CURTEA DE CONTURI A ROMÂNIEI

SERVICIUL PENTRU AUDITUL SISTEMELOR INFORMATICE

REGISTRUL MATRICOL UNIC AL UNIVERSITĂȚILOR DIN ROMÂNIA (RMUR)

Pentru a îndeplini rolul de registru electronic de bază este necesară îmbunătățirea calității informațiilor oferite și a securității bazei de date

Decembrie 2023

De ce a efectuat Curtea de Conturi a României acest audit?

Registrul Matricol Unic al Universităților din România (RMUR) este o bază de date electronică definită drept registru de bază, administrată de Unitatea Executivă pentru Finanțarea Învățământului Superior, a Cercetării, Dezvoltării și Inovării (UEFISCDI), în care sunt înregistrați toți studenții din România. Auditul a vizat evaluarea modului în care RMUR este administrat pentru a îndeplini scopurile pentru care a fost înființat. RMUR urmează a fi înlocuit de RUNIDAS - Registrul unic național integrat al diplomelor şi actelor de studii.

Obiectivele auditului performanței:

- ✓ Evaluarea guvernanței IT;
- ✓ Evaluarea modului în care au fost identificate riscurile asociate cu securitatea informațiilor și a punerii în aplicare a unei strategii de diminuare a riscurilor;
- ✓ Evaluarea măsurii în care sistemul informatic permite realizarea scopurilor colectării și prelucrării datelor studenților.

Recomandările auditului:

- Dezvoltarea unei strategii IT care să contribuie la alinierea activității IT cu obiectivele privind trecerea de la RMUR la RUNIDAS și migrarea în cloud-ul guvernamental.
- Creșterea gradului de securitate a bazei de date, prin efectuarea periodică a unor analize ale riscurilor de securitate și luarea de măsuri suplimentare de securitate; implementarea unor măsuri specifice pentru protecția datelor cu caracter personal.
- Îmbunătățirea gradului de folosire a informațiilor stocate în baza de date și definirea unor proceduri de interconectarea acesteia cu cele deținute de alți actori îndreptățiți să utilizeze aceste date.

Registrul Matricol Unic al Universităților din România (RMUR)

RMUR este utilizat activ pentru îmbunătățirea managementului universitar și a creșterii nivelului de transparență a informațiilor privind studenții, dar pentru a îndeplini rolul de registru electronic de bază, este necesară îmbunătățirea calității informațiilor oferite și a securității bazei de date.

Ce a constatat Curtea de Conturi a României

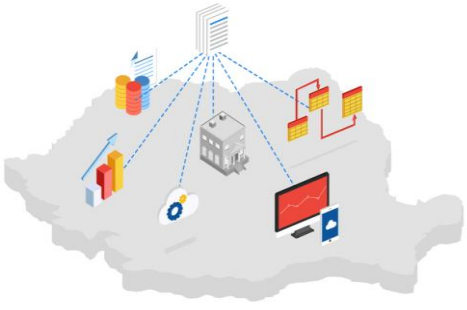
In domeniul guvernanței IT:

- Lipsa unei strategii IT aprobate a condus la implementarea cu unele dificultati de către UEFISCDI a obiectivelor RMUR prevăzute în lege și Regulamentul RMUR;
- Activitățile și operațiunile IT ale UEFISCDI nu au fost conduse de politici și proceduri elaborate formalizat, aprobate și implementate, însă răspunzând la nevoile formulate de Ministerul Educației.

In domeniul securității sistemului informatic:

- Nu a fost efectuată periodic o analiză a riscurilor de securitate a rețelei și a sistemului informatic, însă UEFISCDI a luat masuri pentru asigurarea securitatii;
- Nu sunt implementate Planul de continuitate a activității (BCP) și de recuperare în caz de dezastre (DRP), iar măsurile tehnice și organizatorice pentru protecția datelor cu caracter personal nu sunt complete.

RMUR are nevoie de îmbunătățiri și în ceea ce privește vizualizarea traseului educațional, identificarea situațiilor de dublă finanțare, interoperabilitatea cu operatorii de transport feroviar, furnizarea de date statistice și istorice, accesul la date pentru alte instituţii publice și arhivarea datelor.



Sursă imagine: rei.gov.ro

CUPRINS

Listă de figuri

Listă de abrevieri

AR	Academia Română
ARF	Agenția de Reformă Feroviară
BCP	Plan de asigurare a continuității activității
CCR	Curtea de Conturi a României
CEMU	Consiliul de Etică şi Management Universitar
CNATDCU	Consiliul Naţional de Atestare a Titlurilor, Diplomelor şi Certificatelor Universitare
CNBU	Consiliul Național al Bibliotecilor Universitare
CNFIS	Consiliul Naţional pentru Finanţarea Învăţământului Superior
CNRED	Centrul Naţional de Recunoaştere şi Echivalare a Diplomelor
CNSPIS	Consiliul Național de statistica si Prognoza a Invatamantului superior
DRP	Plan de recuperare în caz de dezastru
GDPR	Regulamentul General privind Protecția Datelor (General Data Protection Regulation)
IIS	Instituţiile de învăţământ superior de stat şi particulare din România, acreditate sau autorizate să funcţioneze provizoriu
IISS	Instituţii de învăţământ superior de stat
INS	Institutul Național de Statistică
ME, MEN, MECS	Ministerul Educației
REI	Registrul Educaţional Integrat

REST API	API sau „Application Programming Interface” este un software care permite unor aplicații să comunice între ele prin internet și diferite dispozitive. REST sau „Representational State Transfer” este un stil arhitectural software care a fost creat pentru a ghida proiectarea și dezvoltarea arhitecturii pentru World Wide Web. REST API este o API care respectă principiile de proiectare REST.
RMUR	Registrul Matricol Unic al Universităţilor din România
ROF	Regulament de organizare și funcționare
UEFISCDI	Unitatea Executivă pentru Finanţarea Învăţământului Superior, a Cercetării, Dezvoltării şi Inovării

Glosar de termeni

Cloud guvernamental	Cloudul guvernamental este livrabilul fundamental al investițiilor în transformarea digitală a României din Planul Național de Redresare și Reziliență, Componenta 7 – Transformare Digitală, care va reuni într-o arhitectură informatică sigură și consolidată instituțiile administrației publice centrale.
Platforma națională de interoperabilitate	Totalitatea proceselor tehnice şi a sistemelor informatice stabilite prin Normele de referinţă pentru realizarea interoperabilităţii în domeniul tehnologiei informaţiei şi comunicaţiilor, pentru asigurarea schimbului de date între sistemele informatice deţinute de participanţii la schimbul de date şi pentru îmbunătăţirea colaborării şi a prestării comune a serviciilor publice.
Rollback	O tehnică folosită pentru a proteja o bază de date împotriva acțiunilor incorecte ale utilizatorului. Starea bazei de date este păstrată și tranzacțiile ulterioare stocate. Dacă utilizatorul decide să implementeze setul total de tranzacții, este emisă o comandă commit. Dacă este folosită comanda rollback, tranzacțiile sunt anulate și nu afectează baza de date.

INTRODUCERE

Registrul Matricol Unic al Universităților din România (RMUR) este o bază de date electronică definită prin Legea educației naționale nr. 1/2011, dar și un registru de bază prevăzut de Legea nr.242/2022 privind schimbul de date între sisteme informatice şi crearea Platformei naţionale de interoperabilitate. În această bază de date sunt înregistrați toți studenții din universitățile de stat sau particulare acreditate ori autorizate să funcționeze provizoriu, precum şi studenții-doctoranzi din Academia Română (AR).

Instituțiile de învățământ superior de stat şi particulare din România, acreditate sau autorizate să funcționeze provizoriu precum şi AR au obligația de a încărca în RMUR datele tuturor studenților din toate ciclurile universitare (licență, master, doctorat).

RMUR ar trebui să asigure un control riguros al diplomelor din învățământul universitar. Registrele matricole ale universităților şi al Academiei Române sunt parte integrantă a RMUR.

Colectarea şi prelucrarea datelor primare privind studenţii şi cursanţii din instituțiile de învățământ superior (IIS) şi AR, prin sistemul RMUR, se fac pentru următoarele **scopuri**[1]:

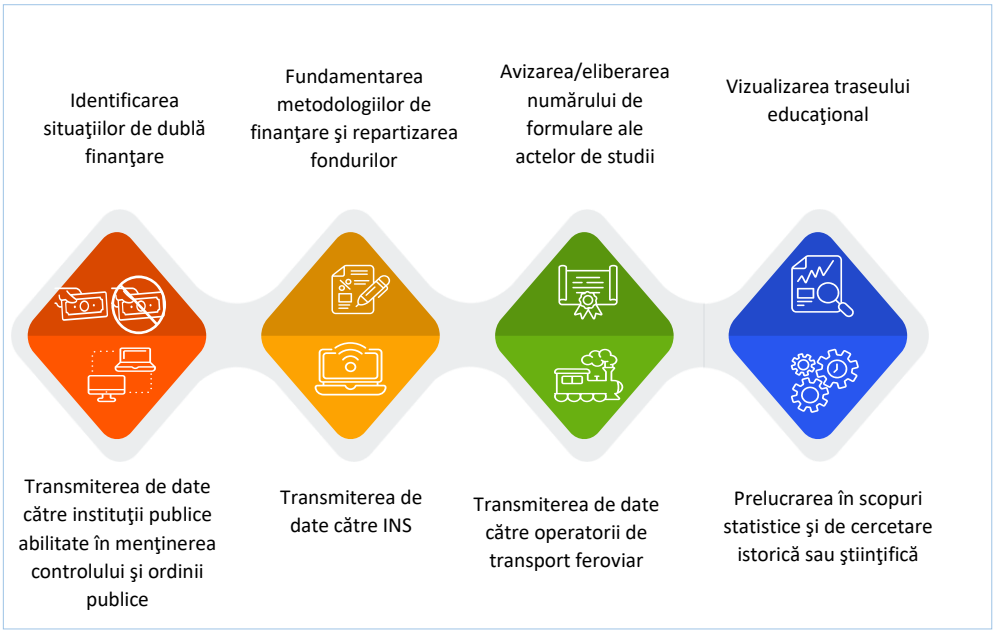


Figura nr. 1 Scopurile pentru care se efectuează colectarea şi prelucrarea datelor primare privind studenţii şi cursanţii din IIS şi AR, prin sistemul RMUR

