



Extinde Ascunde

06.08.2010

Recomandări cu privire la obiectivele de control și 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 și 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 și măsurile de securitate ale Sistemului de Management al Securității Informației (în continuare Recomandări), reprezintă îndrumări ale Băncii Naționale a Moldovei emise în scopul facilitării și 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 și instituțiilor nebancale (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 și prestatorilor de servicii de plată nebancale, 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 următoarele standarde, ghiduri și coduri de practică în domeniu:

- SM GOST R ISO/IEC 27001:2008 (ISO/IEC 27001:2005) - Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe;
- SMV ISO/CEI 27002:2009 (ISO/IEC 27002:2005) - Tehnologia informației. Tehnici de securitate. Cod de buna practică pentru managementul securității informației;
- SMV ISO/CEI 27005:2009 (ISO/IEC 27005:2008) - Tehnologia informației. Tehnici de securitate. Managementul riscului securității informației;
- Standardul Control Objectives for Information and related Technology, emis de Information Systems Audit and Control Association (www.isaca.org ^[1]).
- 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 și îmbunătățirii propriilor Sisteme de Management al Securității Informației (în continuare - SMSI), entitățile pot aplica prezentele Recomandări, precum și alte surse metodologice din domeniul securității informației.

II. Termeni și definiții

În sensul prezentului document, se aplică următoarele noțiuni:

Securitatea informației – păstrarea confidențialității, integrității și disponibilității informației în orice formă a sa (electronică, pe suport hârtie, etc.) și protejarea resurselor implicate la gestiunea acestora, în plus, alte proprietăți precum autenticitatea, responsabilitatea, non-repudierea și 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 și 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 și revizuire a riscurilor de securitate.

Entitate – banca sau instituție nebanară (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 și hardware, destinate pentru procesarea, colectarea, stocarea datelor și 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 și servicii TI etc.) și 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 și 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 și hardware inclusiv serviciile TI, destinate asigurării funcționării sistemului informațional.

Rețea internă a entității – totalitatea echipamentelor și canalelor tehnice de comunicare între componentele infrastructurii TI în cadrul entității.

Zona Demilitarizată – o parte a rețelei (fizic și/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) și are rolul de a separa resursele accesibile din exteriorul rețelei de celelalte resurse interne, în scopul prevenirii accesului nesanționat 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 eșec 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 și 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 și prelucrarea datelor de lucru (serve, 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 și autorizat să utilizeze resursele și serviciile sistemului informațional al entității.

Posesor al datelor – subdiviziunea sau utilizatorul care poartă răspundere primară pentru corectitudinea, integritatea și confidențialitatea datelor.

Posesor al resurselor informaționale – subdiviziunea ce deține în posesia sa resursele informaționale din cadrul SI al entității și care poartă responsabilitate primară pentru securitatea lor.

Zonă de securitate – mediu controlat și monitorizat în scopul evitării acțiunilor nesanționate.

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 și sprijinul pentru securitatea informației în conformitate cu cerințele de afaceri, legislația și actele normative aplicabile.

3.1.1. Conducerea entității elaborează și aprobă documentul de politică a securității informației. Politica de securitate se publică și se comunică tuturor angajaților și terțelor părți relevante.

3.1.2. Politica de securitate se revizuieste 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 stabilește, implementează, operează, monitorizează, revizuieste, menține și îmbunătățește în cadrul unui proces continuu de tipul Planifică- Implementează-Verifică-Îmbunătățește (Plan-Do-Check-Act).

3.2.2. Conducerea entității asigură suportul necesar aferent implementării și menținerii unui SMSI eficient.

3.2.3. Conducerea entității numește și 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 și multidisciplinare a cerințelor de securitate.

3.2.5. Toate rolurile și responsabilitățile pentru securitatea informației se definesc în mod adecvat și clar, se comunică și sunt asumate în cadrul entității.

