Universitatea Politehnica Timișoara  
Facultatea de Automatică și Calculatoare

**Triada CIA**

Securitatea sistemelor de calcul

An universitar 2024-2025

**Negru Briana-Maria**

***Anul 3, Tehnologia Informației***

E-mail: [briana.negru@student.upt.ro](mailto:briana.negru@student.upt.ro)

Cuprins

[Introducere 2](#_Toc193177713)

[Istoric 3](#_Toc193177714)

[Principii 4](#_Toc193177715)

[Confidențialitatea 4](#_Toc193177716)

[Integritatea 5](#_Toc193177717)

[Disponibilitatea 5](#_Toc193177718)

[Relația dintre confidențialitate, integritate și disponibilitate 6](#_Toc193177719)

[Concluzie 6](#_Toc193177720)

[Bibliografie 7](#_Toc193177721)

# Introducere

În societatea contemporană, sistemele de rețea au un rol esențial în facilitarea schimbului de informații, a colaborării în partajarea datelor și în alocarea eficientă a resurselor în diverse sectoare. Securitatea și funcționalitatea sistemelor de rețea au devenit, în ultimii ani, cruciale pentru organizații și companii, dat fiind faptul că acestea depind de infrastructura digitală.

De aproape 40 de ani, termenii „confidențialitate”, „integritate” și „disponibilitate” au fost utilizați pe scară largă în practica securității informațiilor și în literatura academică. Acești 3 termeni formează nucleul unui sistem de securitate a rețelei puternic și rezistent la amenințări (Whitman & Mattord, 2017). „Triada CIA”, așa cum este ea cunoscută, se referă în principiu la elementele fundamentale ale controalelor de securitate în sistemele informatice. Aceste 3 principii fundamentale nu numai că au modelat înțelegerea teoretică a securității informațiilor, ci și practicile prin care securitatea este dezvoltată și implementată în organizații, formând, împreună, un cadru robust și rezistent de securitate a rețelelor.

În mod tradițional, aceste practici de securitate s-au concentrat asupra controalelor tehnice care protejează confidențialitatea, integritatea și disponibilitatea informațiilor. Încă de la începutul anilor 1990, specialiștii în securitatea informațiilor au reevaluat în mod constant încrederea excesivă în controale și au subliniat în mod repetat necesitatea de a lua în considerare diferite aspecte non-tehnice în gestionarea securității.

Triada CIA a fost criticată în mai multe rânduri pentru orientarea și concentrarea sa tehnică îngustă și astfel, utilitatea sa limitată atunci când trebuie luate în considerare aspecte organizaționale și sociale mai largi ale securității (Anderson, 2002; Dhillon și Backhouse, 2000; Dhillon și Torkzadeh, 2006; Harris, 2002; Kolkowska et al., 2009).

Cu toate acestea, experții din domeniul securității informațiilor încă apreciază proprietățile simbolice ale triadei CIA, deoarece aceasta le oferă o modalitate simplă de a înțelege și aborda probleme legate de securitatea informațiilor.

Confidențialitatea este esențială pentru securitatea informațiilor, deoarece garantează că materialul sensibil este disponibil numai persoanelor sau instituțiilor care au primit autorizație. Această măsură protejează eficient împotriva divulgării neautorizate a datelor (Whitman & Mattord, 2017).

Whitman și Mattord (2017) sunt de acord că integritatea servește ca o garanție pentru a asigura precizia și uniformitatea datelor, prin urmare se reduc amenințările potențiale asociate cu manipularea neautorizată sau modificarea acestora.

Conceptul de disponibilitate se referă la asigurarea că resursele și serviciile de rețea sunt ușor accesibile în funcție de necesități, minimizând astfel perioadele de inactivitate și garantarea fluxului neîntrerupt al activităților (Whitman & Mattord, 2017).

# Istoric

În perioada de debut a calculatoarelor și a utilizării acestora, existau doar câteva amenințări la adresa protecției informațiilor. Acest lucru se datorează, în primul rând, faptului că acele calculatoare erau scumpe, rare și bine protejate. Sistemele informatice care conțineau informațiile sensibile erau expuse doar unui număr limitat de persoane specializate în domeniul programării și puteau reprezenta o posibilă amenințare.

Prin urmare, accentul inițial pentru protejarea informațiilor s-a concentrat pe asigurarea fiabilității sistemului în sine, pentru a garanta ca acesta să fie operațional în mod constant. Ca urmare, protecția informațiilor a fost realizată în principal prin controlul accesului fizic la calculatoare.

Pe măsură ce costul tehnologiei informatice a scăzut, iar utilizarea acesteia a crescut, s-a trecut de la protecția calculatoarelor la protecția informațiilor. În timp ce, anterior, fiabilitatea calculatoarelor era dominantă, noțiunile de confidențialitate, integritate și disponibilitate a început să capete importanță.

Rădăcinile triadei CIA sunt adânc legate de mentalitatea de securitate militară, care a fost întotdeauna axată pe protejarea informațiilor împotriva amenințărilor externe. Multe dintre studiile inițiale privind securitatea au fost finanțate fie de guvernul federal, fie de agenții militare.

