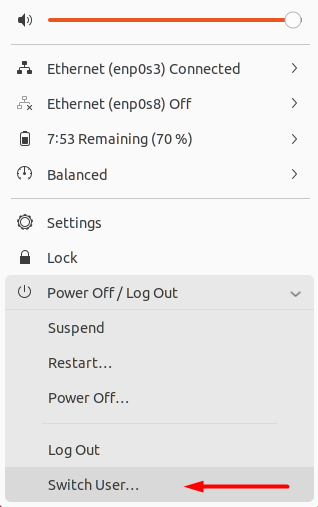


Figura 12. Schimb utilizator pe linux

În figura 13, obsevăm că avem la alegere doi utilizatori. Este nevoie să alegem utilizatorul și să introducem parola.

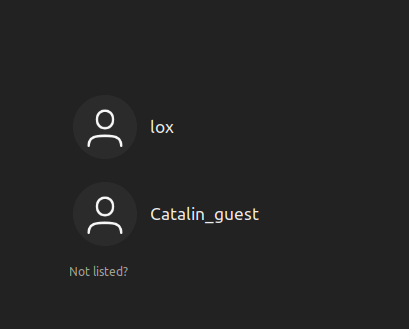


Figura 13. Utilizatori

Acum vom verifica ce accese au ambii utilizatori. Mai întâi verificăm la administrator. Observăm în figura 14, că are toate permisiunile accesibile.

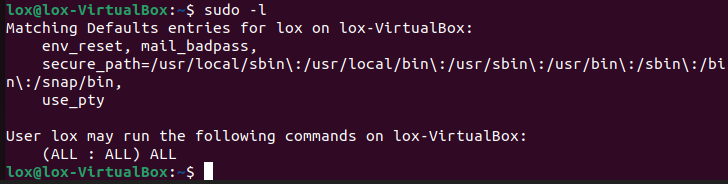


Figura 14. Permisiuni

Acum vom verifica pentru utilizatorul guest. Observăm în figura 15 că are acces limitat. Astfel nu poate folosi toate comenzile și accesa toate documentele.

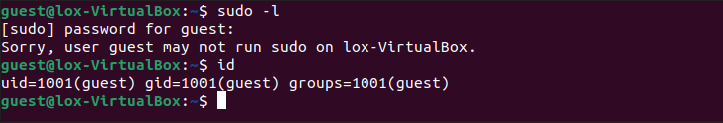


Figura 15. Acces limitat

**3. Metodele de autentificare ale utilizatorilor. Autentificare Multi-Factor (TwoFactorAuth.org)**

Autentificarea utilizatorilor este un proces important pentru a asigura securitatea datelor și accesul la serviciile online. Metodele de autentificare pot varia de la utilizarea unei parole simple până la autentificarea multi-factor.

Autentificarea multi-factor (MFA) este o metodă de autentificare care implică utilizarea a cel puțin două elemente diferite pentru a confirma identitatea unui utilizator. Aceste elemente pot fi de obicei împărțite în trei categorii:

* Ceva ce știe utilizatorul - cum ar fi o parolă, un PIN sau un cod de acces
* Ceva ce are utilizatorul - cum ar fi un token de securitate sau o cheie fizică de autentificare
* Ceva ce este unic utilizatorului - cum ar fi amprenta digitală sau recunoașterea facială

Autentificarea multi-factor este considerată a fi mai sigură decât autentificarea bazată doar pe o parolă, deoarece chiar dacă o parolă este compromisă, atacatorul trebuie să treacă încă peste cel puțin un alt element de autentificare pentru a obține acces. Acest lucru face ca obținerea accesului la contul utilizatorului să fie mult mai dificilă.

Există mai multe opțiuni pentru implementarea autentificării multi-factor, inclusiv prin intermediul aplicațiilor mobile, SMS, e-mail, token-uri de securitate hardware sau software, și altele. Organizațiile pot alege ce opțiuni sunt cele mai potrivite pentru utilizatorii lor și nivelul de securitate pe care doresc să îl ofere.

Un site care oferă mai multe informații și resurse despre autentificarea multi-factor este TwoFactorAuth.org. Este un website care furnizează informații despre autentificarea multi-factor și încurajează utilizarea acesteia pentru a îmbunătăți securitatea conturilor online. Acest site web oferă o listă actualizată a site-urilor web și a serviciilor online care acceptă autentificarea multi-factor și oferă instrucțiuni detaliate despre cum să activați autentificarea multi-factor pentru fiecare dintre aceste servicii. Site-ul oferă, de asemenea, informații detaliate despre diferitele opțiuni de autentificare multi-factor, inclusiv token-uri hardware, aplicații mobile și SMS, și despre avantajele și dezavantajele fiecărei opțiuni. În general, TwoFactorAuth.org își propune să educe utilizatorii despre importanța securității online și să încurajeze utilizarea autentificării multi-factor ca o metodă sigură și eficientă de protejare a conturilor personale și a datelor personale online.

În continuare, pentru exemplu voi arăta cum putem activa autentificare dublă pentru un google cont. Pentru aceasta, mai întâi este necesar să ne logăm pe cont, după care să tastăm pe securitate, cum este arătat în figura 16.

