Structuri și politici de securizare a informației

EMSAPHIR - Protecția datelor personale. Securitatea informațiilor

Securitate societală

Concepte

Școala de la Copenhaga (Barry Buzan, Ole Waever)

COPRI - The Copenhagen Peace Research Institute[1]

SIPRI - Stockholm International Peace Research Institute[2]

Securitatea socială = specifică indivizilor: securitatea financiară, a locului de muncă, familială

Securitatea societală = securitatea identității, a culturii și religiei, ca procese între grupuri și indivizi

Amenințări la adresa securității societate:

- migrația ilegală,
- terorismul,
- crima organizată,
- interzicerea utilizării limbii unei comunități,
- închiderea locurilor de transmitere a educației și de practicare a religiei[3].

Sistemul de management

Datele și informația -

- elementele esențiale pentru desfășurarea activităților unei organizații - publice sau private

↓

protejarea acestora printr-un sistem de management al securității acestora

Stabilirea și implementarea sistemului de management al securității informațiilor este influențată de:

- nevoile și obiectivele organizației
- cerințele de securitate
- procesele organizaționale utilizate
- dimensiunea și structura organizației[4].

Rol important în economia bazată pe cunoaștere, în societatea informațională[5].

„Ne îndreptăm, iarăși, spre o societate non-industrială, numai că acum ea se se bazează pe tehnologia de vârf[6]. Dacă „al doilea val” ne-a dat „proletariatul”, am putea spune că „al treilea val” produce un „cognitariat”, un grup bazat pe cunoaștere, pe folosirea minții, nu pe mușchi. Cognitariatul posedă informații organizate, imaginație și alte calități culturale, esențiale pentru producție. Deține mijloacele de a produce noi informații. Proprietatea esențială devine informația, prima formă de proprietate non-materială, non-tangibilă și potențialmente infinită”.

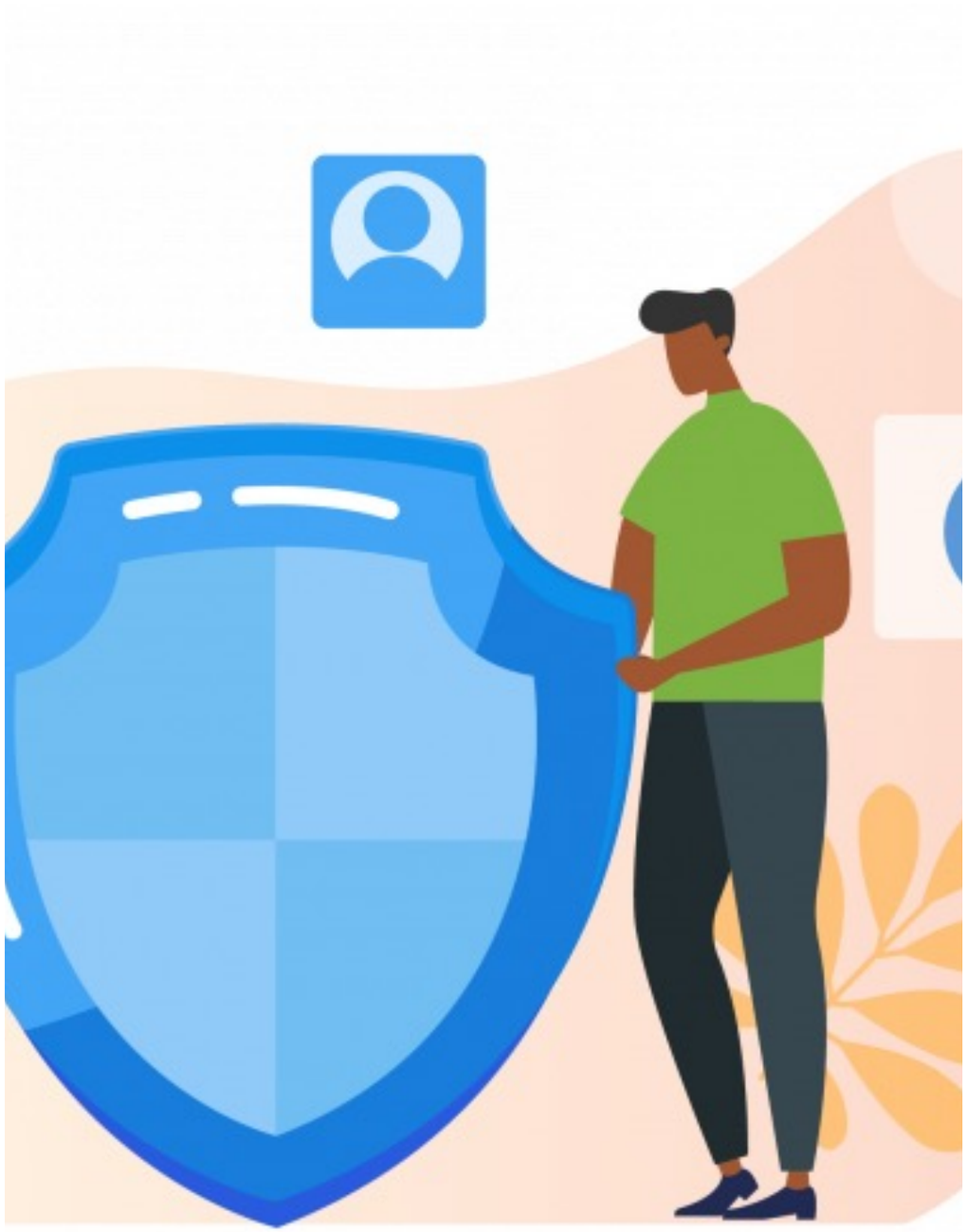
Alvin Toffler, *Previziuni și premise,* trad. Mihnea Columbeanu, Editura Antet, 1996, p. 104, 112-113

