



---

# Material informativ despre Standardul ISO / IEC 17799 și implementarea în instituțiile publice

---

Aprilie, 2005

Elaborarea acestui ghid a fost posibilă prin asistența asigurată de către Centrul Regional de Servicii Budapesta al Agenției Statelor Unite pentru Dezvoltare Internațională, USAID, pentru proiectul RITI dot-GOV, în cadrul Acordului de Cooperare Nr. CA #186-A-00-02-00101-00; LA#GDG-A-00-01-00009-00, implementat de către Internews Network Inc.

Materialul a fost realizat de INFO-LOGICA SILVERLINE, firmă specializată în consultanță și auditul sistemelor informaționale, prin participarea autorilor ing. Florin Iliescu, CISA și Adrian Munteanu, PhD, MCP. Autorii pot fi contactați pe adresa de email [office@infologica.ro](mailto:office@infologica.ro).

Opiniile exprimate în cadrul ghidului aparțin autorului și nu reflectă în mod necesar vederile Agenției Statelor Unite pentru Dezvoltare Internațională.

© Internews Network, Inc., 2004. Acest ghid poate fi utilizat și copiat în scopuri necomerciale atâta vreme cât "Internews Network, RITI dot-GOV" este creditat ca sursă și "USAID" este menționată ca finanțator.

## Introducere

---

Societatea îmbrățișează din ce în ce mai mult tehnologia informației. Informația care până nu de mult avea la bază hârtia, îmbracă acum formă electronică. Informația pe suport de hârtie mai este încă rezervată documentelor oficiale, acolo unde este necesară o semnătură sau o ștampilă. Adoptarea semnăturii electronice deschide însă perspectiva digitizării complete a documentelor, cel puțin din punct de vedere funcțional.

Acest nou mod de lucru, în care calculatorul a devenit un instrument indispensabil și un mijloc de comunicare prin tehnologii precum poșta electronică sau Internetul, atrage după sine riscuri specifice. O gestiune corespunzătoare a documentelor în format electronic face necesară implementarea unor măsuri specifice. Măsurile ar trebui să asigure protecția informațiilor împotriva pierderii, distrugerii sau divulgării neautorizate. Cel mai sensibil aspect este acela de a asigura securitatea informației gestionată de sistemele informatice în noul context tehnologic.

Securitatea informației este un concept mai larg care se referă la asigurarea integrității, confidențialității și disponibilității informației. Dinamica tehnologiei informației induce noi riscuri pentru care organizațiile trebuie să implementeze noi măsuri de control. De exemplu, popularizarea unităților de inscripționat CD-uri sau a memoriilor portabile de capacitate mare, induce riscuri de copiere neautorizată sau furt de date.

Lucrul în rețea și conectarea la Internet induc și ele riscuri suplimentare, de acces neautorizat la date sau chiar fraudă.

Dezvoltarea tehnologică a fost acompaniată și de soluții de securitate, producătorii de echipamente și aplicații incluzând metode tehnice de protecție din ce în ce mai performante. Totuși, în timp ce în domeniul tehnologiilor informaționale schimbarea este exponențială, componenta umană rămâne neschimbată. Asigurarea securității informațiilor nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă umană. Majoritatea incidentelor de securitate sunt generate de o gestiune și organizare necorespunzătoare, și mai puțin din cauza unei deficiențe a mecanismelor de securitate.

Este important ca organizațiile să conștientizeze riscurile asociate cu utilizarea tehnologiei și gestionarea informațiilor și să abordeze pozitiv acest subiect printr-o conștientizare în rândul angajaților a importanței securității informațiilor, înțelegerea tipologiei amenințărilor, riscurilor și vulnerabilităților specifice mediilor informatizate și aplicarea practicilor de control.

*Organizația Internațională pentru Standardizare (ISO)* împreună cu *Comisia Internațională Electrotehnică (IEC)* alcătuiesc un forum specializat pentru standardizare. Organismele naționale care sunt membre ale ISO și IEC participă la dezvoltarea standardelor internaționale prin intermediul comitetelor tehnice. Statele Unite ale Americii, prin Institutul Național de Standardizare, ocupă poziția de Secretar, 24 de țări au statut de Participanți (Brazilia, Franța, Regatul Unit al Marii Britanii, Coreea, Cehia, Germania,

Danemarca, Belgia, Portugalia, Japonia, Olanda, Irlanda, Norvegia, Africa de Sud, Australia, Canada, Finlanda, Suedia, Slovenia, Elveția, Noua Zeelandă și Italia) și alte 40 de țări au statut de Observatori.

