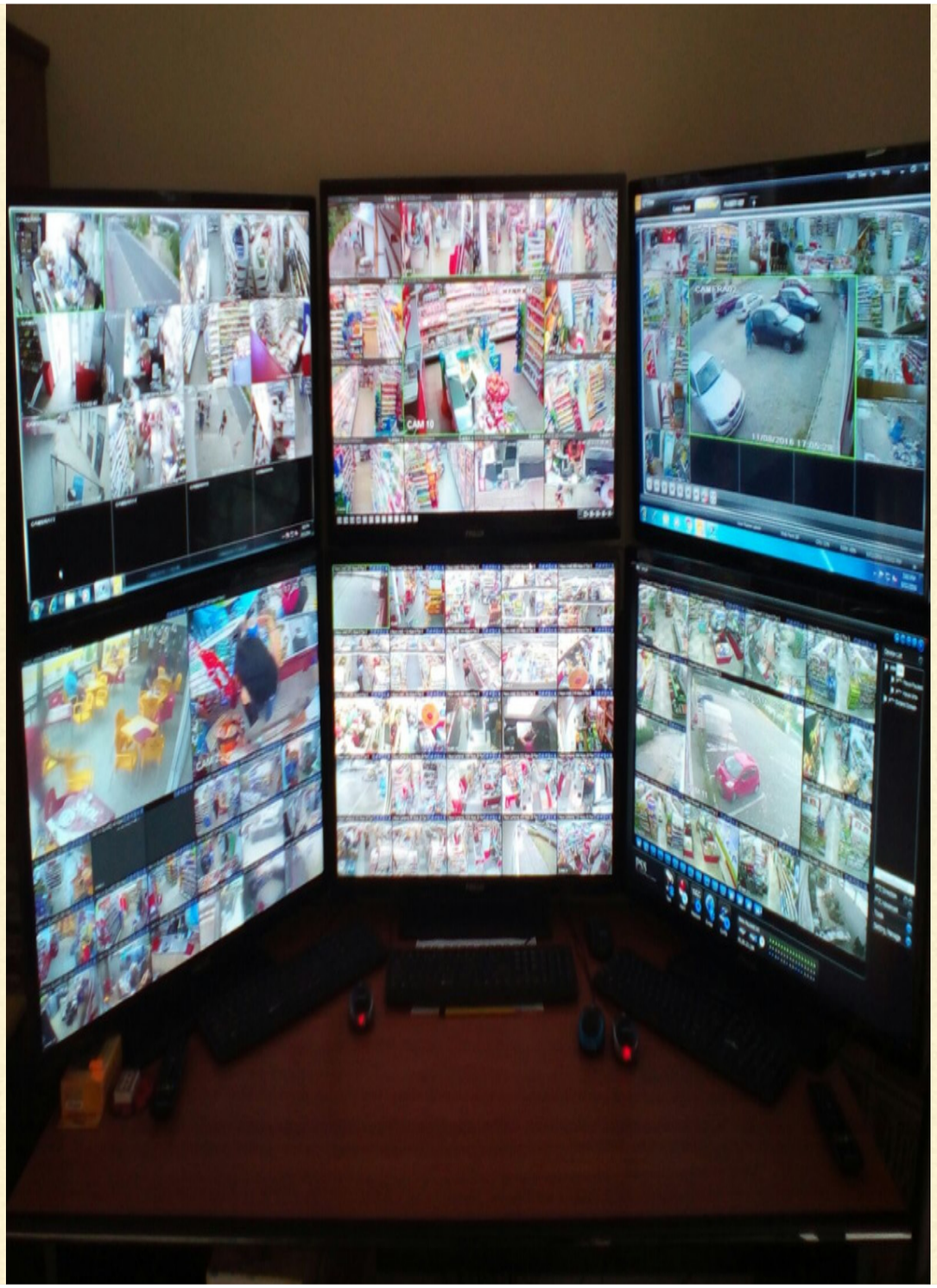
SECURITATE INTEGRATĂ ÎN DOMENIUL INFORMAȚIILOR

1. Securitatea fizică și de mediu
2. Protecția resurselor umane
3. Protecția juridică
4. Securitatea procedurală
5. INFOSEC

SECURITATEA FIZICĂ ȘI DE MEDIU



Definiții

■ **ISO 27001**: Securitatea fizică este:

- o parte importantă a sistemului de management al securității informațiilor și
- se referă la asigurarea unor zone fizice și de mediu sigure, pentru a preveni accesul fizic neautorizat, deteriorarea sau interferența cu datele și informația și instalațiile de procesare ale acestora [1]

■ Securitatea fizică: ansamblul măsurilor de protecție aplicate în spațiile în care sunt gestionate informații clasificate care trebuie protejate împotriva accesului neautorizat, deteriorării, distrugerii, pierderii sau compromiterii [2]

■ Securitatea fizică reprezintă ansamblul reglementărilor și măsurilor aplicate clădirilor, încăperilor sau containerelor destinate protecției informațiilor clasificate cu scopul de a evita compromiterea acestora și de a împiedica pătrunderea persoanelor neautorizate în locurile unde se gestionează asemenea informații [3]

■ **Legea nr.182/2002:**

- protecția fizică este ansamblul măsurilor de pază, securitate și apărare, prin măsuri și dispozitive de control fizic și prin mijloace tehnice, a informațiilor clasificate (art.15, lit. i) [4] ,
- instituțiile deținătoare de informații secrete de stat poartă răspunderea elaborării și aplicării măsurilor procedurale de protecție fizică a acestora, care trebuie să fie conforme standardelor din HG nr.585/2002 (art. 23, alin (1) și (2) [5]

■ Legislația Uniunii Europene (**Decizia 2013/488/UE** din 23 septembrie 2013): securitatea fizică reprezintă aplicarea măsurilor de protecție fizică și tehnică în vederea împiedicării accesului neautorizat la informațiile UE clasificate [6]

Principii generale care stau la baza programelor de securitate fizică:

1. Adaptarea măsurilor de securitate la specificul locației ce trebuie protejată;
2. Eșalonarea în adâncime a măsurilor de securitate prin structurarea acestora pe mai multe dispozitive succesive, dispuse în jurul unei locații unde sunt gestionate informații clasificate:
    a. un „dispozitiv exterior" de securitate care să delimiteze zona protejată și să descurajeze accesul; neautorizat;
    b. un „dispozitiv intermediar" de securitate care să descopere tentativele sau accesul neautorizat în zona protejată și să alerteze forța de securitate;
    c. un „dispozitiv interior" care să să întârzie eventualii intruși în acțiunile lor, suficient de mult timp pentru a fi reținuți de forțele de securitate;
3. Corelarea măsurilor de securitate fizică cu timpul de intervenție a forțelor de securitate:
    a. penetrarea sistemului de securitate să nu fie posibilă sau, la limită, să necesite suficient de mult timp
    b. să permită intervenția forțelor de securitate și anihilarea agresiunii înainte de compromiterea informațiilor;
4. Asigurarea eficacității sistemului de securitate prin: antrenarea și testarea personalului și a sistemului de securitate în ansamblu;
5. Păstrarea performanțelor tehnice ale echipamentelor prin realizarea lucrărilor de întreținere, reparare și înlocuire, periodic și de câte ori e necesar;
6. Realizarea din timp și exersarea unor planuri de răspuns:
    a. pentru situații previzibile de apariție a unor incidente de securitate sau
    b. atunci când este necesară scoaterea din funcțiune, pe o perioadă limitată, a unor elemente ale sistemului de securitate [7] .

Perimetrul de securitate fizică

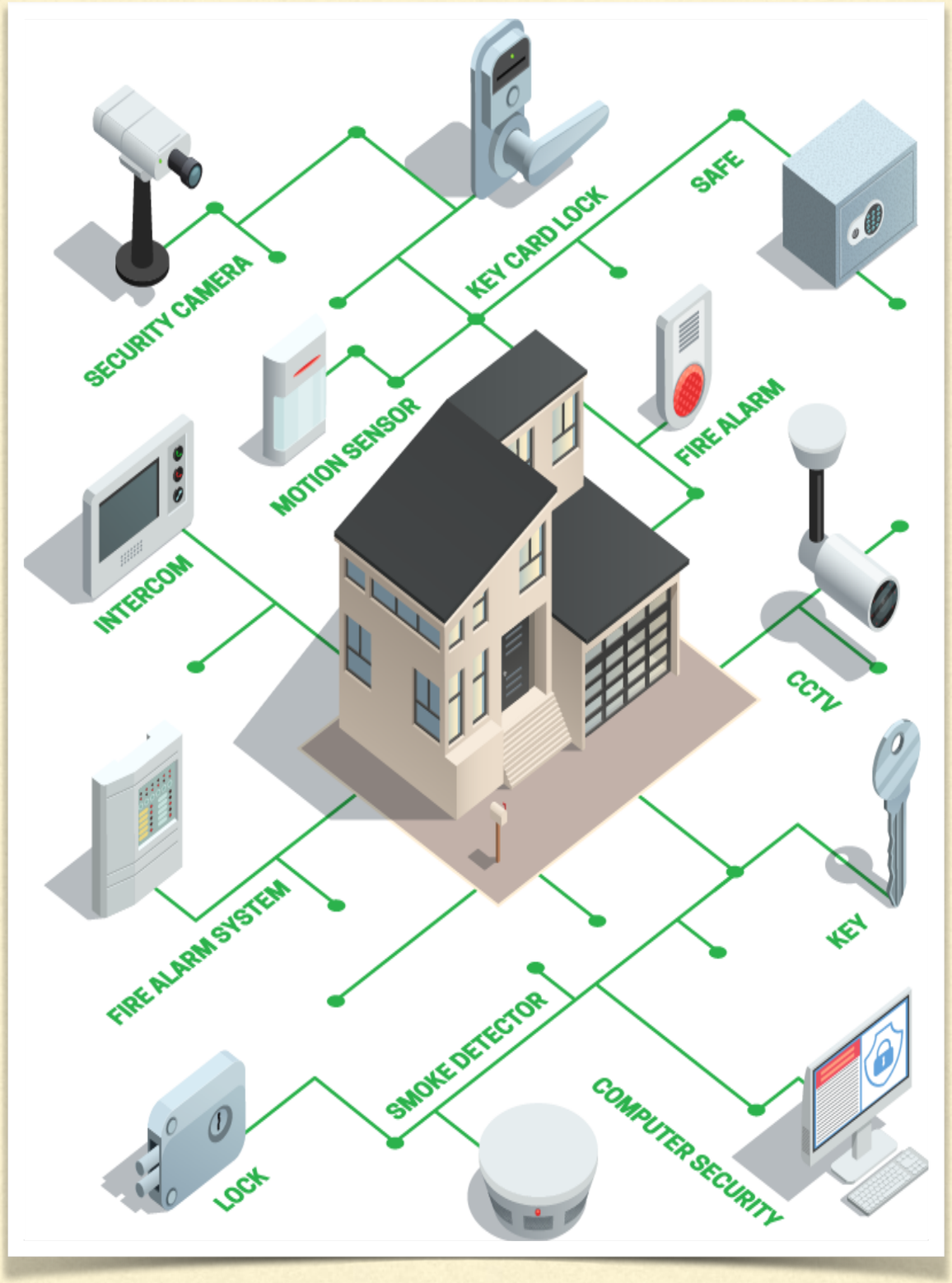
Perimetrul de securitate fizică include limitele și zonele care conțin date și informații sensibile, precum și facilități, inclusiv de natură critică, pentru procesarea acestora (computere, servere, laptopuri).

Un perimetru de securitate fizică este definit ca „orice zonă de tranziție între două locuri cu cerințe diferite de protecție de securitate”, putând fi:

- limita exterioară a zonei, cuprinzând spațiile exterioare și interioare;
- între exteriorul și interiorul unei clădiri și interiorul acesteia;
- între un coridor și birou sau între exteriorul unui dulap de depozitare și interiorul acestuia;
- sediul central al unei întreprinderi cu adresa definită și limitele zonei din jurul său.

Exemple de tipuri de proprietăți și spații pe care o organizație trebuie să le ia în considerare în ceea ce privește securitatea fizică și care pot include:

- centrele de date care găzduiesc active informaționale;
- sediul central;
- lucrători care lucrează de acasă;
- lucrători care călătoresc și prin urmare folosesc hoteluri, sediile clienților;
- birourile închiriate [8] .