RMUR este accesat prin intermediul unei platforme web denumită Registrul Educațional Integrat (REI). Prin intermediul REI, RMUR era prevăzut a fi interoperabil cu alte baze de date electronice, atât ale instituţiilor de învăţământ superior de stat şi particulare, acreditate sau autorizate să

[1] Art. 2 din Regulamentul de organizare, funcţionare şi operaţionalizare a Registrului Matricol Unic al Universităţilor din România aprobat prin OMEN nr. 3714/21 mai 2018

funcţioneze provizoriu, cât şi ale instituţiilor de la nivel central. Interoperabilitatea urma a fi realizată în baza unor proceduri specifice (pentru instituţiile din sistemul de învăţământ superior), respectiv a unor protocoale între ME şi alte ministere sau structuri naţionale de care aparţin instituţiile care gestionează celelalte baze de date de la nivel național[2].

Datele colectate în RMUR trebuie prelucrate în conformitate cu prevederile Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date, precum şi ale legislației naționale aplicabile domeniului protecției datelor.

Principalii actori (și utilizatori) implicați în funcționarea REI/RMUR sunt:

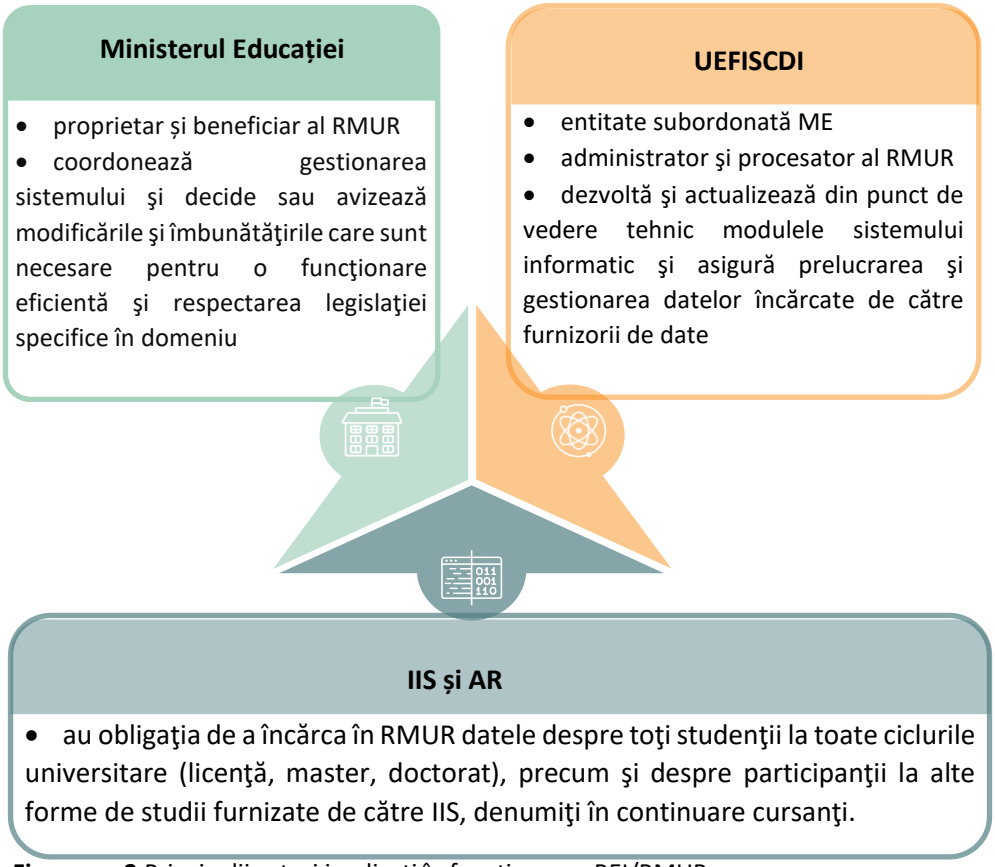


Figura nr. 2 Principalii actori implicați în funcționarea REI/RMUR
Sursă imagine: Curtea de Conturi

În calitatea sa de administrator al RMUR, UEFISCDI are atribuţii[3] atât în domeniul securității sistemului informatic și al rețelei, inclusiv confidențialitatea și disponibilitatea datelor, dar și alte domenii așa cum se poate observa din reprezentarea grafică de mai jos:

[2] Potrivit OMEN nr. 3.714/2018
[3] În conformitate cu prevederile art. 7 din OMEN nr. 3714/2018

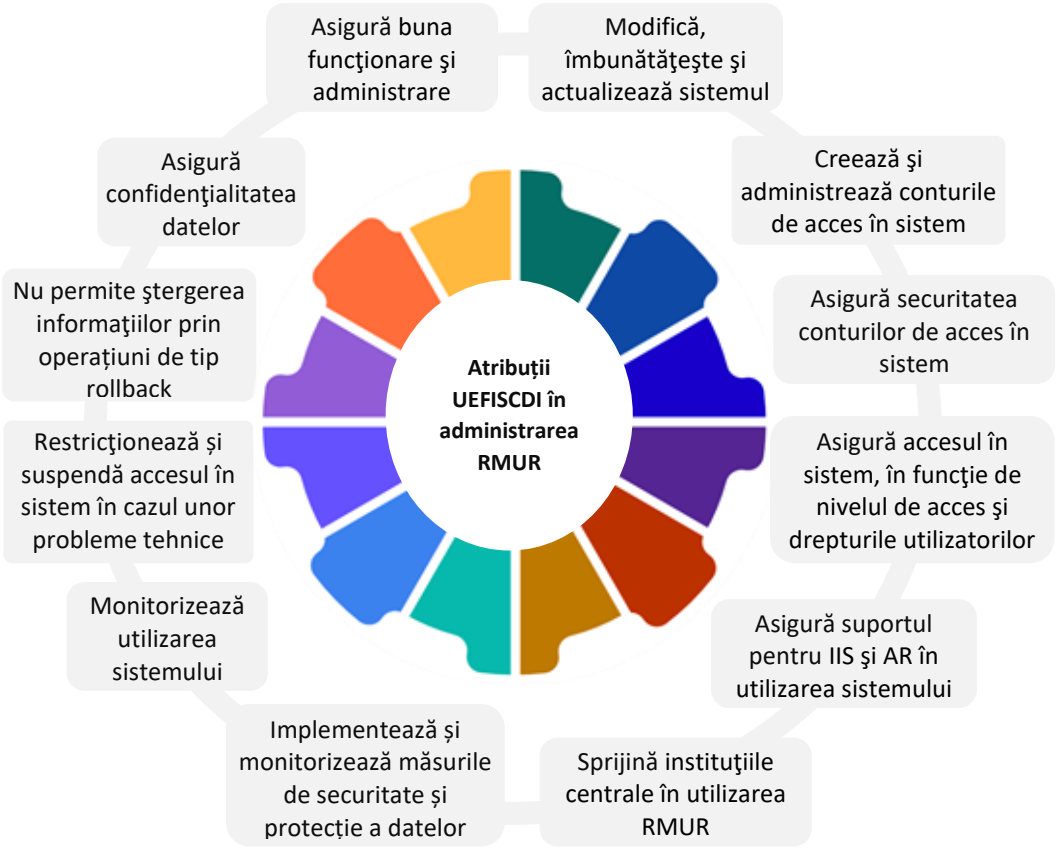


Figura nr. 3 Atribuții UEFISCDI în administrarea RMUR

Sursă imagine: Curtea de Conturi

În sistemul REI/RMUR erau înregistrați în anul universitar 2021-2022 un număr de 535.030 studenți români și străini, de la toate ciclurile universitare ale celor 88 de universități de stat și particulare din România care au încărcat date în sistem[4].

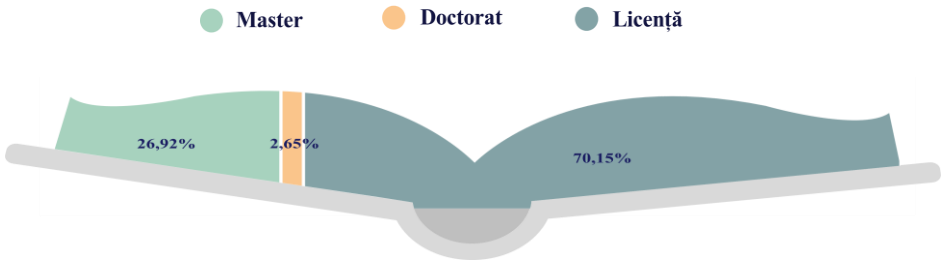


Figura nr. 4 Distribuția studenților în funcție de ciclul de studii în anul universitar 2021-2022

Sursă date: Raport UEFISCDI 2022

[4] Potrivit Raportului UEFISCDI 2022

CONTEXT

Legea educației naționale nr. 1/2011 care a introdus RMUR a fost abrogată de Legea învățământului preuniversitar nr.198/2023 și de Legea învățământului superior nr.199/2023. Potrivit noii legislații, RMUR urmează a fi înlocuit de RUNIDAS - Registrul unic național integrat al diplomelor și actelor de studii.