Managementul informației

- ✓ **proces** care încorporează politici și proceduri pentru gestionarea și partajarea informației;
- ✓ **program organizațional** care gestionează oamenii, procesele și tehnologia;
- ✓ **concept** de sistem informațional al întreprinderii;
- ✓ **controlul** administrării unei organizații asupra activelor sale informaționale;
- ✓ se realizează prin **sistemele de management** al informației concepute special;
- ✓ se concentrează pe modul în care informațiile sunt **partajate** și **livrate** către destinatari[7].

Gestionarea datelor

Avantaje



- Veți fi mai productiv
- Veți economisi bani
- Puteți reacționa mai repede
- Veți atenua riscurile de securitate
- Veți putea lua decizii mai precise

Strategii de gestionare a datelor

Componente comune

- IDENTIFICAREA DATELOR, ce înseamnă acestea, cum sunt structurate, de unde provin și unde se află
- STOCAREA, care permite să accesați, partajați și procesați cu ușurință datele organizației
- ADMINISTRAREA, care permite să organizați datele astfel încât să poată fi reutilizare sau partajate și să adăugați reguli sau linii directoare pentru accesarea acestora
- CONDUCEREA, necesară pentru stabilirea, gestionarea și comunicarea politicilor și mecanismelor existente/necesare pentru utilizarea datelor
- PROCESAREA, care facilitează să mutați sau să combinați datele stocate în sisteme diferite pentru a oferi o vizualizare unificată și unică[8]

Protejarea datelor

Drept fundamental la informație

↓

Obligație fundamentală de apărare

Limite:

- ➡ respectarea drepturilor altuia și al celorlalți;
- ➡ protejarea siguranței și securității persoanelor juridice, a instituțiilor și a statului;
- ➡ apărarea demnității și a moralei[9].

CAUZA: dezvoltarea tehnologiilor de producere a datelor și informației

CONSECINȚA:

- producerea sistemelor de apărare a informației;
- apărarea bazelor de date și a
- sistemelor de transmisie, stocare și valorificare a acestora[10].

