Publicat pe (https://bnm.md)

Extinde Ascunde

06.08.2010

Recomandări cu privire la obiectivele de control şi măsurile de securitate ale Sistemului de Management al Securităţii Informaţiei

APROBAT
Guvernatorul
Băncii Naţionale a Moldovei
Dorin DRĂGUȚANU
6 august 2010

RECOMANDĂRI
cu privire la obiectivele de control şi măsurile de securitate ale Sistemului de Management al Securităţii Informaţiei

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 Securităţii Informaţiei (în continuare Recomandări), reprezintă îndrumări ale Băncii Naţionale a Moldovei emise în scopul facilitării şi acordării suportului metodologic băncilor la implementarea prevederilor Secţiunii 3 din Regulamentul cu privire la sistemele de control intern în bănci, aprobat prin Hotărârea Consiliului de administraţie al Băncii Naţionale a Moldovei nr. 96 din 30.04.2010 (publicat MO nr. 98-99 din 15.06.2010) dar şi instituţiilor nebancare (prestatori de servicii de plată și emitenți de monedă electronică) la implementarea prevederilor Capitolului IV din Regulamentul cu privire la activitatea emitenţilor 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 informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Cerinţe;
b. SMV ISO/CEI 27002:2009 (ISO/IEC 27002:2005) - Tehnologia informaţiei. Tehnici de securitate. Cod de buna practică pentru managementul securităţii informaţiei;
c. SMV ISO/CEI 27005:2009 (ISO/IEC 27005:2008) - Tehnologia informaţiei. Tehnici de securitate. Managementul riscului securităţii informaţiei;
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, menţinerii şi îmbunătăţirii propriilor Sisteme de Management al Securităţii Informaţiei (în continuare - SMSI), entitățile pot aplica prezentele Recomandări, precum şi alte surse metodologice din domeniul securităţii informaţiei.

II. Termeni şi definiţii

În sensul prezentului document, se aplică următoarele noţiuni:

Securitatea informaţiei – păstrarea confidenţialităţii, integrităţii şi disponibilităţii informaţiei în orice formă a sa (electronică, pe suport hârtie, etc.) şi protejarea resurselor implicate la gestiunea acesteia, în plus, alte proprietăţi precum autenticitatea, responsabilitatea, non-repudierea şi fiabilitatea pot fi de asemenea implicate.
Confidenţialitate – proprietatea informaţiei de a fi disponibilă doar persoanelor, sau proceselor autorizate să aibă acces la ea.
Integritate – proprietatea informaţiei de a fi completă.
Disponibilitate – proprietatea informaţiei de a fi disponibilă la cererea unei persoane autorizate.
Risc de securitate a informaţiei – probabilitatea ca un anumit eveniment se va realiza şi va avea impact advers asupra confidenţialităţii, integrităţii sau disponibilităţii resurselor informaţionale;
Măsură de securitate – mijloc de reducere a riscului de securitate, inclusiv politici, standarde, proceduri, structuri organizatorice, soluţii 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 informaţional (SI) – totalitatea sistemelor de gestiune a informaţiei din cadrul unei entități, împreună cu resursele organizaţionale asociate, cum ar fi resursele informaţionale, resursele umane, structurile organizatorice.
Sistem informatic (sisteme TI – totalitatea mijloacelor software şi hardware, destinate pentru procesarea, colectarea, stocarea datelor şi a informaţiei aferente unui sau mai multor procese de activitate ale entităţii.
Sistem de Management al Securităţii Informaţiei – parte componentă a sistemului de control intern, bazat pe abordarea riscurilor de securitate a informaţiei, 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 securităţii informaţiei în cadrul entităţii;
Serviciu TI – serviciu furnizat unei entităţi (ex. aplicaţie, proces, utilizator etc.), bazat pe utilizarea Tehnologiilor Informaţionale.
Echipamentul TI – tehnică de calcul, de comunicaţie, alte mijloacele tehnice ale SI al entităţii.
Resurse – orice prezintă valoare pentru entitate, inclusiv informaţia;
Resurse informaţionale – orice informaţie utilizată în cadrul proceselor de activitate a entităţii, sau orice bun material sau nematerial implicat direct sau indirect în crearea, procesarea, stocarea şi accesarea informaţiei în cadrul proceselor de activitate (de exemplu: date, aplicaţii program, soft de sistem, echipamente de calcul, alte elemente de infrastructură);
Resursă informaţională sensibilă – resursa informaţională, compromiterea securităţii căreia poate implica riscuri majore pentru entitate.
Infrastructura TI – totalitatea mijloacelor software şi hardware inclusiv serviciile TI, destinate asigurării funcţionării sistemului informaţional.
Reţea internă a entităţii – totalitatea echipamentelor şi canalelor tehnice de comunicare între componentele infrastructurii TI în cadrul entităţii.
Zona Demilitarizată – o parte a reţelei (fizic şi/sau logic delimitată) în cadrul căreia sunt amplasate acele servicii ale entităţii ce accesează sau pot fi accesate din afara reţelei interne a entităţii (de obicei din cadrul unui extranet sau din cadrul reţelei Internet) şi are rolul de a separa resursele accesibile din exteriorul reţelei de celelalte resurse interne, în scopul prevenirii accesului nesancţionat la resursele TI din reţelele publice.
Gestiunea resurselor informaţionale – totalitatea acţiunilor direcţionate la atingerea scopurilor predefinite, inclusiv aferent asigurării securităţii acestor resurse.
Eveniment de securitate – situaţie identificată în legătură cu un sistem, un serviciu sau o reţea, care implică o posibilă încălcare a politicii de securitate a informaţiei, un eşec al măsurilor de securitate, sau informaţie ignorată anterior, dar relevantă din punct de vedere al securităţii.
Incident de securitate a informaţiei – un eveniment sau o serie de evenimente de securitate a informaţiei care au o probabilitate semnificativă de a compromite activităţile entităţii şi de a aduce ameninţări securităţii informaţiei.
Staţie de lucru – componenta SI al entităţii cu ajutorul căreia utilizatorul accesează, creează, prelucrează datele de lucru conform atribuţiilor de serviciu.