RUNIDAS va prelua datele şi informațiile existente în RMUR, urmând a fi completat cu toate actele de studii (începând cu finalizarea învățământului liceal) obținute de elevi, studenți, studenți-doctoranzi şi cursanți. Până la operaționalizarea RUNIDAS, va continua să funcționeze RMUR, fără să fie stabilit un termen limită pentru trecerea la RUNIDAS.

În scopul furnizării serviciilor publice, RMUR a fost definit ca registru de bază[5] și alături de alte registre de bază reprezintă fundamentul asigurării interoperabilităţii sistemelor informatice ale autorităţilor şi instituţiilor publice[6].

OBIECTIVUL AUDITULUI

În contextul prezentat mai sus și având în vedere că RMUR urmează a fi migrat în cloud-ul guvernamental, este necesară o evaluare a modului în care acesta este administrat pentru a îndeplini scopurile pentru care a fost înființat. Evaluarea sistemului informatic a avut în vedere domeniile guvernanța IT și securitatea informațiilor. Obiectivul auditului vizează formularea de recomandări pentru ca în RUNIDAS să nu fie perpetuate eventualele slăbiciuni identificate în RMUR.

Pentru a îndeplini obiectivul auditului s-a căutat răspunsul la următoarele întrebări (obiective specifice):

1. UEFISCDI are un sistem funcțional de guvernanță IT care să susțină inclusiv REI/RMUR?

    1.1. Ministerul și/sau UEFISCDI au avut o strategie IT care să cuprindă inclusiv obiective legate de REI/RMUR?

    1.2. UEFISCDI are politici și proceduri adecvate pentru a-și conduce activitățile și operațiunile IT care vizează REI/RMUR ?

2. Au fost identificate riscurile asociate cu securitatea informațiilor și a fost pusă în aplicare o strategie adecvată de diminuare a riscurilor?

    2.1. Există un mecanism bine documentat de identificare și evaluare a riscurilor de securitate a informațiilor, pentru a putea lua măsuri de reducere a acestora?

[5] Art. 7 alin. (1) lit. n) din Legea nr. 242 din 20 iulie 2022 privind schimbul de date între sisteme informatice şi crearea Platformei naţionale de interoperabilitate - reglementează crearea, operaționalizarea și administrarea instrumentului/mijlocului necesar pentru livrarea într-un format integrat a mai multor servicii electronice prin implementarea platformei de interoperabilitate

[6] Art. 6 din Legea nr. 242 din 20 iulie 2022

2.2. Au fost puse în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta că prelucrarea datelor cu caracter personal ale studenților se efectuează în conformitate cu normele legale?

3. În ce măsură sistemul informatic REI/RMUR permite realizarea scopurilor colectării și prelucării datelor studenților și cursanților, în conformitate cu prevederile legale aplicabile?

CRITERIILE DE AUDIT

Pentru a răspunde la întrebările formulate, criteriile de audit avute în vedere sunt prevăzute atât în legislația specifică domeniului auditat cât și în legislația și standardele specifice domeniului IT:

Legislație specifică domeniului auditat	*Legislație și standarde specifice domeniului IT*
• Legea educaţiei naţionale nr. 1/2011, Cap.X Secțiunea 2, art.200-206 • Legea învățământului superior nr. 199/2023, Cap.XVI Secțiunea 2, art. 123-125 • Ordinul MEN nr. 3.714/2018 pentru aprobarea Regulamentului de organizare, funcţionare şi operaţionalizare a Registrului Matricol Unic al Universităţilor din România • O.G. nr. 62/1999 privind înființarea UEFISCDI, aprobată cu modificări prin Legea nr. 150/2000, cu modificările şi completările ulterioare • Regulamentul de organizare și functionare a UEFISCDI aprobat prin Ordinul nr. 5804/2016	• Strategia de securitate cibernetică a României pentru perioada 2022-2027 • Planul de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027 • Regulamentul UE GDPR[7] • Standarde din domeniul IT: – ISO/IEC 27001 Tehnologia informației - Tehnici de securitate - Sisteme de gestionare a securității informațiilor – Cerințe; – ISO/IEC 27002 Tehnologia informației - Tehnici de securitate - Cod de practică pentru controale de securitate a informațiilor; – ISO/IEC 27003 Tehnologia informației - Tehnici de securitate - Sisteme de gestionare a securității informațiilor – Ghid; – COBIT® 2019 Cadru: Introducere și metodologie.

ARIA DE ACOPERIRE ȘI METODOLOGIA

Acțiunea de audit al performanței s-a desfășurat în perioada iulie - decembrie 2023 și a vizat funcționarea și administrarea REI/RMUR în perioada 2022 – 2023.

Pentru desfășurarea misiunii de audit al performanței au fost examinate reglementările legale din domeniu, politicile și procedurile adoptate la nivelul UEFISCDI, Regulamentul RMUR, rapoarte de activitate, alte documente și informații puse la dispoziția echipei de audit de către UEFISCDI.

[7] REGULAMENTUL (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, pus în aplicare potrivit prevederilor Legii nr.190/2018

Pentru a înțelege modul de functionare a sistemului a fost observat modul în care este utilizat sistemul, respectiv ecranul de autentificare, utilizarea meniurilor, generarea rapoartelor.

Pentru a testa unele controale implementate în aplicație și a rezultatelor generate de rapoartele care servesc scopurilor RMUR, au fost folosite 3 conturi de acces în sistem puse la dispoziție de UEFISCDI, cu drepturi de vizualizare, respectiv cont de administrator și cont de utilizator de la nivel de universitate și cont de administrator de sistem REI/RMUR.

Pentru a documenta facilitățile implementate în sistem care contribuie la realizarea scopurilor prevăzute în Regulamentul RMUR, au fost analizate informațiile furnizate de entitate în Chestionarul privind evaluarea funcționalităților sistemului IT.

Pentru înțelegerea funcționalităților sistemului, au fost intervievate persoanele cu atribuții din cadrul UEFISCDI și a fost transmis un chestionar către un eșantion de utilizatori din cadrul universităților.

Obiectivul 1 – UEFISCDI are un sistem funcțional de guvernanță IT care să susțină inclusiv REI/RMUR**?**

1.1. Ministerul și/sau UEFISCDI au avut o strategie IT care să cuprindă inclusiv obiective legate de REI/RMUR **?**

Lipsa unei strategii IT a condus la implementarea cu dificultate a obiectivelor REI/RMUR

Potrivit Regulamentului de organizare și funcționare a UEFISCDI[8], activitatea UEFISCDI trebuie să fie guvernată de un Comitet de monitorizare format din câte un membru al consiliilor consultative ale ME[9] cu atribuţii în domeniul învăţământului superior, cercetării ştiinţifice, dezvoltării şi inovării, de regulă la nivel de preşedinte sau vicepreşedinte al consiliului. Comitetul trebuie să funcţioneze în baza unui regulament propriu şi are atribuţii în monitorizarea activității UEFISCDI şi informarea consiliilor coordonatoare despre rezultatele monitorizării, precum și elaborarea de propuneri referitoare la creşterea calităţii şi eficienţei activităţii UEFISCDI, care se transmit ministerului, ANCSI, conducerii UEFISCDI şi consiliilor coordonatoare.

Elaborarea strategiilor unei organizații este atributul celor însărcinați cu guvernanța, iar Comitetul de monitorizare ar trebui să îndeplinească această funcție prin asigurarea elaborării și aprobării strategiilor UEFISCDI.

O strategie IT este un document care definește obiectivele, direcțiile și politicile unei entități în ceea ce privește tehnologia informației (IT).

[8] Anexa nr.1 la Ordinul MENCS nr. 5804/2016

[9] Consiliul Național pentru Finanțarea Învățământului Superior (CNFIS), Consiliul Național de statistica si Prognoza a Invatamantului superior (CNSPIS), Consiliul de Etică şi Management Universitar (CEMU), Consiliul Național al Bibliotecilor Universitare (CNBU), Consiliul Naţional de Atestare a Titlurilor, Diplomelor şi Certificatelor Universitare (CNATDCU)

Strategia IT furnizează cadrul pentru guvernanța IT, definește obiectivele IT și modul în care acestea vor fi atinse.

Guvernanța IT asigură că aceste obiective sunt atinse prin intermediul unor procese și politici adecvate. Guvernanța IT asigură implementarea strategiei IT și oferă cadrul necesar pentru a asigura că IT este utilizat în mod eficient, sigur și conform cu politicile și reglementările aplicabile.

În concluzie, strategia IT și guvernanța IT sunt două concepte complementare care sunt esențiale pentru succesul oricărei entități. Acestea lucrează împreună pentru a asigura că IT este utilizat în mod eficient, sigur și conform cu politicile și reglementările aplicabile.

Comitetul de monitorizare nu a asigurat guvernanța IT prin elaborarea și aprobarea unei strategii IT a UEFISCDI care să definească obiectivele, direcțiile și politicile legate de IT, strategie care să cuprindă și obiective cu privire la REI/RMUR.

Din probele obținute în timpul auditului a rezultat faptul că acest Comitet de monitorizare nu este constituit și nu a funcționat până la data începerii auditului. De menționat că nu există regulamentul propriu pe baza căruia comitetul să funcționeze, prevăzut de art.36 din Regulamentul de organizare și funcționare a UEFISCDI.