3.2.6. În scopul consolidării culturii organizatorice cu privire la securitatea informației, entitatea încurajează și asigură condițiile necesare pentru menținerea de contacte corespunzătoare cu grupurile specializate de interes și cu asociațiile profesionale în domeniul securității informației.

3.2.7. SMSI al entității se supune unei revizuirii 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 și pentru sistemele de procesare a informației din cadrul proceselor de afaceri 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 și 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 afaceri are capacitatea de a gestiona corespunzător riscurile de securitate și de a respecta cerințele de securitate asumate.

3.4. Externalizarea serviciilor TI

Obiectiv: să asigure securitatea și continuitatea serviciilor TI externalizate către furnizori externi de servicii.

3.4.1 Entitatea asigură că dispune de politici și proceduri interne adecvate privind evaluarea, gestionarea și monitorizarea activităților externalizate, iar sistemul de control intern, sistemul de raportare internă și 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 și 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 și 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 și 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 stabilește un posesor (persoană sau subdiviziune). În cazul în care o resursă informațională este subiectul proprietății a mai multor posesori, atunci drepturile și responsabilitățile de proprietate ale posesorilor se definesc reieșind din importanța resursei informaționale în cadrul activității subdiviziunii și necesitatea subdiviziunii de a controla resursa.

4.1.3. Entitatea stabilește și implementează regulile și normele privind modul de utilizare a resurselor informaționale și asigură monitorizarea, respectării acestora.

4.1.4. Posesorul resurselor informaționale poartă responsabilitate primară pentru controlul adecvat al resurselor (creare, modificare, accesare, securizare). Implementarea și operarea anumitor măsuri de control aferente resurselor poate fi delegată (de ex. către subdiviziunea TI) și 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 și amenințărilor aferente.

4.2.1. Entitatea asigură că un clasificator al informației este definit în conformitate cu legislația în vigoare și necesitățile entității. Informația se clasifică pentru a indica necesitatea, prioritățile și gradul ei de protecție. Un sistem de clasificare a informației este utilizat pentru a defini un set adecvat de niveluri de protecție și a comunica necesitatea măsurilor speciale de gestionare.

4.2.2. Entitatea asigură că informația clasificată din cadrul SI al entității are atașată (la afișare, tipărire și 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 și reprezentanții acestora sunt corespunzător verificați înainte de acordarea accesului la sisteme, iar responsabilitățile pentru securitatea informației sunt adecvat stabilite, comunicate și 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 și verificată trebuie să corespundă responsabilităților funcționale, tipului de informație la care va avea acces angajatul și 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 și reprezentanții acestora.

5.2.1. Entitatea asigură că angajații săi, după caz și terțele părți, beneficiază de instruire privind securitatea informației la un nivel corespunzător funcției, responsabilităților și activităților desfășurate.

5.2.2. Entitatea asigură că cerințele de securitate și responsabilitățile individuale aferente securității informaționale sunt disponibile pentru toți angajații entității, iar după caz și 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 și de reprezentanții acestora, iar responsabilitățile și răspunderea juridică ale acestora sunt stabilite și conștientizate corespunzător.

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

5.3.2. Managementul cere și se asigură că angajații, contractanții și reprezentanții terțelor părți cunosc și respectă cerințele de securitate stabilite prin politicile și procedurile entității.

5.3.3. Entitatea asigură existența unui proces formal disciplinar pentru angajații care produc o încălcare a securității informației.

5.4. Încetarea activității sau schimbarea locului de muncă

Obiectiv: să asigure faptul că angajații, terțele părți, precum și reprezentanții acestora încetează relația cu entitatea într-o manieră controlată din punct de vedere al riscurilor de securitate.

5.4.1. Entitatea asigură că responsabilitățile și procedurile aplicate la încetarea contractului de muncă sau schimbarea locului de muncă sunt în mod clar stabilite.