Raportul Anderson, care a fost comandat de USAF (United States Air Force), a identificat trei categorii de potențiale riscuri de securitate care au devenit în cele din urmă fundamentul triadei CIA: eliberarea neautorizată de informații (a dus la conceptul de confidențialitate), modificarea neautorizată a informațiilor (a dus la conceptul de integritate) și refuzul neautorizat de utilizare (a dus la conceptul de disponibilitate).

Saltzer și Schroeder (1975), au susținut, în lucrarea lor fundamentală intitulată „The Protection of Information in Computer Systems”, noțiunea că principala preocupare a securității ar trebui să fie protecția informațiilor conținute în sistemele informatice, mai degrabă decât protecția sistemului informatic în sine. Prima secțiune a documentului prezenta „principiile de bază” pentru protecția informațiilor, care includ triada CIA - confidențialitate, integritate și disponibilitate.

Primele modele de securitate a informațiilor adoptate pe scară largă se axau în primul rând pe o abordare. Primul dintre aceste modele adoptate timpuriu a fost modelul Bell-LaPadula (David Elliott Bell și Leonard J. LaPadula, 1975). Acest model s-a axat pe stabilirea de reguli pentru asigurarea confidențialității și protejarea informațiilor, prin limitarea accesului la obiectele informaționale. Trei reguli principale au fost aplicate: nicio citire în sus, nicio scriere în jos și citire/scriere numai la același nivel.

Al doilea model care a fost dezvoltat a fost modelul Biba (Kenneth J. Biba, 1975), care s-a axat pe integritatea datelor, în loc de confidențialitate. Obiectivele modelului de integritate Biba au fost acelea de a preveni modificarea datelor de către părți neautorizate, de a preveni modificarea neautorizată a datelor de către părți autorizate și menținerea coerenței interne și externe a datelor.

Modelul Graham-Denning de detectare a intruziunilor s-a concentrat pe apărarea împotriva amenințărilor la adresa disponibilității (1987). Acest model a fost conceput ca un sistem de detectare a intruziunilor în timp real, care este orientat spre detectarea efracțiilor, a pătrunderilor și alte forme de abuz informatic. Acest model se bazează pe ipoteza că încălcările securității pot fi detectate prin monitorizarea înregistrărilor de audit ale unui sistem pentru modele anormale de utilizare a sistemului.

Pe lângă utilizarea sa la scară largă în standardele de guvernanță în materie de securitate, triada CIA se regăsește în principalele programe de securitate, audit și examinare a fraudelor ale diverselor organisme de certificare profesională. Toate aceste certificări au un lucru în comun, și anume faptul că, în programele lor de studii, ele tratează confidențialitatea, integritatea și disponibilitatea activelor informaționale ca un set indispensabil de controale și principii pentru implementarea securității.

# Principii

## Confidențialitatea

Confidențialitatea este un principiu fundamental al securității informațiilor, care își are rădăcinile în mentalitatea militară de a menține o autoritate și un oarecare control asupra celor care au acces la informații, pe baza principiului necesității de a cunoaște.

Aceasta se referă la necesitatea etică și juridică de a proteja informațiile sensibile împotriva accesului neautorizat sau a divulgării. Confidențialitatea se referă la utilizarea anumitor măsuri de protecție pentru a preveni accesul persoanelor neautorizate la informații sensibile. Sugerează că accesul la informațiile sensibile ar trebui să fie limitat exclusiv la persoanele sau instituțiile autorizate oficial.

Camp (1999) afirmă că termenul de confidențialitate implică ideea că datele și informațiile trebuie să fie protejate, astfel încât utilizarea să fie limitată la scopuri autorizate, numai de către persoane autorizate.

În mod similar, Zwick și Dholakia (2004) definesc confidențialitatea ca fiind capacitatea percepută de a efectua o sarcină externă care restricționează fluxul de informații cu privire la ceea ce este dezvăluit în ea și cu privire la cine ajunge să o vadă.

Mavhandu-Mudzusi et al. (2007) afirmă că organizațiile pot suferi pierderi financiare, daune reputaționale reputație și consecințe juridice ca urmare a încălcării securității datelor sau accesului neautorizat.

## Integritatea

Integritatea se referă la protecția informațiilor împotriva modificărilor sau alterărilor neautorizate. Aceasta impune faptul ca informațiile să nu fie modificate fără autorizație corespunzătoare și că orice modificare trebuie să fie înregistrată și documentată.

Integritatea implică, de asemenea menținerea preciziei, coerenței și fiabilității datelor de-a lungul ciclului lor de viață (Carta et al., 2020). Asigurarea integrității datelor prin împiedicarea actorilor rău intenționați să modifice, șteargă sau altereze datele.

Funcțiile Hash și semnăturile digitale sunt metode criptografice utilizate frecvent pentru verificarea integrității datelor, deoarece orice modificare a conținutului original va duce la o modificare sesizabilă a valorii hash.

Menținerea integrității datelor este esențială pentru a preveni diseminarea de informații înșelătoare sau corupte, care ar putea avea repercusiuni grave în sectoare vitale precum sănătate și finanțe.