O altă cauză a lipsei strategiei IT este reprezentată de comunicarea deficitară dintre minister, UEFISCDI, comitetul de monitorizare și alte părți interesate. Dezvoltarea unei strategii IT necesită o înțelegere clară a nevoilor și obiectivelor ministerului și a părților interesate. În condițiile în care comunicarea este inadecvată, este mai puțin probabil să se ajungă la un acord cu privire la o strategie IT aliniată obiectivelor REI/RMUR.

Lipsa unei strategii IT poate avea drept consecințe o abordare reactivă în ceea ce privește provocările tehnologice actuale și nu una pro-activă (anticipare de nevoi, testare și implementare din timp a soluțiilor, înainte ca nevoia pentru ele să devină stringentă, imediată).

Lipsa unei strategii IT poate avea efecte pe termen lung și duce la ezitări în adoptarea unor soluții tehnice adecvate.

Entitățile care nu dispun de o strategie IT pot fi mai puțin eficiente în utilizarea resurselor IT și sunt potential vulnerabile la riscuri IT (cum ar fi atacurile cibernetice și pierderea sau compromiterea datelor).

În concluzie, lipsa unei strategii IT la nivelul UEFISCDI nu a permis implementarea eficientă a tuturor obiectivelor REI/RMUR.

1.2. UEFISCDI are politici și proceduri adecvate pentru a-și conduce activitățile și operațiunile IT care vizează REI/RMUR ?

Activitățile și operațiunile IT nu au fost conduse de politici și proceduri elaborate, aprobate și implementate formal

Potrivit art. 28 din Regulamentul de organizare și funcționare a UEFISCDI[10], Serviciul informatică şi infrastructură suport are atribuţii în asigurarea integrităţii şi protecţiei datelor (politici antivirus, politici de back-up şi politici de recuperare a datelor în caz de dezastru).

Ca urmare UEFISCDI trebuie să documenteze, aprobe și comunice politici și proceduri adecvate pentru a conduce activitățile principale și operațiunile IT pentru îndeplinirea atribuțiilor sale. Politicile, procedurile sau reglementările interne trebuie formulate astfel încât să se asigure gestionarea riscurilor critice.

O politică de securitate IT este un document care definește obiectivele, principiile și procedurile de securitate IT ale unei entități. Această politică este esențială pentru protejarea activelor IT ale UEFISCDI, cum ar fi datele, sistemele și rețelele.

UEFISCDI nu a avut o politică de securitate și drept consecință nici măsuri de implementare a unor controale IT. Cu toate acestea, printre procedurile operaționale elaborate și aprobate în procesul de implementare a controlului intern managerial au fost identificate două proceduri care vizează domeniul IT, respectiv:

- ✓ P.O. 08 - Procedură privind dezvoltarea și utilizarea platformelor IT;
- ✓ P.O. 18 - Procedura privid securitatea IT pentru personalul UEFICSCI.

Aceste proceduri operaționale conțin doar definiții și enumără câteva principii generale privind securitatea IT. Cele două proceduri au fost elaborate în anul 2019 și nu au fost ulterior actualizate.

Actualizarea periodică, cel puțin anual, a unei politici sau proceduri de securitate IT este esențială pentru următoarele motive:

- Pentru adaptarea la noile amenințări și vulnerabilități. Tehnologia se dezvoltă rapid, iar amenințările și vulnerabilitățile de securitate IT apar în mod constant. O politică de securitate IT care nu este actualizată poate fi ineficientă în protejarea activității UEFISCDI de aceste amenințări.
- Pentru a reflecta schimbările în activitate. UEFISCDI poate schimba în timp modul în care funcționează. Acest lucru poate avea un impact asupra necesităților de securitate IT. O politică de securitate IT care nu este actualizată poate să nu reflecte aceste schimbări.
- Pentru a se asigura că politica este implementată și respectată. O politică de securitate IT care nu este actualizată poate fi dificil de implementat și de respectat de către angajații UEFISCDI.

Pe de altă parte, platforma REI/RMUR este accesată de utilizatori din exteriorul UEFISCDI, respectiv utilizatori din cadrul universităților înrolate în sistem, ME, consiliile consultative ale ME etc. Astfel, la data auditului

[10] Aprobat prin Ordinul MENCS nr.5804 din 23.11.2016, publicat în M.O. nr.994 din 9 decembrie 2016

sistemul avea un număr mare de utilizatori, respectiv 3.012 utilizatori[11], din care 1.851 utilizatori din cadrul universităților. Pentru utilizatorii externi, cele două proceduri operaționale menționate nu stabilesc reguli sau proceduri de securitate IT.

În cuprinsul celor două proceduri se fac referiri la o politica de securitate și sunt enumerate câteva principii generale ale unei politici de securitate, dar UEFISCDI nu a avut și nu are la data auditului o politică de securitate.

O politică de securitate definește ce trebuie făcut, în timp ce o procedură de punere în aplicare a unei politici definește cum se face.

O comparație între conținutul unei politici de securitate și conținutul unei proceduri de punere în aplicare a unei politici este prezentat în ilustrația grafică de mai jos.

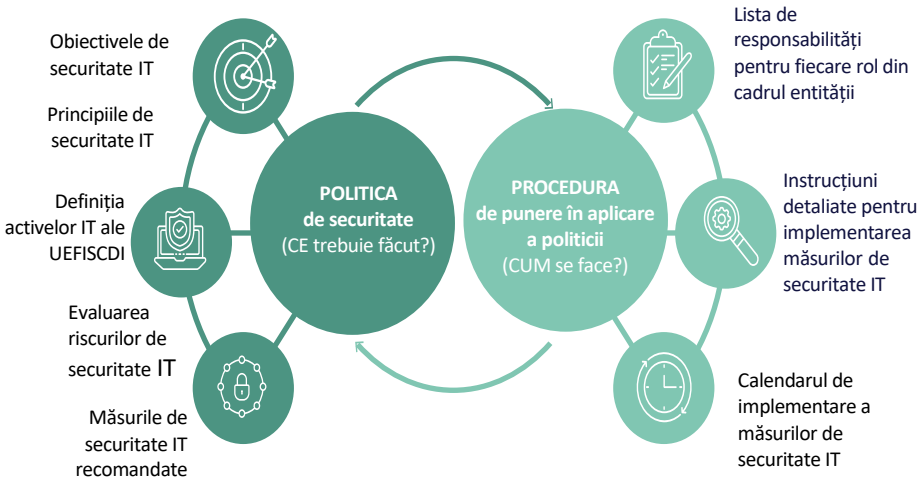


Figura nr. 5 Comparație între conținutul unei politici de securitate și conținutul unei proceduri de punere în aplicare a politicii

Sursă imagine: Curtea de Conturi

De exemplu, o politică de securitate IT ar putea declara că toate datele cu caracter personal ale studenților din REI/RMUR trebuie protejate prin criptarea datelor. Procedura de punere în aplicare a acestei politici ar putea oferi instrucțiuni detaliate despre cum să fie implementată criptarea datelor, de exemplu ce software să fie utilizat, cum să fie configurat software-ul și cum să fie instruiți angajații despre cum să utilizeze software-ul.

O politică de securitate și procedura de punere în aplicare a acesteia ar trebui să fie elaborate împreună pentru a se asigura premisele că politica poate fi implementată în mod eficient.

Cu toate că nu a existat o politică de securitate și o procedură de punere în aplicarea acesteia, compartimentul IT a implementat o serie de controale de securitate, cum ar fi controlul accesului (fizic și logic), dar acestea nu sunt documentate, pentru a se stabili eventuala lor conformitate cu obiectivele de securitate dintr-o politică de securitate. Aceste controale nu sunt aprobate și revizuite periodic de către conducere

[11] UEFISCDI are aprobat un număr maxim de 120 de posturi care pot fi utilizatori.

pentru a se stabili dacă acestea contribuie la realizarea obiectivelor REI/RMUR sau ale obiectivelor generale și specifice ale UEFISCDI.

Pe de altă parte, UEFISCDI nu are o politică antivirus, politică de back-up și politică de recuperare în caz de dezastru care să asigure cadrul pentru integritatea și protecția datelor, în condițiile în care, potrivit ROF, elaborarea acestor politici revenea Serviciului informatică și infrastructură suport. In timpul auditului, au fost luate măsuri de elaborare și aprobare a acestor politici.

Inexistența unor politici pentru securitatea informațiilor a fost determinată de subestimarea necesității acestor politici, motivat de percepția că UEFISCDI este o entitate de dimensiuni reduse, ceea ce a condus la nealocarea resurselor necesare pentru dezvoltarea și implementarea acestor politici. Dezvoltarea și implementarea unei politici de securitate poate fi costisitoare și consumatoare de timp. UEFISCDI are un buget limitat și nu are personal dedicat securității informatice și a considerat dificil sau neprioritar să isi formalize o politică de securitate.

Deși are atribuții în acest sens, compartimentul IT nu a elaborat aceste politici datorită resurselor limitate, compartimentul având un număr de 8 posturi din care 7 erau ocupate la data auditului, în condițiile în care se administrează un număr de 13 platforme informatice.

Absența politicilor IT la nivelul entității a condus la lipsa procedurilor sau instrucțiunilor adecvate, expunând entitatea la vulnerabilități. De exemplu, lipsa unei politici de securitate putea sa faca entitatea vulnerabilă la:

- atacuri cibernetice (cum ar fi: furtul de date, ransomware și malware), ce pot avea un impact semnificativ asupra funcționării REI/RMUR, inclusiv pierderi financiare și de date;
- pierderi de date, ce ar putea duce la furturi de identitate (sistemul stocând date personale) ce pot atrage sancțiuni legale, costuri financiare și afectarea imaginii UEFISCDI;
- incidente de securitate (cum ar fi: acces neautorizat, coruperea datelor sau întreruperi ale serviciilor) ce pot perturba operațiunile REI/RMUR și pot atrage pierderi financiare.