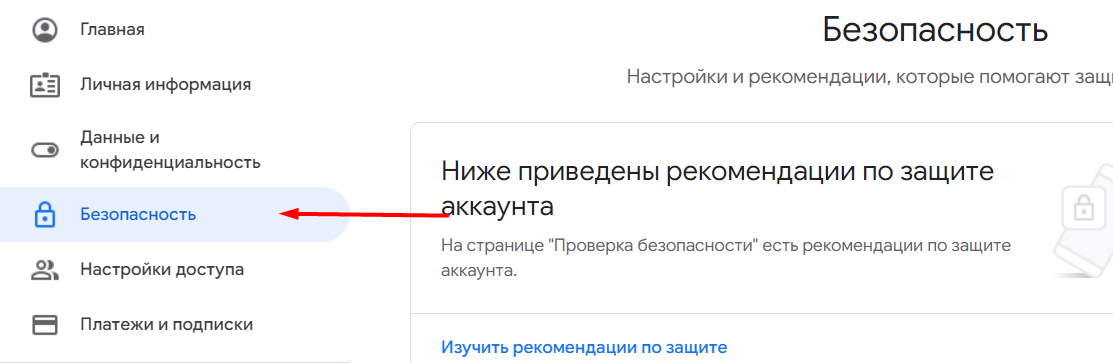


Figura 17. Securitate cont

După care accesăm autentificare dublă. După cum observăm în figura 18, pe contul din exemplu, autentificare dublă este stinsă.

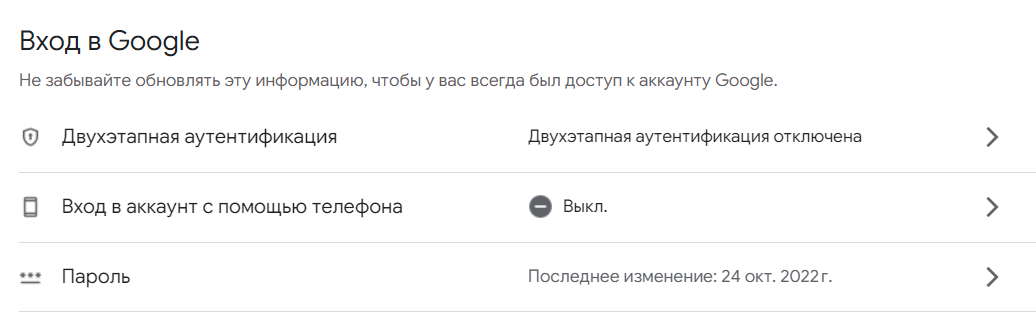
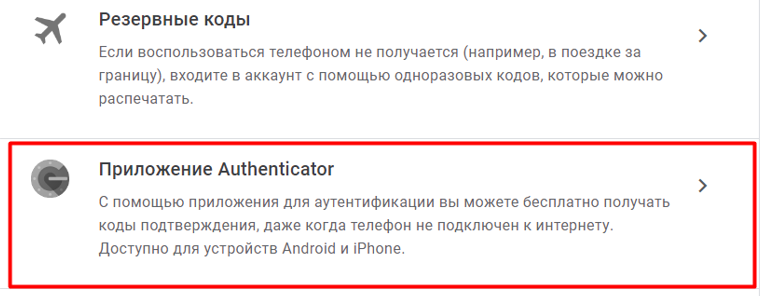


Figura 18. Accesare autentificare dublă

În pasul următor, selectăm aplicație Authenticator ca în figura 19.



În continuare va fi necesar să instalam în telefon, aplicația pe care o vom folosi pentru autentificare. Eu voi folosi google Authentificator. El foarte ușor se poate de instalat din AppStore sau PlayMarket. După care este necesar să creeăm un cont și să tastăm butonul scanare QR-code. QR-codul respectiv al găsim în setări, precum este atașay în figura 20.

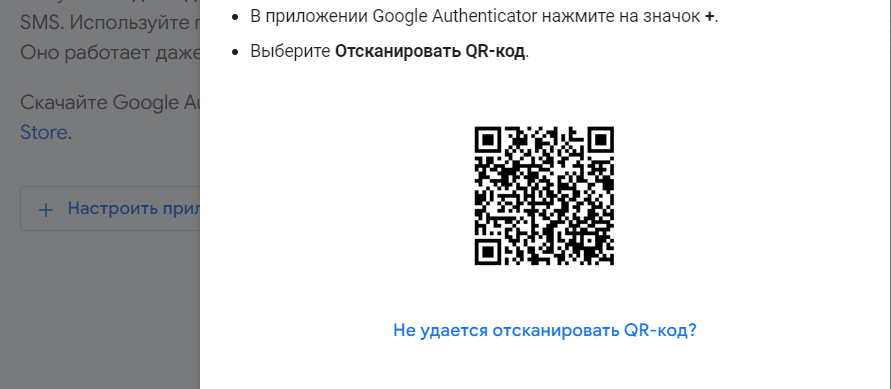


Figura 20. Scanare QR-code

Atât, din acest moment, pentru a ne loga pe contul nostru, va fi nevoie de introdus nu doar parola, dar și codul care este în aplicație, cum observăm în figura 21. Acest cod are un timp limitat, după care se regenerează, pentru a fi cât mai sigur.