5.4.2. Angajații și terțele părți, la încetarea contractului de muncă sau la schimbarea locului de muncă, înapoiază resursele încredințate, iar drepturile de acces avute sunt revocate sau revizuite.

5.4.3. La concedierea angajaților ce au deținut acces administrativ la sistemele entității, se blochează conturile deținute de aceștia, iar toate parolele de administrare relevante se modifică.

VI. Securitatea fizică și a mediului de lucru

6.1. Zone de securitate

Obiectiv: să prevină accesul fizic neautorizat, distrugerile și pătrunderile în interiorul entității, precum și accesul la resursele informaționale.

6.1.1. Securitatea de perimetru (bariere, pereți, uși de intrare în bază de autentificare, sisteme de securitate etc.) este organizată pentru a forma zone de securitate și a proteja resursele informaționale critice. Securitatea de perimetru este asigurată adecvat pentru toate încăperile entității.

6.1.2. Entitatea asigură că sunt clar stabilite zonele de securitate, iar mijloacele de control și nivelul de securitate aferent fiecărei zone corespunde tipului zonei de securitate, sunt determinate în funcție de cerințele de securitate ale resurselor amplasate în zona respectivă și în baza unei analize a riscurilor.

6.1.3. Entitatea asigură că zonele cu acces public, precum cele aferente deservirii clienților, primirii vizitatorilor, livrărilor și încărcărilor, sunt controlate și delimitate de restul zonelor de securitate ale entității.

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 efracție, etc.)

6.1.5. Entitatea asigură că regulile și normele de lucru și acces în zonele de securitate sunt definite și aplicate, iar drepturile de acces la zonele de securitate revizuite și 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 și aplicate.

6.1.7. Entitatea asigură că vizitatorii zonelor de securitate critice sunt supravegheați sau autorizați, iar data și ora intrării și ieșirii acestora este înregistrată.

6.1.8. Entitatea aplică măsuri pentru protecția fizică împotriva incendiilor, inundațiilor, cutremurelor, exploziilor, revoltelor publice și a oricăror forme de dezastre naturale sau produse de oameni.

6.1.9. Entitatea asigură că echipamentul ce asigură securitatea încăperii / localului este instalat și funcțional (ex.: sistem de alarmă incendiară, echipament de stingere a focului, detectoare de fum și temperatură etc.).

6.2. Securitatea echipamentelor

Obiectiv: să prevină pierderea, distrugerea, furtul sau compromiterea echipamentelor TI și întreruperea proceselor de activitate ale entității.

6.2.1. Entitatea asigură că echipamentele TI proprii, în funcție de importanța și riscurile aferente, sunt amplasate și protejate adecvat, astfel încât să se reducă riscurile față de amenințările și pericolele de mediu și față de posibilitatea de acces neautorizat.

6.2.2. Echipamentele TI se protejează împotriva penelor de curent sau a altor întreruperi în funcționarea sistemelor de suport (ex. sisteme de menținere a microclimei).

6.2.3. Pentru a asigura buna funcționare a echipamentului TI critic se monitorizează factorii mediului ambiant aferenți acestuia.

6.2.4. Cablurile de energie și rețelele de telecomunicații purtătoare de date se protejează față de interceptări sau avarii.

6.2.5. Echipamentele TI se mențin și se utilizează adecvat, în scopul asigurării integralității și disponibilității lui.

6.2.6. Pentru echipamentele TI scoase în afara încăperilor entității se asigură o securitate corespunzătoare, ținându-se cont de riscurile aferente echipamentelor și modului de utilizare a acestora (ex. utilizarea calculatoarelor portabile).

6.2.7. Echipamentele TI, informațiile sau produsele software nu se scot în afara spațiului de lucru fără o autorizație

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 și operațiunilor

7.1. Proceduri operaționale și responsabilități

Obiectiv: să asigure operarea corectă și în condiții de securitate a sistemelor de procesare a informației a entității.