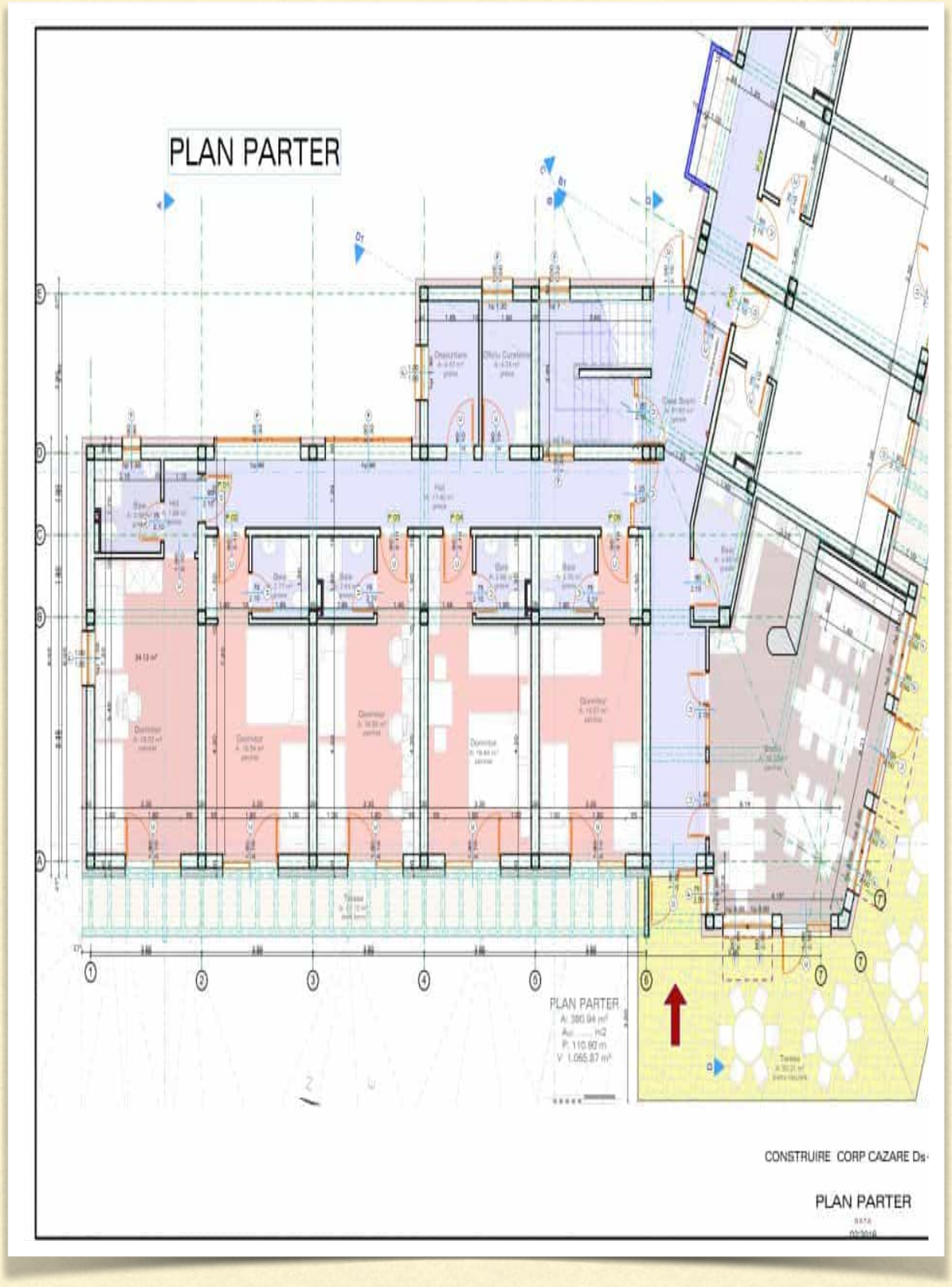
Planul de amplasament

Documentul de bază în definirea perimetrului de securitate este planul de amplasament (al clădirii sau etajului), care însoțește actele de proprietate ale organizației.

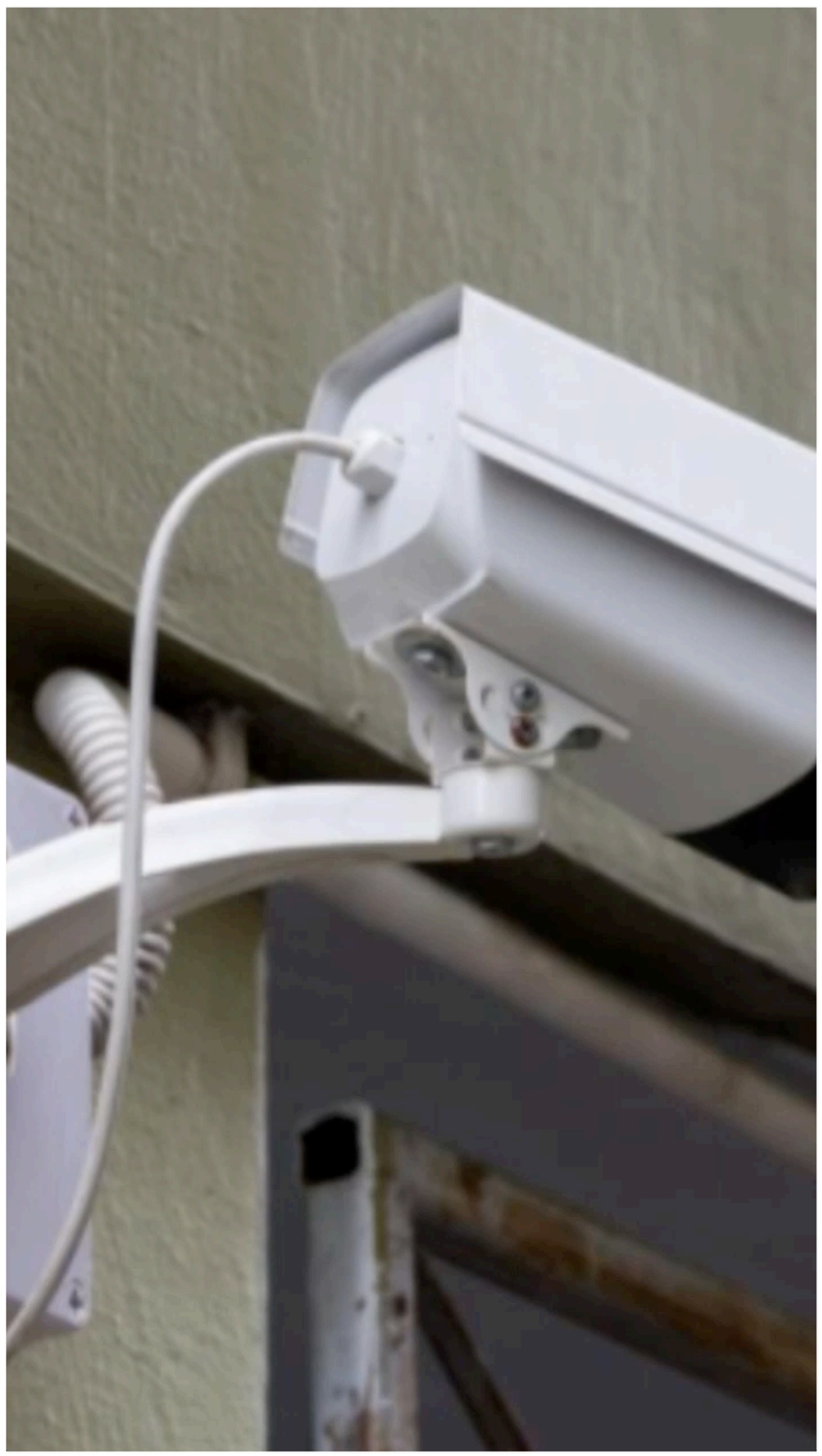
În jurul amplasamentului se fixează linii de demarcare a perimetrului, care urmează perimetrul fizic și zona exterioară, practic între organizație și lumea exterioară: pereți, uși, ferestre, porți, podele, luminatoare - tavanele false trebuie evitate pentru că ascund amenințări.

Se acordă atenție: ascensoarelor, puțurilor și canalelor de acces și întreținere.

Acest plan de amplasament, care arată perimetrul fizic, va fi examinat de auditorul ISO27001, care va evalua riscurile și va identifica punctele slabe, vulnerabilitățile sau lacunele din acest perimetru, care să impună controale fizice adecvate (bariere fizice suplimentare, porți automate, personal de control) [9].



Măsuri de protecție fizică a informațiilor clasificate (România)



HG nr.585/2002 stipulează (art.97 până la art.139 din Standarde) că măsurile includ:

- gratii la ferestre
- încuietori la uși
- pază la intrări
- sisteme automate pentru supraveghere, control, acces
- patrule de securitate
- dispozitive de alarmă
- mijloace pentru detectarea observării, ascultării sau interceptării.

Dimensionate în raport cu:
a) nivelul de secretizare a informațiilor, volumul și localizarea;
b) tipul containerelor în care sunt depozitate informațiile;
c) caracteristicile clădirii și zonei de amplasare;

Spaţiile unde sunt manipulate sau stocate informaţiilor clasificate se organizează şi administrează ca **zone de securitate** (clasa I şi clasa a II - a) constituite în perimetre clar delimitate şi protejate, în care accesul este controlat prin sisteme de recunoaştere individuală:

➡în zonele de securitate **clasa I** se gestionează informații secrete de stat, nivel "strict secret de importanță deosebită" și "strict secret",

➡în zonele de securitate **clasa II-a**, informații secrete de stat, nivel "secret".

În jurul zonelor de securitate poate fi stabilită o **zonă administrativă**, cu perimetru vizibil delimitat, în interiorul căreia să existe posibilitatea de control al personalului și al vehiculelor.

Reguli cu privire la:

- circulația şi ordinea interioară în zonele de securitate,
- un sistem propriu de control al vizitatorilor, astfel încât
- accesul să fie permis exclusiv posesorilor de certificate de securitate şi autorizaţii de acces, cu
- respectarea principiului "necesității de a cunoaște".

Informaţiile clasificate se păstrează în **containere speciale** (clasa A - pentru păstrarea informaţiilor "strict secrete de importanţă deosebită" şi clasa B - pentru păstrarea informaţiilor "strict secrete" şi "secrete"), ale căror cerinţe de securitate şi standarde constructive sunt stabilite de ORNISS [10].

Securitatea fizică a informațiilor clasificate (Uniunea Europeană)

Decizia 2013/488/UE din 23 septembrie 2013 stabilește normele de securitate pentru protecția informațiilor UE clasificate (IUEC), astfel încât:

(a) să garanteze gestionarea și păstrarea IUEC în mod adecvat;

(b) să permită separarea personalului în ceea ce privește accesul acestuia la IUEC, pe baza principiului necesității de a cunoaște și a autorizării de securitate;

(c) să descurajeze, să împiedice și să detecteze acțiunile neautorizate; și

(d) să împiedice sau să întârzie accesul disimulat sau forțat al vreunui intrus.

Cerințe și măsuri de securitate fizică:

Procesul de management al riscului va asigura aplicarea unui nivel de protecție fizică proporțional cu riscul evaluat, în special de:

(a) nivelul de clasificare al IUEC;

(b) forma și volumul IUEC (pot fi necesare măsuri de protecție mai stricte);

(c) mediul înconjurător și structura clădirilor sau o zonelor care adăpostesc IUEC;

(d) evaluarea amenințării reprezentate de serviciile secrete care au drept țintă UE sau statele membre și de sabotaje, acte teroriste, subversive sau alte activități criminale.

Măsuri de securitate fizică

1

Barieră fizică de incintă

protejează limitele unei zone ce necesită protecție

SDI pot fi folosite pentru sporirea nivelului de securitate oferit de o barieră de incintă sau în încăperi sau clădiri, în locul personalului de securitate sau în sprijinul acestuia

2

Sisteme de detectare a intruziunilor

prin: mijloace electronice, electromecanice, de către personalul de securitate sau persoana de la recepție sau prin alte mijloace fizice

3

Controul accesului

pentru descurajarea unui intrus potențial și pentru a asigura lumina necesară penru supravegherea directă de către personalul de securitate sau indirectă, prin TVCI

4

Personalul de securitate

trebuie să fie format și supravegheat și să dețină autorizarea de securitate pentru a descuraja anumite persoane să plănuiască intrarea clandestină

5

Televiziunea cu circuit închis

să verifice incidentele și alarmele declanșate de SDI în spații vaste sau perimetre

6

Iluminatul de securitate

Alte măsuri de securitate

7

menite să descurajeze sau să detecteze accesul neautorizat sau să împiedice pierderea sau deteriorarea IUEC [11]

Măsuri de asigurare a protecției fizice a datelor - ISO 27001

- **Controale fizice la intrare**: accesul se asigură doar personalului autorizat, prin:
  - coduri și cheie de acces; soluții biometrice sau de scanare;
  - testarea și monitorizarea accesului;
  - înregistrarea și auditarea accesului - în special la locațiile închiriate;
  - acces limitat la infrastructura IT și în zonele unde se prelucrează date sensibile sau informații clasificate;
  - control adecvat al vizitatorilor;

- **Securizarea birourilor, încăperilor și facilităților**, prin:
  - revizuirea periodică a accesului (cine, când și cum);
  - stabilirea a: cine poate vedea sau auzi din afară ce se discută în birou
  - actualizarea modului de acces în cazul în care o persoană se transferă sau pleacă din organizație;
  - însoțirea vizitatorilor în zonele protejate;
  - vigilența personalului atunci când apar persoane pe care nu le cunosc (dacă comunică aceste aspecte);
  - protecția datelor și echipamentelor în sălile de ședințe, utilizate împreună cu alte persoane: laptopuri, date scrise pe table, flipchart etc.;