Personalul UEFISCDI a fost pregătit în vederea diminuării potențialelor vulnerabilitati, acesta participând la exercitile naționale legate de securitatea cibernetică precum și prin sistemele informatice implementate prin proiecte naționale prin care au beneficiat o bună parte din institutile publice.

În concluzie, la nivelul UEFISCDI nu au fost elaborate, aprobate şi implementate politici și proceduri formalizate pentru a conduce activitățile principale și operațiunile IT care privesc REI/RMUR intr-un cadru organizat si trasabil, insa a intreprins activitati asociate cu acestea prin initiative institutionale si organizatorice.

Obiectivul 2 – UEFISCDI a identificat riscurile asociate cu securitatea informațiilor și a pus în aplicare o strategie adecvată de diminuare a riscurilor?

2.1. UEFISCDI are un mecanism bine documentat de identificare și evaluare a riscurilor de securitate a informațiilor, pentru a putea lua măsuri de reducere a acestora?

Nu a fost efectuată 0 analiză a riscurilor de securitate a rețelei și a sistemului informatic; sistemele/echipamentele informatice critice și principalele riscuri nu au fost evidențiate

Potrivit art. 28 din Regulamentul de organizare și funcționare a UEFISCDI[12], Serviciul informatică şi infrastructură suport are atribuţii în asigurarea integrității şi protecţiei datelor.

Ca urmare, UEFISCDI trebuie să efectueze şi să actualizeze periodic o analiză a riscurilor de securitate a reţelei şi sistemului informatic, identificând sistemele/echipamentele informatice critice pentru funcționarea REI/RMUR şi principalele riscuri.

În acest context, este necesară de asemenea elaborarea și punerea în aplicare a unui program de asigurare a securităţii personalului prin care să se identifice obiective şi să fie stabilite cerinţe de securitate pentru fiecare etapă a relaţiei cu angajaţii UEFISCDI și cu utilizatorii externi REI/RMUR.

UEFISCDI nu are o procedură de identificare și evaluare a riscurilor și nu deține un registru al riscurilor de securitate cibernetică. Nu s-a efectuat periodic o analiză a riscurilor de securitate a reţelei şi a sistemului informatic care asigură funcționarea REI/RMUR.

Totuși, UEFISCDI a întreprins măsuri de securitate de ordin tehnic.

În fișele posturilor și în contractele de muncă ale personalui IT nu se regăsesc clauze privind responsabilitățile personalului în ceea ce privește asigurarea securității, atât pe durata activității în cadrul UEFISCDI, cât și după încetarea contractului. De asemenea, nu există documente din care să rezulte asumarea de către personalul universităților care operează în RMUR și a utilizatorilor din ME sau alte entitati cu acces in sistem, a unor angajamente legate de respectarea unor cerințe minime de securitate.

În ce privește crearea și administrarea conturilor de utilizator, nu au fost elaborate și aprobate proceduri, care să conțină cerințe minime de complexitate a parolelor, durata minimă de valabilitate a acestora, etc. În sistem existau la data auditului 1.851 conturi de utilizator la nivel de universități, din care 469 de conturi (25,33% din total) care nu folosesc adrese oficiale de email asociate domeniilor web deținute de universități. Astfel, sistemul permite folosirea conturilor gratuite de email cum ar Google, Yahoo, Hotmail etc. Nu a fost identificat vreun control care să testeze periodic valabilitatea conturilor de email și să certifice autenticitatea conturilor de utilizator.

În medie, 70% din utilizatorii de la nivelul IIS care au răspuns la chestionarul privind utilizarea REI/RMUR, au indicat faptul că există implementate cerințe cu privire la parole: schimbarea parolei la prima autentificare,

[12] Aprobat prin Ordinul MENCS nr.5804 din 23.11.2016, publicat în M.O. nr.994 din 9 decembrie 2016

lungimea și complexitatea acesteia. Datele sunt prezentate în graficul de mai jos:

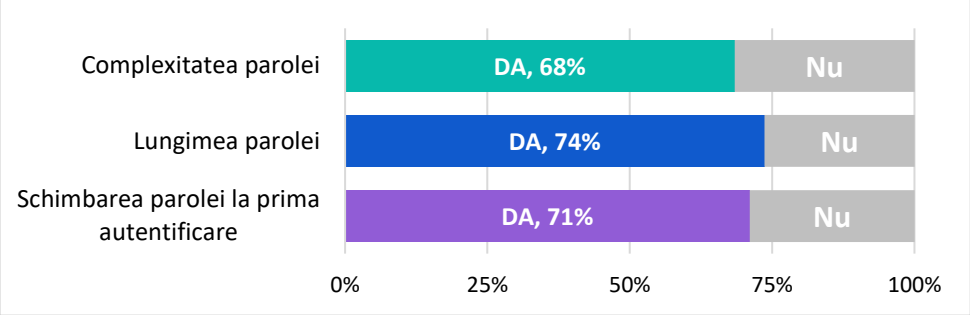


Figura nr. 5 Grafic privind răspunsurile utilizatorilor de la nivelul IIS referitor la cerințele pentru parole

P.O. 18 - Procedura privind securitatea IT pentru personalul UEFISCDI, elaborată în anul 2019 fără a mai fi ulterior revizuită, nu răspunde cerințelor actuale pentru un program de securitate a personalului și nu are referințe la standardele general acceptate în domeniu. Procedura este aplicabilă doar personalului UEFISCDI, iar UEFISCDI ca administrator al sistemului nu are cerințe de securitate elaborate, aprobate și comunicate pentru utilizatorii externi.

Utilizatorii REI/RMUR au exprimat unele îngrijorări cu privire la securitatea și confidențialitatea datelor. În răspunsurile la chestionar, a fost sugerată necesitatea separării drepturilor de acces. De exemplu, respondenții consideră că în cazul utilizatorilor de nivel secretariate IIS ar trebui eliminate drepturile de acces la datele de la școlile doctorale și invers.

Sistemul informatic REI/RMU, permite însă stabilirea drepturilor de acces institutional pentru utilizatorii acreditați de către reprezentații desemnați de universitati in acest sens.

Aspectele prezentate mai sus ce țin de neluarea măsurilor necesare pentru asigurarea integrității şi protecţiei datelor au drept cauze:

- Subestimarea importanței și necesității unei proceduri de identificare și evaluare a riscurilor, motivat de percepția că UEFISCDI este o entitate de dimensiuni reduse și nu dispune de resursele necesare pentru dezvoltarea și implementarea unei astfel de proceduri.
- Resurse limitate financiare și de personal: Dezvoltarea și implementarea unei proceduri pentru identificarea și evaluarea riscurilor implică costuri financiare, alocare de timp și/sau personal dedicat.

Lipsa unei proceduri de identificare și evaluare a riscurilor IT poate expune sistemul REI/RMUR la amenințări semnificative, entitatea devenind vulnerabilă la atacuri cibernetice, pierderi de date și alte incidente de securitate.

Lipsa măsurilor de securitate IT poate duce la expunerea la o serie de riscuri, cum ar fi:

- Acces neautorizat la informații confidențiale. Angajații UEFISCDI și ai ME sau utilizatorii externi ar putea avea acces la informații confidențiale,

cum ar fi datele personale. Acest lucru ar putea duce la furtul sau utilizarea neautorizată a informațiilor din bazele de date.

- Modificarea sau ștergerea datelor. Angajații UEFISCDI și ai ME sau utilizatorii externi ar putea modifica sau șterge date importante. Acest lucru ar putea perturba operațiunile IT sau ar putea duce la pierderea de date.

Folosirea conturilor gratuite de email pentru crearea de conturi de utilizator prezintă o serie de riscuri, printre care:

- Scurgerea datelor: Conturile gratuite de email sunt mai vulnerabile la atacuri cibernetice care pot duce la scurgerea datelor, cum ar fi parolele, informațiile de contact și alte informații personale. Acest lucru se datorează faptului că furnizorii de servicii de email gratuite au resurse limitate pentru a-și proteja infrastructura de atacuri.

- Spam și phishing: Conturile gratuite de email sunt adesea ținta campaniilor de spam și phishing. Acest lucru se datorează faptului că aceste conturi sunt mai susceptibile de a fi abandonate sau de a fi utilizate de persoane care nu sunt conștiente de riscurile cibernetice.

- Acces neautorizat: Conturile gratuite de email pot fi accesate neautorizat de către persoane rău intenționate. Acest lucru se poate face prin furtul parolei, prin compromiterea serverelor furnizorului de servicii de email sau prin alte metode.

Respondenții la chestionarul privind utilizarea REI/RMUR sunt în general încrezători în securitatea și confidențialitatea datelor stocate în REI/RMUR, așa cum rezultă din graficul de mai jos:

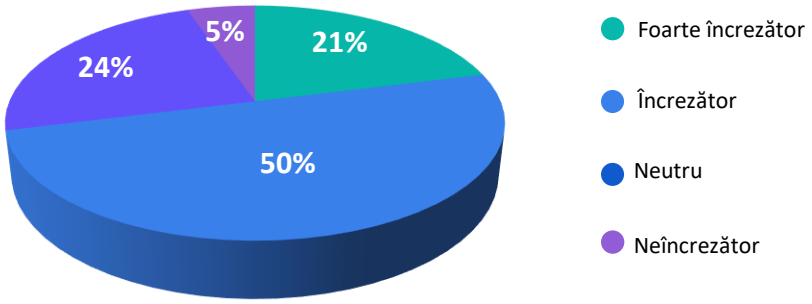


Figura nr. 6 Gradul de încredere al utilizatorilor de la nivelul IIS în securitatea și confidențialitatea datelor

În concluzie, UEFISCDI nu a efectuat periodic o analiză formala a riscurilor de securitate a reţelei şi a sistemului informatic care asigură furnizarea REI/RMUR și nu a identificat sistemele/echipamentele informatice critice pentru funcționarea REI/RMUR precum şi principalele riscuri, dar a implementat măsri tehnice de securitate.