Securizarea informației

Triada

Securizarea datelor și a informației trebuie să asigure:

- **confidențialitatea** - protejarea împotriva dezvăluirii către utilizatori neautorizați
- **integritatea** - asigurarea împotriva modificărilor necorespunzătoare și menținerea fiabilității și acurateței
- **disponibilitatea** - accesarea acestora atunci când este necesar de către persoanele îndrituite să aibă acces

SECURIZARE ABSOLUTĂ?

Proces

NU

Scop

POLITICI și PRACTICI
pentru:
definirea, direcționarea și sprijinirea organizației[11]

Organizarea sistemului de management al securității informației

Leadership și conducere - acțiuni

1. să se asigure că politicile de securitate ale datelor și informației sunt stabilite și compatibile cu direcția strategică a organizației;
2. să asigure integrarea sistemului de management al securității informației în procesele organizației;
3. să se asigure că sunt disponibile resursele necesare pentru sistemul de management al securității informației;
4. să comunice importanța unei gestionări eficiente a securității informației și să îndeplinească cerințele sistemului de management al securității informației;
5. să se asigure că sistemul de management al securității informației obține rezultatele scontate;
6. să direcționeze să să sprijine persoanele fizice să contribuie la îmbunătățirea sistemului de management al securității informației;
7. să promoveze îmbunătățirea continuă;
8. să sprijine alte roluri manageriale pentru aplicarea principiilor în domeniile lor de responsabilitate.

Politici de securizare a informației

Criterii conform ISO 27001: 2022 (E)

(a) să fie adecvate scopului organizației;
(b) includă obiective de securitate a informației sau să ofere cadrul pentru stabilirea obiectivelor de securitate a informației:
    1) să fie în concordanță cu politicile de securitate
    2) să fie măsurabile (dacă este posibil)
    3) să țină seama de cerințele aplicabile în materie de securitate a datelor și de rezultatele evaluării și tratării riscurilor
    4) să fie monitorizate
    5) să fie actualizate
    6) să fie comunicate
    7) să fie disponibile sub formă de informații documentate
    8) să se cunoască ce se va face
    9) ce resurse vor fi necesare
    10) cine va fi responsabil
    11) când va fi finalizată
    12) modul cum vor fi evaluate rezultatele.
(c) includă un angajament de a îndeplini cerințele aplicabile legate de securitatea datelor și a informației;
(d) sistemul de management al securității informațiilor să fie îmbunătăți continuu;
(e) să fie disponibile sub formă de informații documentate
(f) să fie comunicate în cadrul organizației
(g) să fie puse la dispoziția părților interesate, după caz[12].

PROTECȚIA INFORMAȚIILOR

CADRUL NORMATIV

ELEMENTE	
	• POLITICĂ ȘI CULTURĂ
	• STRATEGIE
	• PLAN DE ACȚIUNE
	• CONCEPȚIE
	• NORME ȘI STANDARDE
	• ANGAJAMENTE

STRUCTURI DE SECURITATE

PROIECTARE ȘI REALIZARE

CERINȚE	
	• EVOLUȚIA PARALELĂ A TEHNOLOGIILOR DE SECURITATE ȘI DE CRIMĂ ORGANIZATĂ
	• DEZINFORMAREA ȘI SUFOCAREA INFORMAȚIONALĂ
	• MUTAȚII FUNDAMENTALE ÎN TEHNOLOGIA IT
	• INSUFICIENȚA RESURSELOR PENTRU SECURITATE

STRUCTURI DE PROTECȚIE

CRITERII

ASPECTE DE PROTECȚIE

- ❖ LOC, ROL ȘI COMPETENȚE
- ❖ RESURSE FINANCIARE
- ❖ COMPONENTELE DE SECURITATE
- ❖ AUTORIZAREA PERSONALULUI
- ❖ ANALIZĂ ȘI CONTROL
- ❖ CARACTERISTICI DE PROCES
- ❖ ANALIZĂ DE RISC