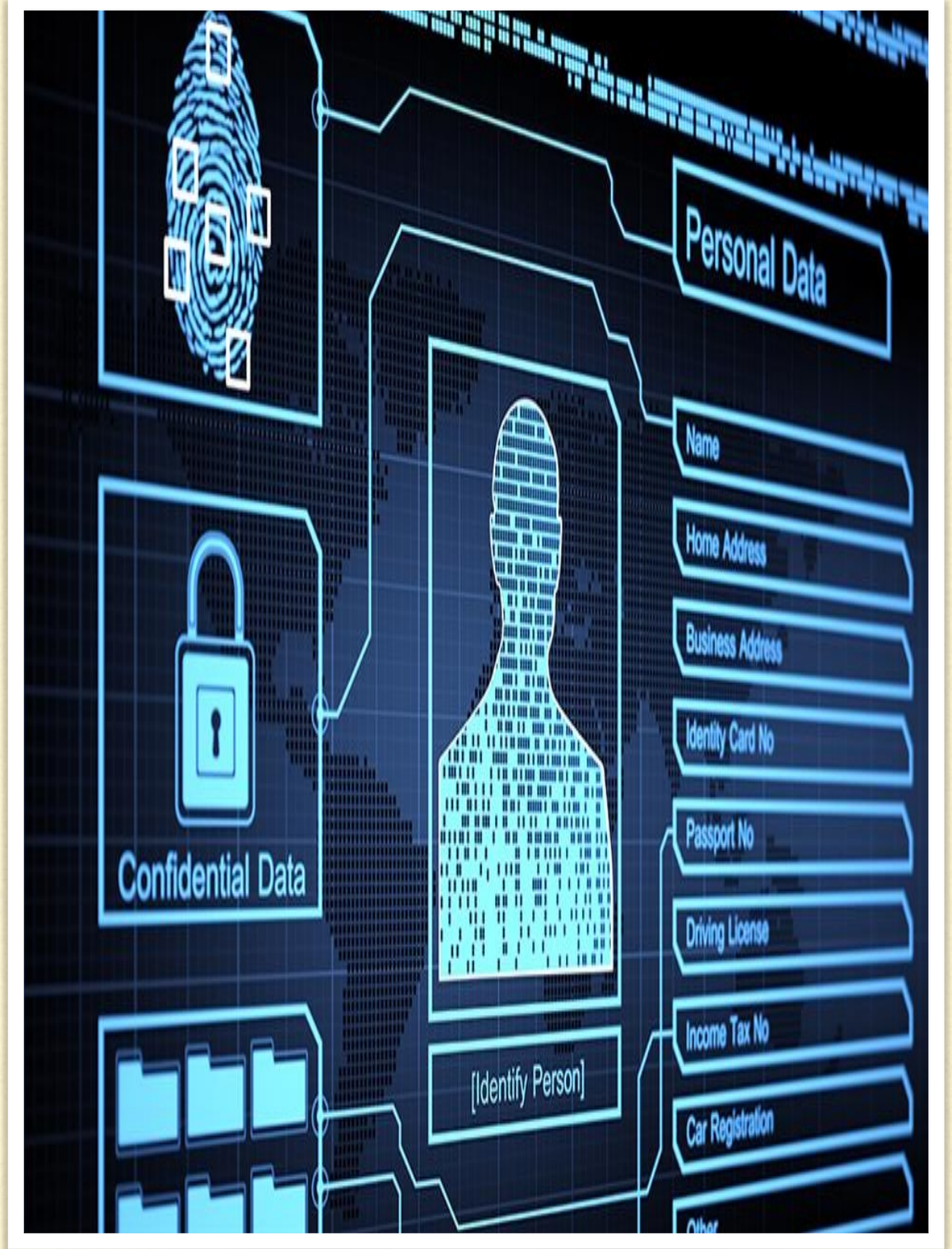
- **Protecția împotriva amenințărilor externe și de mediu**:
  - descrierea măsurilor de prevenire și protecție fizică împotriva dezastrelor naturale (inundații, tornade, fulgere) sau provocate de om (atacuri rău intenționate, scurgeri de apă în instalații, tulburări civile);
  - respectarea recomandărilor de mediu în cazul amplasării în zone de risc (inundabile, de ex.);
  - cunoașterea a ceea ce se află în imediată apropiere (vulnerabilități care apar în mod natural sau provocate de om);

Măsuri de asigurare a protecției fizice a datelor - ISO 27001

- Activitatea în zone securizate, prin:
  - controale procedurale referitoare la riscurile care pot apărea în interiorul zonei securizate:
    - cunoașterea restrânsă a funcției zonelor securizate;
    - restricții privind utilizarea echipamentelor de înregistrare în zonele securizate;
  - restricții privind munca nesupravegheată în zone protejate
  - monitorizare la ieșire;

- Zonele de livrare și încărcare:
  - persoanele neautorizate care ar putea să intre în incintă trebuie controlate și izolate de facilitățile de procesare a datelor pentru evitarea accesului neautorizat;
  - locurile de muncă digitale sau în cloud nu necesită politici de control fizic;
  - pază suplimentară în locațiile situate separat sau departe de clădirea principală;
  - monitorizare și înregistrare prin CCTV;
  - prevenirea accesului extern și intern deschis în același timp;
  - controlul materialelor care intră (livrările) și a celor care ies (prevenirea scurgerilor de informații) [12].

PROTECȚIA RESURSELOR UMANE



Definiții

- **Legea nr.182/2002** definește protecția personalului ca ansamblul verificărilor și măsurilor destinate persoanelor cu atribuții de serviciu în legătură cu informațiile clasificate, spre a preveni și înlătura riscurile de securitate pentru protecția informațiilor clasificate.

- **Decizia 2013/488/UE** stabilește că securitatea personalului înseamnă aplicarea unor măsuri care să garanteze că accesul la IUEC este acordat numai persoanelor care:
  - prezintă necesitatea de a cunoaște;
  - au primit autorizare de securitate pentru nivelul corespunzător, dacă este cazul; și
  - au fost informate cu privire la responsabilitățile care le revin.

- **ISO 27001:2022** menționează (capitolul 7.1 - Resurse) că organizația determină și furnizează resursele necesare pentru stabilirea, implementarea și îmbunătățirea sistemului de management al securității informațiilor și trebuie:
  - să determine competența necesară a persoanei (persoanelor) care efectuează activitatea sub controlul lor pentru asigurarea performanței în materie de securitate a informațiilor;
  - să se asigure că aceste persoane sunt competente pe baza unei educații, a unei formări sau a unei experiențe adecvate
  - să ia măsuri pentru a dobândi competența necesară (furnizare de formare, mentorat sau repartizarea către angajații actuali sau angajarea de persoane competente) și pentru a evalua eficacitatea acțiunilor întreprinse; și
  - să păstreze informații documentate adecvate ca dovadă a competenței.

Măsuri de protecție a personalului (HG nr.585/2002)

Conform HG nr.585/2002 (art.140), măsurile de protecție a personalului **au drept scop:**

(a) să prevină accesul persoanelor neautorizate la informații secrete de stat;

(b) să garanteze ca informațiile secrete de stat sunt distribuite deținătorilor de certificate de securitate/ autorizații de acces, cu respectarea principiului necesității de a cunoaște;

(c) să permită identificarea persoanelor care, prin acțiunile sau inacțiunile lor, pot pune în pericol securitatea informațiilor secrete de stat și să prevină accesul acestora la astfel de informații.

Protecția personalului **se realizează prin**:

(a) selecționarea,

(b) verificarea,

(c) avizarea și autorizarea accesului la informațiile secrete de stat,

(d) revalidarea,

(e) controlul și

(f) instruirea personalului,

(g) retragerea certificatului de securitate sau autorizației de acces.

Lista funcțiilor cu acces la informații clasificate:

(a) conducătorii autorităţilor, instituțiilor publice, agenţilor economici cu capital integral sau parţial de stat şi celorlalte persoane juridice de drept public sau privat aprobă listele funcțiilor care presupun accesul la informaţii clasificate:

(1) este necesară evaluarea atribuţiilor specifice fiecărei funcţii din statul de organizare al instituţiei, pentru a stabili dacă necesită acces la informaţii clasificate şi nivelul de secretizare aferent;.

(b) selecţionarea persoanelor care urmează să ocupe funcţii ce presupun accesul la informaţii clasificate se derulează integral şi exclusiv în cadrul fiecărei instituţii deţinătoare de informaţii clasificate;

(c) la dimensionarea listei funcţiilor care presupun acces la informaţii clasificate se au în vedere:

(1)includerea tuturor funcţiilor care presupun accesul la informaţii clasificate, chiar dacă unele dintre acestea sunt vacante;

(2)realizarea concordanţei între nivelul de acces solicitat şi nivelul de secretizare a informaţiilor.

(d) lista funcţiilor se actualizează ori de câte ori este necesar şi se comunică autorităţii desemnate de securitate competentă.

Măsuri de protecție a personalului (ISO 27001)

ISO 27001:2022 (tabelul A.1, 6.1-6.8) tratează **problemele legate de securitate înainte de angajare**, ținând seama de:

- legile, reglementările și etica aplicabile și proporționale cu cerințele comerciale;
- clasificarea informațiilor care trebuie accesate și riscurile percepute;
- obiectivul de a reduce riscurile de pierdere a informațiilor prin eroare umană, fraudă sau utilizarea necorespunzătoare a echipamentelor.

Fișa postului trebuie să conțină:

- o descriere a competențelor necesare pentru rol
- o declarație în sensul că fiecare angajat trebuie să cunoască politica organizației privind securitatea informațiilor (o copie a politicii poate fi atașată la fișa postului);
- trebuie atrasă atenția angajatului asupra responsabilității de a proteja activele împotriva accesului neautorizat, dezvăluirii, modificării, distrugerii sau interferențelor, regulilor de clasificare și manipulare a informațiilor, contoarelor de acces (fizice și logice), procedura de raportare a incidentelor și faptul că angajatul va fi tras la răspundere pentru actele de comitere sau omisiune;
- precizări clare că încălcarea controalelor de securitate a informațiilor poate fi considerată contravenție conform politicii disciplinare a organizației și că încălcarea acesteia poate duce la concediere;
- responsabilitățile de securitate informațiilor care se aplică anumitor funcții:
  - ofițerul sau consilierul pentru securitatea informațiilor,
  - membrii managementului: securității informațiilor și IT, personalul de suport IT și care gestionarea rețelele și siturile web,
  - personalul de securitate a sediului,
  - HR (recrutare și formare personal),
  - personal cu atribuții financiare, juridice, secretariat,
  - echipa de continuitate a afacerii și de răspuns la situații de urgență,
  - directorii generali;
- o declarație de responsabilitate pentru securitatea informațiilor dată de persoanele care au roluri în asigurarea confidențialității, integrității și disponiblității informațiilor în organizație, semnată și datată de angajat [13] .

Procedura de verificare

Scop:
identificarea vulnerabilităţilor de securitate - caracteristici de personalitate care:
a)pun în pericol securitatea informaţiilor clasificate,
b)pot fi exploatate pentru a se influenţa persoana să se implice în acte de diseminare neautorizată de informaţii clasificate - persoane care sprijină obiectivele unor structuri informative, grupuri de interese de a avea acces la informaţii; clasificate,
c) pentru a se preveni apariţia riscului de securitate – accesul la informaţii clasificate va avea drept consecinţă compromiterea și/sau diseminarea acestora

Verificarea în vederea avizării **se realizează de către**: SRI, MApN, MAI, SIE, MJ, SPP, STS [14]

Formulare de securitate:

I. date personale despre solicitant (de identificare),
II.domiciliu permanent și flotant,
III.situația familială,
IV.locurile de muncă,
V.funcția solicitată (conform listei funcțiilor)
VI.referințe,
VII.relații cu societăți comerciale din țară și străinătate,
VIII.declarația de conformitate.

Se vor furniza date suplimentare la solicitarea funcționarului de securitate în cazul unor eventuale neclarități (Anexele 15-17 în HG nr.585/2002).

Criteriile investigațiilor de securitate

HG nr.585/2002 (art.158):

(a) trăsăturile de caracter

(b) situațiile și împrejurările din care pot rezulta amenințări și vulnerabilități de securitate;

(c) caracterul, conduita profesională și socială

(d) concepțiile și mediul de viață al soțului/ soției sau concubinului/concubinei persoanei solicitante.

➡ corectitudinii în gestionarea informațiilor secrete de stat;

➡ oportunității accesului neînsoțit în compartimente, obiective, zone și locuri de securitate în care se află informații secrete de stat;

➡ respectării reglementărilor privind protecția informațiilor secrete de stat din domeniul său de activitate.

Decizia privind avizarea eliberării autorizației de acces sau certificatului de securitate se ia pe baza tuturor informațiilor disponibile și are în vedere (art.157):

(a) loialitatea indiscutabilă a persoanei;

(b) caracterul, obiceiurile, relațiile și discreția persoanei, care să ofere garanții asupra:

Decizia Consilului Uniunii Europene 2013/488/UE: investigația de securitate va stabili:

(a) loialitatea persoanei;

(b) onestitatea și încrederea inspirată de o persoană în scopul autorizării de securitate [15].

Elemente de incompatibilitate (HG nr.585/2002)

Sunt imputabile **solicitantului** și **soțului/soției, concubinului/ concubinei** acestuia:

(a) comiterea de acte de spionaj, terorism, trădare ori alte infracțiuni contra siguranței statului (prin comitere, intenție, complicitate, completare, instigare);

(b) dacă a cooperat sau a sprijinit acțiuni de spionaj, terorism ori persoane suspectate de a se încadra în această categorie sau de a fi membre ale unor organizații ori puteri străine inamice (inclusiv încercarea, susținerea și participarea);

(c) dacă este sau a fost membru al unei organizații care a încercat, încearcă sau susține răsturnarea ordinii constituționale prin mijloace violente, subversive sau alte forme ilegale;

(d) dacă este sau a fost un susținător al vreunei organizații prevăzute la lit. c), este sau a fost în relații apropiate cu membrii unor astfel de organizații intr-o formă de natură să ridice suspiciuni temeinice cu privire la încrederea și loialitatea persoanei; precum și oricare din următoarele situații:

(e) dacă în mod deliberat a ascuns, a interpretat eronat sau a falsificat informații cu relevanță în planul siguranței naționale ori a mințit în completarea formularelor tip sau în cursul interviului de securitate;

(f) are antecedente penale sau a fost sancționat contravențional pentru fapte care indică tendințe infracționale;

(g) are dificultăți financiare serioase sau există o discordanță semnificativă între nivelul său de trai și veniturile declarate;

(h) consumă în mod excesiv băuturi alcoolice ori este dependent de alcool, droguri sau de alte substanțe interzise prin lege care produc dependență;

(i) are sau a avut comportamente imorale sau deviații de comportament care pot genera riscul ca persoana să fie vulnerabilă la șantaj sau presiuni;

(j) a demonstrat lipsa de loialitate, necinste, incorectitudine sau indiscreție;

(k) a încălcat reglementările privind protecția informațiilor clasificate;

(l) suferă sau a suferit de boli fizice sau psihice care îi pot cauza deficiențe de discernământ confirmate prin investigație medicală efectuată cu acordul persoanei solicitante;

(m) poate fi supus la presiuni din partea rudelor sau persoanelor apropiate care ar putea genera vulnerabilități exploatabile de către serviciile de informații ale căror interese sunt ostile României și aliaților săi.