Nu există un program de asigurare a securităţii personalului prin care să fie identificate obiective şi să fie stabilite cerinţe de securitate pentru fiecare etapă a relaţiei cu angajaţii UEFISCDI și cu utilizatorii externi REI/RMUR.

2.2. UEFISCDI a pus în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta că prelucrarea datelor cu caracter personal ale studenților se efectuează în conformitate cu normele legale?

Planurile de continuitate a activității (BCP) și de recuperare în caz de dezastre (DRP) nu sunt implementate, iar măsurile tehnice și organizatorice pentru protecția datelor cu caracter personal nu sunt complete

Pentru a se îndeplini cerințele Regulamentului UE privind GDPR și a proteja drepturile persoanelor vizate, trebuie să se ia măsuri tehnice și organizatorice adecvate, destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a expunerii datelor și să se integreze garanțiile necesare în cadrul prelucrării acestora.

Securitatea datelor cu caracter personal este reglementată de art.32 Securitatea prelucrării din Regulamentul UE GDPR, astfel:

(1) Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

(a) pseudonimizarea și criptarea datelor cu caracter personal;

(b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;

(c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

(d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

(2) La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

Potrivit art. 28 din Regulamentul de organizare și funcționare a UEFISCDI[13], Serviciul informatică şi infrastructură suport are atribuţii în asigurarea integrității şi protecţiei datelor.

Datele cu caracter personal sunt informații care pot fi folosite pentru a identifica o persoană fizică, cum ar fi numele, adresa, numărul de telefon sau adresa de e-mail. Aceste date sunt colectate, stocate și utilizate de UEFISCDI în scopurile prevăzute de Regulamentul RMUR.

Protecția datelor cu caracter personal este importantă deoarece aceste date pot fi folosite pentru a încălca confidențialitatea, integritatea sau securitatea unei persoane. De exemplu, dacă datele cu caracter personal

[13] Aprobat prin Ordinul MENCS nr.5804 din 23.11.2016, publicat în M.O. nr.994 din 9 decembrie 2016

sunt furate sau pierdute, o persoană poate fi victima fraudei, a hărțuirii sau a altor abuzuri.

O politică de securitate care face referire și la protecția datelor cu caracter personal este esențială pentru orice entitate sau organizație care prelucrează date cu caracter personal. Această politică ar trebui să stabilească principiile și măsurile de securitate care trebuie implementate pentru a proteja aceste date.

UEFISCDI nu are o politică de securitate sau de protecție a datelor care să includă și protecția și securitatea datelor cu caracter personal.

Cu toate acestea în REI/RMUR sunt aplicate unele măsuri tehnice care protejează o parte din datele cu caracter personal. Astfel, CNP-ul este pseudonimizat, dar nu sunt sunt implementate tehnici de pseudonimizare și pentru alte câmpuri din baza de date, cum ar fi numele și prenumele etc.

Datele cu caracter personal nu sunt criptate în sistemul REI/RMUR desi criptarea datelor cu caracter personal este o măsură de securitate eficientă care poate ajuta la protejarea acestor date de accesul neautorizat, de modificarea sau de distrugerea lor.

Sistemul REI/RMU are o arhitectură complexă care asigură disponibilitatea acestora. Desi nu există o politică de back-up, se fac salvări regulate ale datelor, dar acestea se stochează în aceeași locație sau pe servere aflate în același oraș, deci în locații supuse acelorași tipuri de riscuri.

Entitatea nu are un plan de recuperare în caz de dezastru (DRP) și nici un plan de continuitate a activității (BCP) pentru a restabili disponibilitatea datelor cu caracter personal în timp util, în caz de incidente.

Planul de continuitate a activității (BCP) și planul de recuperare în caz de dezastru (DRP) sunt două documente esențiale pentru orice entitate. Acestea ajută la protejarea activității în cazul unei întreruperi neașteptate, cum ar fi un dezastru natural, un atac cibernetic sau o eroare umană.

Deși Serviciul informatică şi infrastructură suport are atribuţii în asigurarea integrității şi protecţiei datelor, nu au fost stabilite în sarcina acestuia măsuri sau competențe pentru protejarea datelor cu caracter personal.

Există o serie de cauze posibile pentru care UEFISCDI nu are un BCP/DRP pentru a restabili disponibilitatea datelor cu caracter personal în timp util în cazul unor incidente tehnice sau fizice. Acestea includ:

- Lipsa de conștientizare a importanței BCP/DRP. Multe entități nu înțeleg pe deplin importanța unui BCP/DRP, cum ar fi reducerea riscurilor de întrerupere a activității și îmbunătățirea capacității de recuperare în caz de incident;
- Lipsa de resurse sau de timp. Dezvoltarea și implementarea unui BCP/DRP poate fi o sarcină complexă și costisitoare. Entitățile cu resurse

limitate sau cu un program încărcat pot fi reticente să investească în BCP/DRP.

Există o lipsă de claritate în ceea ce privește atribuirea specifică a responsabilităților pentru protecția datelor cu caracter personal în cadrul compartimentelor UEFISCDI. Efectul neaplicării tehnicilor de pseudonimizare pentru toate datele cu caracter personal ar putea fi acela de expunere a persoanele vizate la riscuri semnificative, cum ar fi:

- Pierderea confidențialității: fără pseudonimizare, datele cu caracter personal pot fi identificate și utilizate în mod neautorizat. Acest lucru ar putea duce la încălcarea confidențialității persoanelor vizate, precum și la alte consecințe negative, cum ar fi discriminarea sau hărțuirea.
- Riscul de atacuri cibernetice: datele cu caracter personal care nu sunt pseudonimizate pot fi mai vulnerabile la atacuri cibernetice, cum ar fi furtul de date sau ransomware-ul. Acest lucru ar putea duce la pierderea datelor cu caracter personal sau la utilizarea acestora în scopuri malițioase.
- Sancțiuni legale: în unele cazuri, entitățile care nu iau măsuri adecvate pentru a proteja datele cu caracter personal pot fi supuse sancțiunilor legale aplicate de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Efectul lipsei unui BCP/DRP pentru a restabili disponibilitatea datelor cu caracter personal în timp util în cazul unor incidente poate fi semnificativ, atât pentru persoanele ale căror date sunt prelucrate, cât și pentru entitățile care le prelucrează.

Pentru UEFISCDI care prelucrează date cu caracter personal, lipsa unui BCP/DRP poate avea următoarele efecte:

- Un atac cibernetic poate duce la întreruperea sistemului informatic REI/RMUR, ceea ce poate împiedica UEFISCDI și ministerul să acceseze datele cu caracter personal ale studenților.
- Un dezastru poate duce la deteriorarea serverelor, ceea ce poate duce la pierderea datelor cu caracter personal ale studenților.
- Riscul de sancțiuni legale: în unele cazuri, entitățile care nu iau măsuri adecvate pentru a proteja datele cu caracter personal cum ar fi anonimizarea sau criptarea pot fi supuse sancțiunilor legale.

În concluzie, UEFISCDI nu are elaborate și aprobate politici, proceduri sau reglementări interne astfel încât să se asigure gestionarea riscurilor critice privind securitatea datelor cu caracter personal stocate în REI/RMUR.

Nu au fost luate toate măsurile tehnice și organizatorice destinate să pună în aplicare în mod eficient principiile de protecție a datelor cu caracter personal.

UEFISCDI nu are un plan de continuitate a activității (BCP) și un plan de recuperare în caz de dezastre (DRP).

Obiectivul 3 – În ce măsură sistemul informatic REI/RMUR permite realizarea scopurilor colectării şi prelucrării datelor studenților și cursanților, în conformitate cu prevederile legale aplicabile?

3.1. Vizualizarea traseului educaţional şi verificarea autenticității actelor de studii

RMUR are potențialul de a oferi o vizualizare completă a traseului educațional, dar acest lucru nu este pe deplin realizat

Potrivit art.2 pct.1 din Regulamentul RMUR, colectarea şi prelucrarea datelor primare privind studenţii şi cursanţii din IIS şi AR, prin sistemul RMUR, se face pentru:

- vizualizarea de către ME a traseului educaţional al studenţilor şi cursanţilor din instituţiile de învăţământ superior din România şi Academia Română în vederea fundamentării, formulării şi implementării politicilor publice în domeniu şi, implicit, corelării ofertei educaţionale cu cerinţele pieţei muncii şi
- verificarea autenticităţii actelor de studii, a documentelor şcolare şi a parcursului şcolar în vederea aplicării vizei ME prin Centrul Naţional de Recunoaştere şi Echivalare a Diplomelor (CNRED).

Pentru a permite realizarea acestui scop, în sistemul informatic REI/RMUR a fost implementat:

- un raport predefinit denumit *Raport A2 - Toti studenții cu specializare și traseu (central*), care se generează doar la solicitare (fiind vizibile numai 100 de înregistrari), respectiv alte rapoarte naționale la nivel de persoană și școlaritate, utilizate pentru realizarea de studii sau analize naționale;
- o interfață de căutare si vizualizare al acestuia;
- o serie de rapoarte statistice, predefinite, utilizate de către ME, care permit analiza traseului educațional anual la nivel de cohorte sau rapoarte solicitate periodic de instituțiile administrative naționale, locale și regionale, privind populația școlară de învățământ superior.

