06.08.2010

Recomandări cu privire la obiectivele de control şi măsurile de securitate ale Sistemului de Management al Securității Informației

APROBAT
Guvernatorul
Băncii Naționale a Moldovei
Dorin DRĂGUȚANU
6 august 2010

RECOMANDĂRI
cu privire la obiectivele de control şi măsurile de securitate ale Sistemului de Management al Securității Informației

Modificată prin:

Hotărârea Guvernatorului BNM din 01.07.2015

I. Prevederi generale

1.1. Recomandările cu privire la obiectivele de control şi măsurile de securitate ale Sistemului de Management al Securității Informației (în continuare Recomandări), reprezintă îndrumări ale Băncii Naționale a Moldovei emise în scopul facilitării şi acordării suportului metodologic băncilor la implementarea prevederilor Secțiunii 3 din Regulamentul cu privire la sistemele de control intern în bănci, aprobat prin Hotărârea Consiliului de administrație al Băncii Naționale a Moldovei nr. 96 din 30.04.2010 (publicat MO nr. 98-99 din 15.06.2010) dar şi instituțiilor nebancare (prestatori de servicii de plată și emitenți de monedă electronică) la implementarea prevederilor Capitolului IV din Regulamentul cu privire la activitatea emitenților de monedă electronică şi prestatorilor de servicii de plată nebancari, aprobat prin HCA al BNM nr.123 din 27.06. 2013 (publicat MO nr. 173-176 din 09.08.2013, art. 1221).

1.2. Prezentele recomandări au fost elaborate luând în considerare următoarelor standarde, ghiduri şi coduri de practică în domeniu:
a. SM GOST R ISO/IEC 27001:2008 (ISO/IEC 27001:2005) - Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe;
b. SMV ISO/CEI 27002:2009 (ISO/IEC 27002:2005) - Tehnologia informației. Tehnici de securitate. Cod de buna practică pentru managementul securității informației;
c. SMV ISO/CEI 27005:2009 (ISO/IEC 27005:2008) - Tehnologia informației. Tehnici de securitate. Managementul riscului securității informației;
d. Standardul Control Objectives for Information and related Technology, emis de Information Systems Audit and Control Association (www.isaca.org [1]).
e. Payment Card Industry Data Security Standard, emis de Payment Card Industry Data Security Council (https://www.pcisecuritystandards.org [2]).

1.3. În scopul stabilirii, implementării, operării, monitorizării, revizuirii, menținerii şi îmbunătățirii propriilor Sisteme de Management al Securității Informației (în continuare - SMSI), entitățile pot aplica prezentele Recomandări, precum şi alte surse metodologice din domeniul securității informației.

II. Termeni şi definiții

În sensul prezentului document, se aplică următoarele noțiuni:
Securitatea informației – păstrarea confidențialității, integrității şi disponibilității informației în orice formă a sa (electronică, pe suport hârtie, etc.) şi protejarea resurselor implicate la gestiunea acesteia, în plus, alte proprietăți precum autenticitatea, responsabilitatea, non-repudierea şi fiabilitatea pot fi de asemenea implicate.
Confidențialitate – proprietatea informației de a fi disponibilă doar persoanelor, sau proceselor autorizate să aibă acces la ea.

Integritate – proprietatea informației de a fi completă.
Disponibilitate – proprietatea informației de a fi disponibilă la cererea unei persoane autorizate.
Risc de securitate a informației – probabilitatea ca un anumit eveniment se va realiza şi va avea impact advers asupra confidențialității, integrității sau disponibilității resurselor informaționale;
Măsură de securitate – mijloc de reducere a riscului de securitate, inclusiv politici, standarde, proceduri, structuri organizatorice, soluții TI etc.;
Evaluarea riscului – proces de măsurare a riscului în conformitate cu criteriile stabilite.
Gestiunea riscului – proces coordonat de identificare, analiză, evaluare, tratare, monitorizare şi revizuire a riscurilor de securitate.
Entitate – banca sau instituție nebancară (prestatori de servicii de plată și emitenți de monedă electronică).
Sistem informațional (SI) – totalitatea sistemelor de gestiune a informației din cadrul unei entități, împreună cu resursele organizaționale asociate, cum ar fi resursele informaționale, resursele umane, structurile organizatorice.
Sistem informatic (sisteme TI – totalitatea mijloacelor software şi hardware, destinate pentru procesarea, colectarea, stocarea datelor şi a informației aferente unui sau mai multor procese de activitate ale entității.
Sistem de Management al Securității Informației – parte componentă a sistemului de control intern, bazat pe abordarea riscurilor de securitate a informației, constituit dintr-un complex de măsuri tehnico-organizatorice, (de ex. acte normative, proceduri interne, resurse umane, procese TI, resurse şi servicii TI etc.) şi orientat spre atingerea obiectivelor de asigurare a securității informației în cadrul entității;
Serviciu TI – serviciu furnizat unei entități (ex. aplicație, proces, utilizator etc.), bazat pe utilizarea Tehnologiilor Informaționale.
Echipamentul TI – tehnică de calcul, de comunicație, alte mijloacele tehnice ale SI al entității.
Resurse – orice prezintă valoare pentru entitate, inclusiv informația;
Resurse informaționale – orice informație utilizată în cadrul proceselor de activitate a entității, sau orice bun material sau nematerial implicat direct sau indirect în crearea, procesarea, stocarea şi accesarea informației în cadrul proceselor de activitate (de exemplu: date, aplicații program, soft de sistem, echipamente de calcul, alte elemente de infrastructură);
Resursă informațională sensibilă – resursa informațională, compromiterea securității căreia poate implica riscuri majore pentru entitate.
Infrastructura TI – totalitatea mijloacelor software şi hardware inclusiv serviciile TI, destinate asigurării funcționării sistemului informațional.
Rețea internă a entității – totalitatea echipamentelor şi canalelor tehnice de comunicare între componentele infrastructurii TI în cadrul entității.
Zona Demilitarizată – o parte a rețelei (fizic şi/sau logic delimitată) în cadrul căreia sunt amplasate acele servicii ale entității ce accesează sau pot fi accesate din afara rețelei interne a entității (de obicei din cadrul unui extranet sau din cadrul rețelei Internet) şi are rolul de a separa resursele accesibile din exteriorul rețelei de celelalte resurse interne, în scopul prevenirii accesului nesancționat la resursele TI din rețelele publice.
Gestiunea resurselor informaționale – totalitatea acțiunilor direcționate la atingerea scopurilor predefinite, inclusiv aferent asigurării securității acestor resurse.
Eveniment de securitate – situație identificată în legătură cu un sistem, un serviciu sau o rețea, care implică o posibilă încălcare a politicii de securitate a informației, un eşec al măsurilor de securitate, sau informație ignorată anterior, dar relevantă din punct de vedere al securității.
Incident de securitate a informației – un eveniment sau o serie de evenimente de securitate a informației care au o probabilitate semnificativă de a compromite activitățile entității şi de a aduce amenințări securității informației.
Stație de lucru – componenta SI al entității cu ajutorul căreia utilizatorul accesează, creează, prelucrează datele de lucru conform atribuțiilor de serviciu.
Tehnică de calcul – componentele SI al entității utilizate pentru accesarea, păstrarea şi prelucrarea datelor de lucru (servere, stocuri de date, stații de lucru, imprimante, scanere etc.).
Administrator – angajat, care conform funcțiilor de serviciu este responsabil de gestionarea resurselor TI ale SI al entității.
Utilizator – angajat al entității sau a unei terțe părți, înregistrat în cadrul SI al entității şi autorizat să utilizeze resursele şi serviciile sistemului informațional al entității.
Posesor al datelor – subdiviziunea sau utilizatorul care poartă răspundere primară pentru corectitudinea, integritatea şi confidențialitatea datelor.
Posesor al resurselor informaționale – subdiviziunea ce deține în posesia sa resursele informaționale din cadrul SI al entității şi care poartă responsabilitate primară pentru securitatea lor.
Zonă de securitate – mediu controlat şi monitorizat în scopul evitării acțiunilor nesancționate.
Zona utilizatorului – mediu situat în afara zonei de securitate în care se utilizează resursele informaționale ale entității (de exemplu, utilizarea calculatoarelor portabile în afara sediului entității).
Informație publică – totalitatea datelor aferente activității entității supusă publicării conform actelor normative sau care pot fi publicate fără a implica riscuri de securitate.