7.1.1. Entitatea asigură că procedurile de gestiune și operare a echipamentelor și sistemelor TI sunt documentate și puse la dispoziția persoanelor responsabile. De asemenea, toate procedurile de gestiune și 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 și 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 și monitorizare altor resurse informaționale etc.).

7.1.3. Entitatea asigură că mediile de dezvoltare, testare și 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 și politicii de securitate a entității.

7.2.1. Entitatea se asigură că măsurile de securitate și 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 și normele de securitate ale entității. Rapoartele și înregistrările furnizate de terța parte se evaluează și se revizuiesc periodic.

7.2.3. Modificările privind furnizarea serviciilor, inclusiv menținerea și îmbunătățirea politicilor existente de securitate a informației, procedurilor și măsurilor de securitate se efectuează în mod controlat, ținând cont de rezultatele reevaluării riscurilor pentru sistemele TI și procesele de afacere.

7.3. Planificarea și acceptanța sistemelor TI

Obiectiv: să reducă riscurile aferente implementării noilor sisteme și modificărilor în sistemele existente.

7.3.1. Modificările aferente sistemelor TI se efectuează conform unei proceduri documentate și aprobate în cadrul entității.

7.3.2. Entitatea asigură că sistemele noi, modificările aferente sistemelor existente și 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 și modificările la sistemele existente se stabilesc în mod clar. Până la acceptarea în producție a sistemelor noi și a modificărilor la sistemele existente, se efectuează testări adecvate.

7.3.4. Entitatea asigură că utilizarea echipamentelor TI este monitorizată și optimizată, iar necesitățile curente și 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 și informația entității de activitatea malițioasă a virușilor de calculator.

7.4.1. Entitatea asigură că toate căile posibile de pătrundere a softului cu potențial dăunător în SI sunt identificate și că măsuri adecvate de securitate ce să asigure detectarea și prevenirea răspândirii acestuia sunt implementate.

7.4.2. Entitatea asigură că soluțiile antivirus se actualizează periodic, rulează permanent și 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 viruși în cadrul entității, precum și funcționarea soluțiilor antivirus, sunt monitorizate adecvat.

7.5. Copii de rezervă

Obiectiv: să asigure integritatea și disponibilitatea informației entității și 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 și păstrarea lor în condiții de siguranță. Politica de efectuare a copiilor de rezervă trebuie să stabilească tipul datelor, frecvența efectuării copiilor de rezervă, tipul copiilor și modalitatea de păstrare a lor, ținând cont de importanța informației, cerințele actelor normative în vigoare și rezultatele analizei de risc.

7.5.2. Copiile de rezervă se păstrează în condiții ce să asigure integritatea și disponibilitatea lor în caz de necesitate.

7.5.3. Entitatea asigură că pentru toată informația importantă din cadrul sistemelor entității există copii de rezervă păstrate în afara localului de bază. Vechimea ultimei copii de rezervă pentru acest tip de informație nu trebuie să depășească o săptămână.

7.5.4. Entitatea asigură că copii de rezervă pentru softul de sistem și softul aplicativ din cadrul SI al entității 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 documentația în formă electronică a entității sunt efectuate și păstrate în condiții de siguranță.

7.5.6. Entitatea stabilește și aplică proceduri de testare a copiilor de rezervă a entității, în scopul asigurării integrității și disponibilității acestora.

7.6. Securitatea rețelelor de comunicații electronice

Obiectiv: să asigure protecția rețelelor de comunicații electronice și protecția infrastructurii de suport.

7.6.1. Entitatea asigură că rețeaua corporativă a entității este adecvat gestionată și controlată, pentru a asigura securitatea informației, sistemelor și aplicațiilor ce utilizează rețelele de comunicații electronice.

7.6.2. Entitatea asigură că cerințele de securitate aferente serviciilor TI prestate prin intermediul rețelei, sunt definite și implementate.