Tehnică de calcul – componentele SI al entităţii utilizate pentru accesarea, păstrarea şi prelucrarea datelor de lucru (servere, stocuri de date, staţii de lucru, imprimante, scanere etc.).
Administrator – angajat, care conform funcţiilor de serviciu este responsabil de gestionarea resurselor TI ale SI al entităţii.
Utilizator – angajat al entităţii sau a unei terţe părţi, înregistrat în cadrul SI al entităţii şi autorizat să utilizeze resursele şi serviciile sistemului informaţional al entităţii.
Posesor al datelor – subdiviziunea sau utilizatorul care poartă răspundere primară pentru corectitudinea, integritatea şi confidenţialitatea datelor.
Posesor al resurselor informaţionale – subdiviziunea ce deţine în posesia sa resursele informaţionale din cadrul SI al entităţii şi care poartă responsabilitate primară pentru securitatea lor.
Zonă de securitate – mediu controlat şi monitorizat în scopul evitării acţiunilor nesancţionate.
Zona utilizatorului – mediu situat în afara zonei de securitate în care se utilizează resursele informaţionale ale entităţii (de exemplu, utilizarea calculatoarelor portabile în afara sediului entităţii).
Informaţie publică – totalitatea datelor aferente activităţii entităţii supusă publicării conform actelor normative sau care pot fi publicate fără a implica riscuri de securitate.

III. Cadrul de organizare a securităţii informaţiei

3.1. Politica de securitate a informaţiei

Obiectiv: să asigure orientarea generală de management şi sprijinul pentru securitatea informaţiei în conformitate cu cerinţele de afacere, legislaţia şi actele normative aplicabile.

3.1.1. Conducerea entităţii elaborează şi aprobă documentul de politică a securităţii informaţiei. Politica de securitate se publică şi se comunică tuturor angajaţilor şi terţelor părţi 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 securităţii informaţiei.

3.2.1. SMSI al entităţii se stabileşte, implementează, operează, monitorizează, revizuieşte, menţine şi îmbunătăţeşte în cadrul unui proces continuu de tipul Planifică- Implementează-Verifică-Îmbunătăţeşte (Plan-Do-Check-Act).
3.2.2. Conducerea entităţii asigură suportul necesar aferent implementării şi menţinerii unui SMSI eficient.|
3.2.3. Conducerea entităţii numeşte şi desemnează responsabilitatea pentru coordonarea procesului de management al securităţii informaţiei la nivel de entitate (ofiţer pe securitatea informaţiei).
3.2.4. Organizarea SMSI se efectuează cu implicarea tuturor subdiviziunilor entităţii, în scopul asigurării unei abordări complexe şi multidisciplinare a cerinţelor de securitate.
3.2.5. Toate rolurile şi responsabilităţile pentru securitatea informaţiei se definesc în mod adecvat şi clar, se comunică şi sunt asumate în cadrul entităţii.
3.2.6. În scopul consolidării culturii organizatorice cu privire la securitatea informaţiei, entitatea încurajează şi asigură condiţiile necesare pentru menţinerea de contacte corespunzătoare cu grupurile specializate de interes şi cu asociaţiile profesionale în domeniul securităţii informaţiei.
3.2.7. SMSI al entităţii se supune unei revizuiri independente cel puţin o dată în an, în scopul asigurării funcţionării lui corespunzătoare.