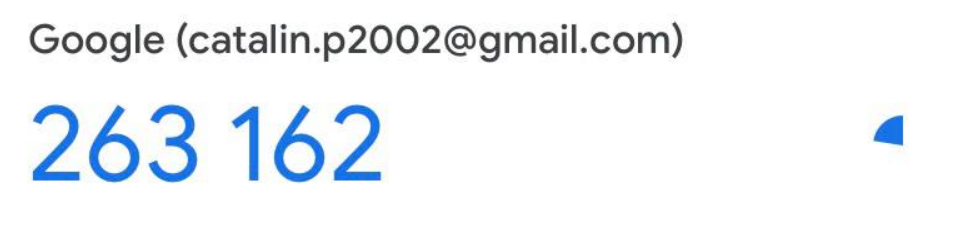
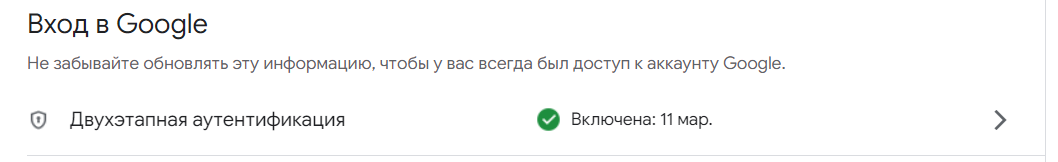


Figura 21. Vizualizare cod

După urmarea acestor pasi, în securitate va fi deja o afișare respectivă.



**4. Information rights management (IRC)**

Information Rights Management (IRM) poate fi definit ca o metodă de protejare a informațiilor prin aplicarea unui set de politici și tehnologii care asigură că doar persoanele autorizate au acces la anumite informații și că aceste informații sunt utilizate numai în modul permis. Această metodă se bazează pe criptare și autentificare și asigură controlul asupra documentelor, fișierelor și altor tipuri de conținut digital.

IRM este o metodă de securitate care ajută la protejarea informațiilor sensibile, cum ar fi informațiile despre clienți, proprietate intelectuală sau alte informații confidențiale. Soluțiile IRM oferă o serie de funcții pentru protejarea informațiilor, inclusiv:

* Criptarea - IRM utilizează criptarea pentru a proteja informațiile sensibile, astfel încât acestea să nu poată fi citite de persoanele care nu au acces la acestea.
* Controlul accesului - IRM permite controlul precis al accesului la informații, ceea ce înseamnă că doar persoanele autorizate pot accesa informațiile protejate.
* Autentificare - IRM utilizează autentificarea pentru a verifica identitatea utilizatorilor și pentru a se asigura că doar persoanele autorizate au acces la informațiile protejate.
* Audit - IRM urmărește accesul și utilizarea informațiilor protejate, astfel încât să se poată detecta orice încercare de acces sau utilizare neautorizată.

IRM poate fi utilizat într-o varietate de industrii și poate fi aplicat la diferite tipuri de conținut, cum ar fi documente, prezentări, e-mail-uri și fișiere media. Soluțiile IRM sunt utilizate în mod obișnuit în mediul de afaceri, în special în domeniul financiar și în domeniul medical, unde protejarea informațiilor cu caracter personal este critică.

În general, IRM este o metodă puternică de protejare a informațiilor sensibile și poate ajuta organizațiile să îndeplinească reglementările de conformitate și să protejeze activitatea de afaceri și reputația.

**Concluzie**

Înțelegerea și implementarea acestor concepte esențiale în cadrul unei organizații poate ajuta la asigurarea securității și protecției informațiilor sensibile și critice. Tipurile de conturi de utilizator, precum administrator, guest și standard, pot fi utilizate pentru a limita accesul la anumite informații și pentru a asigura că numai persoanele autorizate au acces la acestea. Drepturile de acces la fișiere și dosare pot fi utilizate pentru a limita accesul la anumite fișiere și dosare și pentru a controla modul în care acestea sunt utilizate și partajate. Metodele de autentificare ale utilizatorilor, inclusiv autentificarea multi-factor (MFA), pot fi utilizate pentru a verifica identitatea utilizatorilor și pentru a se asigura că doar persoanele autorizate au acces la informațiile protejate. IRM utilizează o combinație de politici și tehnologii pentru a proteja informațiile sensibile și pentru a asigura că acestea sunt utilizate numai în modul permis. IRM poate fi utilizat pentru a proteja informațiile comerciale și de afaceri confidentiale împotriva pierderii, accesului neautorizat sau expunerii.

În concluzie, abordarea cuprinzătoare prezentată în această lucrare de laborator poate ajuta organizațiile să protejeze informațiile sensibile și să respecte reglementările de conformitate. Implementarea acestor concepte poate fi critică pentru protejarea activităților de afaceri și a reputației organizației.