7.6.3. Entitatea asigură că toate conexiunile de rețea între oficiile entității efectuate prin intermediul rețelelor terțelor părți utilizează tehnologii de asigurare a confidențialității și integrității datelor.

7.6.4. Securitatea de perimetru pentru rețeaua corporativă a entității se asigură prin organizarea zonei demilitarizate. Sistemele și serviciile disponibile în zona demilitarizată se protejează corespunzător.

7.6.5. Rețeaua corporativă a entității se divizează în sub-rețele în scopul protejării sistemelor, serviciilor și grupurilor de utilizatori critici. Între sub-rețelele entității se stabilesc și se implementează reguli de acces corespunzătoare.

7.6.6. Sisteme de prevenire și detectare a intruziunilor se utilizează pentru a proteja resursele rețelei corporative.

7.7. Gestionarea suporturilor de informație

Obiectiv: să prevină divulgarea neautorizată și modificarea informației, distrugerea, furtul sau pierderea suporturilor de informație.

7.7.1. Entitatea asigură că toate cazurile de utilizare a suporturilor mobile de informație în cadrul entității sunt explicit autorizate, la bază fiind necesitățile afacerii.

7.7.2. Proceduri de gestiune securizată a suporturilor mobile de informație se stabilesc și se implementează în scopul asigurării confidențialității, disponibilității datelor și a integrității fizice a acestora.

7.7.3. Retragerea din utilizare a suporturilor de informație se efectuează într-un mod care să asigure confidențialitatea datelor stocate până la acel moment (ex.: distrugerea informației, distrugerea suporturilor).

7.7.4. Entitatea asigură că suporturile de informație sunt protejate adecvat în cazul transportării în afara entității.

Informația sensibilă păstrată pe aceste suporturi trebuie să fie criptată.

7.8. Schimbul de informație

Obiectiv: să asigure schimbul securizat de informație și pachete soft cu terțele părți, precum și în interiorul entității.

7.8.1. Schimbul de informații între entitate și terțele părți se efectuează în baza unui acord semnat, ce să includă mijloacele, cerințele și responsabilitățile aferente securității informației.

7.8.2. Transmiterea / expedierea componentelor și modulelor produselor soft pe cale electronică se efectuează în baza acordurilor semnate, care vor stabili și mijloacele de protecție necesar a fi implementate în scopul asigurării confidențialității, autenticității și integrității mesajelor și fișierelor recepționate.

7.8.3. Informația sensibilă transmisă în formă electronică în afara entității se protejează corespunzător pentru a nu permite divulgarea sau modificarea ei.

7.8.4. Proceduri și mijloace adecvate de control se implementează pentru a asigura schimbul securizat de informație între aplicațiile program și diferite componente ale SI al entității.

7.8.5. Entitatea asigură că informația făcută public este autorizată în mod corespunzător. Informația publicată pe pagina web oficială a entității 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 stabilește politici și proceduri pentru gestiunea și 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 și disponibilitatea lor doar pentru persoanele autorizate.

7.9.3. Utilizarea mijloacelor criptografice în cadrul entității se monitorizează continuu în scopul asigurării utilizării și gestiunii lor conform politicilor și 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 și reacționării corespunzătoare pentru înlăturarea acestora.

7.11. Monitorizarea

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

7.11.1. Entitatea asigură că jurnalele de audit care înregistrează activitățile utilizatorului, excepțiile și evenimentele de securitate a informației sunt formate și păstrate pentru o perioadă de timp determinată pentru a facilita investigațiile viitoare și 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 stabilește și implementează proceduri de monitorizare a utilizării resurselor informaționale, iar rezultatele activităților de monitorizare se înregistrează și se revizuiesc periodic. Instrumente ce să asigure monitorizarea eficientă a sistemelor și serviciilor TI trebuie să fie implementate și 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 și gestionează într-o manieră ce să asigure integritatea și 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 și sigură.