3.3. Relaţia cu terţele părţi

Obiectiv: să asigure securitatea informaţiei în relaţia cu terţele părţi care prestează sau beneficiază de servicii ce implică informaţia entităţii.

3.3.1. Entitatea asigură că riscurile pentru informaţia din cadrul entităţii şi pentru sistemele de procesare a informaţiei din cadrul proceselor de afacere care implică terţe părţi se identifică, iar înainte de acordarea accesului sau iniţierea relaţiei, se implementează măsuri de securitate corespunzătoare.
3.3.2. Entitatea asigură că orice relaţie cu o terţă parte, care presupune accesul la resursele informaţionale se

iniţiază şi se conduce în baza unui acord semnat între părţi, care să acopere toate riscurile de securitate identificate.
3.3.3. Entitatea se asigură că terţa parte cu care iniţiază o relaţie de afacere are capacitatea de a gestiona corespunzător riscurile de securitate şi de a respecta cerinţele 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 activităţilor externalizate, iar sistemul de control intern, sistemul de raportare internă şi funcţiile auditului intern sunt adaptate la specificul activităţilor externalizate.
3.4.2 La externalizarea serviciilor TI de importanţă materială, entitatea se asigură că prin acţiunile de externalizare nu va crea o dependenţă operaţională excesivă faţă 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 importanţă materială, entitatea efectuează o analiză complexă a scenariilor de risc şi elaborează în acest sens un plan de asigurare a continuităţii cu proceduri detaliate de restabilire a activităţilor externalizate (inclusiv a scenariilor de revenire la producerea serviciilor cu resurse proprii, în sediul entităţii).

IV. Managementul resurselor informaţionale

4.1. Responsabilitatea pentru resurse
Obiectiv: să asigure stabilirea şi asumarea responsabilităţii pentru protecţia corespunzătoare a resurselor informaţionale ale entității.

4.1.1. Entitatea asigură că resursele informaţionale proprii sunt clar identificate, totodată fiind efectuată şi menţinută inventarierea lor. Registrul de evidenţă a resurselor este actualizat continuu, pe măsura modificărilor în lista resurselor.
4.1.2. Pentru toate resursele informaţionale se stabileşte un posesor (persoană sau subdiviziune). În cazul în care o resursă informaţională este subiectul proprietăţii a mai multor posesori, atunci drepturile şi responsabilităţile de proprietate ale posesorilor se definesc reieşind din importanţa resursei informaţionale în cadrul activităţii subdiviziunii şi necesitatea subdiviziunii de a controla resursa.
4.1.3. Entitatea stabileşte şi implementează regulile şi normele privind modul de utilizare a resurselor informaţionale şi asigură monitorizarea, respectării acestora.
4.1.4. Posesorul resurselor informaţionale 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 informaţiei
Obiectiv: să asigure faptul că informaţia beneficiază de un nivel de protecţie adecvat, proporţional importanţei ei, reglementărilor aplicabile şi ameninţărilor aferente.

4.2.1. Entitatea asigură că un clasificator al informaţiei este definit în conformitate cu legislaţia în vigoare şi necesităţile entităţii. Informaţia se clasifică pentru a indica necesitatea, priorităţile şi gradul ei de protecţie. Un sistem de clasificare a informaţiei este utilizat pentru a defini un set adecvat de niveluri de protecţie şi a comunica necesitatea măsurilor speciale de gestionare.
4.2.2. Entitatea asigură că informaţia clasificată din cadrul SI al entităţii are ataşată (la afişare, tipărire şi circulaţie) un marcator ce va indica clasa din care face parte informaţia.

V. Cerinţe de securitate privind resursele umane

5.1. Asigurarea securităţii la angajare

Obiectiv: să asigure faptul că noii angajaţi, terţele părţi, precum şi reprezentanţii acestora sunt corespunzător verificaţi înainte de acordarea accesului la sisteme, iar responsabilităţile pentru securitatea informaţiei sunt adecvat stabilite, comunicate şi asumate.