Elemente de incompatibilitate (Decizia Consilului 2013/488/UE)

Criteriile includ observația dacă persoana respectivă:

(a) a comis sau a încercat să comită, a conspirat la, a acordat ajutor sau a incitat o altă persoană să comită orice act de spionaj, terorism, sabotaj, trădare sau instigare la rebeliune;

(b) este sau a fost asociată cu spioni, teroriști, sabotori sau persoane suspectate, pe baza unor motive întemeiate, de a fi fost asociate reprezentanților unor organizații ale altor state, inclusiv ai serviciilor secrete, care pot amenința securitatea Uniunii și/sau a statelor membre, cu excepția cazurilor în care astfel de asocieri au fost autorizate pentru îndeplinirea unor atribuții oficiale;

(c) este sau a fost membră a unei organizații care încearcă, prin mijloace violente, subversive sau alte mijloace ilegale, *inter alia*, să înlăture guvernul unui stat membru, să schimbe ordinea constituțională a unui stat membru sau să schimbe forma sau politicile de guvernare ale unui stat membru;

(d) este sau a fost susținătoare a unei organizații descrise la litera (c) sau este sau a fost asociată îndeaproape cu membrii unor astfel de organizații;

(e) a ascuns, denaturat sau falsificat în mod intenționat informații semnificative, în special referitoare la securitate, sau a mințit cu bună-știință în cursul completării chestionarului privind securitatea personalului sau în timpul interviului de securitate;

(f) a fost condamnată în urma uneia sau mai multor infracțiuni;

(g) are un istoric de dependență de alcool, de folosire a unor substanțe stupefiante ilegale și/sau de folosire abuzivă a unor substanțe legale;

(h) a manifestat sau manifestă comportamente care ar putea antrena riscul de vulnerabilitate la șantaj sau presiuni;

(i) prin fapte sau limbaj, a demonstrat lipsă de onestitate și loialitate, incapacitate de a inspira încredere;

(j) a încălcat în mod grav sau repetat regulamentele de securitate; sau a încercat sau a reușit să desfășoare o activitate neautorizată legată de sistemele informatice și de comunicații; și

(k) poate fi expus la presiuni (de exemplu, în virtutea deținerii uneia sau mai multor cetățenii ale unor state care nu sunt membre UE sau prin intermediul unor rude sau asociați apropiați care ar putea fi vulnerabili față de servicii secrete străine, grupări teroriste sau alte organizații sau persoane subversive, ale căror scopuri pot amenința interesele de securitate ale Uniunii și/sau ale statelor membre).

Situația financiară și medicală a unei persoane și comportamentul și situația soțului/soției, partenerului/partenerei sau ale unui membru apropiat al familiei pot fi considerate relevante în cadrul investigației de securitate [16].

Verificări asupra personalului (ISO 27001)

Verificări de bază care trebuie realizate:
(a) verificări asupra caracterului și onestității persoanei, atât în plan personal cât și de afaceri. Referințele telefonice, date de o terță parte, trebuie să fie scrise în forma unor note detaliate, semnate și datate, fiind realizate de un membru cu competență al organizației;
(b) o verificare a completitudinii și acurateței CV-ului angajatului, prin intermediul referințelor scrise furnizate de angajatori anteriori sau organizații terțe (vor exista documente standard care sunt trimise pentru a ghida aceste terțe părți în răspuns). Angajatorul trebuie să fie metodic în se asigura că toate faptele sunt coroborate și toate formulare sunt returnate într-o perioadă de timp definită (10 zile), iar în caz de nereturnare formularul trebuie completat printr-un interviu telefonic cu angajatorul anterior;
(c) confirmarea pregătirii profesionale și academice și a calificărilor prin obținerea de la candidat a unor copii ale certificatelor sau a unei alte declarații de calificare. Se pot angaja servicii independente de verificare a CV-urilor, prin care firme specializate pot efectua, contra unor sume stabilite, verificări detaliate ale CV-urilor;
(d) este necesară o verificare independentă de identitate pe baza unui pașaport sau a unui document de identitate care arată o fotografie a angajatului;
(e) situația financiară candidatului/ angajatului, trebuie verificată, fie la numirea inițială, fie la promovare, în cazul în care implică accesul persoanei la facilități de procesare a informațiilor , în special prelucrarea de date sensibile (financiare sau confidențiale). În cazul persoanelor cu funcții de autoritate în firmă, această verificare trebuie repetată în mod regulat (trimestrial sau anual, după caz).

În cazul în care personalul este furnizat de o altă organizație (în IT, unde personalul poate fi angajat printr-o agenție), contractul cu terța parte trebuie să stabilească în mod clar responsabilitatea acesteia de a efectua verificări la un nivel similar [17] .

Statistic, există probabilitatea ca organizația să descopere că mai mulți membri ai personalului său au **CV-uri incorecte sau false.** Organizația trebuie:

- să stabilească în ce măsură persoana amenință securitatea informațiilor;
- experiența directă a angajatului în mediul de lucru poate oferi dovezi pentru a acționa sau elimina inexactitatea din CV;
- angajatul trebuie să fie conștient că inexactitatea a fost descoperită, pentru a evita astfel de comportamente pe viitor.

Revizuirea verificărilor:
Performanța angajaților cu acces la informații sensibile trebuie revizuită (anual, cel puțin) pentru a se asigura că standardele stabilite de organizație sunt menținute.
Revizuirea poate fi realizată prin:
(a) includerea unor întrebări în sistemul de evaluare anuală existent;
(b) managerii vor evalua, zi de z/periodic, comportamentul neobișnuit al salariaților (semne de stres, probleme personale sau provocări financiare);
(c) angajații trebuie ajutați să facă față acestor provocări, care afectează performanța oamenilor (și poate avea implicații pentru securitatea informațiilor) și pot determina unele persoane să comită infracțiuni sau fraude;
(d)managerii trebuie instruiți corespunzător pentru a identifica și gestiona aceste situații în limitele legislației.

Acordul de confidențialitate

ISO 27001 stabilește că angajații, contractații și terții semnează un contract care conține termeni și condiții care acoperă responsabilitățile lor și ale organizației pentru securitatea informației.

Acest contract include acordul de confidențialitate, care stabilește:

- acoperă informațiile obținute înaintea și în timpul angajării și al cărui efect va continua și după încheierea angajării;
- face parte din contractul de muncă - acceptarea condițiilor de angajare include automat și acordul de confidențialitate;
- clauzele contractuale în care se precizează că angajatul are responsabilitate pentru securitatea informațiilor se atașează la fișa postului, însoțită de declarația separată responsabilităților în materie de securitate a informațiilor;
- clauzele de securitate a informațiilor includ îndrumări privind confidențialitatea, clasificarea, responsabilitățile cu privire la informațiile primite de la terți, manipularea datelor cu caracter personal, reguli în afara orelor de program și în orice mediu care nu este de lucru (de ex., acasă); se precizează în mod clar care sunt responsabilitățile angajatului în ceea ce privește utilizarea abuzivă a computerelor;
- în cazul angajaților pe termen scurt, acordul de confidențialitate trebuie inclus în contractul de furnizare de servicii sau să fie independent și trebuie să cuprindă sancțiunile suplimentare recomandate de avocații organizației pentru acoperirea situațiilor în care o persona este expusă la informații confidențiale;
- trebuie să acopere responsabilitățile legale și drepturile în domeniul protecției dreptului de autor, proprietății intelectuale, legislația privind protecția datelor, informații confidențiale sau sensibile (financiare, în special);
- orice organizație căreia i se vor fi dezvăluit date confidențiale în urma unei tranzacții trebuie să semneze un acord de nedivulgare;
- acordul trebuie semnat, datat și returnat organizației înainte ca individului să i se acorde acces la informații confidențiale și trebuie revizuit atunci când acesta urmează să părăsească organizația (angajatului i se reamintesc obligațiile care îi revin în temeiul contractului după încetarea raporturilor de muncă, în special dacă a avut acces la cantități substanțiale de informații confidențiale [18].

PROTECȚIA JURIDICĂ

DURA LEX, SED LEX

(Proverb latin)

Protecția juridică reprezintă ansamblul normelor constituționale și al celorlalte dispoziții legale în vigoare, care reglementează protejarea informațiilor clasificate - Legea nr.182/2002

Scopurile protecției juridice

Scopurile protecției juridice sunt:

- prevenirea compromiterii informațiilor clasificate;
- cercetarea și evidența incidentelor de securitate;
- declasificarea informațiilor compromise.

Instituția publică deținătoare de informații clasificate are obligații pentru:

- cunoașterea/aplicarea reglementărilor legale;
- stabilirea de norme interne de aplicare a reglementărilor legale;
- consiliere/explicare a prevederilor legale;
- instruire și însușire norme interne.

Serviciul Român de informații are responsabilități privind:

- elaborarea standardelor de protecție a informațiilor clasificate;
- consilierea structurii de securitate;
- efectuarea de cercetări și sesizarea organelor de urmărire penală;
- acordarea sprijinului pentru evaluarea prejudiciilor și recuperarea informațiilor [19].

Conform ISO 27002, ediția 2022, protecția juridică a informațiilor se realizează prin:

(A)cerințe legale, statutare, de reglementare și contractuale;
(B)drepturi de proprietate intelectuală;
(C)protecția înregistrărilor;
(D)confidențialitatea și protecția datelor cu caracter personal;
(E)revizuirea independentă a securității informațiilor;
(F)respectarea politicilor, regulilor și standardelor pentru securitatea informațiilor
(G)proceduri de operare documentate [20] .

Compromiterea informațiilor

Conducătorii unităților deținătoare de informații secrete de stat au obligația de a înștiinta, în scris, potrivit competențelor, prin cel mai operativ sistem de comunicare, despre compromiterea unor astfel de informații:

- Ministerul Apărării Naționale,
- Ministerul de Interne,
- Ministerul Justiției,
- Serviciul Român de Informații,
- Serviciul de Informații Externe,
- Serviciul de Protecție și Paza și
- Serviciul de Telecomunicații Speciale,

care stabilesc, pentru domeniile lor de activitate și responsabilitate, structuri și măsuri proprii privind coordonarea și controlul activităților referitoare la protecția informațiilor secrete de stat, potrivit legii.

Înștiințarea trebuie să conțină:

(a) prezentarea informațiilor compromise, respectiv clasificarea, marcarea, conținutul, data emiterii, numărul de înregistrare și de exemplare, emitentul și persoana sau compartimentul care le-a gestionat;

(b) o scurtă prezentare a împrejurărilor în care a avut loc compromiterea, inclusiv data constatării, perioada în care informațiile au fost expuse compromiterii și persoanele neautorizate care au avut sau ar fi putut avea acces la acestea, dacă sunt cunoscute;

(c) precizări cu privire la eventuala informare a emitentului.

La solicitarea instituțiilor competente, înștiințările preliminare vor fi completate pe măsura derulării cercetărilor.
Documentele privind evaluarea prejudiciilor și activitățile ce urmează a fi întreprinse ca urmare a compromiterii vor fi prezentate instituțiilor competente (art. 88 HG nr.585/2002).

Cercetarea de securitate

Orice încălcare a reglementărilor de securitate va fi cercetată pentru a se stabili:

(a) dacă informațiile respective au fost compromise;

(b) dacă persoanele neautorizate care au avut sau ar fi putut avea acces la informații secrete de stat prezintă suficientă încredere și loialitate, astfel încât rezultatul compromiterii să nu creeze prejudicii;

(c) măsurile de remediere - corective, disciplinare sau juridice - care sunt recomandate.

Măsuri:

- în situația în care informațiile clasificate au fost accesate de persoane neautorizate, acestea vor fi instruite pentru a preveni producerea de eventuale prejudicii;
- În cazul săvârșirii de infracțiuni la protecția secretului de stat, unitățile deținătoare au obligația de a sesiza organele de urmărire penală și de a pune la dispoziția acestora datele și materialele necesare probării faptelor (articolul 90 din Standarde).
- structura/funcționarul de securitate are obligația de a tine evidența cazurilor de încălcare a reglementărilor de securitate, a documentelor de cercetare și a măsurilor de soluționare și să le pună la dispoziția autorităților desemnate de securitate, conform competențelor ce le revin. Documentele menționate se păstrează timp de cinci ani.

Litigiile cu privire la calitatea de emitent ori deținător sau cele determinate de conținutul informațiilor secrete de stat, inclusiv drepturile patrimoniale ce revin emitentului din contractele de cesiune și licență, precum și litigiile referitoare la nerespectarea dispozițiilor legale privind dreptul de autor și drepturile conexe, invențiile și inovațiile, protecția modelelor industriale, combaterea concurenței neloiale și a celor stipulate în tratatele, acordurile și înțelegerile la care România este parte, sunt de competența instanțelor judecătorești (art. 92 HG nr.585/2002).