VIII. Controlul accesului la resursele informaționale

8.1. Politica de control al accesului

Obiectiv: să stabilească principiile adecvate pentru controlul accesului la resursele informaționale ale entității.

8.1.1. Entitatea stabilește politica de control a accesului la resursele și 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 și alte resurse informaționale ale entității.

8.2.1. Entitatea asigură că este stabilită o procedură de acordare, modificare, revizuire și retragere a drepturilor de acces la toate sistemele și resursele sale. Procedura trebuie să vizeze atât angajații entității, cât și utilizatorii terțelor 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 aceștia.

8.2.5. Entitatea stabilește politici adecvate de utilizare a parolilor pentru toate sistemele sale.

8.2.6. Entitatea stabilește 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 parolilor pentru conturile respective și disponibilitatea acestora în situații de incident.

8.2.7. Entitatea asigură că toate parolele implicite pentru echipamentele și 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 și furtul sau pierderea de informații.

8.3.1. Entitatea asigură că utilizatorilor săi li se comunică regulile de utilizare a rechetitelor de acces la sisteme și 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 stabilește o politică de tipul „birou curat, ecran protejat” și o comunică tuturor utilizatorilor pentru a fi aplicată în scopul evitării păstrării documentelor pe biroul de lucru și lăsării stațiilor de lucru neprotejate.

8.4. Controlul accesului la rețea

Obiectiv: să protejeze informația și serviciile de rețea.

8.4.1. Entitatea asigură că toate conexiunile la rețeaua sa sunt autorizate și 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 și de ieșire din rețea este corespunzător controlat de către entitate.

8.4.4. Entitatea asigură că regulile de rutare a traficului intern și extern sunt stabilite pentru a implementa politica de acces la resurse și 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 și 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 și corespunzător protejat.

8.5. Controlul accesului la sistemele de operare și mediile de virtualizare

Obiectiv: să prevină accesul neautorizat la sistemele de operare și mediile de virtualizare.

8.5.1. Entitatea asigură că există proceduri și măsuri de securitate care să permită accesul la sistemele de operare pe stațiile utilizatorilor și pe servere doar pentru utilizatorii autorizați.

8.5.2. Entitatea implementează măsuri de securitate care să asigure: identificarea și autentificarea utilizatorului, înregistrarea evenimentelor de securitate (de ex. accesărilor reușite sau nereușite către sistem), limitarea accesului la resursele autorizate (de ex. sistemul de fișiere local, aplicațiile instalate, porturi și 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 și a serviciilor găzduite.

8.5.4. Pentru stațiile de lucru critice și 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 și rularea utilităților de sistem nu trebuie să fie permisă.

8.5.6. Entitatea asigură că utilizarea aplicațiilor și serviciilor de sistem care asigură dirijarea la distanță a stațiilor de lucru este limitată și 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 și informații

Obiectiv: să prevină accesul neautorizat la informația deținută în sistemele de aplicații.

8.6.1. Accesul la funcțiile sistemelor de aplicații și 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 și eficiente în scopul limitării accesului doar pentru utilizatorii autentificați și doar în limita drepturilor autorizate.

IX. Achiziționarea, dezvoltarea și 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 și 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 greșită a informațiilor în cadrul aplicațiilor.

9.2.1. Datele de intrare ale aplicațiilor se validează pentru a se asigura că aceste date sunt corecte și 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 și măsuri de securitate corespunzătoare sunt identificate și implementate.

9.2.4. Datele de ieșire 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 fișierelor de sistem

Obiectiv: să asigure securitate fișierelor 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 și 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. Fișierele de configurație ale sistemelor de aplicație se protejează corespunzător. Parolele existente în fișierele de configurație se criptează.

9.4. Securitatea în procesul de dezvoltare și de suport

Obiectiv: să mențină securitatea sistemelor de aplicații.

9.4.1. Entitatea stabilește o procedură formală pentru implementarea controlată a tuturor modificărilor aferente sistemelor de aplicații.