Prin activitatea susținută de Ministerul Comunicațiilor și Tehnologiei Informației (MCTI) de adoptare la nivel național a standardelor europene și internaționale recunoscute, standardul ISO/IEC 17799 - "Tehnologia Informației – Cod de bună practică pentru managementul securității informației" a fost adoptat și în România de către Asociația de Standardizare din România (ASRO), din toamna anului 2004. Standardul este recunoscut în rezoluțiile Consiliului Europei, implementarea acestuia la nivelul organizațiilor fiind opțională. Singurul loc de unde se poate achiziționa legal versiunea în limba română a standardului este ASRO ([www.asro.ro](http://www.asro.ro)).

## **Ce reprezintă securitatea Informațiilor?**

---

Ca și acțiunile prin care o organizație își apară angajații și bunurile, securitatea informațiilor este folosită în primul rând pentru a oferi asigurări că drepturile care derivă din proprietatea intelectuală sunt protejate în mod corespunzător.

Obiectivul principal al unui program pentru protecția informațiilor îl reprezintă asigurarea încrederii partenerilor de afaceri, avantajul competitiv, conformitatea cu cerințele legale și maximizarea investițiilor.

Indiferent de forma pe care o îmbracă, mijloacele prin care este memorată, transmisă sau distribuită, informația trebuie protejată.

ISO/IEC 17799 tratează securitatea informațiilor prin prisma a trei elemente principale:

- Confidențialitatea – informațiile sunt accesibile doar persoanelor autorizate
- Integritatea – asigurarea acurateții și completitudinii metodelor prin care se realizează prelucrarea informațiilor
- Disponibilitatea – utilizatorii autorizați au acces la informații și la activele asociate în momente oportune.

Pentru a putea realiza un program de securitate eficient este nevoie de politici, proceduri, practici, standarde, descrieri ale sarcinilor și responsabilităților de serviciu, precum și de o arhitectură generală a securității.

Aceste controale trebuie implementate pentru a se atinge obiectivele specifice ale securității și pe cele generale ale organizației.

## **De ce este nevoie de securitate?**

---

Dependența din ce în ce mai mare de sistemele informaționale conduce la creșterea tipologiei vulnerabilităților cărora organizațiile trebuie să le facă față. Mai mult, problema protecție trebuie să aibă în vedere de multe ori interconectarea rețelelor private cu serviciile publice. Dacă la acest aspect

mai adăugăm și problema partajării informațiilor se conturează un tablou destul de complicat în care implementarea unor controale eficiente devine o sarcină dificilă pentru specialistul IT&C.

Multe din sistemele existente pe piață au fost proiectate după metodologia structurată dar nu au avut ca principal obiectiv și asigurarea unui anumit grad de securitate pentru că la momentul respectiv tehnologia nu era atât de dezvoltată și nici atât de accesibilă neinițiaților. Odată însă cu proliferarea Internetului ca și mijloc important al comunicării moderne nevoia unor mecanisme de securitate proactivă a devenit o certitudine. În practică remarcăm că multe instituții apelează la soluții tehnice externe care să le rezolve problemele de securitate fără a căuta să-și identifice nevoile și cerințele specifice.

Identificarea controalelor interne care să asigure un grad corespunzător de securitate activelor informaționale ale unei instituții presupune o planificare riguroasă și identificarea exactă a obiectivelor respectivei instituții. Pentru a fi însă eficiente aceste controale trebuie să aibă în vedere pe toți angajații și nu doar pe cei din compartimentul IT sau care au legătură directă cu acest domeniu.

Securitatea informațiilor nu este doar o problemă tehnică. Ea este în primul rând o problemă managerială.

Standardul de securitate ISO/IEC 17799 răspunde nevoilor organizațiilor de orice tip, publice sau private, printr-o serie de practici de gestiune a securității informațiilor. Standardul poate fi folosit în funcție de gradul de expunere a fiecărei organizații în parte, pentru a conștientiza la nivelul conducerii aspectele legate de securitatea informației, sau pentru a crea o cultura organizațională în ceea ce privește securitatea informațiilor, sau pentru a obține certificarea sistemului de securitate.

Gradul de expunere a sistemelor informaționale variază cu industria în care activează fiecare organizație. Cu cât acest risc este mai mare, atenția care trebuie acordată securității datelor ar trebui să fie mai mare.