ISO/IEC 27002/2022 (E)

Securitatea informației, securitatea cibernetică și protecția vieții private –
Mijloace de control al securității informației

ISO/IEC 27002/2022 (E) - Securitatea informației, securitatea cibernetică și protecția vieții private – Mijloace de control al securității informației

(A)Cerințele legale, statutare, de reglementare și contractuale
trebuie luate în considerare la:

(a) elaborarea politicilor și procedurilor de securitate a informațiilor;
(b) proiectarea, implementarea sau modificarea controalelor de securitate a informațiilor;
(c) clasificarea informațiilor și a altor active asociate ca parte a procesului de stabilire a cerințelor de securitate a informațiilor pentru nevoi interne sau pentru acordurile cu furnizorii;
(d) efectuarea de evaluări ale riscului de securitate a informațiilor și determinarea activităților de tratare a riscului de securitate a informațiilor;
(e) determinarea proceselor împreună cu rolurile și responsabilitățile aferente referitoare la securitatea informațiilor;
(f) determinarea cerințelor contractuale ale furnizorilor relevante pentru organizație și sfera furnizării de produse și servicii.

Legislație și reglementări
Organizația trebuie:

(a) să identifice toate actele normative din legislație și reglementările relevante pentru securitatea informațiilor organizației pentru a fi la curent cu cerințele pentru tipul lor de activitate;
(b) să ia în considerare conformitatea în toate țările relevante, dacă organizația:
- desfășoară afaceri în alte țări;
- folosește produse și servicii din alte țări în care legile și reglementările pot afecta organizația;
- transferă informații peste granițele jurisdicționale în care legile și reglementările pot afecta organizația;

(c) să cunoască revizuirea legislației și a reglementărilor identificate în mod regulat pentru a fi la curent cu modificările și pentru a identifica noi legislații;
(d) să definească și să documenteze procesele specifice și responsabilitățile individuale pentru îndeplinirea acestor cerințe.

Criptografia
Criptografia este un domeniu care are adesea cerințe legale specifice:

(a) restricții privind importul sau exportul de hardware și software de calculator pentru îndeplinirea funcțiilor criptografice;
(b) restricții privind importul sau exportul de hardware și software de calculator care este conceput pentru a avea funcții criptografice adăugate;
(c) restricții privind utilizarea criptografiei;
(d) metode obligatorii sau discreționare de acces de către autoritățile țărilor la informații criptate;
(e) valabilitatea semnăturilor, sigiliilor și certificatelor digitale.

Contracte
Cerințele contractuale legate de securitatea informațiilor ar trebui să includă cele menționate în:

(a) contracte cu clienții;
(b) contracte cu furnizorii;
(c) contracte de asigurare.

ISO/IEC 27002/2022 (E) - Securitatea informației, securitatea cibernetică și protecția vieții private – Mijloace de control al securității informației

(B)Drepturi de proprietate intelectuală

Organizația trebuie să implementeze proceduri adecvate pentru a proteja drepturile de proprietate intelectuală.
Următoarele **îndrumări** ar trebui luate în considerare:

(a) definirea și comunicarea unei politici tematice privind protecția drepturilor de proprietate intelectuală;
(b) publicarea procedurilor pentru respectarea drepturilor de proprietate intelectuală care definesc utilizarea conformă a software-ului și a produselor informaționale;
(c) achiziționarea de software numai prin surse cunoscute și de renume, pentru a se asigura că drepturile de autor nu sunt încălcate;
(d) menținerea registrelor adecvate de active și identificarea tuturor activelor cu cerințe de protecție a drepturilor de proprietate intelectuală;
(e) păstrarea dovezilor deținerii licențelor, manualelor etc.;
(f) asigurarea că orice număr maxim de utilizatori sau resurse [de ex. unități centrale de procesare (CPU)] permise în cadrul licenței nu este depășită;
(g) efectuarea de revizuiri pentru a se asigura că sunt instalate numai software-ul autorizat și produsele licențiate;
(h) furnizarea de proceduri pentru menținerea condițiilor adecvate de licență;
(i) furnizarea de proceduri pentru eliminarea sau transferul de software către terți;
(j) respectarea termenilor și condițiilor pentru software și informații obținute din rețele publice și surse externe;
(k) să nu realizeze duplicarea, convertirea în alt format sau extragerea din înregistrări comerciale (video, audio) altele decât cele permise de legea dreptului de autor sau de licențele aplicabile;
(l) să nu copieze, integral sau parțial, standarde (de exemplu, standarde internaționale ISO/IEC), cărți, articole, rapoarte sau alte documente, altele decât cele permise de legea dreptului de autor sau de licențele aplicabile.

Produsele software proprietare sunt de obicei furnizate în baza unui **acord de licență** care specifică termenii și condițiile de licență, de exemplu, limitând utilizarea produselor la anumite mașini sau limitând copierea la crearea de copii de rezervă numai.
Consultați seria ISO/IEC 19770 pentru detalii despre managementul activelor IT.

Datele pot fi achiziționate din surse externe. În general, aceste date sunt obținute în condițiile unui **acord de partajare a datelor** sau a unui instrument juridic similar. Astfel de acorduri de partajare a datelor ar trebui să clarifice ce prelucrare este permisă pentru datele achiziționate. De asemenea, este recomandabil ca proveniența datelor să fie precizată în mod clar. Consultați ISO/IEC 23751:—1) pentru detalii despre acordurile de partajare a datelor.

Încălcarea drepturilor de autor poate duce la **acțiuni legale**, care pot implica amenzi și proceduri penale.
Pe lângă faptul că organizația trebuie să își respecte obligațiile față de drepturile de proprietate intelectuală ale terților, ar trebui gestionate și riscurile ca personalul și terții să nu respecte drepturile de proprietate intelectuală ale organizației.

ISO/IEC 27002/2022 (E) - Securitatea informației, securitatea cibernetică și protecția vieții private – Mijloace de control al securității informației

(C) Protecția înregistrărilor

Înregistrările trebuie protejate împotriva pierderii, distrugerii, falsificării, accesului neautorizat și eliberării neautorizate.

Organizația trebuie să realizeze următorii **pași** pentru a proteja autenticitatea, fiabilitatea, integritatea și capacitatea de utilizare a înregistrărilor, deoarece contextul lor de afaceri și cerințele pentru managementul lor se modifică în timp:

(a) emite orientări privind păstrarea, manipularea lanțului de custodie și eliminarea înregistrărilor, care include prevenirea manipulării înregistrărilor. Aceste linii directoare trebuie să fie aliniate cu politica organizației specifică subiectului privind gestionarea înregistrărilor și alte cerințe privind înregistrările;

(b) să întocmească un program de păstrare care să definească înregistrările și perioada de timp pentru care acestea trebuie păstrate.

Sistemul de depozitare și manipulare trebuie:

(a)să asigure identificarea înregistrărilor și a perioadei de păstrare a acestora, luând în considerare legislația sau reglementările naționale, precum și așteptările comunității sau societății, dacă este cazul;

(b) să permită distrugerea corespunzătoare a înregistrărilor după această perioadă, dacă organizația nu are nevoie de ele;

(c) implementate în conformitate cu recomandările furnizate de producătorii de medii de stocare. Există posibilitatea deteriorării suporturilor utilizate pentru stocarea înregistrărilor.

Clasificarea corespunzătoare a **securității informațiilor**, bazată pe schema de clasificare a organizației:

(a) înregistrările trebuie să fie clasificate în tipuri de înregistrări (de exemplu, înregistrări contabile, înregistrări ale tranzacțiilor comerciale, înregistrări ale personalului, înregistrări juridice),

(b) fiecare înregistrare are detalii despre perioadele de păstrare și tipul de suport de stocare permis care poate fi fizic sau electronic.

Sistemele de stocare a datelor:

(a) trebuie alese astfel încât înregistrările necesare să poată fi recuperate într-un interval de timp și un format acceptabile, în funcție de cerințele care trebuie îndeplinite;

(b) în cazul în care sunt alese medii de stocare electronice, trebuie stabilite proceduri care să asigure capacitatea de a accesa înregistrările (atât mediile de stocare, cât și lizibilitatea formatului) pe toată durata perioadei de păstrare pentru a se proteja împotriva pierderilor cauzate de viitoarele schimbări tehnologice;

(c) orice chei criptografice și programe asociate cu arhivele criptate sau semnăturile digitale trebuie păstrate pentru a permite decriptarea înregistrărilor pe perioada de timp în care înregistrările sunt păstrate.

ISO/IEC 27002/2022 (E) - Securitatea informației, securitatea cibernetică și protecția vieții private – Mijloace de control al securității informației

(D) Confidențialitatea și protecția datelor cu caracter personal

Organizația trebuie să identifice și să îndeplinească cerințele privind păstrarea confidențialității și protecția datelor cu caracter personal în conformitate cu legile și reglementările aplicabile și cerințele contractuale.

Modalitatea de realizare a securității datelor personale:

(a) organizația trebuie să stabilească și să comunice tuturor părților interesate relevante o politică specifică privind confidențialitatea și protecția datelor cu caracter personal;
(b) organizația trebuie să dezvolte și să implementeze proceduri pentru respectarea vieții private și protecția datelor cu caracter personal. Aceste proceduri trebuie comunicate tuturor părților interesate relevante implicate în prelucrarea informațiilor de identificare personală;
(c) respectarea acestor proceduri, a tuturor aspectelor din legislație și a reglementărilor relevante privind păstrarea confidențialității și protecția datelor cu caracter personal necesită roluri, responsabilități și controale adecvate. Acest lucru se realizează cel mai bine prin numirea unei persoane responsabile, cum ar fi un ofițer de protecție a datelor (DPO), care trebuie să ofere îndrumări personalului, furnizorilor de servicii și altor părți interesate cu privire la responsabilitățile lor individuale și procedurile specifice care ar trebui urmate;
(d) responsabilitatea pentru gestionarea datelor cu caracter personal ar trebui să fie tratată ținând cont de legislația și reglementările relevante (GDPR în UE).
(e) trebuie implementate măsuri tehnice și organizatorice adecvate pentru a proteja datelor cu caracter personal;
(f) un număr de țări au introdus legislație care stabilește controale asupra colectării, procesării, transmiterii și ștergerii informațiilor personale. În funcție de legislația națională respectivă, astfel de controale pot impune obligații celor care colectează, prelucrează și difuzează date cu caracter personal și pot, de asemenea, să restrângă autoritatea de a transfera PII în alte țări.

Standarde:

(1) ISO/IEC 29100 oferă un cadru de nivel înalt pentru protecția datelor cu caracter personal în cadrul sistemelor TIC;
(2) informații suplimentare despre sistemele de management al informațiilor privind confidențialitatea pot fi găsite în ISO/IEC 27701;
(3) informații specifice privind gestionarea informațiilor privind confidențialitatea pentru cloud-urile publice care acționează ca procesoare ale datelor cu caracter personal pot fi găsite în ISO/IEC 27018;
(4) ISO/IEC 29134 oferă orientări pentru evaluarea impactului asupra vieții private (PIA) și oferă un exemplu de structură și conținut al unui raport PIA;
    a. în comparație cu ISO/IEC 27005, acesta este axat pe procesarea datelor cu caracter personal și este relevant pentru acele organizații care procesează date cu caracter personal. Acest lucru poate ajuta la identificarea riscurilor de confidențialitate și a posibilelor atenuări pentru a reduce aceste riscuri la niveluri acceptabile.

ISO/IEC 27002/2022 (E) - Securitatea informației, securitatea cibernetică și protecția vieții private – Mijloace de control al securității informației

(E) Revizuirea independentă a securității informației

Abordarea organizației în ceea ce privește gestionarea securității informației și implementarea acesteia, inclusiv oamenii, procesele și tehnologiile, trebuie revizuite independent la intervale planificate sau atunci când apar schimbări semnificative.

Scopul acestei revizuiri este asigurarea, adecvarea și eficacitatea continuă a abordării organizației în ceea ce privește gestionarea securității informației. Organizația trebuie să aibă procese pentru a efectua evaluări independente.

Modalitatea de realizare:

(a) conducerea trebuie să planifice și să inițieze revizuiri independente periodice:
- evaluările trebuie să includă evaluarea oportunităților de îmbunătățire și a necesității de modificări ale abordării securității informației,
- inclusiv politica de securitate a informațiilor, politicile specifice unui subiect și alte controale;

(b) astfel de analize trebuie să fie efectuate de persoane independente de domeniul analizat (de exemplu, funcția de audit intern, un manager independent sau o organizație externă specializată în astfel de analize):
- persoanele care efectuează aceste analize ar trebui să aibă competența corespunzătoare;
- persoana care efectuează evaluările nu ar trebui să fie în linia de autoritate pentru a se asigura că are independența necesară pentru a face o evaluare;

(c) rezultatele evaluărilor independente trebuie raportate conducerii care a inițiat revizuirile și, dacă este cazul, conducerii de top. Aceste înregistrări trebuie păstrate;

(d) dacă evaluările independente identifică că abordarea și implementarea organizației pentru gestionarea securității informației sunt inadecvate, conducerea ar trebui să inițieze acțiuni corective:
- de ex. obiectivele și cerințele documentate nu sunt îndeplinite sau nu sunt conforme cu direcția de securitate a informației menționată în politica de securitate a informațiilor și politicile specifice subiectului.