III. Cadrul de organizare a securității informației

3.1. Politica de securitate a informației
Obiectiv: să asigure orientarea generală de management şi sprijinul pentru securitatea informației în conformitate cu cerințele de afacere, legislația şi actele normative aplicabile.

3.1.1. Conducerea entității elaborează şi aprobă documentul de politică a securității informației. Politica de securitate se publică şi se comunică tuturor angajaților şi terților părți relevante.
3.1.2. Politica de securitate se revizuieşte anual sau atunci când apar schimbări semnificative la nivelul SI sau reglementărilor aferente.|

3.2. Organizarea SMSI
Obiectiv: să asigure cadrul intern adecvat pentru managementul securității informației.

3.2.1. SMSI al entității se stabileşte, implementează, operează, monitorizează, revizuieşte, menține şi îmbunătățeşte în cadrul unui proces continuu de tipul Planifică- Implementează-Verifică-Îmbunătățeşte (Plan-Do-Check-Act).
3.2.2. Conducerea entității asigură suportul necesar aferent implementării şi menținerii unui SMSI eficient.|
3.2.3. Conducerea entității numeşte şi desemnează responsabilitatea pentru coordonarea procesului de management al securității informației la nivel de entitate (ofițer pe securitatea informației).
3.2.4. Organizarea SMSI se efectuează cu implicarea tuturor subdiviziunilor entității, în scopul asigurării unei abordări complexe şi multidisciplinare a cerințelor de securitate.
3.2.5. Toate rolurile şi responsabilitățile pentru securitatea informației se definesc în mod adecvat şi clar, se comunică şi sunt asumate în cadrul entității.
3.2.6. În scopul consolidării culturii organizatorice cu privire la securitatea informației, entitatea încurajează şi asigură condițiile necesare pentru menținerea de contacte corespunzătoare cu grupurile specializate de interes şi cu asociațiile profesionale în domeniul securității informației.
3.2.7. SMSI al entității se supune unei revizuiri independente cel puțin o dată în an, în scopul asigurării funcționării lui corespunzătoare.

3.3. Relația cu terțele părți
Obiectiv: să asigure securitatea informației în relația cu terțele părți care prestează sau beneficiază de servicii ce implică informația entității.

3.3.1. Entitatea asigură că riscurile pentru informația din cadrul entității şi pentru sistemele de procesare a informației din cadrul proceselor de afacere care implică terțe părți se identifică, iar înainte de acordarea accesului sau inițierea relației, se implementează măsuri de securitate corespunzătoare.
3.3.2. Entitatea asigură că orice relație cu o terță parte, care presupune accesul la resursele informaționale se inițiază şi se conduce în baza unui acord semnat între părți, care să acopere toate riscurile de securitate identificate.
3.3.3. Entitatea se asigură că terța parte cu care inițiază o relație de afacere are capacitatea de a gestiona corespunzător riscurile de securitate şi de a respecta cerințele de securitate asumate.

3.4. Externalizarea serviciilor TI
Obiectiv: să asigure securitatea şi continuitatea serviciilor TI externalizate către furnizori externi de servicii.

3.4.1 Entitatea asigură că dispune de politici şi proceduri interne adecvate privind evaluarea, gestionarea şi monitorizarea activităților externalizate, iar sistemul de control intern, sistemul de raportare internă şi funcțiile auditului intern sunt adaptate la specificul activităților externalizate.
3.4.2 La externalizarea serviciilor TI de importanță materială, entitatea se asigură că prin acțiunile de externalizare nu va crea o dependență operațională excesivă față de un furnizor extern de servicii TI, astfel încât să aibă capacitatea de a relua în orice moment controlul direct asupra serviciilor externalizate.
3.4.3 La externalizarea serviciilor TI de importanță materială, entitatea efectuează o analiză complexă a scenariilor de risc şi elaborează în acest sens un plan de asigurare a continuității cu proceduri detaliate de restabilire a activităților externalizate (inclusiv a scenariilor de revenire la producerea serviciilor cu resurse proprii, în sediul entității).

IV. Managementul resurselor informaționale

4.1. Responsabilitatea pentru resurse

Obiectiv: să asigure stabilirea şi asumarea responsabilității pentru protecția corespunzătoare a resurselor informaționale ale entității.