Traseul educațional poate fi vizualizat individual, pentru un singur student sau cursant, prin selectarea unui CNP. Acest tip de vizualizare permite verificarea autenticităţii actelor de studii, a documentelor şcolare şi a parcursului şcolar în vederea aplicării vizei ME prin CNRED.

Deși sunt utilizate datele din RMUR pentru o serie de studii/analize/rapoarte realizate de UEFISCDI, ME sau alte instituții, cu aprobarea ME, considerăm ca fiind necesară și generarea unui set de rapoarte statistice mai detaliate, pe baza unor specificații agreate de decident, care să poată fi utilizate facil și periodic de către acesta, ca suport pentru fundamentarea, formularea şi implementarea politicilor publice în domeniu.

Acest aspect se datorează faptului că nu a fost elaborată și aprobată o metodologie pe baza căreia să fie implementat un raport care să permită

vizualizarea informatiilor aferente traseului educațional al studenților și cursanților și care să stea la baza fundamentării, formulării şi implementării politicilor publice în domeniu.

În lipsa acestor informații agregate suplimentar într-o serie de rapoarte statistice specifice, politicile publice în domeniul educației ar putea fi elaborate fără o fundamentare adecvată iar oferta educațională ar putea fi necorelată cu cerințele pieței muncii.

În concluzie, RMUR permite verificarea autenticităţii actelor de studii, a documentelor şcolare şi a parcursului şcolar în vederea aplicării vizei Ministerului Educaţiei prin Centrul Naţional de Recunoaştere şi Echivalare a Diplomelor (CNRED).

Totuși, RMUR nu este utilizat la capacitatea sa deplină pentru vizualizarea traseului educațional al studenţilor şi cursanţilor din instituţiile de învăţământ superior din România şi Academia Română în vederea fundamentării, formulării şi implementării politicilor publice în domeniu şi, implicit, corelării ofertei educaţionale cu cerinţele pieţei muncii.

3.2. Identificarea situaţiilor de dublă finanţare a studenților din cadrul instituțiilor de învățământ superior de stat

Rapoartele implementate în sistem nu permit intuitiv identificarea situațiilor de dublă finanțare

Potrivit art.142, alin.(6) din Legea educației naționale nr.1/2011, o persoană poate beneficia de finanţare de la buget pentru un singur program de licenţă, pentru un singur program de master şi pentru un singur program de doctorat.

Potrivit art.2 pct.4 din Regulamentul RMUR, colectarea şi prelucrarea datelor primare privind studenţii şi cursanţii din IIS şi AR, prin sistemul RMUR, se face pentru identificarea situaţiilor de dublă finanţare a studenţilor din cadrul instituţiilor de învăţământ superior de stat (IISS).

Pentru a se răspunde acestui scop, în REI/RMUR a fost implementat Raportul nr.9.2 *Verificare studenți cu școlarizare multiplă în RMU (univ.) v2.*

Pentru testarea acestui raport, echipa de audit a folosit 3 conturi distincte, respectiv cont de administrator de la nivel de universitate, cont de utilizator de la nivel de universitate, precum și cont de administrator de sistem REI/RMUR.

Raportul rulat folosind contul de administrator de sistem REI/RMUR nu a identificat nici o situație de dublă finanțare, așa cum se poate vizualiza în captura de ecran de mai jos.

Figura nr. 7 Captură de ecran rulare raport 9.2, cont administrator de sistem REI/RMUR
Sursă imagine: Sistem REI/RMUR

Același raport rulat, folosind un cont de administrator și apoi un cont de utilizator de la nivel de universitate, a furnizat erori ilustrate în captura de mai jos, erori care au fost prezentate personalului de specialitate al UEFISCDI.

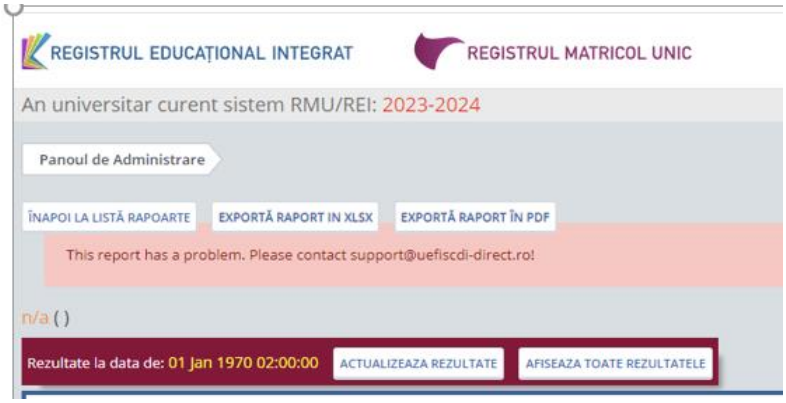


Figura nr. 8 Captură de ecran rulare raport 9.2, cont administrator/utilizator de la nivel de universitate

Sursă imagine: Sistem REI/RMUR

Pentru generarea raportului, sistemul informatic REI/RMUR nu permite selectarea parametrilor de individualizare, de exemplu programul de studii și/sau anul universitar.

La data auditului, la nivelul ME se află în curs de elaborare o serie de specificații pentru diferite rapoarte naționale de verificare a datelor din RMUR, printre care și cele pentru restructurarea și simplificarea raportului existent privind școlaritatea multiplă și implicit dubla finanțare.

Pentru identificarea intuitivă a situațiilor de dublă finanțare este necesară actualizarea și detalierea rapoartelor și eventual, suplimentarea lor conform specificațiilor pentru generarea rapoartelor naționale de verificare a datelor din RMUR, printre care și cele privind școlaritatea multiplă și implicit dubla finanțare.

În concluzie, rapoartele implementate în sistem pentru identificarea situațiilor de dublă finanțare nu generau niciun rezultat sau generau erori la momentul auditului și nu erauconfigurabile pentru selectarea programului de studiu sau al anului universitar. Pe perioada auditului situatia punctuala

a fost remediata, dar sunt necesare măsuri pentru a asigura verificarea periodică a funcționalității depline a tuturor rapoartelor.

3.3. Transmiterea de date pentru acordarea facilităților la transportul feroviar

Lipsa conectării între RMUR și bazele de date ale operatorilor de transport feroviar, ca urmare a unor neclarități în procedurile de implementare, nu oferă studenților facilitatea de a achiziționa online bilete pentru transportul feroviar

Potrivit art.2 pct.5 din Regulamentul RMUR, colectarea şi prelucrarea datelor primare privind studenţii şi cursanţii din IIS şi AR, prin sistemul RMUR, se face pentru transmiterea de date către operatorii de transport feroviar şi metrou, conform Hotărârii Guvernului nr. 42/2017 pentru aprobarea Normelor metodologice privind acordarea facilităţilor de transport intern feroviar şi cu metroul pentru elevi şi studenţi.

Până la data auditului, studenții au putut beneficia de transport feroviar public gratuit doar prin prezentarea la casele de bilete/abonamente ale operatorilor de transport feroviar și cu metroul a legitimației de student eliberată și vizată de instituția de învățământ.

Chiar daca au avut loc o serie de discuții și dezbateri între ME și MT (Ministerului Transporturilor și Infrastructurii), respectiv ARF (Autoritatea pentru Reformă Feroviară) și CFR (Societatea Națională de Transport Feroviar de Călători “C.F.R. Călători”-S.A) pentru ultima forma de HG și pe normele de implementare, în perioada auditată nu a existat o procedură sau o modalitate tehnică de transmitere către acești operatori de transport feroviar a datelor prin interconectarea bazelor de date sau prin interogare online. La data auditului se analiza posibilitatea introducerii unui serviciu de tip REST API, agreat de părțile interesate, bazat pe interogare a unor parametri, cum ar fi numărul de legițimatie student, CNP sau numărul pașaportului.

La nivelul sistemului REI/RMUR există un serviciu de interconectare cu Agenția de Reformă Feroviară (ARF), dar nu a fost utilizat niciodată din cauze procedurale.

Entitățile implicate nu au agreat până la data auditului o formă finală a modului de interconectare, fie din cauza constrângerilor existente, fie datorită faptului că studenții puteau beneficia de facilitatea decontării transportului feroviar prin prezentarea carnetului de student la casele de bilete/abonamente ale operatorilor de transport feroviar.

Neutilizarea unor soluții de transmitere electronică a datelor către operatorii de transport feroviar are efect direct asupra modului în care studenții achiziționează tichetele sau abonamentele de călătorie. Aceștia nu pot beneficia în timp real de validarea online a calității de student prin plaforma integrată administrată de ARF.

În concluzie, studenții nu pot beneficia pe deplin de facilitatea unei interconectări sau interoperabilități ale RMUR cu bazele de date ale operatorilor de transport feroviar.

Transmiterea de date către Institutul Național de Statistică nu este reglementată printr-o procedură formalizată

3.4. Transmiterea de date către Institutul Național de Statistică

Potrivit art.2 pct.6 din Regulamentul RMUR, colectarea şi prelucrarea datelor primare privind studenţii şi cursanţii din IIS şi AR, prin sistemul RMUR, se face pentru transmiterea de date către Institutul Naţional de Statistică (INS) conform Regulamentului (UE) 2015/759 al Parlamentului European şi al Consiliului din 29 aprilie 2015 de modificare a Regulamentului (CE) nr. 223/2009 şi a Convenţiei MEN - INS privind prelucrarea datelor în vederea producerii statisticilor oficiale de educaţie şi formare profesională.