STRUCTURI DE SECURITATE

PRINCIPII FUNCȚIONALE

- ➡ CONFIDENȚIALITATE
- ➡ AUTONOMIE ACȚIONALĂ
- ➡ RESPONSABILITATE JURIDICĂ
- ➡ PUTERE DECIZIONALĂ
- ➡ MULTIFUNCȚIONALITATE
- ➡ ADAPTABILITATE
- ➡ INTEGRITATE MORALĂ
- ➡ PROFESIONALISM

STRUCTURI DE PROTECȚIE

Elemente de decizie

FACTORI DE REALIZARE

- ★ SPECIFIC ȘI INTERESE
- ★ NIVEL DE INFORMATIZARE
- ★ VULNERABILITĂȚI ȘI RISCURI
- ★ FONDURI
- ★ CONSECINȚE EVENIMENTE NEDORITE
- ★ MEDIUL DE SECURITATE[13]

ELABORAREA POLITICII DE SECURITATE

PRINCIPII GENERALE

- ❖ În ipoteza că oricât de prevăzători și procedurali am fi, un incident de securitate IT tot vom avea (măcar o dată). Trebuie să căutam căi prin care să scădem probabilitatea de apariție, să minimizăm dimensiunile unui astfel de incident precum și să împingem apariția acelui incident cât mai departe în timp;
- ❖ Fiind vorba de colecții de reguli coercitive, trebuie să luam în calcul gradul ridicat de insatisfacție ce poate apărea la unii din cei vizați de planul și politica de securitate. Dacă este prea grea (complexă), mulți vor încerca să o ocolească;
- ❖ Rata de evoluție a riscurilor are o dinamică ridicată și ele trebuie reanalizate periodic, independent de rata de evoluție a firmei / instituției;
- ❖ Dacă va afecta în mod negativ productivitatea, ea va eșua;
- ❖ Trebuie să exprime clar ce se poate și ceea ce este interzis pe echipamentele instituției; trebuie evitat jargonul sau descrierile complexe, dar, totodată, trebuie să fie cât mai cuprinzătoare posibil;
- ❖ Trebuie să conțină o frază de tipul: “Angajații nu au voie să descarce jocuri, wallpaper-e, screen-saver-e, imagini, clipuri video, sau orice alt fel de aplicații sau fișiere multimedia”. Ceea ce este scris cu caractere italice trebuie să acopere tot ce nu a fost explicit specificat în enumerarea anterioară;
- ❖ Trebuie să acopere toate departamentele și toată ierarhia administrativă; ea trebuie să fie asumată, respectată și sprijinită pornind de la cel mai înalt nivel (nu se acceptă standarde duble);
- ❖ Trebuie să conțină clauze care să specifice clar consecințele cu care se vor confrunta în cazul nerespectării politicii de securitate;
- ❖ Trebuie actualizată în concordanță cu noile tehnologii (ex.: medii de stocare USB, dispozitive mobile de tip smart);
- ❖ Se recomandă avizul unui consilier juridic prin care să se ofere garanția ca politica respectivă respectă legislația în vigoare și nu încalcă nici unul din drepturile celor vizați de ea.