Instituțiile financiare, industria apărării, aerospațială, industria tehnologiei informației, industria electronica sunt sectoarele cu cel mai mare grad de risc în ceea ce privește securitatea informațiilor. Tot în această categorie de risc ridicat intră și instituțiile guvernamentale, motiv pentru care adoptarea unei culturi organizaționale pe baza standardului ISO/IEC 17799 are un rol fundamental.

## **Stabilirea cerințelor**

---

Este important ca fiecare organizație să poată să-și identifice propriile cerințe de securitate. Pentru aceasta ea trebuie să facă apel la trei surse principale:

- Analiza riscurilor
- Legislația existentă
- Standardele și procedurile interne

Folosind o metodologie corespunzătoare pentru a analiza riscurile organizația își poate identifica propriile cerințe legate de securitate. Un astfel de proces presupune în general patru etape principale:

- Identificare activelor care trebuie protejate
- Identificarea riscurilor/amenințărilor specifice fiecărui activ
- Ierarhizarea riscurilor
- Identificarea controalelor prin care vor fi eliminate/diminuate riscurile

Nu trebuie însă trecute cu vederea nici aspectele financiare.

Fiind un obiectiv comun, dictat de cerințele de afacere, pentru că până la urmă orice activitate derulată de o organizație are o rațiune economică, în implementarea unei arhitecturi de securitate trebuie puse în balanță costurile și beneficiile.

Un mecanism de control nu trebuie să coste organizația mai mult decât bunul ce trebuie protejat.

Stabilirea cerințelor de securitate, a măsurilor necesare pentru a asigura nivelul de control dorit, are o componentă deseori subiectivă, fiind dificil de cuantificat în termeni monetari pierderea suferită în cazul unui incident de securitate. Aspectele intangibile precum alterarea imaginii organizației pe piață, credibilitatea în fața clienților sau efectele indirecte ale unui incident de securitate major, sunt cel mai greu de apreciat. Aceasta este rațiunea și pentru care adoptarea unor standarde și practici general acceptate, susținute de evaluări periodice independente este de recomandat.

Acest proces nu este unul static, altfel spus trebuie avute în permanență în vedere schimbările care intervin în viața organizației pentru a fi reflectate corespunzător în planul de securitate. Dacă spre exemplu apare o modificare legislativă cu impact asupra instituției, trebuie avut în vedere din nou modelul folosit pentru evaluarea riscurilor pentru a vedea dacă acesta reflectă riscurile apărute ca urmare a acestei modificări.

În acest sens, ISO/IEC 17799 propune o serie de obiective de securitate și controale din rândul cărora profesioniștii le pot selecta pe acelea care corespund afacerii în care funcționează. Pe de altă parte acest standard nu trebuie considerat un panaceu al securității informațiilor atât timp cât el oferă doar recomandări celor care răspund de implementarea și managementul unui sistem de securitate în cadrul unei organizații.

## **De unde se începe**

---

Controalele interne pot fi considerate principiile care stau la baza implementării unui sistem de management al securității. Chiar dacă sursele unor astfel de măsuri pot fi destul de variate, punctul de plecare într-un astfel de demers îl reprezintă legislația aplicabilă. Este foarte important ca cel care se ocupă de implementarea unui sistem de management al securității să aibă cunoștințe despre actualele cerințe legislative:

- Legea nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției.

- Legea nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.
- Legea nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
- Legea nr. 455 din 18 iulie 2001 privind semnătura electronică.
- Legea nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
- Hotărârea nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
- Ordinul Avocatului Poporului nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
- Ordinul Avocatului Poporului nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
- Ordinul Avocatului Poporului nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.
- Hotărârea nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
- Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

Pe lângă legislația internă trebuie avute în vedere și *Convențiile internaționale și Reglementările comunitare* semnate de România sau în care România este parte.

Selectarea controalelor trebuie să țină cont de specificul organizației. Nu toate recomandările pot fi aplicate, cum nu toate sunt justificate din punct de vedere al costurilor. Eficacitatea sistemului de securitate depinde de:

- Stabilirea unor obiective de securitate care să reflecte cerințele organizației;
- Sprijinului conducerii;
- Existența abilităților necesare realizării analizei riscurilor, a vulnerabilităților și a analizei de impact;
- Instruirea angajaților;
- Monitorizată controalelor implementate.