4.1.1. Entitatea asigură că resursele informaționale proprii sunt clar identificate, totodată fiind efectuată şi menținută inventarierea lor. Registrul de evidență a resurselor este actualizat continuu, pe măsura modificărilor în lista resurselor.
4.1.2. Pentru toate resursele informaționale se stabileşte un posesor (persoană sau subdiviziune). În cazul în care o resursă informațională este subiectul proprietății a mai multor posesori, atunci drepturile şi responsabilitățile de proprietate ale posesorilor se definesc reieşind din importanța resursei informaționale în cadrul activității subdiviziunii şi necesitatea subdiviziunii de a controla resursa.
4.1.3. Entitatea stabileşte şi implementează regulile şi normele privind modul de utilizare a resurselor informaționale şi asigură monitorizarea, respectării acestora.
4.1.4. Posesorul resurselor informaționale poartă responsabilitate primară pentru controlul adecvat al resurselor (creare, modificare, accesare, securizare). Implementarea şi operarea anumitor măsuri de control aferente resurselor poate fi delegată (de ex. către subdiviziunea TI) şi se formalizează obligatoriu printr-un document. Totodată, responsabilitatea primară rămâne a posesorului.

4.2. Clasificarea informației
Obiectiv: să asigure faptul că informația beneficiază de un nivel de protecție adecvat, proporțional importanței ei, reglementărilor aplicabile şi amenințărilor aferente.

4.2.1. Entitatea asigură că un clasificator al informației este definit în conformitate cu legislația în vigoare şi necesitățile entității. Informația se clasifică pentru a indica necesitatea, prioritățile şi gradul ei de protecție. Un sistem de clasificare a informației este utilizat pentru a defini un set adecvat de niveluri de protecție şi a comunica necesitatea măsurilor speciale de gestionare.
4.2.2. Entitatea asigură că informația clasificată din cadrul SI al entității are ataşată (la afişare, tipărire şi circulație) un marcator ce va indica clasa din care face parte informația.

V. Cerințe de securitate privind resursele umane

5.1. Asigurarea securității la angajare
Obiectiv: să asigure faptul că noii angajați, terțele părți, precum şi reprezentanții acestora sunt corespunzător verificați înainte de acordarea accesului la sisteme, iar responsabilitățile pentru securitatea informației sunt adecvat stabilite, comunicate şi asumate.

5.1.1. Entitatea asigură că responsabilitățile de securitate pentru noii angajați sunt comunicate la etapa de angajare.
5.1.2. Informația despre candidații la angajare sau angajații transferați se supune verificărilor de rigoare, în limitele cadrului legal. Nivelul de informație solicitată şi verificată trebuie să corespundă responsabilităților funcționale, tipului de informație la care va avea acces angajatul şi riscurilor aferente funcției ce va fi ocupată.
5.1.3. În scopul asigurării confidențialității informațiilor, la angajarea personalului entitatea poate prevedea încheierea unui acord de confidențialitate. Acordul va prevedea obligația angajatului privind păstrarea confidențialității informațiilor la care a obținut acces sau pe care le-au aflat, inclusiv pentru perioada de după încetarea activității sau în perioada suspendării activității.

5.2. Instruirea
Obiectiv: să asigure faptul că cerințele de securitate sunt cunoscute în măsură suficientă de către angajații entității, terțele părți, precum şi reprezentanții acestora.

5.2.1. Entitatea asigură că angajații săi, după caz şi terțele părți, beneficiază de instruire privind securitatea informației la un nivel corespunzător funcției, responsabilităților şi activităților desfăşurate.
5.2.2. Entitatea asigură că cerințele de securitate şi responsabilitățile individuale aferente securității informaționale sunt disponibile pentru toți angajații entității, iar după caz şi pentru terțe părți.

5.3. Asigurarea securității în activitatea angajaților
Obiectiv: să asigure faptul că cerințele de securitate sunt respectate necondiționat de către angajații entității, terțele părți, precum şi de reprezentanții acestora, iar responsabilitățile şi răspunderea juridică ale acestora sunt stabilite şi conştientizate corespunzător.

5.3.1. Entitatea asigură că cerințele de securitate a informației sunt respectate necondiționat de toți angajații entității, precum şi de terțe părți, în cazul în care acestea sunt autorizate să acceseze resursele informaționale ale entității.

5.3.2. Managementul cere şi se asigură că angajaţii, contractanţii şi reprezentanţii terţelor părţi cunosc şi respectă cerinţele de securitate stabilite prin politicile şi procedurile entităţii.
5.3.3. Entitatea asigură existenţa unui proces formal disciplinar pentru angajaţii care produc o încălcare a securităţii informaţiei.

5.4. Încetarea activităţii sau schimbarea locului de muncă
Obiectiv: să asigure faptul că angajaţii, terţele părţi, precum şi reprezentanţii acestora încetează relaţia cu entitatea într-o manieră controlată din punct de vedere al riscurilor de securitate.

5.4.1. Entitatea asigură că responsabilităţile şi procedurile aplicate la încetarea contractului de muncă sau schimbarea locului de muncă sunt în mod clar stabilite.
5.4.2. Angajaţii şi terţele părţi, la încetarea contractului de muncă sau la schimbarea locului de muncă, înapoiază resursele încredinţate, iar drepturile de acces avute sunt revocate sau revizuite.
5.4.3. La concedierea angajaţilor ce au deţinut acces administrativ la sistemele entităţii, se blochează conturile deţinute de aceştia, iar toate parolele de administrare relevante se modifică.

VI. Securitatea fizică şi a mediului de lucru

6.1. Zone de securitate
Obiectiv: să prevină accesul fizic neautorizat, distrugerile şi pătrunderile în interiorul entităţii, precum şi accesul la resursele informaţionale.