ELABORAREA PLANULUI DE SECURITATE

PRINCIPII DE CARE SE ȚINE CONT

- ❖ utilizarea acceptabilă a resurselor IT
- ❖ se face un inventar pentru a putea răspunde la următoarele întrebări:
  - ✦ ce tipuri de informații există și unde?
  - ✦ cum sunt folosite și protejate informațiile?
  - ✦ cine are acces la informații si în ce circumstanțe?
- ❖ se creează mai multe niveluri de securitate
  - ✦ accesul fizic
  - ✦ securizarea rețelei la nivelul 2 + 3
  - ✦ securizarea serverelor / website-urilor
  - ✦ securizarea stațiilor de lucru
  - ✦ securizarea la nivelul utilizatorilor
- ❖ se creează proceduri de detecție a incidentelor
- ❖ proceduri de backup al datelor si, uneori, chiar al echipamentelor
- ❖ se creează planuri de recuperare in caz de pierderi / furt de date, de dezastre
- ❖ se antrenează angajații pentru recunoașterea, raportarea si (non)acțiunea în cazuri de:
  - ✦ social engineering
  - ✦ phishing
  - ✦ fraude online
  - ✦ falși antiviruși
  - ✦ spyware, adware, malware in general
  - ✦ software malițios
  - ✦ cererea de date de identitate prin telefon
- ❖ securitatea la nivel internet (set de reguli pentru o navigare sigura) si a serviciilor de tip iCloud
- ❖ politica parolelor puternice si a timpului de expirare a lor
- ❖ securizarea si criptarea rețelei wireless; izolarea vizitatorilor de angajați
- ❖ politica de update-uri ale OS-urilor dar si aplicațiilor
- ❖ daca accesul de la distanta este permis, asigurați-vă că este sigur (Ex. VPN + autentificare in doi pași)
- ❖ utilizarea doar a mediilor de stocare USB inventariate și verificate ca fiind “sigure”
- ❖ utilizarea email-urilor (dezvoltarea unei politici specifice)
- ❖ asigurarea unui filtru anti-spam
  - ✦ instruirea angajaților in vederea utilizării responsabile a email-ului
  - ✦ protejarea informațiilor sensibile trimise prin email
  - ✦ dispozitive mobile
  - ✦ utilizarea programelor de securitate
  - ✦ actualizări la zi
  - ✦ criptarea datelor
  - ✦ utilizarea unor parole de acces puternice
  - ✦ proceduri in cazul pierderii / furtului
  - ✦ asigurați-vă ca toate dispozitivele sunt curate (wiped) înainte de a fi eliminate din uz
- ❖angajații
  - ✦ controale de fond si de acces
  - ✦ relațiile cu terții
  - ✦ instruiri periodice
  - ✦ checklist-uri
- ❖securitatea facilităților
  - ✦ protejarea materialelor tipărite cu informații sensibile
  - ✦ securitatea corespondentei clasice (posta, firme de curierat)
  - ✦ distrugerea deșeurile ce conțin date sensibile (hârtie, alte medii de stocare, echipamente electronice, etc.)
- ❖proceduri operaționale
  - ✦ identificarea informațiilor critice
  - ✦ analiza si evaluarea riscurilor
  - ✦ analiza vulnerabilităților
- ❖răspunsul la incidente
  - ✦ notificarea autoritarilor dacă este necesară
  - ✦ coerența între echipele tehnice si de conducere
  - ✦ începerea procedurilor de recuperare
  - ✦ ținerea unei ședințe pentru a se învața din greșeli

Legea europeană privind guvernanța datelor

Deceniul digital - Politici

Legea va sprijini crearea și dezvoltarea unor **spații europene comune ale datelor** în domenii strategice, implicând atât actorii privați, cât și cei publici, în sectoare precum sănătatea, mediul, energia, agricultura, mobilitatea, finanțele, industria prelucrătoare, administrația publică și competențele

Guvernanța datelor a intrat în vigoare la 23 iunie 2022 și, după o perioadă de grație de 15 luni, se aplică din septembrie 2023.

Obiective cheie

- instrument transsectorial care reglementează reutilizarea datelor protejate în mod public/deținute (inclusiv datele protejate: datele cu caracter personal și datele comerciale confidențiale), prin:
    - ◉ stimularea schimbului de date prin reglementarea noilor intermediari de date;
    - ◉ încurajarea schimbului de date în scopuri altruiste: atât datele cu caracter personal, cât și cele fără caracter personal intră în domeniul de aplicare al legii - GDPR se aplică ori de câte ori sunt vizate datele cu caracter personal.

