



Cofinanțat de
Uniunea Europeană



FONDUL SOCIAL EUROPEAN PLUS (FSE+)

Programul Educație și Ocupare (PEO) 2021-2027

Prioritate: P9.Consolidarea participării populației în procesul de învățare pe tot parcursul vieții pentru facilitarea tranzițiilor și a mobilității

Obiectiv specific: ESO4.7_Promovarea învățării pe tot parcursul vieții, în special a oportunităților flexibile de actualizare a competențelor și de recalificare pentru toți, ținând seama de competențele antreprenoriale și digitale, printr-o mai bună anticipare a schimbării și a cerințelor de noi competențe bazate pe nevoile pieței muncii, precum și prin facilitarea tranzițiilor profesionale și promovarea mobilității profesionale

Titlu Apel: Competențe digitale pentru piața muncii - Regiuni mai puțin dezvoltate

Titlu proiect: TransformDigital

Cod Apel: PEO/375/PEO_P9/OP4/ESO4.7/PEO_A34

Cod proiect: 336830

Backup-ul datelor – de ce trebuie să ne protejăm documentele înainte să le pierdem

Un document important este aproape finalizat. Ai lucrat la el câteva ore sau poate câteva zile. Calculatorul se blochează, fișierul nu se mai deschide sau descoperi că ai modificat din greșeală versiunea de care aveai nevoie. În acel moment, una dintre primele întrebări este: „Există vreo copie?”

Din păcate, importanța backup-ului este înțeleasă cel mai bine tocmai atunci când informația a fost deja pierdută.

Documentele digitale pot fi afectate de erori umane, probleme tehnice, defectarea unui dispozitiv, programe malițioase sau ștergeri accidentale. Nici experiența utilizatorului și nici calitatea echipamentului nu pot elimina complet aceste riscuri.

Backup-ul reprezintă una dintre măsurile prin care consecințele unui astfel de incident pot fi reduse. Iar regula esențială este simplă: o copie de siguranță este utilă doar dacă există înainte de apariția problemei.

Ce este, de fapt, un backup?

Backup-ul reprezintă o copie de siguranță a datelor, păstrată astfel încât informațiile să poată fi recuperate dacă versiunea utilizată în mod curent este pierdută, deteriorată, ștersă sau devine inaccesibilă.

În funcție de sistemele utilizate, copiile de siguranță pot fi realizate pe alte dispozitive, pe servere, în sisteme de stocare dedicate sau prin servicii online autorizate.

Pentru angajat, important nu este neapărat să cunoască toate detaliile tehnice ale procesului, ci să înțeleagă unde trebuie păstrate documentele profesionale și ce mecanisme de protecție sunt utilizate de organizație.

Salvarea unui fișier într-un loc ales la întâmplare poate face ca documentul respectiv să nu fie inclus în sistemele de backup existente.





**Cofinanțat de
Uniunea Europeană**



„Am salvat documentul” și „am o copie de siguranță” nu înseamnă același lucru

Salvarea este operațiunea prin care păstrăm modificările realizate asupra unui document.

Backup-ul presupune existența unei copii care poate fi utilizată dacă documentul original nu mai este disponibil.

Dacă un fișier există într-un singur loc, pe un singur dispozitiv, salvarea lui nu elimină riscul pierderii.

De exemplu, un document poate fi salvat perfect pe calculator, dar dacă dispozitivul se defectează și nu există o altă copie, informația poate deveni inaccesibilă.

Această diferență este importantă deoarece simplul fapt că vedem fișierul în folder nu înseamnă automat că datele sunt protejate.

De ce se pot pierde documentele?

Pierderea informațiilor nu apare doar în urma unor defecțiuni majore.

Uneori este suficientă o acțiune obișnuită realizată din greșeală.