Accesul la baza de date REI/RMUR a fost permis pe baza unei convenții de colaborare încheiate în anul 2016 între MENCS și INS. Convenția a fost reînnoită automat, fără modificări, deși ulterior au intrat în vigoare noi reglementări cum ar fi cele privind protecția datelor cu caracter personal sau Regulamentul RMUR. Deși convenția nu menționează responsabilități detaliate ale UEFISCDI în procesul de colaborare și respectiv transmitere a datelor, UEFISCDI a permis accesul la baza de date fără a avea la bază o procedură formalizată și aprobată de managementul UEFISCDI.

Furnizarea de informații și acces la date în condițiile inexistenței unei proceduri aprobate de conducere, chiar dacă există o convenție de colaborare, are potențial efecte asupra asumării responsabilității cu privire la datele transmise și folosite pentru statistica națională.

În concluzie, transmiterea de date către INS pentru prelucrare în vederea producerii statisticilor oficiale de educaţie şi formare profesională s-a făcut fără a exista o procedură formalizată și aprobată.

RMUR nu arhivează datele colectate despre persoanele care nu mai au statutul de student sau cursant

3.5. Prelucrarea în scopuri statistice și de cercetare, arhivarea datelor

Potrivit art.2 pct.8 din Regulamentul RMUR, colectarea şi prelucrarea datelor primare privind studenţii şi cursanţii din IIS şi AR, prin sistemul RMUR, se face pentru prelucrarea în scopuri statistice şi de cercetare istorică sau ştiinţifică sau în alte scopuri la solicitarea ME, în conformitate cu prevederile legale.

Art.3 din același regulament prevede că datele primare se actualizează doar pentru perioada în care persoana vizată are statutul de student sau cursant la alte forme de studii furnizate de către universitate. Ulterior, datele colectate vor fi arhivate, fără posibilitatea intervenirii asupra lor, şi vor fi utilizate doar în scopuri de interes public, statistic şi de cercetare istorică sau ştiinţifică, în conformitate cu reglementările legislative privind protecţia datelor şi circulaţia acestora.

Solicitările de prelucrare statistică de la alte entități (pentru realizarea de rapoarte statistice) primite și aprobate de către ME, se înaintează UEFISCDI. Acesta analizează solicitarea și, dacă nu există un raport predefinit, generează un raport adecvat.

Acest proces de analiză a cererilor, prelucrare a datelor, generarea de rapoarte și/sau furnizare a datelor, nu este procedurat - definit, reglementat și aprobat - astfel că el se reia de fiecare dată când apare o astfel de solicitare.

De asemenea, s-a constatat că, după ce persoana vizată nu mai are statutul de student sau cursant la alte forme de studii furnizate de către universități, datele colectate despre această persoană nu sunt arhivate, așa cum prevede art.3 alin.(2) din Regulamentul RMUR aprobat prin Ordinul nr. 3714/2018. Datele sunt menținute în baza de date RMUR în mod identic și la un loc cu datele care privesc persoanele care au statutul de student sau cursant.

Aspectele prezentate mai sus se datorează următoarelor cauze:

- Nu a fost elaborată, aprobată și comunicată o procedură care să prevadă modalitatea tehnică de transmitere a datelor către entități pentru prelucrarea în scopuri statistice și de prelucrare istorică.
- Nu a fost elaborată și aprobată o procedură privind arhivarea datelor înregistrate în RMUR după ce persoanele nu mai au statutul de student sau cursant.

Lipsa unei proceduri care să prevadă modalitatea tehnică de transmitere a datelor către entități pentru prelucrarea în scopuri statistice și de prelucrare istorică ar putea duce la întârzieri sau mărirea timpilor de furnizare a datelor din RMUR.

Păstrarea în baza de date activă a datele persoanelor care nu mai au calitatea de student sau cursant și nearhivarea lor ar putea expune aceste date, în situația apariției unor eventuale incidente de securitate (expunerea, compromiterea, pierderea datelor).

În concluzie, procesul de furnizare a datelor în scopul prelucrării statistice sau istorice (inclusiv a datelor persoanelor care nu mai statutul de student/cursant) nu este reglementat printr-o procedură formalizată, iar datele colectate nu sunt arhivate după ce persoana nu mai are statutul de student/cursant.

CONCLUZII GENERALE

REI/RMUR este utilizat în mod activ pentru îmbunătățirea managementului universitar și a creșterii nivelului de transparență a informațiilor existente privind studenții și cursanții, putând concluziona că RMUR:

- oferă o imagine completă și actualizată a tuturor studenților și cursanților din învățământul superior din România;
- poate fi utilizat pentru a genera rapoarte și indicatori statistici care pot fi utilizați pentru a fundamenta deciziile de management;
- poate fi utilizat pentru a îmbunătăți comunicarea și colaborarea între universități și alte instituții implicate în domeniul învățământului superior;
- permite interconectarea cu bazele de date ale operatorilor de transport public local și feroviar.

Pe lângă aspectele de bună practică prezentate mai sus, au fost identificate unele deficiențe care impiedică RMUR să-și atingă pe deplin potențialul de a fi un instrument util pentru fundamentarea, formularea și implementarea politicilor publice în domeniul învățământului superior.

Astfel, s-a identificat necesitatea îmbunătățirii unor aspecte cu privire la:


Guvernanța IT;


Securitatea IT;


Gradul de indeplinire a obiectivelor stabilite prin Regulamentul RMUR.

Sistemul RMUR conține unele deficiențe în privința calității și exhaustivității informațiilor disponibile, iar securitatea bazelor de date poate fi îmbunătățită conform standardelor în domeniu. Aceste lacune constituie riscuri semnificative pentru integritatea datelor, cu potențiale consecințe grave în asigurarea confidențialității informațiilor despre studenți.

RECOMANDĂRI

Pentru ca REI/RMUR să-și atingă pe deplin potențialul de a fi un instrument util pentru fundamentarea, formularea și implementarea politicilor publice în domeniul învățământului superior, trebuie îmbunătățită calitatea și securitatea bazei de date RMUR, ceea ce ar avea un impact pozitiv asupra activităților desfășurate de UEFISCDI și de alte instituții care folosesc această bază de date.

Recomandări privind guvernanța IT:

1. Dezvoltarea unei strategii IT care să contribuie la alinierea activității IT cu obiectivele privind trecerea de la RMUR la RUNIDAS, inclusiv migrarea în cloud-ul guvernamental.
2. Elaborarea și aprobarea de către UEFISCDI de politici, proceduri și reglementări interne care să asigure gestionarea riscurilor critice privind securitatea informațiilor din bazele de date REI/RMUR.

Recomandări privind securitatea sistemului informatic:

3. Efectuarea unei analize periodice a riscurilor de securitate a rețelei și a sistemului informatic care susține REI/RMUR.
4. Elaborarea și implementarea unui set de proceduri în domeniul securității IT pentru personalul UEFISCDI și utilizatorii externi ai REI/RMUR.
5. Luarea unor măsuri suplimentare de securitate pentru protecția datelor în cazul în care UEFISCDI va permite în continuare utilizarea conturilor gratuite de email pentru înregistrarea și crearea de conturi de utilizator.
6. Elaborarea și aprobarea de politici, proceduri și reglementări interne care să asigure gestionarea riscurilor critice privind protecția datelor cu caracter personal din bazele de date și implementarea tehnicilor de pseudonimizare și pentru alte câmpuri din baza de date care stochează informații cu caracter personal.
7. Analizarea eficienței introducerii criptării bazelor de date care stochează date cu caracter personal, astfel încât să se asigure alinierea la cadrul legal privind protecția datelor cu caracter personal.
8. Elaborarea și implementarea și testarea unui plan de continuitate a activității (BCP) și a unui plan de recuperare în caz de dezastru (DRP) pentru ca în cazul unor incidente să se poată restabili disponibilitatea datelor cu caracter personal în timp util.

Recomandări privind gradul de folosire a conținutului bazei de date:

9. Elaborarea și aprobarea unei metodologii pentru implementarea unui raport care să permită vizualizarea informațiilor aferente traseului educațional al studenților și cursanților. Acest raport ar putea fi folosit pentru fundamentarea, formularea și implementarea politicilor publice în domeniul educației.

10. Îmbunătățirea capacității RMUR de a identifica situațiile de dublă finanțare. Acest lucru ar putea fi realizat prin dezvoltarea de noi rapoarte configurabile și prin implementarea de mecanisme de avertizare în timp real.
11. Interconectarea și/sau interoperabilitatea RMUR cu bazele de date electronice ale operatorilor de transport feroviar. Acest lucru ar simplifica procesul de obținere a facilităților de transportului feroviar pentru studenți și ar putea elimina posibilele fraude.
12. Elaborarea unei proceduri formalizate prin care să fie reglementat procesul de furnizare a datelor în scopul prelucrării statistice sau istorice pentru a asigura că datele sunt prelucrate în mod legal și transparent, iar drepturile persoanelor ale căror date sunt colectate sunt protejate. Arhivarea datelor colectate după ce persoana nu mai are statutul de student/cursant pentru a se asigura faptul că datele sunt disponibile pentru cercetare și analiză istorică.

COMENTARII UEFISCDI

CCR a transmis către UEFISCDI proiectul Raportului de audit și al Scrisorii către management. UEFISCDI a formulat în termenul legal un punct de vedere conținând obiecții la constatările formulate. Proiectul raportului de audit a fost conciliat și nu au rămas constatări în divergență, CCR acceptând obiecțiile formulate de UEFISCDI în definitivarea raportului de audit.