6.1.1. Securitatea de perimetru (bariere, pereţi, uşi de intrare în bază de autentificare, sisteme de securitate etc.) este organizată pentru a forma zone de securitate şi a proteja resursele informaţionale critice. Securitatea de perimetru este asigurată adecvat pentru toate încăperile entităţii.
6.1.2. Entitatea asigură că sunt clar stabilite zonele de securitate, iar mijloacele de control şi nivelul de securitate aferent fiecărei zone corespunde tipului zonei de securitate, sunt determinate în funcţie de cerinţele de securitate ale resurselor amplasate în zona respectivă şi în baza unei analize a riscurilor.
6.1.3. Entitatea asigură că zonele cu acces public, precum cele aferente deservirii clienţilor, primirii vizitatorilor, livrărilor şi încărcărilor, sunt controlate şi delimitate de restul zonelor de securitate ale entităţii.
6.1.4. Entitatea asigură că zonele de securitate sunt dotate cu mijloace adecvate de control al accesului pentru a asigura că doar persoanele autorizate vor avea acces (ex. lacăte, cartele de acces, supraveghere video, detectori efracţie, etc.)
6.1.5. Entitatea asigură că regulile şi normele de lucru şi acces în zonele de securitate sunt definite şi aplicate, iar drepturile de acces la zonele de securitate revizuite şi reînnoite în mod regulat.
6.1.6. Entitatea asigură că regulile de gestiune a rechizitelor de acces (chei, card-uri, coduri, etc.) sunt stabilite, comunicate şi aplicate.
6.1.7. Entitatea asigură că vizitatorii zonelor de securitate critice sunt supravegheaţi sau autorizaţi, iar data şi ora intrării şi ieşirii acestora este înregistrată.
6.1.8. Entitatea aplică măsuri pentru protecţia fizică împotriva incendiilor, inundaţiilor, cutremurelor, exploziilor, revoltelor publice şi a oricăror forme de dezastre naturale sau produse de oameni.
6.1.9. Entitatea asigură că echipamentul ce asigură securitatea încăperii / localului este instalat şi funcţionabil (ex.: sistem de alarmă incendiară, echipament de stingere a focului, detectoare de fum şi temperatură etc.).

6.2. Securitatea echipamentelor
Obiectiv: să prevină pierderea, distrugerea, furtul sau compromiterea echipamentelor TI şi întreruperea proceselor de activitate ale entităţii.

6.2.1. Entitatea asigură că echipamentele TI proprii, în funcţie de importanţa şi riscurile aferente, sunt amplasate şi protejate adecvat, astfel încât să se reducă riscurile faţă de ameninţările şi pericolele de mediu şi faţă de posibilitatea de acces neautorizat.
6.2.2. Echipamentele TI se protejează împotriva penelor de curent sau a altor întreruperi în funcţionarea sistemelor de suport (ex. sisteme de menţinere a microclimei).
6.2.3. Pentru a asigura buna funcţionare a echipamentului TI critic se monitorizează factorii mediului ambiant aferenţi acestuia.
6.2.4. Cablurile de energie şi reţelele de telecomunicaţii purtătoare de date se protejează faţă de interceptări sau avarii.
6.2.5. Echipamentele TI se menţin şi se utilizează adecvat, în scopul asigurării integralităţii şi disponibilităţii lui.
6.2.6. Pentru echipamentele TI scoase în afara încăperilor entităţii se asigură o securitate corespunzătoare, ţinându-se cont de riscurile aferente echipamentelor şi modului de utilizare a acestora (ex. utilizarea calculatoarelor portabile).
6.2.7. Echipamentele TI, informaţiile sau produsele software nu se scot în afara spaţiului de lucru fără o autorizaţie

prealabilă.
6.2.8. Toate echipamentele ce conțin medii de stocare se verifică minuțios înainte de casare sau transmitere, pentru a asigura că orice date importante sau produse soft licențiate au fost înlăturate sau suprascrise într-un mod ce să asigure irecuperabilitatea lor.

VII. Managementul comunicațiilor şi operațiunilor

7.1. Proceduri operaționale şi responsabilități
Obiectiv: să asigure operarea corectă şi în condiții de securitate a sistemelor de procesare a informației a entității.

7.1.1. Entitatea asigură că procedurile de gestiune şi operare a echipamentelor şi sistemelor TI sunt documentate şi puse la dispoziția persoanelor responsabile. De asemenea, toate procedurile de gestiune şi operare se mențin în stare actuală, iar toate modificările aferente lor, se autorizează la un nivel adecvat.
7.1.2. Entitatea asigură că obligațiunile funcționale şi domeniile de responsabilitate sunt adecvat segregate, pentru a reduce posibilitățile de utilizare abuzivă a resurselor informaționale ale entității (ex. segregarea funcțiilor de elaborare, testare implementare a sistemelor informatice, administrare a bazelor de date, a sistemelor de operare, a serviciilor de rețea, administrarea şi monitorizare altor resurse informaționale etc.).
7.1.3. Entitatea asigură că mediile de dezvoltare, testare şi producere sunt separate pentru a reduce riscul de acces neautorizat sau de modificări neautorizate asupra mediului de producție.

7.2. Managementul serviciilor terțelor părți
Obiectiv: să mențină un nivel corespunzător de securitate aferent serviciilor terțelor părți, conform prevederilor contractuale şi politicii de securitate a entității.

7.2.1. Entitatea se asigură că măsurile de securitate şi parametrii de furnizare a serviciilor terțelor părți sunt respectate de către terți în procesul de prestare a serviciilor.
7.2.2. Entitatea asigură că serviciile prestate de către părțile terțe sunt monitorizate pentru a asigura corespunderea acestora cu condițiile contractuale, politica şi normele de securitate ale entității. Rapoartele şi înregistrările furnizate de terța parte se evaluează şi se revizuiesc periodic.
7.2.3. Modificările privind furnizarea serviciilor, inclusiv menținerea şi îmbunătățirea politicilor existente de securitate a informației, procedurilor şi măsurilor de securitate se efectuează în mod controlat, ținând cont de rezultatele reevaluării riscurilor pentru sistemele TI şi procesele de afacere.

7.3. Planificarea şi acceptanța sistemelor TI
Obiectiv: să reducă riscurile aferente implementării noilor sisteme şi modificărilor în sistemele existente.

7.3.1. Modificările aferente sistemelor TI se efectuează conform unei proceduri documentate şi aprobate în cadrul entității.
7.3.2. Entitatea asigură că sistemele noi, modificările aferente sistemelor existente şi noile versiuni sunt analizate din punct de vedere al conformării la cerințele de securitate, iar impactul lor asupra mediului de producție este evaluat înainte de implementare.
7.3.3. Criteriile de acceptare pentru sistemele noi şi modificările la sistemele existente se stabilesc în mod clar. Până la acceptarea în producție a sistemelor noi şi a modificărilor la sistemele existente, se efectuează testări adecvate.
7.3.4. Entitatea asigură că utilizarea echipamentelor TI este monitorizată şi optimizată, iar necesitățile curente şi viitoare privind capacitatea de procesare sunt estimate în scopul asigurării performanței necesare pentru sistemele TI.