Printre situațiile care pot afecta datele se numără:

- ștergerea accidentală a unui fișier;
- suprascrierea unei versiuni importante;
- defectarea unui calculator sau a unui dispozitiv de stocare;
- deteriorarea unui document;
- pierderea sau furtul dispozitivului;
- atacurile informatice și programele malițioase;
- erorile apărute în timpul unor operațiuni;
- salvarea documentelor într-o locație greșită;
- modificarea accidentală a unor informații importante.

Nu toate aceste situații pot fi prevenite complet.

Putem însă reduce impactul lor printr-o gestionare responsabilă a informațiilor și prin existența unor mecanisme de recuperare.

Documentele profesionale trebuie păstrate în locurile stabilite de organizație

O greșeală frecventă este păstrarea documentelor importante exclusiv în locații personale sau temporare: pe desktop, în folderul de descărcări, pe un dispozitiv extern propriu sau în alte spații care nu fac parte din sistemul de lucru stabilit.

Chiar dacă documentul este ușor de găsit pentru persoana care l-a creat, este posibil ca acesta să nu fie protejat prin mecanismele organizației și să nu poată fi accesat de persoanele autorizate atunci când este necesar.



**Cofinanțat de
Uniunea Europeană**



Din acest motiv, angajații trebuie să cunoască regulile privind stocarea datelor:

Unde se salvează documentele? Ce spații sunt autorizate? Există un sistem de backup? Ce informații pot fi păstrate local și ce informații trebuie salvate în spațiile comune?

Respectarea acestor reguli face parte din utilizarea responsabilă a tehnologiei.

Cloud-ul și backup-ul nu sunt întotdeauna același lucru

Stocarea online poate oferi funcții utile pentru protejarea informațiilor, precum sincronizarea, istoricul versiunilor sau recuperarea anumitor fișiere.

Totuși, simpla păstrare a unui document într-un serviciu cloud nu trebuie confundată automat cu existența unei strategii complete de backup.

Dacă o modificare sau o ștergere este sincronizată, aceasta se poate reflecta și în spațiul online. Posibilitatea de recuperare depinde de serviciul utilizat, de setările acestuia și de politica organizației.

De aceea, angajații nu ar trebui să presupună că „este în cloud, deci nu se poate pierde”.

Este mai important să cunoască soluțiile aprobate și procedurile de recuperare aplicabile la locul de muncă.

Versiunile anterioare pot salva ore întregi de muncă

Unele aplicații și sisteme de stocare permit păstrarea istoricului modificărilor.

Această funcție poate fi extrem de utilă atunci când un document a fost modificat greșit sau când informații importante au fost eliminate.

În loc să refacem întregul document, poate exista posibilitatea revenirii la o versiune anterioară.

Dar această funcție trebuie cunoscută înainte de apariția problemei.

Este util ca angajații să știe dacă sistemele pe care le folosesc păstrează versiuni, cât timp sunt disponibile și care este procedura corectă pentru recuperarea lor.

Backup-ul nu trebuie improvizat cu soluții nesigure

Teama de pierdere a documentelor poate conduce și la o practică greșită: realizarea de copii în cât mai multe locuri, fără a ține cont de securitatea informațiilor.

Un document profesional nu trebuie trimis către adresa personală de e-mail sau încărcat într-un cont personal de stocare doar pentru a avea „o copie de rezervă”, dacă regulile organizației nu permit acest lucru.

În același mod, utilizarea unor dispozitive USB personale sau a unor servicii online neautorizate poate crea riscuri privind confidențialitatea și securitatea datelor.

Backup-ul trebuie să protejeze informația, nu să genereze o nouă vulnerabilitate.



**Cofinanțat de
Uniunea Europeană**



De aceea, soluțiile utilizate trebuie să fie cele aprobate pentru activitatea profesională.

O copie de siguranță este valoroasă dacă informația poate fi recuperată

Scopul backup-ului nu este simpla existență a unei copii, ci posibilitatea de a recupera informația atunci când este necesar.