Pe lângă evaluările periodice independente, organizația trebuie să ia în considerare efectuarea de **evaluări independente** atunci când:

(a) legile și reglementările afectează sau impun modificarea organizației;

(b) apar incidente semnificative;

(c)organizația începe o nouă afacere sau schimbă o afacere curentă;

(d) organizația începe să utilizeze un nou produs sau serviciu sau modifică utilizarea unui produs sau serviciu curent;

(e) organizația modifică în mod semnificativ controalele și procedurile de securitate a informației.

ISO/IEC 27007 și ISO/IEC TS 27008 oferă îndrumări pentru efectuarea evaluărilor independente.

ISO/IEC 27002/2022 (E) - Securitatea informației, securitatea cibernetică și protecția vieții private – Mijloace de control al securității informației

(F) Respectarea politicilor, regulilor și standardelor pentru securitatea informației

Conformitatea cu politica de securitate a informației a organizației, politicile specifice subiectului, regulile și standardele trebuie revizuite în mod regulat de către o organizație, pentru a se asigura că securitatea informațiilor este implementată și operată în conformitate cu politica de securitate a informațiilor a acesteia, politicile specifice subiectului, regulile și standardele.

Managerii, proprietarii de servicii, produse sau informații trebuie să identifice cum să revizuiască cerințele de securitate a informațiilor definite în politica de securitate a informațiilor, politicile specifice subiectului, regulile, standardele și alte reglementări aplicabile. Instrumentele automate de măsurare și raportare ar trebui luate în considerare pentru o revizuire periodică eficientă.

În cazul în care se constată o neconformitate în urma revizuirii, managerii trebuie:

(a) să identifice cauzele neconformității;
(b) să evalueze necesitatea unor acțiuni corective pentru a atinge conformitatea;
(c) implementează acțiuni corective adecvate;
(d) revizuiește acțiunile corective luate pentru a verifica eficacitatea acestora și pentru a identifica eventualele deficiențe sau puncte slabe.

Rezultatele revizuirilor și acțiunilor corective efectuate de către manageri, proprietarii de servicii, produse sau informații ar trebui înregistrate și aceste înregistrări trebuie păstrate. Managerii trebuie să raporteze rezultatele persoanelor care efectuează evaluări independente atunci când are loc o evaluare independentă în zona de responsabilitate a acestora.

Acțiunile corective trebuie efectuate în timp util, în funcție de risc. Dacă nu este finalizat până la următoarea revizuire programată, progresul ar trebui cel puțin abordat la acea revizuire.

(G) Proceduri de operare documentate

Procedurile de operare pentru instalațiile de procesare a informației ar trebui să fie documentate și puse la dispoziția personalului care are nevoie de ele, pentru a asigura funcționarea corectă și sigură a instalațiilor de prelucrare a informațiilor.

Trebuie pregătite proceduri documentate pentru activitățile operaționale ale organizației asociate cu securitatea informațiilor, de exemplu:

(a) când activitatea trebuie efectuată în același mod de mai multe persoane;
(b) când activitatea se desfășoară rar și la următoarea desfășurare procedura este probabil să fi fost uitată;
(c) când activitatea este nouă și prezintă un risc dacă nu este efectuată corect;
(d) înainte de predarea activității către personal nou.

Procedurile de operare trebuie să specifice:

(a) persoanele responsabile;
(b) instalarea și configurarea în siguranță a sistemelor;
(c) prelucrarea și manipularea informațiilor, atât automate cât și manuale;
(d) backup și rezistență/reziliență;
(e) cerințe de planificare, inclusiv interdependențe cu alte sisteme;
(f) instrucțiuni pentru tratarea erorilor sau a altor condiții excepționale [de ex. restricții privind utilizarea programelor utilitare, care pot apărea în timpul execuției jobului;
(g) contacte de asistență și escaladare, inclusiv contacte de asistență externă în cazul unor dificultăți operaționale sau tehnice neașteptate;
(h) instrucțiuni de manipulare a suporturilor de stocare;
(i) repornirea sistemului și procedurile de recuperare pentru utilizare în caz de defecțiune a sistemului;
(j) gestionarea pistei de audit și a informațiilor din jurnalul de sistem și sisteme de monitorizare video;
(k) proceduri de monitorizare precum capacitatea, performanța și securitatea;
(l) instrucțiuni de întreținere.

Incidentele de securitate a datelor și informației

Obiectivele trebuie convenite cu managementul în raport cu:
(a) prioritățile organizației pentru gestionarea incidentelor de securitate a datelor și informației,
(b) intervalul de timp de rezolvare pe baza consecințelor potențiale și a gravității;
(c) trebuie implementate proceduri de gestionare a incidentelor pentru a îndeplini aceste obiective și priorități.

Planul de management al incidentelor de securitate a datelor și informației, ia în considerare diferite scenarii și proceduri care sunt dezvoltate și implementate pentru următoarele activități:
(a) evaluarea evenimentelor de securitate a datelor și informației conform criteriilor pentru ceea ce constituie un incident de securitate a informațiilor;
(b) monitorizarea, detectarea, clasificarea, analiza și raportarea a evenimentelor și incidentelor de securitate a datelor și informației (prin mijloace umane sau automate);
(c) gestionarea incidentelor de securitate a datelor și informației până la încheiere, inclusiv răspunsul și escaladarea, în funcție de tipul și categoria incidentului, posibila activare a managementului crizei și activarea planurilor de continuitate, recuperarea controlată de la un incident și comunicarea către părțile interesate externe;
(d) coordonarea cu părțile interesate interne și externe, cum ar fi autoritățile, grupurile și forumurile de interese externe, furnizorii și clienții;
(e) înregistrarea activităților de gestionare a incidentelor;
(f) manipularea probelor;
(g) analiza cauzei principale sau proceduri post-incident;
(h) identificarea lecțiilor învățate și a oricăror îmbunătățiri ale procedurilor de gestionare a incidentelor sau ale controalelor de securitate a datelor și informației în general care sunt necesare.

Răspunsul la incidentele de securitate a datelor și informației

Sunt necesare proceduri documentate și o echipă competentă, pentru a asigura un răspuns eficient și eficient la incidente.

Răspunsul trebuie să includă următoarele:
(a) conținând, dacă consecințele incidentului se pot răspândi, sistemele afectate de incident;
(b) colectarea probelor cât mai curând posibil după producerea evenimentului;
(c) reducere/dezescaladare, după cum este necesar, inclusiv activități de gestionare a crizelor și eventual invocarea planurilor de continuitate a activității;
(d) asigurarea faptului că activitățile de răspuns implicate sunt înregistrate pentru o analiză ulterioară;
(e) comunicarea existenței incidentului de securitate a informațiilor sau a oricăror detalii relevante ale acestuia tuturor părților interesate interne și externe relevante, conform principiului necesității de a cunoaște;
(f) coordonarea cu părțile interne și externe: autoritățile, grupurile și forumurile de interese externe, furnizorii și clienții, pentru a îmbunătăți eficiența răspunsului și a ajuta la minimizarea consecințelor pentru alte organizații;
(g) odată ce incidentul a fost rezolvat cu succes, închiderea formală și înregistrarea acestuia;
(h) efectuarea de analize criminalistice de securitate a datelor, după cum este necesar;
(i) efectuarea analizei post-incident pentru a identifica cauza principală. Asigurați-vă că este documentat și comunicat conform procedurilor definite (vezi 5.27 din ISO 27002);
(j) identificarea și gestionarea vulnerabilităților și punctelor slabe în securitatea informațiilor, inclusiv cele legate de controalele care au cauzat, au contribuit la sau nu au reușit să prevină incidentul.

Seria ISO/IEC 27035 oferă îndrumări suplimentare privind gestionarea incidentelor.

SECURITATEA PROCEDURALĂ

Protecția prin măsuri procedurale (România)

Legea nr.182/2002: protecția informațiilor clasificate vizează protecția procedurală, această modalitate cuprinzând ansamblul reglementărilor prin care emitenții și deținătorii de informații clasificate stabilesc măsurile interne de lucru și de ordine interioară destinate protecției informațiilor.

Instituțiile deținătoare de informații secrete de stat poartă răspunderea (prin conducătorul acesteia) elaborării și aplicării măsurilor procedurale de protecție fizică și a personalului care are acces la informațiile din această categorie, conforme cu Standardele naționale de protecție a informațiilor clasificate.

Conform **HG nr.585/2002** (art.94), măsurile procedurale de protecție a informațiilor secrete de stat vor fi integrate în **programul de prevenire a scurgerii de informații clasificate (PPSIC)**, întocmit potrivit anexei nr. 10 din Standarde, care va fi prezentat, spre avizare, autorității abilitate să coordoneze activitatea și să controleze măsurile privitoare la protecția informațiilor clasificate, potrivit legii.

Sunt **exceptate** de obligativitatea prezentării, spre avizare, a programului de prevenire a scurgerii de informații instituțiile prevăzute la art. 25 alin. (4) din Legea nr. 182/2002 (Parlamentul, Administrația Prezidențială, Guvernul și Consiliul Suprem de Apărare a Țării), care stabilesc măsuri proprii privind protecția informațiilor secrete de stat, potrivit legii.
Serviciul Român de Informații asigură acestor instituții asistență de specialitate.

Protecția prin măsuri procedurale (România)

Programul de prevenire a scurgerii de informații clasificate prevede (HG nr 585/2002, Anexa nr.10, capitolul 5.2) măsuri procedurale de protecție a datelor, informațiilor, documentelor ori a activităților clasificate:

(a) reguli de evidență, procesare, manipulare, accesare, multiplicare, transmitere, păstrare și stocare a datelor, informațiilor și documentelor clasificate indiferent de suport (aprobate de conducerea instituției/ agentului economic);
(b) reguli de acces pentru personalul propriu;
(c) reguli de acces pentru personalul/persoanele din afara instituției/ agentului economic, inclusiv pentru străini sau reprezentanți mass-media.

În **chestionarul de securitate industrială** (prevăzut în anexa nr.25, 7.1.4) sunt prevăzute măsurile procedurale de protecție a informațiilor secrete de stat sau a activităților cu caracter secret de stat, care trebuie integrate în procedurile elaborate privind:

(a) clasificarea informațiilor după nivelul de securitate;
(b) accesul pentru personalul propriu;
(c) accesul pentru personalul din afară, inclusiv pentru reprezentanți ai mass-media;
(d) multiplicarea, transportul și circulația documentelor în interiorul și în afara instituției, atât în timpul, cât şi în afara programului de lucru;
(e) protecția sistemului/subsistemului informatic și de telecomunicații;
(f) controlul intern, activitatea de analiză și evaluare a modului în care se respectă prevederile legale în vigoare, din care să reiasă periodicitatea controalelor, cine le execută, documentele ce se întocmesc și cum se valorifică, răspunderi și sancțiuni;
(g) instruirea personalului autorizat a avea acces.

Agenții constatatori verifică dacă au fost elaborate, actualizate sau completate documentele procedurale stabilite:

1. Programul de prevenire a scurgerii de informații clasificate;
2. Planul de pază și apărare a obiectivelor, sectoarelor și locurilor care prezintă importanță deosebită pentru protecția informațiilor clasificate;
3. Normele interne de protecție a informațiilor clasificate;
4. Ghidul pe baza căruia se realizează încadrarea corectă și uniformă în nivelurile de secretizare a informațiilor secrete de stat.

Protecția prin măsuri procedurale (Uniunea Europeană)

Decizia Consilului UE din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate (**2013/488/UE**) stabilește (articolul 9) măsuri procedurale și administrative pentru managementul informațiilor clasificate pentru a controla IUEC pe durata ciclului lor de viață, contribuind astfel la descurajarea și detectarea compromiterii sau pierderii deliberate sau accidentale a informațiilor.

Măsurile sunt detaliate în **Anexa III** și se referă, în special, la crearea, înregistrarea, copierea, traducerea, reducerea nivelului de clasificare, declasificarea, transportul și distrugerea IUEC.

Managementul riscului de securitate, prevăzut în articolul 5, stabilește că riscul la adresa IUEC este gestionat ca un proces, care urmărește:

(a) determinarea riscurilor de securitate cunoscute;
(b) definirea măsurilor de securitate destinate reducerii acestor riscuri la un nivel acceptabil în conformitate cu principiile de bază și standardele minime de securitate stabilite în prezenta decizie aplicarea măsurilor respective în conformitate cu conceptul apărării în profunzime;
(c) eficacitatea acestor măsuri este evaluată permanent.

Măsurile de securitate pentru protejarea IUEC pe durata ciclului de viață al acestora sunt proporționale, în special, cu:

(a) clasificarea de securitate a acestora;
(b) forma și volumul informațiilor sau al materialelor;
(c) amplasarea și construcția obiectivelor care adăpostesc IUEC; și
(d) evaluarea locală a amenințării reprezentate de activități rău-intenționate și/sau criminale, inclusiv spionaj, sabotaj și terorism.

Planurile de urgență iau în considerare necesitatea protejării IUEC în situații de urgență, pentru a împiedica accesul neautorizat, divulgarea sau pierderea integrității sau a disponibilității.

Măsurile de prevenire și de recuperare destinate minimizării impactului erorilor sau incidentelor majore survenite în timpul gestionării și păstrării IUEC sunt incluse în planurile de continuare a activității.

Concepte UE

„Apărarea în profunzime" înseamnă aplicarea unor măsuri de securitate organizate pe niveluri de apărare multiple.

„Gestionarea" IUEC înseamnă toate acțiunile posibile al căror obiect îl pot face IUEC de-a lungul ciclului lor de viață. Aceasta cuprinde crearea, prelucrarea, transportul, reducerea nivelului de clasificare, declasificarea și distrugerea. În relație cu SIC, aceasta cuprinde, de asemenea, colectarea, afișarea și păstrarea.