## **ISO/IEC 17799 – Cele mai bune practici în managementul securității informațiilor**

---

ISO/IEC 17799 a fost dezvoltat ca punct de plecare în dezvoltarea unui sistem de management al securității specific fiecărei instituții în parte. De aici rezultă caracterul său general, controalele prezentate în standard putând fi luate ca exemple pentru situații specifice fiecărei instituții în parte.

Primele două secțiuni ale standardului prezintă *Scopul* respectiv *Termeni și Definiții*. Scopul standardului ISO/IEC 17799 stabilește rolul acestui document ca fiind un ghid pentru domeniul securității informaționale.

Prin prezentarea Termenilor și Definițiilor din secțiunea a doua, standardul asigură un limbaj comun pentru profesioniștii domeniului. Următoarele secțiuni prezintă obiectivele de control și măsurile prin care se pot atinge aceste obiective.

În continuare sunt prezentate pe scurt secțiunile standardului de securitate ISO / IEC 17799.

### **Politica de securitate**

---

Obiectivul politicii de securitate este să ofere managementului instituției sprijinul necesar asigurării securității informațiilor din cadrul organizației.

Conducerea oricărei instituții trebuie să ofere suportul necesar prin elaborarea unui document intitulat Politică de Securitate, document care trebuie adus la cunoștința tuturor angajaților.

Fără un astfel de document există riscul ca rolurile și responsabilitățile relative la asigurarea securității informaționale să fie greșit înțelese. Nedezvoltarea unui astfel de document și neaducerea la cunoștința angajaților a politicii de securitate a companiei induce de cele mai multe ori o stare de superficialitate în tratarea acestor aspecte. Existența unei viziuni clare a conducerii și o comunicare efectivă a acesteia către angajați este fundamentală pentru asigurarea eficienței oricăror proceduri și măsuri de securitate specifice.

### **Organizarea securității**

---

Organizarea securității are ca obiectiv asigurarea unei administrări unitare în cadrul organizației.

Fiecare utilizator al sistemului informațional este responsabil cu asigurarea securității datelor pe care le manipulează. Existența unei structuri organizatorice unitare care să inițieze și să controleze implementarea mecanismelor de securitate în cadrul organizației, presupune un punct central de coordonare – responsabil cu securitatea.

Rolul și atribuțiile persoanei care ocupă poziția de responsabil cu securitatea informațiilor se referă la coordonarea și urmărirea respectării procedurilor și politicilor de securitate.

Organizarea securității nu se limitează doar la personalul intern, trebuie avute în vedere și riscurile induse de terți sau subcontractori care au acces la sistemul informațional. Acest risc nu este deloc de neglijat, ultimile tendințe ale pieței globale ne arată o reconsiderare a poziției companiilor față de externalizarea funcțiilor IT, tocmai datorită riscului mare indus de subcontractarea acestora.

Obiectivul organizării securității, așa cum este documentat în standard este și menținerea securității tuturor facilităților IT și activelor informaționale accesate de către terțe persoane, fiind recomandată stabilirea unui proces prin care accesul terților să fie controlat.

## **Clasificarea și controlul activelor**

---

Măsurile de protecție sunt proiectate în funcție de gradul de sensibilitate, și de semnificația economică a resurselor vizate. Perimetrele în care sunt amplasate echipamentele de procesare, vor fi protejate cu bariere de acces suplimentare. La fel și telecomunicațiile cu un nivel ridicat de confidențialitate ar trebui criptate. Pentru a avea totuși o abordare coerentă asupra măsurilor specifice de protecție, în funcție de gradul de sensibilitate al fiecărei resurse în parte se practică o clasificare a informațiilor.

Clasificarea informațiilor este necesară atât pentru a permite alocarea resurselor necesare protejării acestora, cât și pentru a determina pierderile potențiale care pot să apară ca urmare a modificărilor, pierderii/distrugerii sau divulgării acestora.

Obiectivul clasificării este crearea premizelor necesare asigurării unei protecții corespunzătoare valorii activelor instituției. Toate activele organizației trebuie să aibă asociat un proprietar. Politica de securitate trebuie să identifice angajații cu rol de proprietar, custode, client, utilizator.

## **Securitatea personalului**

---

Cele mai multe incidente de securitate sunt generate de personal din interiorul organizației, prin acțiuni rău intenționate sau chiar erori sau neglijență în utilizarea resurselor informaționale.