O organizație poate avea proceduri clare pentru realizarea copiilor și restaurarea datelor, iar angajatul trebuie să știe cui se adresează atunci când apare o problemă.

În cazul unei ștergeri accidentale, este recomandat să evităm acțiunile improvizate care pot agrava situația și să urmăm procedura stabilită.

Cu cât incidentul este identificat și comunicat mai clar, cu atât pot exista șanse mai bune ca informația să fie recuperată prin mecanismele disponibile.

Organizarea documentelor ajută și la protejarea lor

Backup-ul nu poate compensa complet lipsa organizării.

Dacă există numeroase copii ale aceluiași document, cu denumiri neclare, poate deveni dificil să identificăm versiunea care trebuie recuperată.

O structură coerentă a folderelor și o denumire clară a fișierelor ajută atât activitatea zilnică, cât și situațiile în care trebuie identificată o versiune anterioară.

În loc de „document_nou_final2”, o denumire stabilită după o regulă comună poate permite identificarea mai rapidă a conținutului și a versiunii.

Protejarea datelor începe, așadar, și cu modul în care acestea sunt organizate.

Prevenția durează mai puțin decât refacerea unui document

Unul dintre motivele pentru care backup-ul este amânat este faptul că, atunci când totul funcționează, nu pare urgent.

Problema este că pierderea datelor nu ne anunță înainte să se producă.

Câteva minute necesare pentru salvarea documentului în locația corectă, verificarea sincronizării sau respectarea procedurilor de lucru pot preveni ore sau chiar zile de refacere a informațiilor.

De aceea, protejarea datelor trebuie privită ca parte a activității obișnuite, nu ca o măsură luată doar după apariția unui incident.

Competența digitală înseamnă și să îți protejezi rezultatul muncii

Competențele digitale nu se limitează la capacitatea de a crea un document sau de a utiliza o aplicație.





**Cofinanțat de
Uniunea Europeană**



Un utilizator competent trebuie să înțeleagă și ce se întâmplă cu informația după ce a fost creată: unde este salvată, cine o poate accesa, cum este protejată și dacă poate fi recuperată în cazul unei probleme.

Din această perspectivă, backup-ul este legat direct de utilizarea responsabilă a tehnologiei.

Nu este necesar ca fiecare angajat să administreze sisteme complexe de stocare. Este însă important să cunoască regulile aplicabile propriilor documente și să evite comportamentele care pot pune informațiile în pericol.

Pentru că momentul potrivit pentru a ne întreba „Avem o copie de siguranță?” este înainte ca răspunsul să devină urgent.

Dezvoltarea competențelor digitale prin TransformDigital – ID 336830

În cadrul proiectului TransformDigital – ID 336830, angajații din grupul țintă beneficiază de evaluarea competențelor digitale pentru identificarea nivelului existent și a nevoilor de dezvoltare. În funcție de rezultatele evaluării, participanții sunt orientați către programul Competențe digitale de bază sau către programul de formare Operator introducere, validare și prelucrare date (OIVPD).

Dezvoltarea competențelor digitale presupune și formarea unor comportamente responsabile privind gestionarea informațiilor: organizarea documentelor, utilizarea spațiilor de stocare potrivite, protejarea datelor și înțelegerea mecanismelor prin care informațiile pot fi recuperate.

Astfel, formarea poate contribui la o utilizare mai sigură, eficientă și responsabilă a tehnologiei și la reducerea riscului ca o eroare sau o problemă tehnică să conducă la pierderea rezultatelor activității profesionale.

#TransformDigital #CompetențeDigitale #BackupDate #SiguranțaDatelor #DezvoltareProfesională

Proiect finanțat din Fondul Social European Plus (FSE+) prin Programul Educație și Ocupare (PEO) 2021–2027, în cadrul apelului „Competențe digitale pentru piața muncii – Regiuni mai puțin dezvoltate”.