„Ghidul clasificărilor de securitate" (GCS) înseamnă un document care descrie elementele unui program sau ale unui contract clasificat, precizând nivelurile aplicabile de protecție a informațiilor. GCS poate fi extins pe toată durata programului sau a contractului respectiv, iar informațiile pot fi reclasificate sau le poate fi redus nivelul de clasificare.

„Instrucțiuni de securitate pentru program/proiect" (ISP) înseamnă o listă de proceduri de securitate care sunt aplicate unui program/proiect specific în scopul standardizării procedurilor de securitate. Acestea pot fi revizuite pe parcursul programului/proiectului.

„Proces de management al riscului de securitate" înseamnă întregul proces de identificare, control și reducere a influenței evenimentelor neprevăzute care pot afecta securitatea unei organizații sau a oricăruia dintre sistemele pe care aceasta le folosește. Procesul acoperă întregul spectru al activităților legate de risc, inclusiv evaluarea, tratarea, acceptarea și comunicarea [21].

II

(Acte fără caracter legislativ)

DECIZII

DECIZIA CONSILIULUI
din 23 septembrie 2013
privind normele de securitate pentru protecția informațiilor UE clasificate

(2013/488/UE)

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 240 alineatul (3),

având în vedere Decizia 2009/937/UE a Consiliului din 1 decembrie 2009 de adoptare a regulamentului său de procedură [1], în special articolul 24,

întrucât:

(1) În vederea desfășurării activităților Consiliului în toate domeniile care necesită gestionarea informațiilor clasificate, se impune instituirea unui sistem de securitate cuprinzător pentru protecția informațiilor clasificate, care să includă Consiliul, Secretariatul General al Consiliului și statele membre.

(2) Prezenta decizie ar trebui să se aplice în cazurile în care Consiliul, grupurile de pregătire ale acestuia și Secretariatul General al Consiliului (SGC) gestionează informații UE clasificate (IUEC).

(3) Statele membre ar trebui, în conformitate cu actele cu putere de lege și reglementările naționale și în măsura necesară pentru funcționarea Consiliului, să respecte prezenta decizie în cazurile în care autoritățile competente, personalul sau contractanții acestora gestionează IUEC, astfel încât fiecare dintre ele să aibă garanția acordării unui nivel echivalent de protecție a IUEC.

(4) Consiliul, Comisia și Serviciul European de Acțiune Externă (SEAE) își asumă angajamentul de a aplica standarde echivalente de securitate pentru protecția IUEC.

(5) Consiliul subliniază importanța asocierii, dacă este cazul, a Parlamentului European și a altor instituții, organisme, oficii sau agenții ale Uniunii la principiile, standardele și normele pentru protecția informațiilor clasificate necesare pentru protejarea intereselor Uniunii și ale statelor sale membre.

(6) Consiliul ar trebui să stabilească cadrul corespunzător pentru partajarea IUEC deținute de Consiliu cu alte instituții, organisme, oficii sau agenții ale Uniunii, după caz, în conformitate cu prezenta decizie și cu acordurile interinstituționale în vigoare.

(7) Organismele și agențiile Uniunii instituite în temeiul titlului V capitolul 2 din Tratatul privind Uniunea Europeană (TUE), Europol și Eurojust ar trebui să aplice, în cadrul organizării lor interne, principiile de bază și standardele minime stabilite în prezenta decizie pentru protecția IUEC, în cazul în care actul de înființare a acestora prevede astfel.

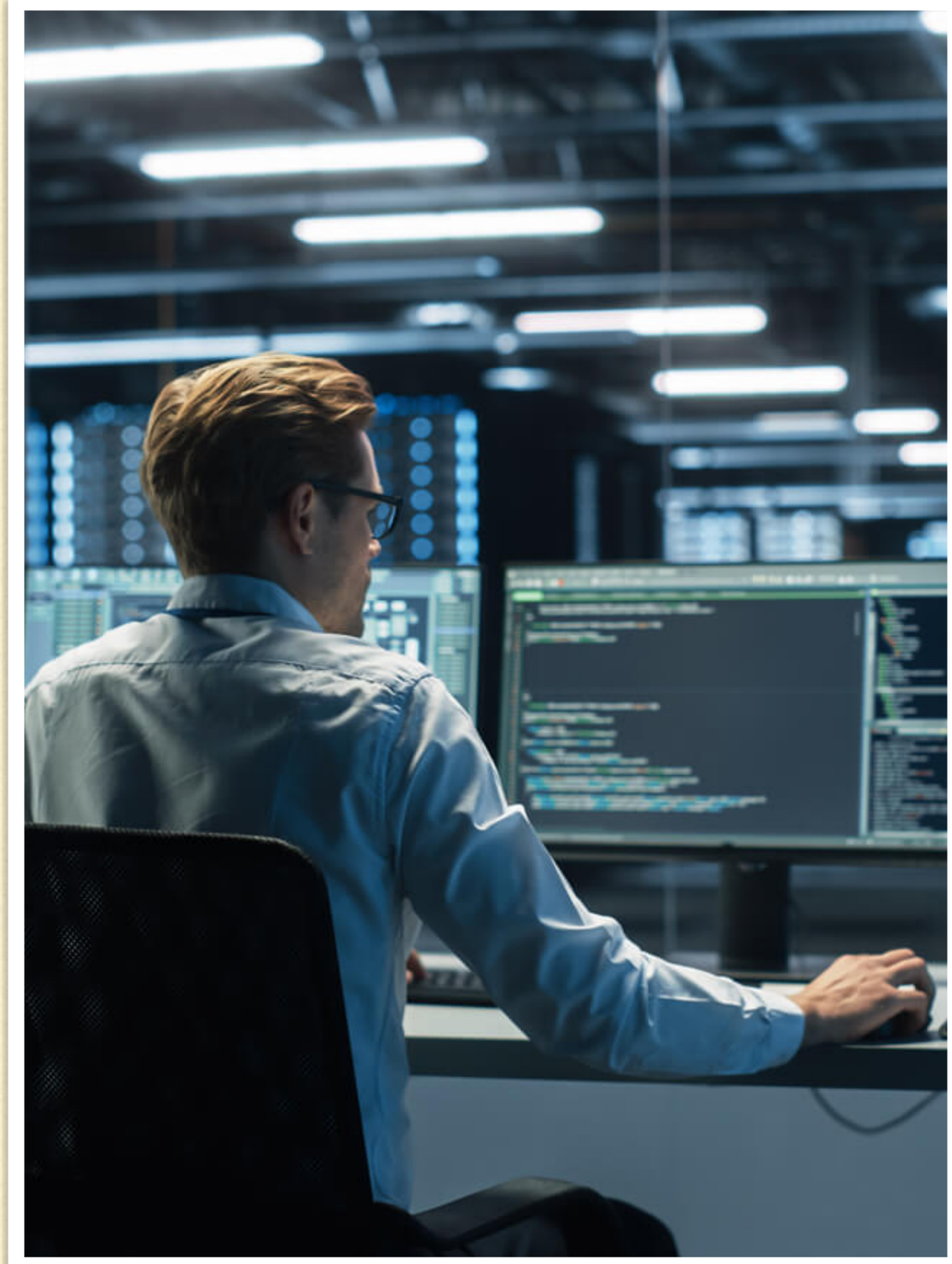
(8) Operațiile de gestionare a crizelor instituite în temeiul titlului V capitolul 2 din TUE și personalul operațiilor în cauză ar trebui să aplice normele de securitate pentru protecția IUEC adoptate de Consiliu în cazul în care actul Consiliului de înființare a acestora prevede astfel.

(9) Reprezentanții Speciali ai UE și membrii echipelor acestora ar trebui să aplice normele de securitate adoptate de Consiliu pentru protecția IUEC în cazul în care actul relevant al Consiliului prevede astfel.

(10) Prezenta decizie se adoptă fără a aduce atingere articolelor 15 și 16 din Tratatul privind funcționarea Uniunii Europene (TFUE) și instrumentelor de punere în aplicare a acestora.

(11) Prezenta decizie se adoptă fără a aduce atingere practicilor existente în interiorul statelor membre cu privire la informarea parlamentelor lor naționale despre activi-

INFOSEC - SECURITATEA INFORMAȚIEI ÎN FORMAT ELECTRONIC



INFOSEC - ansamblul măsurilor și structurilor de protecție a informațiilor clasificate care sunt prelucrate, stocate sau transmise prin intermediul sistemelor informatice de comunicații și al altor sisteme electronice, împotriva amenințărilor și a oricăror acțiuni care pot aduce atingere confidențialității, integrității, disponibilității autenticității și nerepudierii informațiilor clasificate precum și afectarea funcționării sistemelor informatice, indiferent dacă acestea apar accidental sau intenționat (HG, nr.585/2002, art.237)

SECURITATEA INFORMAȚIILOR CLASIFICATE ÎN FORMAT ELECTRONIC

Informația în format electronic reprezintă texte, date, imagini, sunete, înregistrate pe dispozitive electronice de stocare sau pe suporturi magnetice, optice, electrice ori transmise sub formă de curenți, tensiuni sau câmp electromagnetic, în eter sau în rețele de comunicații.

Informație în format electronic întâlnim în sistemele de calcul, în rețelele de transmisii date, în telefonia fixă sau mobilă, în transmisiile radio, etc. Informația clasificată în format electronic reprezintă orice informație în format electronic de interes pentru securitatea națională, care, datorită nivelurilor de importanță și consecințelor care s-ar produce ca urmare a dezvăluirii și diseminării neautorizate, trebuie să fie protejată.

Nu se poate vorbi despre informație clasificată în format electronic decât în strânsă legătură cu sistemele informatice si de comunicație (SIC) care le procesează, stochează sau transmit între diverse componente prin diverse medii de transmitere (fir, aer, mediu de stocare).

Securitatea informației în format electronic – stare de siguranță în care se află informația – se realizează prin măsuri de protecție asupra sistemelor informatice și de comunicații, a căror implementare duce la înlăturarea riscului de securitate (probabilitatea ca o amenințare la adresa securității unui sistem informatic și de comunicații să exploateze o vulnerabilitate a acestuia, efectul fiind compromiterea obiectivelor de securitate, respectiv: confidențialitatea, integritatea, disponibilitatea, autenticitatea și nerepudierea informațiilor clasificate vehiculate prin acel sistem informatic).

Potrivit Standardelor naționale de protecție a informațiilor clasificate în România securitatea informațiilor clasificate în format electronic acoperă securitatea calculatoarelor, a mediilor de stocare, a comunicațiilor, precum și depistarea și prevenirea amenințărilor la care sunt expuse informațiile și sistemele informatice.

Există legislație în domeniu, începând cu Legea nr.182, Standardele de protecție a informațiilor clasificate, Ordinele Directorului ORNISS în care sunt prezentate în amănunt măsurile de protecție ce trebuie luate pentru protecția informației clasificate în format electronic. Sunt măsuri și proceduri care trebuie urmate începând de la achiziție, operaționalizare, acreditare și scoatere din uz a sistemelor informatice.

Standardele naționale de protecție a informațiilor clasificate operează cu următoarele componente INFOSEC:

(a) Securitatea personalului;
(b) Securitatea fizică;
(c) Controlul accesului la SIC;
(d) Securitatea informațiilor clasificate în format electronic;
(e) Controlul și evidența informațiilor în format electronic;
(f) Manipularea și controlul mediilor de stocare a informațiilor clasificate în format electronic;
(g) Declasificarea și distrugerea mediilor de stocare a informațiilor în format electronic.

A. Securitatea calculatoarelor

Securitatea calculatoarelor – COMPUSEC - aplicarea la nivelul fiecărui calculator a facilităților de securitate hardware, firmware și software, pentru a preveni divulgarea, manevrarea, modificarea sau ștergerea neautorizată a informațiilor clasificate ori invalidarea neautorizată a unor funcții
Mecanismele de securitate hardware, firmware și software pot contribui individual și în combinație la securitatea calculatoarelor.

Securitatea hardware și firmware utilizează caracteristicile de securitate asigurate de către fabricant prin componentele fizice ale calculatoarelor și se referă la următoarele aspecte:

(a) proceduri și documentație de securitate pentru pornirea/oprirea echipamentelor de calcul;
(b) instrucțiuni și proceduri de securitate referitoare la conectarea/ deconectarea echipamentelor în/de la rețea;
(c) proceduri pentru efectuarea unor verificări regulate ale sigiliilor de pe echipamente și asigurarea că modulele hardware sunt păstrate încuiate, în mod normal, în carcasa echipamentului;
(d) configurația calculatorului trebuie să îi asigure acestuia posibilitatea de a putea funcționa în condiții variate (de exemplu trebuie precizat ce terminale / stații de lucru sau periferice pot fi conectate sau deconectate într-o situație specifică de exploatare);
(e) proceduri de securizare a configurației calculatorului pregătit pentru întreținere și reparare;
(f) proceduri care trebuie urmate în caz de cedare hardware, cu descrierea acțiunilor care trebuie întreprinse și de către cine, în vederea securizării calculatorului la deconectare și ce date trebuie păstrate referitoare la astfel de incidente hardware;
(g) proceduri pentru reconectarea terminalelor / stațiilor de lucru de la distanță care au fost deconectate din motive de securitate.