Standardul ISO/IEC 17799 tratează riscurile de natură umană ce pot fi induse din interiorul organizației prin măsuri specifice precum includerea responsabilităților legate de securitatea informațiilor în descrierea și sarcinile de serviciu ale postului, implementarea unor politici de verificare a angajaților, încheierea unor acorduri de confidențialitate și prin clauze specifice în contractele de muncă.

Securitatea informațiilor este un aspect ce trebuie avut în vedere încă din etapa de selecție a angajaților. Angajații trebuie monitorizați pe întreaga perioadă de valabilitate a contractului de muncă și trebuie să aibă cunoștință de prevederile politicilor de securitate. Clauzele de confidențialitate, definirea conflictelor de interese, distribuirea și divulgarea informațiilor trebuie avute în vedere pentru fiecare post în parte.

Pentru a evita neglijența sau greșelile de operare, utilizatorii ar trebui informați cu privire la amenințările la care sunt supuse informațiile manipulate. Instruirea ar trebui să ofere cunoștințele necesare asigurării securității acestora în timpul programului normal de lucru.

Utilizatorii trebuie instruiți cu privire la procedurile de securitate ce trebuie urmate și utilizarea facilităților IT în conformitate cu politica organizației.

Ar trebui să existe un program coerent de instruire a angajaților pe diverse niveluri de interes, pe lângă o instruire generală în gestiunea securității fiind necesare și specializări pentru administratorii sistemului informatic în tehnologii de securitate specifice.

Chiar dacă securitatea unei anumite zone IT, cum ar fi securitatea rețelei revine unei entități externe, este o practică bună ca și în interiorul organizației să existe competențele și abilitatea de a evalua cum sunt satisfăcute cerințele de securitate.

Instruirea este necesară și pentru a crea abilitatea de reacție la apariția unor incidente de securitate.

Raportarea incidentelor de securitate are ca obiectiv minimizarea efectelor negative sau a incorectei funcționări a echipamentelor. Monitorizarea unor astfel de incidente permite determinarea performanței sistemelor de securitate și îmbunătățirea continuă.

Politicile și procedurile de securitate trebuie implementate astfel încât să asigure un răspuns consistent la astfel de incidente.

## **Securitatea fizică**

---

Delimitarea zonelor securizate are ca obiectiv prevenirea accesului neautorizat sau afectarea facilităților oferite de sistemul informațional.

Această secțiune vizează mecanismele prin care se asigură securitatea fizică a imobilului în care organizația își desfășoară activitatea.

Alt aspect important al securității fizice este cel legat de protecția echipamentelor, prin prevenirea pierderii, distrugerii sau compromiterii funcționării echipamentelor care pot afecta funcționarea organizației.

Echipamentele de calcul trebuie să fie protejate fizic împotriva amenințărilor voite sau accidentale. În acest sens trebuie dezvoltate standarde și proceduri pentru securizarea atât a serverelor, cât și a stațiilor de lucru ale utilizatorilor.

Măsurile de control al accesului, implementate la nivelul aplicației, bazelor de date sau rețelei pot deveni inutile dacă există și o protecție fizică corespunzătoare.

## **Managementul comunicațiilor și al operării**

---

Operarea calculatoarelor trebuie să asigure funcționarea fără riscuri și în bune condiții a resurselor organizației. Această funcție vizează atât echipamentele și aplicațiile software, cât și celelalte elemente necesare procesării informației și susținerii funcțiilor de afaceri.

Practicile de control recomandate pentru asigurarea operării de o manieră corectă și sigură, constau în documentarea procedurilor de operare, controlul modificărilor aduse sistemului informatic, atât la nivel hardware cât și software, formalizarea tratării incidentelor de securitate și separarea responsabilităților.

Dinamica mediului informațional dată de schimbările tehnologice continue cât și de apariția de noi cerințe din partea afacerii supune sistemul informatic la noi dezvoltări. Dezvoltarea și testarea modificărilor aduse sistemului existent pot cauza probleme serioase operării curente. Pentru a controla aceste riscuri sunt recomandate separări clare ale responsabilităților între dezvoltare, testare și exploatare susținute și de o separare a mediilor folosite pentru aceste activități.

Accesul programatorilor pe mediul de producție nu ar trebui permis, iar dacă anumite situații excepționale o cer, atunci ar trebui controlat îndeaproape.