7.4. Protecția contra softului cu potențial dăunător
Obiectiv: să protejeze softul şi informația entității de activitatea malițioasă a viruşilor de calculator.

7.4.1. Entitatea asigură că toate căile posibile de pătrundere a softului cu potențial dăunător în SI sunt identificate şi că măsuri adecvate de securitate ce să asigure detectarea şi prevenirea răspândirii acestuia sunt implementate.
7.4.2. Entitatea asigură că soluțiile antivirus se actualizează periodic, rulează permanent şi nu pot fi stopate neautorizat.
7.4.3. Entitatea asigură că utilizatorii SI al entității cunosc normele de protecție contra softului cu potențial dăunător, în scopul diminuării riscului aferent factorului uman.
7.4.4. Entitatea asigură că activitatea la viruşi în cadrul entității, precum şi funcționarea soluțiilor antivirus, sunt monitorizate adecvat.

7.5. Copii de rezervă
Obiectiv: să asigure integritatea şi disponibilitatea informației entității şi a sistemelor de procesare a informației.

7.5.1. Entitatea asigură că este stabilită o politică de efectuare a copiilor de rezervă ce să asigure efectuarea regulată a copiilor de rezervă şi păstrarea lor în condiţii de siguranţă. Politica de efectuare a copiilor de rezervă trebuie să stabilească tipul datelor, frecvenţa efectuării copiilor de rezervă, tipul copiilor şi modalitatea de păstrare a lor, ţinând cont de importanţa informaţiei, cerinţele actelor normative în vigoare şi rezultatele analizei de risc.
7.5.2. Copiile de rezervă se păstrează în condiţii ce să asigure integritatea şi disponibilitatea lor în caz de necesitate.
7.5.3. Entitatea asigură că pentru toată informaţia importantă din cadrul sistemelor entităţii există copii de rezervă păstrate în afara localului de bază. Vechimea ultimei copii de rezervă pentru acest tip de informaţie nu trebuie să depăşească o săptămână.
7.5.4. Entitatea asigură că copii de rezervă pentru softul de sistem şi softul aplicativ din cadrul SI al entităţii sunt efectuate regulat. Regulile de efectuare a copiilor de rezervă sunt stabilite astfel, încât în caz de necesitate să fie restabilite ultimele versiuni ale softului aflat în utilizare în momentul incidentului.
7.5.5. Entitatea asigură că copii de rezervă pentru toată documentaţia în formă electronică a entităţii sunt efectuate şi păstrate în condiţii de siguranţă.
7.5.6. Entitatea stabileşte şi aplică proceduri de testare a copiilor de rezervă a entităţii, în scopul asigurării integrităţii şi disponibilităţii acestora.

7.6. Securitatea reţelelor de comunicaţii electronice
Obiectiv: să asigure protecţia reţelelor de comunicaţii electronice şi protecţia infrastructurii de suport.

7.6.1. Entitatea asigură că reţeaua corporativă a entităţii este adecvat gestionată şi controlată, pentru a asigura securitatea informaţiei, sistemelor şi aplicaţiilor ce utilizează reţelele de comunicaţii electronice.
7.6.2. Entitatea asigură că cerinţele de securitate aferente serviciilor TI prestate prin intermediul reţelei, sunt definite şi implementate.
7.6.3. Entitatea asigură că toate conexiunile de reţea între oficiile entităţii efectuate prin intermediul reţelelor terţelor părţi utilizează tehnologii de asigurare a confidenţialităţii şi integrităţii datelor.
7.6.4. Securitatea de perimetru pentru reţeaua corporativă a entităţii se asigură prin organizarea zonei demilitarizate. Sistemele şi serviciile disponibile în zona demilitarizată se protejează corespunzător.
7.6.5. Reţeaua corporativă a entităţii se divizează în sub-reţele în scopul protejării sistemelor, serviciilor şi grupurilor de utilizatori critici. Între sub-reţelele entităţii se stabilesc şi se implementează reguli de acces corespunzătoare.
7.6.6. Sisteme de prevenire şi detectare a intruziunilor se utilizează pentru a proteja resursele reţelei corporative.

7.7. Gestionarea suporturilor de informaţie
Obiectiv: să prevină divulgarea neautorizată şi modificarea informaţiei, distrugerea, furtul sau pierderea suporturilor de informaţie.

7.7.1. Entitatea asigură că toate cazurile de utilizare a suporturilor mobile de informaţie în cadrul entităţii sunt explicit autorizate, la bază fiind necesităţile afacerii.
7.7.2. Proceduri de gestiune securizată a suporturilor mobile de informaţie se stabilesc şi se implementează în scopul asigurării confidenţialităţii, disponibilităţii datelor şi a integrităţii fizice a acestora.
7.7.3. Retragerea din utilizare a suporturilor de informaţie se efectuează într-un mod care să asigure confidenţialitatea datelor stocate până la acel moment (ex.: distrugerea informaţiei, distrugerea suporturilor).
7.7.4. Entitatea asigură că suporturile de informaţie sunt protejate adecvat în cazul transportării în afara entităţii. Informaţia sensibilă păstrată pe aceste suporturi trebuie să fie criptată.

7.8. Schimbul de informaţie
Obiectiv: să asigure schimbul securizat de informaţie şi pachete soft cu terţele părţi, precum şi în interiorul entităţii.

7.8.1. Schimbul de informaţii între entitate şi terţele părţi se efectuează în baza unui acord semnat, ce să includă mijloacele, cerinţele şi responsabilităţile aferente securităţii informaţiei.
7.8.2. Transmiterea / expedierea componentelor şi modulelor produselor soft pe cale electronică se efectuează în baza acordurilor semnate, care vor stabili şi mijloacele de protecţie necesar a fi implementate în scopul asigurării confidenţialităţii, autenticităţii şi integrităţii mesajelor şi fişierelor recepţionate.
7.8.3. Informaţia sensibilă transmisă în formă electronică în afara entităţii se protejează corespunzător pentru a nu permite divulgarea sau modificarea ei.
7.8.4. Proceduri şi mijloace adecvate de control se implementează pentru a asigura schimbul securizat de informaţie între aplicaţiile program şi diferite componente ale SI al entităţii.
7.8.5. Entitatea asigură că informaţia făcută public este autorizată în mod corespunzător. Informaţia publicată pe pagina web oficială a entităţii se protejează pentru a preveni modificarea neautorizată a ei.