Beneficii

Inițiativa urmărește: să pună la dispoziție mai multe date și să faciliteze schimbul de date între sectoare și țările UE, pentru a valorifica potențialul datelor în beneficiul cetățenilor și al întreprinderilor europene.

- Buna gestionare a datelor și schimbul de date vor permite industriilor să dezvolte produse și servicii inovatoare și vor face multe sectoare ale economiei mai eficiente și mai durabile. De asemenea, este esențial pentru formarea sistemelor de IA.
- Cu mai multe date disponibile, sectorul public poate elabora politici mai bune, conducând la o guvernanță mai transparentă și la servicii publice mai eficiente.
- Inovarea bazată pe date va aduce beneficii pentru întreprinderi și persoane fizice, făcând viața și munca noastră mai eficiente prin:
    - **date privind sănătatea**: îmbunătățirea tratamentelor personalizate, asigurarea unei asistențe medicale mai bune și sprijinirea vindecării bolilor rare sau cronice;
    - **date privind mobilitatea**: economisirea a milioane de ore de timp pentru utilizatorii de transport public și a miliarde EUR pe an în ceea ce privește costurile cu forța de muncă ale conducătorilor auto, datorită navigației în timp real;
    - **date privind mediul**: combaterea schimbărilor climatice, reducerea emisiilor de CO_2 și combaterea situațiilor de urgență, cum ar fi inundațiile și incendiile forestiere;
    - **date agricole**: dezvoltarea agriculturii de precizie, a unor noi produse în sectorul agroalimentar și a unor noi servicii în general în zonele rurale;
    - **date privind administrația publică**: furnizarea de statistici oficiale mai bune și mai fiabile și contribuția la decizii bazate pe dovezi.

Cum va funcționa acest lucru în practică?

UE va stimula dezvoltarea unor sisteme fiabile de schimb de date prin intermediul a 4 seturi largi de măsuri:

1. **Mecanisme de facilitare a reutilizării anumitor date din sectorul public care nu pot fi puse la dispoziție ca date deschise. Cerințele tehnice pentru sectorul public vor asigura că viața privată și confidențialitatea datelor sunt pe deplin respectate și vor include**:
    a. soluții tehnice: anonimizarea, pseudonimizarea sau accesarea datelor în medii de prelucrare securizate (săli de date)
    b. mijloace contractuale: acorduri de confidențialitate între organismul din sectorul public și reutilizator; acorduri exclusive de reutilizare a datelor, date unei societăți în cazuri specifice de interes public;
2. **Măsuri de asigurare a faptului că intermediarii de date (piețele de date) vor funcționa ca organizatori de încredere ai schimbului de date sau ai punerii în comun în cadrul spațiilor europene comune ale datelor**:
    a. Este propus un model bazat pe neutralitatea și transparența intermediarilor de date (platformele Big Tech, care au un grad ridicat de putere pe piață și controlează mari cantități de date);
    b. Intermediarii de date vor funcționa ca părți terțe care conectează persoanele fizice și companiile cu utilizatorii de date, putând percepe taxe pentru schimbul de date între părți, dar fără a putea să le utilizeze pentru profit financiar (vânzare către terți sau utilizat pentru dezvoltarea propriului produs);
3. **Măsuri menite să faciliteze punerea la dispoziție de către cetățeni și întreprinderi a datelor lor în beneficiul societății**:
    a. Organismul din sectorul public va ajuta reutilizatorul să solicite consimțământul persoanei fizice de a reutilizare datele sale personale. Informațiile confidențiale (secretele comerciale) pot fi divulgate în vederea reutilizării numai cu un astfel de consimțământ sau permisiune;
    b. Altruismul în materie de date se referă la persoane fizice și companii care își dau consimțământul sau permisiunea de a pune la dispoziție datele pe care le generează - în mod voluntar și fără recompensă - pentru a fi utilizate în interesul public. Entitățile bazate pe altruism vor avea caracter non-profit și vor îndeplini cerințele de transparență și reglementare.
4. **Măsuri de facilitare a schimbului de date, în special pentru a permite utilizarea datelor la nivel transsectorial și transfrontalier și pentru a permite identificarea datelor corecte în scopul corect** [15]:
    a. Statele membre vor alege organismele competente care vor sprijini organismele din sectorul public care acordă acces la reutilizare prin: asigurarea unui mediu de prelucrare securizat și prin consilierea acestora cu privire la cea mai bună structură și stocare a datelor pentru a le face ușor accesibile.
    b. Statele vor înființa un punct unic de informare, pentru a ajuta reutilizatorii să găsească informații relevante cu privire la datele deținute de autoritățile publice;
    c. Comisia a creat Registrul european al datelor protejate, deținut de sectorul public, care are posibilitatea de căutare a informațiilor compilate de punctele unice de informare naționale pentru a facilita reutilizarea datelor pe piața internă și în afara acesteia[16].