Planificarea capacității sistemului este un alt obiectiv al operării calculatoarelor care are ca obiectiv minimizarea riscurilor întreruperii sistemului ca urmare a atingerii capacității maxime de procesare.

Asigurarea unei capacități corespunzătoare de procesare implică o planificare riguroasă a activităților sprijinite de sistemul informațional.

Trebuie dezvoltate proceduri și mecanisme de raportare care să identifice utilizarea necorespunzătoare a resurselor precum și perioadele de utilizare.

Protecția împotriva software-ului malițios este un aspect important întrucât cea mai mare amenințare a activelor informatice este dată de pierderea sau indisponibilitatea datelor ca urmare a infestării cu viruși informatici. În toate sondajele, virușii se află printre primele locuri ca sursă a incidentelor de securitate. Milioane de viruși informatici sunt raportați anual. Protecția împotriva virușilor nu o asigură doar administratorul sistemului, ci și utilizatorul.

Asigurarea integrității datelor și a aplicațiilor software necesită măsuri de protecție prin care să se prevină și să se detecteze introducerea unor aplicații ilegale în sistemul organizației.

Aplicațiile tip antivirus trebuie instalate pe toate calculatoarele din sistem iar utilizatorii trebuie instruiți cu privire la folosirea acestora.

Alte aspecte ce fac obiectul managementului operării și comunicațiilor vizează:

- Întreținerea sistemului, incluzând realizarea copiilor de siguranță, întreținerea jurnalelor de operare, menținerea înregistrărilor cu erori de operare și execuție.
- Managementul rețelei, necesar asigurării rețelelor de calculatoare.
- Manipularea și securitatea mediilor de stocare, pentru a preveni întreruperea activităților afacerii.
- Schimbul de aplicații și date între organizații, pentru a preveni pierderea, alterarea sau utilizarea improprie a informației.

Întreținerea sistemului are ca obiectiv menținerea disponibilității și integrității serviciilor IT.

Trebuie dezvoltate proceduri specifice care să descrie acțiunile prin care se realizează întreținerea serviciilor și echipamentelor IT. Întreținerea sistemului trebuie să fie un proces continuu care să includă obligatoriu instalarea corecțiilor de securitate a aplicațiilor, sistemelor de operare și sistemelor de gestiune a bazelor de date, realizarea copiilor de siguranță, jurnalizarea activităților realizate în și de către sistem.

Managementul rețelei are ca obiectiv asigurarea protecției datelor transmise prin rețea și a infrastructurii fizice a rețelei.

Pentru protecția rețelei sunt disponibile tehnologii specializate ce pot fi folosite în implementarea măsurilor de securitate și atingerea obiectivelor de control:

- Filtru – set de reguli implementate la nivelul unui router sau firewall prin care acesta permite tranzitarea sau nu a traficului către și dinspre rețeaua unei companii;
- Firewall – dispozitiv prin care este controlat traficul dintre rețeaua companiei și rețelele externe acesteia;
- Sistem pentru Detectarea Intruziunilor (IDS – Intrusion Detection System), dispozitiv (hardware sau software) dedicat inspectării traficului unei rețele cu scopul identificării automate a activităților ilicite;
- Criptare comunicații – procesul prin care datele sunt aduse într-o formă neinteligibilă persoanelor neautorizate;
- Rețea Virtuală Privată (VPN – Virtual Private Network) - o rețea care permite comunicarea între două dispozitive prin intermediul unei infrastructuri publice (nesigure)
- Zona demilitarizată (DMZ) este o parte a rețelei care permite accesul controlat din rețeaua Internet. Mașinile dependente de accesul direct la rețeaua Internet, cum ar fi serverele de email și cele de web sunt adesea plasate în astfel de zone, izolate de rețeaua internă a organizației.

Măsurile tehnice singure nu pot asigura nivelul de protecție necesar, fără un management corespunzător. Standardul ISO/IEC 17799 prezintă controalele necesare gestiunii corespunzătoare a securității comunicațiilor.

Prevenirea distrugerii mediilor de stocare al cărei efect s-ar concretiza în întreruperea serviciilor sistemului informatic s-ar putea asigura prin controlarea și protejarea mediilor de stocare. Trebuie dezvoltate proceduri prin care este controlat accesul la orice mediu de stocare și la documentația sistemului.