7.9. Gestiunea mijloacelor criptografice

Obiectiv: să asigure utilizarea securizată a mijloacelor de protecție criptografică a informației.

7.9.1. Entitatea stabileşte politici şi proceduri pentru gestiunea şi utilizarea securizată a mijloacelor de protecție criptografică a informației, luând în considerare cerințele normative aplicabile.
7.9.2. Mijloacele criptografice se gestionează într-o manieră ce să asigure integritatea lor fizică şi disponibilitatea lor doar pentru persoanele autorizate.
7.9.3. Utilizarea mijloacelor criptografice în cadrul entității se monitorizează continuu în scopul asigurării utilizării şi gestiunii lor conform politicilor şi procedurilor stabilite.

7.10. Managementul vulnerabilităților
Obiectiv: să prevină existența vulnerabilităților pentru resursele entității.

7.10.1. Toate sistemele entității se configurează securizat, în acest scop fiind stabilite standarde de configurare securizată.
7.10.2. Proceduri formale se stabilesc în scopul urmăririi noilor vulnerabilități aferente sistemelor entității şi reacționării corespunzătoare pentru înlăturarea acestora.

7.11. Monitorizarea
Obiectiv: să asigure identificarea în timp util a activităților neautorizate de accesare a informației şi utilizare a resurselor informaționale.

7.11.1. Entitatea asigură că jurnalele de audit care înregistrează activitățile utilizatorului, excepțiile şi evenimentele de securitate a informației sunt formate şi păstrate pentru o perioadă de timp determinată pentru a facilita investigațiile viitoare şi pentru monitorizarea accesului. Perioada de păstrare a jurnalelor de audit nu trebuie să fie mai mică de 12 luni.
7.11.2. Entitatea asigură că toate resursele informaționale importante au asociate jurnale de audit, în care să se înregistreze toate evenimentele ce pot avea impact asupra securității resurselor informaționale.
7.11.3. Entitatea stabileşte şi implementează proceduri de monitorizare a utilizării resurselor informaționale, iar rezultatele activităților de monitorizare se înregistrează şi se revizuiesc periodic. Instrumente ce să asigure monitorizarea eficientă a sistemelor şi serviciilor TI trebuie să fie implementate şi utilizate.
7.11.4. La stabilirea responsabilității pentru analiza jurnalelor de audit se ține cont de necesitatea segregării funcțiilor.
7.11.5. Jurnalele de audit se păstrează şi gestionează într-o manieră ce să asigure integritatea şi autenticitatea informației conținute.
7.11.6. Entitatea asigură că toate activitățile utilizatorilor critici sunt înregistrate (ex. administratorul de sistem).
7.11.7. Ceasurile tuturor sistemelor din cadrul entității se sincronizează cu o sursă de timp precisă şi sigură.

VIII. Controlul accesului la resursele informaționale

8.1. Politica de control al accesului
Obiectiv: să stabilească principii adecvate pentru controlul accesului la resursele informaționale ale entității.

8.1.1. Entitatea stabileşte politica de control a accesului la resursele şi sistemele sale, având la bază principiul accesului minim conform necesităților de afacere, în scopul realizării atribuțiilor de serviciu sau a celor contractuale.

8.2. Managementul accesului utilizatorilor
Obiectiv: să asigure controlul corespunzător al accesului la informație şi alte resurse informaționale ale entității.

8.2.1. Entitatea asigură că este stabilită o procedură de acordare, modificare, revizuire şi retragere a drepturilor de acces la toate sistemele şi resursele sale. Procedura trebuie să vizeze atât angajații entității, cât şi utilizatorii terților părți.
8.2.2. Accesul la toate resursele informaționale ale entității se acordă în strictă conformitate cu necesitățile de serviciu.
8.2.3. Toate cazurile de utilizare a resurselor informaționale ale entității necesită a fi autorizate. La stabilirea drepturilor de acces se va aplica principiul „este interzis tot ce nu este permis”.
8.2.4. Entitatea asigură că toți utilizatorii săi dețin identificatori unici în cadrul sistemelor accesate, iar rechizitele de acces (parola, token, cheie, etc) sunt deținute sau cunoscute doar de aceştia.
8.2.5. Entitatea stabileşte politici adecvate de utilizare a parolelor pentru toate sistemele sale.
8.2.6. Entitatea stabileşte o procedură specială pentru gestiunea conturilor cu drepturi privilegiate la resursele entității (administratori, super utilizatori, etc). Procedura va asigura păstrarea în condiții de confidențialitate a parolelor pentru conturile respective şi disponibilitatea acestora în situații de incident.
8.2.7. Entitatea asigură că toate parolele implicite pentru echipamentele şi sistemele entității se schimbă înainte de lansarea în exploatare.
8.2.8. Toate drepturile de acces ale utilizatorilor se revizuiesc la intervale regulate, însă nu mai rar de o dată în an.

8.3. Responsabilitățile utilizatorilor
Obiectiv: să prevină accesul neautorizat la resursele entității, precum şi furtul sau pierderea de informații.

8.3.1. Entitatea asigură că utilizatorilor săi li se comunică regulile de utilizare a rechizitelor de acces la sisteme şi li se cere respectarea strictă a acestora.
8.3.2. Utilizatorii entității se asigură că echipamentul TI aflat în dotare este protejat în mod corespunzător.
8.3.3. Entitatea stabileşte o politică de tipul „birou curat, ecran protejat" şi o comunică tuturor utilizatorilor pentru a fi aplicată în scopul evitării păstrării documentelor pe biroul de lucru şi lăsării stațiilor de lucru neprotejate.

8.4. Controlul accesului la rețea
Obiectiv: să protejeze informația şi serviciile de rețea.

8.4.1. Entitatea asigură că toate conexiunile la rețeaua sa sunt autorizate şi efectuate numai după analiza potențialului lor impact asupra securității informației.
8.4.2. Entitatea asigură că identificarea automată a echipamentului conectat la rețea este utilizată ca o metodă de autentificare a conexiunilor.
8.4.3. Entitatea asigură că tot traficul de intrare în rețeaua corporativă şi de ieşire din rețea este corespunzător controlat de către entitate.
8.4.4. Entitatea asigură că regulile de rutare a traficului intern şi extern sunt stabilite pentru a implementa politica de acces la resurse şi servicii.
8.4.5. Utilizarea rețelelor WiFi în cadrul entității se controlează într-un mod strict. Accesul la rețelele WiFi se autorizează în mod corespunzător. Utilizarea protocolului WEP în cadrul rețelelor WiFi trebuie evitată.
8.4.6. Conexiunea la distanță a utilizatorilor prin intermediul rețelelor publice se autorizează în mod corespunzător. Entitatea asigură că soluții eficiente de securitate sunt utilizate pentru autentificarea nominală a utilizatorilor, limitarea accesului la resursele necesare şi asigurarea confidențialității comunicațiilor.
8.4.7. Entitatea asigură că utilizatorii serviciilor în rețea ale entității au acces doar la serviciile pentru care au fost autorizați în mod specific.
8.4.8. Entitatea asigură că accesul la interfețele de administrare pentru echipamentele de rețea este limitat şi corespunzător protejat.