Note bibliografice

[1] https://en.wikipedia.org/wiki/Copenhagen_Peace_Research_Institute (accesat la: 27.02.2024)
[2] https://www.sipri.org/ (accesat la: 27.02.2024)
[3] Constantin Zamfir, *Securitatea civilă și globalizarea* (teză de doctorat), FED Print S.A., București, 2009, pp.208-212
[4] *Standardul ISO 27001 - Securitatea informațiilor, securitatea cibernetică și protecția vieții private. Sisteme de gestionare a securității informațiilor. Cerințe.* Ediția a II-a, 2022-10, ISO/IEC 27001: 2022(E), ISO/IEC 2022
[5] Vasile-Adrian Cămărășan, Anca-Gabriela Petrescu, Marius Petrescu, Florentina-Raluca Bîlcan, *Instrumente și mecanisme privind managementul informațiilor clasificate - de la teorie la practică*, Editura Bibliotheca, 2017, p.49
[6] Cristian Popa, Teodoru Ștefan, Ion Ivan, *Măsuri organizatorice și structuri funcționale privind accesul accesul la informații. Protecția informațiilor clasificate*, Editura Academiei Naționale de Informații, București, 2008, p.10
[7] https://medium.com/@joshuaquilingan4/information-management-vs-data-management-db6d86a925a6 (accesat la: 15.01.2024)
[8] https://www.jotform.com/what-is-data-management/ (accesat: 15.01.2024)
[9] Cristian Popa, Teodoru Ștefan, Ion Ivan, *Măsuri organizatorice și structuri funcționale privind accesul accesul la informații. Protecția informațiilor clasificate*, Editura Academiei Naționale de Informații, București, 2008, p.18
[10] Ibidem, p.19
[11] *Information Security - An Overview of general Concepts*, March 30, 2021, disponibil la: https://www.filecloud.com/blog/2021/03/information-security-an-overview-of-general-concepts/ (accesat la 11.12.2023)
[12] *Standardul ISO 27001 - Securitatea informațiilor, securitatea cibernetică și protecția vieții private. Sisteme de gestionare a securității informațiilor. Cerințe*. Ediția a II-a, 2022-10, ISO/IEC 27001: 2022(E), ISO/IEC 2022
[13] Ion Ciobanu, Gheorghe Ilie, Aurel Nour, *Confruntarea informațională și protecția informațiilo*r, Editura Detectiv, București, 2006, pp. 241-249
[14] Constantin Avramescu, *Cum pot ajuta Politica și Planul de Securitate la îmbunătățirea gradului de siguranță al unei instituții,* în: Revista Spell IT, , nr.4, 2012-2013, pp.1-13
[15] https://digital-strategy.ec.europa.eu/ro/policies/data-governance-act (accesat la 16.01.2024)
[16] https://digital-strategy.ec.europa.eu/ro/policies/data-governance-act-explained (accesat la 16.01.2024)