## **Controlul accesului**

---

Confidențialitatea vizează protejarea informațiilor împotriva oricărui acces neautorizat. Uneori este interpretat în mod greșit că această cerință este specifică domeniului militar și serviciilor de informații care trebuie să-și

protejeze planurile de luptă, amplasamentul depozitelor de muniție sau al rachetelor strategice, notele informative. Este însă la fel de importantă pentru o organizație care dorește să-și apere proprietatea intelectuală, rețetele de producție, datele despre personalul angajat, etc. Pentru o instituție publică, datorită caracterului informației pe care o gestionează este important să asigure în primul rând integritatea și disponibilitatea datelor.

Controlul accesului începe cu stabilirea cerințelor de acordare a drepturilor de utilizare a informațiilor.

Accesul la facilitățile și serviciile oferite de sistemul informațional trebuie controlat în funcție de specificul și cerințele mediului în care își desfășoară activitatea organizația.

Pentru a răspunde acestor cerințe sunt în general definite o serie de reguli de acces corelate cu atribuțiile fiecărui utilizator al sistemului informatic. Menținerea acestor reguli în linie cu cerințele organizației implică un proces de gestiune a accesului utilizatorilor sistemului. Obiectivul acestui proces este să prevină utilizarea neautorizată a calculatoarelor.

Trebuie să existe proceduri formale prin care să se controleze alocarea drepturilor de acces la serviciile și resursele IT.

Utilizatorii autorizați trebuie instruiți cu privire la maniera în care trebuie raportate activitățile sau acțiunile considerate suspecte.

Fiecare componentă a sistemului informațional trebuie să facă obiectul măsurilor de control al accesului, datele trebuie protejate indiferent de forma sau starea care le caracterizează, fie că este vorba de aplicații software, sisteme de operare, baze de date sau rețele de comunicații. Tehnologiile mai vechi de gestiune a bazelor de date precum Fox Pro, de exemplu, nu pot asigura o protecție a informațiilor la nivelul bazei de date, acestea fiind stocate în fișiere necriptate, accesibile oricărui utilizator, indiferent de drepturile de acces care i-au fost atribuite la nivelul aplicației. Sistemele de operare precum DOS sau Windows 95/98 nu au mecanisme de control al accesului, nefiind posibilă restricționarea drepturilor de utilizare a datelor la acest nivel. Standardul prevede însă măsuri de control pentru fiecare nivel al sistemului informațional:

- Controlul accesului la serviciile rețelei - conexiunile la serviciile rețelei trebuie controlate iar pentru obținerea accesului la astfel de servicii este recomandată implementarea unei proceduri formale.
- Controlul accesului la nivelul sistemului de operare – sistemul de operare trebuie să prevadă măsuri de restricționare a accesului la date existente pe calculatoare.
- Controlul accesului la aplicații - prevenirea accesului neautorizat la informațiile gestionate de aplicațiile software.

Oricât de elaborate ar fi măsurile de control al accesului există totdeauna posibilitatea unei intruziuni, sau utilizarea inadecvată a resurselor existente. Pentru a detecta potențialele activități neautorizate este necesară monitorizarea accesului și utilizării sistemului informatic.

Monitorizarea are un caracter continuu și implică păstrarea și revizuirea periodică a înregistrărilor cu evenimentele de sistem, și a activității utilizatorilor.

## **Dezvoltarea și întreținerea sistemului**

---

Aproape mereu, atunci când e vorba de dezvoltarea și implementarea unui sistem informatic, cerințele de securitate sunt neglijate. Eforturile sunt îndreptate mai mult spre aspectele funcționale și mai puțin pe controlul riscurilor de integritate și confidențialitate a informațiilor. Organizațiile se expun la riscuri majore de operare ce pot rezulta în pierderi financiare semnificative prin neglijarea unor măsuri minimale de control al procesului de dezvoltare și implementare. Testarea aplicațiilor nu este formalizată, ceea ce nu garantează calitatea dezvoltărilor, programatorilor li se permite accesul la mediul de producție pentru corectarea unor erori nedetectate în procesul de testare, inducând riscuri de integritate și disponibilitate a datelor.

Aspectele de securitate nu trebuie neglijate în partea de dezvoltare și implementare, deși acestea s-ar putea să deranjeze și să nu aducă aparent nici un beneficiu. Fără a ține cont de recomandările de control ale acestui proces, organizația riscă să investească într-o aplicație sau echipament care să nu-i ofere nici o garanție asupra informațiilor gestionate.