8.5. Controlul accesului la sistemele de operare şi mediile de virtualizare
Obiectiv: să prevină accesul neautorizat la sistemele de operare şi mediile de virtualizare.

8.5.1. Entitatea asigură că există proceduri şi măsuri de securitate care să permită accesul la sistemele de operare pe stațiile utilizatorilor şi pe servere doar pentru utilizatorii autorizați.
8.5.2. Entitatea implementează măsuri de securitate care să asigure: identificarea şi autentificarea utilizatorului, înregistrarea evenimentelor de securitate (de ex. accesărilor reuşite sau nereuşite către sistem), limitarea accesului la resursele autorizate (de ex. sistemul de fişiere local, aplicațiile instalate, porturi şi echipamente periferice).
8.5.3. Entitatea asigură că mediile de virtualizare sunt implementate în baza unei analize de risc, într-o manieră ce să prevină compromiterea sistemelor şi a serviciilor găzduite.
8.5.4. Pentru stațiile de lucru critice şi calculatoarele portabile entitatea asigură securitate suplimentară (de ex.: parolă power on, utilizarea cartelei de acces, criptare, etc.).
8.5.5. Entitatea asigură că drepturile utilizatorilor la nivelul sistemelor de operare corespund necesităților de serviciu. Instalarea şi rularea utilitarelor de sistem nu trebuie să fie permisă.
8.5.6. Entitatea asigură că utilizarea aplicațiilor şi serviciilor de sistem care asigură dirijarea la distanță a stațiilor de lucru este limitată şi strict monitorizată.
8.5.7. Instalarea de aplicații program pe stațiile de lucru ale utilizatorilor se efectuează doar de persoanele responsabile.

8.6. Accesul la aplicații şi informații
Obiectiv: să prevină accesul neautorizat la informația deținută în sistemele de aplicații.

8.6.1. Accesul la funcțiile sistemelor de aplicații şi informația din sisteme se restricționează în conformitate cu politica de control al accesului stabilită în entitate.
8.6.2. Entitatea asigură că sistemele de aplicații dispun de măsuri de protecție suficiente şi eficiente în scopul limitării accesului doar pentru utilizatorii autentificați şi doar în limita drepturilor autorizate.

IX. Achiziționarea, dezvoltarea şi mentenanță sistemelor de aplicații

9.1. Cerințele de securitate pentru sistemele aplicative

Obiectiv: să asigure că cerințele de securitate sunt considerate la planificarea, elaborarea, implementarea şi modificarea sistemelor de aplicații.

9.1.1. Entitatea asigură că cerințele pentru noile sisteme sau pentru îmbunătățirea sistemelor existente cuprind în mod specific cerințele de securitate.

9.2. Procesarea corectă a datelor în cadrul aplicațiilor
Obiectiv: să prevină erorile, pierderile, modificările neautorizate sau folosirea greşită a informațiilor în cadrul aplicațiilor.

9.2.1. Datele de intrare ale aplicațiilor se validează pentru a se asigura că aceste date sunt corecte şi corespunzătoare.
9.2.2. În cadrul aplicațiilor se implementează verificări de validare pentru a detecta orice modificare a informației prin procesare eronată sau prin acte deliberate.
9.2.3. Entitatea asigură că cerințele pentru integritatea mesajelor electronice în cadrul aplicațiilor sunt stabilite şi măsuri de securitate corespunzătoare sunt identificate şi implementate.
9.2.4. Datele de ieşire din cadrul aplicațiilor se validează pentru a se asigura că procesarea informației stocate este corectă.
9.2.5. Toate activitățile importante în cadrul sistemelor aplicative se înregistrează pentru a asigura monitorizarea utilizării sistemului aplicativ.

9.3. Securitatea fişierelor de sistem
Obiectiv: să asigure securitate fişierelor de sistem pentru aplicații.

9.3.1. Entitatea asigură că toate modificările aferente mediului de operare pentru sistemele de aplicații sunt strict controlate. Orice modificare în prealabil se testează şi se autorizează.
9.3.2. Mediile de operare pentru sistemele de aplicații critice se izolează de alte medii, pentru a evita compromiterea securității lor în rezultatul compromiterii securității sistemelor mai puțin critice.
9.3.3. Entitatea asigură că accesul la codurile sursă ale sistemelor de aplicații este strict limitat.
9.3.4. Fişierele de configurație ale sistemelor de aplicație se protejează corespunzător. Parolele existente în fişierele de configurație se criptează.

9.4. Securitatea în procesul de dezvoltare şi de suport
Obiectiv: să mențină securitatea sistemelor de aplicații.

9.4.1. Entitatea stabileşte o procedură formală pentru implementarea controlată a tuturor modificărilor aferente sistemelor de aplicații.
9.4.2. Datele de testare se selectează, protejează şi controlează în mod adecvat.
9.4.3. Entitatea asigură că accesul la mediul de producție pentru persoanele ce participă la elaborarea sistemelor, este limitat. Toate modificările aferente aplicațiilor program din mediul de producție se testează şi autorizează.
9.4.4. Aplicațiile critice, în cazul modificărilor în componentele hard sau aferente mediului de operare, se testează pentru a se asigura că nu există impact advers asupra funcționării acestora.
9.4.5. Elaborarea sistemelor de aplicații de către terțe părți se efectuează în baza acordurilor formale între părți şi în baza unui proces documentat ce corespunde politicilor stabilite de entitate.
9.4.6. Entitatea asigură că toate sistemele aplicative, dezvoltate intern sau achiziționate din exterior, sunt adecvat documentate.

X. Managementul incidentelor de securitate a informației

10.1. Identificarea şi raportarea incidentelor
Obiectiv: să asigure identificarea şi reacționarea în timp util la incidentele de securitate a informației.