9.4.2. Datele de testare se selectează, protejează și 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 și 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 și 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 și raportarea incidentelor

Obiectiv: să asigure identificarea și reacționarea în timp util la incidentele de securitate a informației.

10.1.1. Entitatea stabilește 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 și utilizatorii terți la care aceștia vor fi instruiți să raporteze cât mai curând orice incident sau problemă legată de utilizarea sistemelor și tehnologiilor entității.

10.1.3. Toți angajații, contractanții și utilizatorii terți ai sistemelor și 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 și procedurile de reacțiune la incidentele de securitate sunt explicit stabilite

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

XI. Managementul continuității activității

11.1. Planificarea continuității afacerii

Obiectiv: să minimizeze impactul întreruperilor în sisteme și servicii asupra proceselor de activitate ale entității.

- 11.1.1. Entitatea definește și implementează un proces complex de planificare a continuității activității și restabilire a sistemelor TI în situații de incident.
- 11.1.2. Entitatea elaborează, testează, aprobă și menține în stare actuală un plan de continuitate a afacerii și 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 revizuieste cel puțin anual.

11.2. Restabilirea sistemelor TI

Obiectiv: să asigure restabilirea sistemelor și serviciilor în termeni și condiții acceptabile pentru afacere.

- 11.2.1. Cerințele afacerii pentru nivelul de continuitate și restabilire a sistemelor și serviciilor TI se stabilesc și se aprobă în cadrul entității (ex. timpul de restabilire, momentul restabilirii datelor, etc).
- 11.2.2. Entitatea asigură proceduri documentate de restabilire a sistemelor și 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 și serviciilor. Testele trebuie să asigure că toți angajații antrenați în procesul de restabilire sunt conștienți de acțiunile efectuate.
- 11.2.4. Entitatea asigură un local de rezervă și infrastructura necesară pentru restabilirea sistemelor și serviciilor critice în situații de incident major.
- 11.2.5. Entitatea asigură că localul de rezervă nu este expus aceluiași riscuri precum localul de bază și dispune de capacitățile necesare pentru susținerea procesului de restabilire.

XII. Conformitatea

12.1. Conformitatea cu cerințele legale și regulatorii

Obiectiv: să evite încălcarea actelor normative ce țin de securitatea informației.

- 12.1.1. Entitatea identifică și 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 și datele angajaților entității.

XIII. Securitatea datelor de carduri bancare

13.1. Securitatea datelor de carduri în posesia entității

Obiectiv: să asigure 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 și transmise de entitate.

XIV. Auditul intern al securității informației

14.1. Planificarea și organizarea auditului

Obiectiv: să asigure organizarea și 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 și a proiectelor planificate sau derulate.

14.1.3. Entitatea asigură că toate sistemele și 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 și 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]

Sursa URL:

<http://bnm.md/ro/content/recomandari-cu-privire-la-obiectivele-de-control-si-masurile-de-securitate-ale-sistemului-de>

Legături conexe:

[1] <http://www.isaca.org> [2] <https://www.pcisecuritystandards.org/> [3] [http://bnm.md/ro/search?hashtags\[0\]=securitatea informației](http://bnm.md/ro/search?hashtags[0]=securitatea%20informației) [4] [http://bnm.md/ro/search?hashtags\[0\]=confidențialitate](http://bnm.md/ro/search?hashtags[0]=confidențialitate) [5] [http://bnm.md/ro/search?hashtags\[0\]=integritatea informației](http://bnm.md/ro/search?hashtags[0]=integritatea%20informației) [6] [http://bnm.md/ro/search?hashtags\[0\]=risc de securitate a informației](http://bnm.md/ro/search?hashtags[0]=risc%20de%20securitate%20a%20informației) [7] [http://bnm.md/ro/search?hashtags\[0\]=sistem informatic](http://bnm.md/ro/search?hashtags[0]=sistem%20informatic)