5.1.1. Entitatea asigură că responsabilităţile de securitate pentru noii angajaţi sunt comunicate la etapa de angajare.
5.1.2. Informaţia despre candidaţii la angajare sau angajaţii transferaţi se supune verificărilor de rigoare, în limitele cadrului legal. Nivelul de informaţie solicitată şi verificată trebuie să corespundă responsabilităţilor funcţionale, tipului de informaţie la care va avea acces angajatul şi riscurilor aferente funcţiei ce va fi ocupată.
5.1.3. În scopul asigurării confidențialității informaţiilor, la angajarea personalului entitatea poate prevedea încheierea unui acord de confidenţialitate. Acordul va prevedea obligaţia angajatului privind păstrarea confidenţialităţii informaţiilor la care a obţinut acces sau pe care le-au aflat, inclusiv pentru perioada de după încetarea activităţii sau în perioada suspendării activităţii.

5.2. Instruirea
Obiectiv: să asigure faptul că cerinţele de securitate sunt cunoscute în măsură suficientă de către angajaţii entității, terţele părţi, precum şi reprezentanţii acestora.

5.2.1. Entitatea asigură că angajaţii săi, după caz şi terţele părţi, beneficiază de instruire privind securitatea informaţiei la un nivel corespunzător funcţiei, responsabilităţilor şi activităţilor desfăşurate.
5.2.2. Entitatea asigură că cerinţele de securitate şi responsabilităţile individuale aferente securităţii informaţionale sunt disponibile pentru toţi angajaţii entităţii, iar după caz şi pentru terţe părţi.

5.3. Asigurarea securităţii în activitatea angajaţilor
Obiectiv: să asigure faptul că cerinţele de securitate sunt respectate necondiţionat de către angajaţii entității, terţele părţi, precum şi de reprezentanţii acestora, iar responsabilităţile şi răspunderea juridică ale acestora sunt stabilite şi conştientizate corespunzător.

5.3.1. Entitatea asigură că cerinţele de securitate a informaţiei sunt respectate necondiţionat de toţi angajaţii entităţii, precum şi de terţe părţi, în cazul în care acestea sunt autorizate să acceseze resursele informaţionale ale entităţii.
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 entității, 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 entității.

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 conţin medii de stocare se verifică minuţios înainte de casare sau transmitere, pentru a asigura că orice date importante sau produse soft licenţiate au fost înlăturate sau suprascrise într-un mod ce să asigure irecuperabilitatea lor.

VII. Managementul comunicaţiilor şi operaţiunilor

7.1. Proceduri operaţionale şi responsabilităţi
Obiectiv: să asigure operarea corectă şi în condiţii de securitate a sistemelor de procesare a informaţiei a entității.

7.1.1. Entitatea asigură că procedurile de gestiune şi operare a echipamentelor şi sistemelor TI sunt

documentate şi puse la dispoziţia persoanelor responsabile. De asemenea, toate procedurile de gestiune şi operare se menţin în stare actuală, iar toate modificările aferente lor, se autorizează la un nivel adecvat.
7.1.2. Entitatea asigură că obligaţiunile funcţionale şi domeniile de responsabilitate sunt adecvat segregate, pentru a reduce posibilităţile de utilizare abuzivă a resurselor informaţionale ale entităţii (ex. segregarea funcţiilor de elaborare, testare implementare a sistemelor informatice, administrare a bazelor de date, a sistemelor de operare, a serviciilor de reţea, administrarea şi monitorizare altor resurse informaţionale 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 producţie.

7.2. Managementul serviciilor terţelor părţi
Obiectiv: să menţină un nivel corespunzător de securitate aferent serviciilor terţelor părţi, 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 terţelor părţi sunt respectate de către terţi în procesul de prestare a serviciilor.
7.2.2. Entitatea asigură că serviciile prestate de către părţile terţe sunt monitorizate pentru a asigura corespunderea acestora cu condiţiile contractuale, politica şi normele de securitate ale entităţii. Rapoartele şi înregistrările furnizate de terţa parte se evaluează şi se revizuiesc periodic.
7.2.3. Modificările privind furnizarea serviciilor, inclusiv menţinerea şi îmbunătăţirea politicilor existente de securitate a informaţiei, procedurilor şi măsurilor de securitate se efectuează în mod controlat, ţinând cont de rezultatele reevaluării riscurilor pentru sistemele TI şi procesele de afacere.