10.1.1. Entitatea stabileşte o procedură formală privind managementul incidentelor de securitate a informației.
10.1.2. Pentru raportarea în timp util a incidentelor de securitate a informației, entitatea asigură un singur punct de contact pentru toți angajații săi, contractanții şi utilizatorii terți la care aceştia vor fi instruiți să raporteze cât mai curând orice incident sau problemă legată de utilizarea sistemelor şi tehnologiilor entității.
10.1.3. Toți angajații, contractanții şi utilizatorii terți ai sistemelor şi serviciilor informaționale se instruiesc pentru a raporta orice vulnerabilitate de securitate observată sau suspectată în cadrul sistemelor sau a serviciilor.

10.2. Reacțiunea la incidentele de securitate
Obiectiv: să asigure reacțiunea corespunzătoare la incidentele de securitate.

10.2.1. Entitatea asigură că responsabilitățile şi procedurile de reacțiune la incidentele de securitate sunt explicit stabilite în

cadrul entității, pentru a asigura un răspuns rapid, eficient şi sistematic la incidentele de securitate a informației.
10.2.2. Probele aferente incidentelor de securitate se colectează şi păstrează în condiții de siguranță în scopul investigării incidentelor şi asigurării suportului în cazul eventualelor acțiuni legale legate de incidentele petrecute.
10.2.3. Entitatea asigură un proces de analiză a incidentelor de securitate şi învățarea din acestea, pentru a nu admite repetarea incidentelor similare.
10.2.4. Entitatea asigură înregistrarea, documentarea completă şi raportarea incidentelor de securitate.

XI. Managementul continuității activității

11.1. Planificarea continuității afacerii
Obiectiv: să minimizeze impactul întreruperilor în sisteme şi servicii asupra proceselor de activitate ale entității.

11.1.1. Entitatea defineşte şi implementează un proces complex de planificare a continuității activității şi restabilire a sistemelor TI în situații de incident.
11.1.2. Entitatea elaborează, testează, aprobă şi menține în stare actuală un plan de continuitate a afacerii şi de restabilire în situații de incident.
11.1.3. Planul de continuitate a afacerii se elaborează în baza unei analize la impact asupra proceselor de activitate ale entității provocat de riscurile de securitate a informației.
11.1.4. Planul de continuitate a afacerii se revizuieşte cel puțin anual.

11.2. Restabilirea sistemelor TI
Obiectiv: să asigure restabilirea sistemelor şi serviciilor în termeni şi condiții acceptabile pentru afacere.

11.2.1. Cerințele afacerii pentru nivelul de continuitate şi restabilire a sistemelor şi serviciilor TI se stabilesc şi se aprobă în cadrul entității (ex. timpul de restabilire, momentul restabilirii datelor, etc).
11.2.2. Entitatea asigură proceduri documentate de restabilire a sistemelor şi serviciilor critice conform necesităților afacerii.
11.2.3. Procedurile de restabilire se testează la intervale regulate, sau ori de câte ori sunt efectuate modificări importante aferente sistemelor şi serviciilor. Testele trebuie să asigure că toți angajații antrenați în procesul de restabilire sunt conştienți de acțiunile efectuate.
11.2.4. Entitatea asigură un local de rezervă şi infrastructura necesară pentru restabilirea sistemelor şi serviciilor critice în situații de incident major.
11.2.5. Entitatea asigură că localul de rezervă nu este expus aceloraşi riscuri precum localul de bază şi dispune de capacitățile necesare pentru susținerea procesului de restabilire.

XII. Conformitatea

12.1. Conformitatea cu cerințele legale şi regulatorii
Obiectiv: să evite încălcarea actelor normative ce țin de securitatea informației.

12.1.1. Entitatea identifică şi este la curent cu toate modificările aferente actelor normative aplicabile în sfera securității informației.
12.1.2. Entitatea se asigură că nu încalcă actele normative la utilizarea produselor ce pot fi subiect al drepturilor de autor (ex. produse soft, materiale, etc).
12.1.3. Entitatea asigură protecția corespunzătoare a datelor cu caracter personal în conformitate cu actele normative. Considerate trebuie să fie atât datele personale ale clienților, cât şi datele angajaților entității.

XIII. Securitatea datelor de carduri bancare

13.1. Securitatea datelor de carduri în posesia entității
Obiectiv: să asigurare respectarea actelor normative ce țin de securitatea datelor de carduri bancare.

13.1.1. În cazul în care entitatea deține date ale cardurilor bancare, este necesar de asigurat efectuarea analizei de risc pentru utilizarea cardurilor bancare în cadrul serviciilor oferite de entitate clienților săi.
13.1.2. Entitatea asigură că standardul PCI DSS este luat în considerare la asigurarea unui cadru de control al securității datelor cardurilor bancare accesate, procesate şi transmise de entitate.

XIV. Auditul intern al securității informației

14.1. Planificarea şi organizarea auditului
Obiectiv: să asigure organizarea şi planificarea eficientă a auditului intern al securității informației.

14.1.1. Entitatea asigură că auditorii interni TI sunt independenți în raport cu responsabilitățile operaționale aferent ariilor de audit TI.
14.1.2. Planul de audit TI se elaborează în baza unei analize a riscurilor pentru toate sistemele, serviciile, procesele TI şi a proiectelor planificate sau derulate.
14.1.3. Entitatea asigură că toate sistemele şi serviciile TI utilizate în cadrul proceselor de activitate de bază vor fi supuse auditului cel puțin o dată în trei ani. Suplimentar, se asigură că audite ale eficienței şi eficacității proceselor TI importante sunt efectuate.
14.1.4. Auditul intern al SMSI al entității se efectuează cel puțin anual.

Vezi și

Tag-uri
securitatea informației [3]
confidențialitate [4]
integritatea informației [5]
risc de securitate a informației [6]
sistem informatic [7]

Legături conexe:

[1] http://www.isaca.org [2] https://www.pcisecuritystandards.org/ [3] http://www.bnm.md/ro/search?hashtags[0]=securitatea informației [4] http://www.bnm.md/ro/search?hashtags[0]=confidențialitate [5] http://www.bnm.md/ro/search?hashtags[0]=integritatea informației [6] http://www.bnm.md/ro/search?hashtags[0]=risc de securitate a informației [7] http://www.bnm.md/ro/search?hashtags[0]=sistem informatic