Obiectivele de control prevăzute în această secțiune a standardului sunt menite să asigure că noile sisteme dezvoltate au prevăzute mecanisme de securitate, prin:

- Dezvoltarea cerințelor și analiza specificațiilor de securitate;
- Validarea datelor de intrare
- Controlul procesării interne
- Autentificarea mesajelor transmise electronic
- Validarea datelor de ieșire
- Utilizarea tehnicilor de criptare
- Utilizarea mecanismelor de semnare electronică
- Protejarea codului aplicațiilor și a fișierelor sistemului de operare

De asemenea, este necesară și asigurarea securității mediilor de dezvoltare și a serviciilor suport. Mediile în care se dezvoltă aplicații sau proiecte noi trebuie strict controlate. Mediul de testare trebuie separat de mediul de producție, datelor de test asigurându-li-se protecția corespunzătoare.

## **Planificarea continuității afacerii**

---

Un plan de continuitate a afacerii reprezintă o serie de măsuri de reacție în caz de urgență, de operare alternativă și de restaurare a situației în caz de dezastru pentru a asigura disponibilitatea resurselor critice și pentru a permite continuarea activității în cazul unor incidente majore. Majoritatea companiilor nu au un astfel de plan de continuitate, de cele mai multe ori

aceste aspecte sunt neglijate sau sunt limitate la achiziționarea unor echipamente de rezervă sau tolerante la defecte.

Scopul unui plan de continuitate este de a asista organizațiile în a continua să funcționeze atunci când activitatea normală este întreruptă. Este mult mai bine ca acest lucru să fie planificat în avans, printr-o atitudine proactivă.

Planurile pentru continuitatea afacerii trebuie să asigure disponibilitatea proceselor considerate critice pentru funcționarea organizației în cazul apariției unor dezastre sau întreruperi de funcționare.

Asigurarea continuității afacerii presupune parcurgerea etapelor de documentare, testare și implementare a planului de continuitate a afacerii. Implementarea presupune instruirea personalului și dezvoltarea unor procese speciale de gestiune a situației de criză, precum și de actualizare periodică.

## **Conformitatea**

---

Proiectarea, operarea sau gestiunea sistemelor informaționale pot face obiectul unor reglementări, legi sau angajamente contractuale în ceea ce privește securitatea.

Pentru a evita încălcarea dispozițiilor statutare sau legale, standardul prevede o serie de măsuri precum:

- Identificarea legislației aplicabile
- Utilizarea adecvată a licențelor software sau a materialelor protejate de drepturi de autor
- Protejarea înregistrărilor organizației (înregistrări contabile, chei de criptare, jurnale de activitate, medii de stocare, proceduri de lucru)

Pentru a asigura conformitatea cu politicile și standardele de securitate ale organizației, securitatea sistemului informațional trebuie revizuită periodic pentru a reflecta schimbările tehnologice sau organizatorice.

## **Concluzii**

---

Odată cu adoptarea de noi tehnologii, complexitatea protejării informațiilor continuă să crească. Managementul sistemelor informaționale nu se poate realiza decât prin implementarea unui cadru procedural bazat pe standarde de securitate recunoscute precum ISO/IEC 17799 sau CobiT (Obiective de Control pentru Tehnologia Informației) și prin adoptarea cu succes a tehnologiilor de securitate specifice.

ISO/IEC 17799 nu este un standard tehnic, orientat pe un anumit produs sau tehnologie. Ca și metodologie de evaluare a securității unui sistem informațional se pot utiliza alte standarde cum ar fi ISO/IEC 15408 părțile 1,2, și 3 sau ISO 13569 pentru sectorul instituțiilor financiare.

În timp ce ISO/IEC 17799 este un ghid care sprijină implementarea mecanismelor de securitate, oferind sugestii și recomandări sub forma unei colecții a celor mai bune practici ale domeniului, alte standarde precum BS

7799 Partea a doua reprezintă un ghid pentru auditul securității pe baza unor cerințe concrete.

Implementarea unei abordări sistematice de gestiune a securității informaționale presupune implicarea conducerii organizației, selectarea și instruirea echipelor de implementare. Următorul pas foarte important este definirea scopului proiectului prin realizarea unei analize de risc și evaluarea vulnerabilităților și impactului pe care le pot avea riscurile specifice asupra organizației. Pe baza acestor evaluări se pot defini specificațiile unui sistem de management al securității, incluzând politici, proceduri, scheme de organizare, dar și tehnologii specifice de securitate.