O definiție mai tehnică a integrității poate fi regăsită în secțiunea 3542 din titlul 44 din Codul SUA, care definește integritatea ca fiind prevenirea „modificării sau distrugerii necorespunzătoare a informațiilor”, și include în mod specific autenticitatea și non-repudierea informațiilor (von Solms, 2013). În ultima parte a definiției, autenticitatea și non-repudierea sunt doi termeni de securitate foarte strâns legați. Mai exact, autenticitatea nu garantează non-repudierea, însă non-repudierea garantează autenticitatea.

Non-repudierea implică incapacitatea de a sfida o anumită tranzacție sau a comunicării între două părți, de unde rezultă faptul că un proces adecvat de autentificare a avut loc cu succes în primul rând.

Autenticitatea denotă calitatea de a fi original și autentic și, prin urmare autentificarea este procesul de verificare, la un anumit nivel de încredere dorit, a faptului că identificatorul pretins este valid și este într-adevăr asociat cu un anumit obiect sau persoană.

## Disponibilitatea

Conceptul de disponibilitate se referă la asigurarea că persoanele autorizate pot accesa cu ușurință informațiile, atunci când este necesar. Acest lucru sugerează că este esențială protejarea sistemelor informatice împotriva întreruperilor care ar putea împiedica accesul utilizatorilor la informații.

Termenul disponibilitate înseamnă, în contextul securității, „accesul și utilizarea în timp util și fiabil a informațiilor” (44 USC Sec. 3542). Din perspectiva ingineriei utilizabilității, un sistem este considerat utilizabil atunci când este eficace și eficient, iar utilizatorii săi sunt în general mulțumiți de îndeplinirea de către acesta a unor sarcini specifice într-un anumit mediu (Weir et al., 2009).

În cazul software-ului de securitate, Padayachee (2012) îi citează pe Whitten și Tygar (1999) menționând că utilizabilitatea este, de asemenea, asociată cu capacitatea de a evita erorile periculoase și de a face utilizatorii conștienți în mod fiabil de sarcinile pe care trebuie să le îndeplinească.

Disponibilitatea se referă la asigurarea accesibilității și a capacității de utilizare a resurselor, serviciilor și datelor din rețea, în special atunci când cele cu autorizația corespunzătoare au nevoie de ele (Sayyad et al., 2021).

Perioadele neprevăzute de inactivitate operațională, generate fie de disfuncționalități tehnologice, fie de intruziuni cibernetice au capacitatea de a împiedica procesele organizaționale, de a genera deficite financiare și de a afecta poziția unei entități în sfera publică (Sayyad et al., 2021).

## Relația dintre confidențialitate, integritate și disponibilitate

Triada CIA este de obicei ilustrată sub forma unui triunghi, în care fiecare vârf al triunghiului simbolizează unul dintre cele trei concepte: confidențialitate, integritate și disponibilitate. Cele trei principii prezintă interdependență, astfel încât încălcarea unui principiu le poate afecta pe celelalte două.

De exemplu, în cazul unei încălcări de confidențialitate, integritatea și disponibilitatea ar putea fi, de asemenea afectate. În cazul unei încălcări a integrității, există un potențial de compromis în ceea ce privește disponibilitatea. În cazul unei încălcări a disponibilității, confidențialitatea și integritatea pot fi, de asemenea, compromise.

# Concluzie

Triada CIA, formată din Confidențialitate, Integritate și Disponibilitate, este un concept fundamental în cadrul securității informațiilor. Importanța acestei structuri în evaluarea și dezvoltarea sistemelor sigure este larg recunoscută, acoperind multe domenii, cum ar fi sisteme informatice și tehnologii viitoare precum IoT și SDN-uri.

Pe parcursul a peste 40 de ani de istorie, triada CIA a fost supusă unui proces discret de reinventare și reconfigurare, pentru a se adapta la creșterea exponențială a tehnologiei informației și la schimbările semnificative de viziune asupra securității - evoluând de la accentul inițial la transferul de date și informații și, în cele din urmă, la securitatea cibernetică.

# Bibliografie

1. S. Samonas and D. Coss, “The CIA strikes back: Redefining confidentiality, integrity, and availability in security,” *J. Inf. Syst. Secur.*, vol. 10, no. 3.
2. O. M. C. Osazuwa, “Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature,” *Int. J. Innov. Sci. Res. Technol.*, vol. 8, no. 12, Dec. 2023.
3. S. Mohanty, M. Ganguly, and P. K. Pattnaik, “CIA Triad for Achieving Accountability in Cloud Computing Environment,” *Int. J. Comput. Sci. Mob. Appl.*, vol. 6, no. 3, pp. 38-43, Mar. 2018.
4. K. Y. Chai and M. F. Zolkipli, “Review on confidentiality, integrity and availability in information security,” *J. ICT Educ.*, vol. 8, no. 2, pp. 34–42, 2021.
5. A. Tchernykh, U. Schwiegelsohn, E. Talbi, and M. Babenko, “Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability,” *J. Comput. Sci.*, vol. 36, 100581, Sep. 2019.