Securitatea software are în vedere utilizarea și controlul oricăror facilități de protecție furnizate prin software: sistem de operare, programe utilitare, programe de aplicație:

(a) metode de identificare a utilizatorilor, proceduri de stabilire a conturilor utilizatorilor, a grupurilor de utilizatori și de alocare a identificatorilor utilizatorilor, proceduri de ștergere a conturilor utilizatorilor în cazul plecării personalului de la post sau atunci când a fost detectată o compromitere a contului respectiv;
(b) metode de autentificare, inclusiv protecția informațiilor de autentificare (de exemplu, parole de acces), proceduri de control și schimbare a mecanismelor de autentificare;
(c) mecanisme de control al accesului și proceduri de implementare a controlului accesului utilizatorilor pentru utilizarea serviciilor și resurselor sistemelor informatice;
(d) evidența software-lui, a versiunilor sistemelor de operare și a programelor utilitare, inclusiv cele care vor fi folosite în situații deosebite;
(e) controlul asupra facilităților de copiere sau de modificare a: datelor, sistemului de operare, programelor utilitare și a programelor de aplicație;
(f) măsuri de precauție ce trebuie luate înainte și după procesare sau în timpul pregătirii diferitelor tipuri de activități clasificate, incluzând rutine de ștergere a memoriei principale, reguli de declasificare sau de suprascriere a versiunilor anterioare și proceduri care să asigure că bufferele sunt curățate și că toate datele din fișierele jurnalelor de audit și de evidență a deschiderii sesiunilor de lucru ale utilizatorilor sistemului au fost listate și suprascrise.

B. Securitatea mediilor de stocare a informațiilor

Într-un sistem informatic și de comunicații, volumul și densitatea informațiilor stocate sau procesate, accesibilitatea lor, ușurința și viteza de copiere a informațiilor, uneori și de la stații aflate la distanță, subliniază nevoia luării unor măsuri de securitate a informațiilor – a mediilor de stocare a acestora.

Aceste măsuri vizează următoarele aspecte:

(a) proceduri corespunzătoare pentru clasificarea mediilor de stocare;
(b) responsabilități și proceduri pentru înregistrarea, controlul și evidența mediilor de stocare;
(c) proceduri pentru achiziția, păstrarea, evidența și controlul mediilor de stocare pentru calculatoare;
(d) proceduri pentru primirea, schimbul și diseminarea documentelor electronice, inclusiv proceduri de verificare privind existența virușilor de calculatoare și a software ului nociv, aplicate tuturor mediilor de stocare care provin din afara sistemului informatic;
(e) responsabilități și proceduri pentru declasificarea / distrugerea documentelor electronice și a mediilor de stocare.

Toate mediile de stocare secrete de stat se identifică și se controlează în mod corespunzător nivelului de secretizare. Pentru informațiile neclasificate sau secrete de serviciu se aplică regulamente de securitate interne.

Identificarea evidența și controlul mediilor de stocare trebuie să respecte următoarele cerințe:

- mijloc de identificare – numărul, seria și marcajul nivelului de clasificare - pentru fiecare astfel de mediu, în mod separat;
- proceduri bine definite pentru emiterea, primirea, retragerea, distrugerea sau păstrarea mediilor de stocare;
- să existe evidențe manuale sau tipărite la imprimantă, indicând conținutul și nivelul de secretizare a informațiilor înregistrate pe mediile de stocare.

Pentru nivelul strict secret și strict secret de importanță deosebită, informațiile detaliate asupra mediului de stocare, incluzând conținutul și nivelul de clasificare, se țin într-un registru adecvat.

Când un mediu de stocare urmează să iasă din uz, trebuie să fie declasificat suprimându-se orice marcaje de clasificare, ulterior putând fi utilizat ca mediu de stocare nesecret.
Informațiile clasificate înregistrate pe medii de stocare refolosibile se șterg doar în conformitate cu procedurile operaționale de securitate.

Dacă mediul de stocare nu poate fi declasificat, atunci trebuie distrus printr-o procedură aprobată. Sunt interzise declasificarea și refolosirea mediilor de stocare care conțin informații strict secrete de importanță deosebită, acestea putând fi numai distruse, în conformitate cu procedurile operaționale de securitate.
Informațiile clasificate în format electronic stocate pe un mediu de unică folosință - cartele, benzi perforate - trebuie distruse conform prevederilor procedurilor operaționale de securitate.

C. Securitatea comunicațiilor

Securitatea comunicațiilor – aplicarea măsurilor de securitate în telecomunicații, cu scopul de a proteja mesajele dintr-un sistem de telecomunicații, care ar putea fi interceptate, studiate, analizate și, prin reconstituire, pot conduce la dezvăluiri de informații clasificate.

Securitatea comunicațiilor reprezintă un ansamblu de proceduri, incluzând :

- măsuri de securitate a transmisiilor;
- măsuri de securitate împotriva radiațiilor - TEMPEST;
- măsuri de securitate criptografică.

Securitatea transmisiilor.
Toate mijloacele folosite pentru transmiterea informațiilor clasificate prin emisii radio se
supun instrucțiunilor de securitate a comunicațiilor emise de către instituția desemnată la nivel național pentru protecția informațiilor clasificate.
Mecanismele de securitate a transmisiilor concură la asigurarea disponibilității și confidențialității informațiilor.
Totodată, ca o consecință a îmbunătățirii disponibilității, prin intermediul mecanismelor utilizate pentru a contracara încercările de a bruia sau de a intercepta transmisia propriu- zisă, integritatea datelor este asigurată.

Sunt necesare măsuri pentru contracararea unor amenințări cum ar fi:

- interceptarea neautorizată;
- bruiajul;
- interferențele;
- inducerea în eroare;
- analiza traficului.

Concret pentru un sistem informatic aceste probleme apar la rețelele wireless atunci când schimbul de date între server și celelalte componente ale rețelei se face prin echipamente radio nu prin fire.
Securitatea emisiilor are în vedere ansamblul măsurilor de testare și de realizare a securității împotriva scurgerii de informații, prin intermediul emisiilor electromagnetice parazite - TEMPEST.
Sistemele informatice care stochează, procesează sau transmit informații secrete de stat, vor fi protejate corespunzător față de vulnerabilitățile de securitate cauzate de radiațiile compromițătoare.
Așa că, un observator care poate capta, cu ajutorul unui telescop, de exemplu, lumina difuză, reflectată de pereți, mobilă sau alte asemenea obiecte aflate în apropierea ecranului și poate transforma fluxul luminos în semnal electric, poate obține, după aplicarea unei filtrări corespunzătoare, semnalul video care a produs-o. Specificațiile standardizate de testare a protecției Tempest în cazul emisiei energetice de natură electromagnetică, sunt acelea ale limitei spațiului controlat. Acesta se definește ca distanța față de sursă la care atacatorul poate avea acces și unde raportul semnal/zgomot trebuie să fie de valoare suficient de mică pentru a împiedica separarea radiației compromițătoare de zgomotul de fond și decodificarea acesteia. Instalarea inițială a sistemului informatic și de comunicații sau orice modificare majoră adusă acestuia vor fi executate de persoane autorizate, în condițiile de securitate prezentate în
standarde. Lucrările vor fi permanent supravegheate de personal tehnic calificat, care are acces la informații de cel mai înalt nivel de clasificare pe care respectivul sistem informatic le va stoca, procesa sau transmite.

Securitatea criptografică.
Sistemul ori subsistemul informatic destinat preluării, prelucrării, stocării și transmisiei de date și informații secrete de stat trebuie să fie prevăzut cu sistem de secretizare prin metode, mijloace și echipamente pentru asigurarea integrității, confidențialității și disponibilității acestora.

D. Securitatea fizică

Măsurile de securitate fizică sunt necesare pentru:

- a asigura prevenirea accesului neautorizat la informații clasificate, efectuării de operațiuni neautorizate, blocării resurselor și serviciilor calculatoarelor și
- pentru protejarea echipamentelor de calcul (furturi, distrugeri, etc).

Securitatea fizică a sistemelor de calcul și comunicație – ca o componentă INFOSEC – are în vedere mediul în care acestea funcționează (încăperile în care sunt amplasate, alimentarea cu energie electrică, condițiile de mediu, protecția împotriva incendiilor a inundațiilor, funcționarea în situații de urgență), dar și accesul personalului în zonele în care sunt amplasate.

Orice persoană capabilă să intre într-un loc care conține echipament de calcul poate fi în situația de a interacționa sau de a avaria echipamentul și poate avea acces la informațiile clasificate prelucrate de acesta. Amenințările la adresa securității calculatoarelor pot veni din partea oricărei persoane care are pregătirea profesională și cunoștințe corespunzătoare despre sistemele de calcul și posibilitatea de acces la acestea.

Astfel, în zonele în care sunt amplasate sisteme informatice care procesează informații clasificate, este necesar să se aplice **măsuri generale de securitate**, cum ar fi:

(a) intrarea personalului și a materialelor, precum și plecarea în/din aceste zone să fie controlate prin mijloace bine stabilite;

(b) zonele și locurile în care securitatea sistemelor informatice poate fi afectată, nu trebuie să fie niciodată ocupate de un singur angajat autorizat (regula celor doi);

Persoanelor care solicită acces temporar sau cu intermitențe în aceste zone trebuie să li se autorizeze accesul, ca vizitatori, fiind însoțiți permanent, pentru a avea garanția că nu pot avea acces la informații clasificate și nici la echipamentele utilizate.

Protecția antivirus – ca o componentă a protecției sistemelor informatice, a informației în format electronic, trebuie să conțină proceduri și mecanisme de protecție antivirus atât manuale cât și automate și include următoarele măsuri de securitate:

(a) verificarea sistemelor de operare instalate, a pachetelor software și a programelor utilitare, privind prezența virușilor sau a altui software nociv, cu proceduri pentru ștergerea acestora în cazul detectării lor;

(b) verificarea în permanență a fișierelor-datelor stocate în sistemele de calcul – verificare antivirus în timpul procesării, accesării, la introducerea/extragerea datelor în/din sistemele de calcul sau la intervale de timp bine stabilite;

(c) verificarea conținutului mediilor de stocare (informații și software) primite din surse externe, cu proceduri pentru dezinfectarea lor;

(d) actualizarea în permanență a versiunilor de programe antivirus și utilizarea mai multor produse antivirus (binențeles licențiate) – atât pe server-e cât și pe stațiile de lucru;

(e) raportarea incidentelor cauzate de viruși, atât către expeditorul mediului

Modul în care este prezentată informația în clar, chiar dacă se utilizează codul prescurtat de transmisie sau reprezentarea binară ori alte forme de transmitere la distanță, nu trebuie să influențeze nivelul de clasificare acordat informațiilor respective

Note bibliografice:

[1] 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

[2] Vasile-Adrian Cămărășan, Anca-Gabriela Petrescu, Marius Petrescu, Florentina-Raluca Bîlcan, I*nstrumente și mecanisme privind managementul informațiilor clasificate - de la teorie la practică,* Editura Bibliotheca, 2017, p.122

[3] Marius Petrescu, Anca-Gabriela Petrescu, Florentina-Raluca Bîlcan, Vasile-Adrian Cămărășan, *Managementul securității informațiilor, Note de curs*, Editura Bibliotheca, 2018, p.24.

[4] Legea nr.182 din 12 aprilie 2002 privind protecția informațiilor clasificate, Monitorul oficial, nr. 248 din 12 aprilie 2002

[5] Standardele naționale de protecție a informațiilor clasificate, aprobate prin Hotărârea de Guvern nr.585 din 13 iunie 2002 pentru protecția informațiilor secrete de stat și de serviciu, Monitorul oficial, nr. 485 din 5 iulie 2002

[6] https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:02013D0488-20210701 (accesat: 03.02.2024), în continuare se va cita: Decizia 2013/488/UE

[7] Vasile-Adrian Cămărășan, *op.cit.*, pp.122-123

[8] https://www.isms.online/iso-27001/annex-a-11-physical-and-environmental-security/ (accesat: 29.01.2024)

[9] Alan Calder, Steve Watkins, *IT Governance, a Manager's Guide to data Security and ISO 27001/ISO27001*, 4th edition, Kogan Page ltd, London and Philadelphia, 2008, pp.145-146.

[10] Serviciul Român de Informații, *Protecția informațiilor clasificate - Ghid practic*, pp.38-39; disponibil la: https://www.sri.ro/fisiere/protectia-inf-cls-ghid.pdf

[11] Decizia 2013/488/UE, art.8 și Anexa II

[12] https://www.isms.online/iso-27001/annex-a-11-physical-and-environmental-security/

[13] Alan Calder, Steve Watkins, *op.cit.*, pp.129-131

[14] Serviciul Român de Informații, *op.cit.*, pp.12-15;

[15] https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:02013D0488-20210701 (accesat la 06.02.2024)

[16] https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:02013D0488-20210701 (accesat la: 06.02.2024

[17] Alan Calder, Steve Watkins, *op.cit.*, pp.131-133

[18] Alan Calder, Steve Watkins, *op.cit.*, pp.133-136

[19] Constantin Raicu, *Protecția informațiilor clasificate*, Editura Academiei Naționale de Informații „Mihai Viteazul", 2009, pg.43

[20] ISO/IEC 27002/2022 (E) - Information security, cybersecurity and privacy protection — Information security controls (Securitatea informației, securitatea cibernetică și protecția vieții private. Mijloace de control al securității informației).pdf

[21] https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013D0488 (accesat: 23.02.2024)

[22] Serviciul Român de Informații, *op.cit.*, pp.57-67.

EMSAPHIR - EXPERTIZĂ ÎN PROTECȚIA DATELOR PERSONALE ȘI SECURITATEA INFORMAȚIILOR

DATE DE CONTACT

- telefon: 0755 544 575
- e-mail: contact@emsaphir.ro