7.3. Planificarea şi acceptanţa 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 entităţii.
7.3.2. Entitatea asigură că sistemele noi, modificările aferente sistemelor existente şi noile versiuni sunt analizate din punct de vedere al conformării la cerinţele de securitate, iar impactul lor asupra mediului de producţie 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 producţie 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 necesităţile curente şi viitoare privind capacitatea de procesare sunt estimate în scopul asigurării performanţei necesare pentru sistemele TI.

7.4. Protecţia contra softului cu potenţial dăunător
Obiectiv: să protejeze softul şi informaţia entităţii de activitatea maliţioasă a viruşilor de calculator.

7.4.1. Entitatea asigură că toate căile posibile de pătrundere a softului cu potenţial 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 soluţiile antivirus se actualizează periodic, rulează permanent şi nu pot fi stopate neautorizat.
7.4.3. Entitatea asigură că utilizatorii SI al entităţii cunosc normele de protecţie contra softului cu potenţial dăunător, în scopul diminuării riscului aferent factorului uman.
7.4.4. Entitatea asigură că activitatea la viruşi în cadrul entităţii, precum şi funcţionarea soluţiilor antivirus, sunt monitorizate adecvat.

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

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 protecţie criptografică a informaţiei.

7.9.1. Entitatea stabileşte politici şi proceduri pentru gestiunea şi utilizarea securizată a mijloacelor de protecţie criptografică a informaţiei, luând în considerare cerinţele 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 entităţii se monitorizează continuu în scopul asigurării utilizării şi gestiunii lor conform politicilor şi procedurilor stabilite.

7.10. Managementul vulnerabilităţilor
Obiectiv: să prevină existenţa vulnerabilităţilor pentru resursele entităţii.

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

7.11. Monitorizarea
Obiectiv: să asigure identificarea în timp util a activităţilor neautorizate de accesare a informaţiei şi utilizare a resurselor informaţionale.

7.11.1. Entitatea asigură că jurnalele de audit care înregistrează activităţile utilizatorului, excepţiile şi evenimentele de securitate a informaţiei sunt formate şi păstrate pentru o perioadă de timp determinată pentru a facilita investigaţiile 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 informaţionale importante au asociate jurnale de audit, în care să se înregistreze toate evenimentele ce pot avea impact asupra securităţii resurselor informaţionale.
7.11.3. Entitatea stabileşte şi implementează proceduri de monitorizare a utilizării resurselor informaţionale, iar rezultatele activităţilor 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 responsabilităţii pentru analiza jurnalelor de audit se ţine cont de necesitatea segregării funcţiilor.
7.11.5. Jurnalele de audit se păstrează şi gestionează într-o manieră ce să asigure integritatea şi autenticitatea informaţiei conţinute.
7.11.6. Entitatea asigură că toate activităţile utilizatorilor critici sunt înregistrate (ex. administratorul de sistem).
7.11.7. Ceasurile tuturor sistemelor din cadrul entităţii se sincronizează cu o sursă de timp precisă şi sigură.

VIII. Controlul accesului la resursele informaţionale

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

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

8.2. Managementul accesului utilizatorilor
Obiectiv: să asigure controlul corespunzător al accesului la informaţie şi alte resurse informaţionale ale entităţii.

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 angajaţii entităţii, cât şi utilizatorii terţelor părţi.
8.2.2. Accesul la toate resursele informaţionale ale entităţii se acordă în strictă conformitate cu necesităţile de serviciu.
8.2.3. Toate cazurile de utilizare a resurselor informaţionale ale entităţii 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 toţi utilizatorii săi deţin identificatori unici în cadrul sistemelor accesate, iar rechizitele de acces (parola, token, cheie, etc) sunt deţinute 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 entităţii (administratori, super utilizatori, etc). Procedura va asigura păstrarea în condiţii de confidenţialitate a parolelor pentru conturile respective şi disponibilitatea acestora în situaţii de incident.
8.2.7. Entitatea asigură că toate parolele implicite pentru echipamentele şi sistemele entităţii 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. Responsabilităţile utilizatorilor
Obiectiv: să prevină accesul neautorizat la resursele entității, precum şi furtul sau pierderea de informaţii.

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 entităţii 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 staţiilor de lucru neprotejate.

8.4. Controlul accesului la reţea
Obiectiv: să protejeze informaţia şi serviciile de reţea.

8.4.1. Entitatea asigură că toate conexiunile la reţeaua sa sunt autorizate şi efectuate numai după analiza potenţialului lor impact asupra securităţii informaţiei.
8.4.2. Entitatea asigură că identificarea automată a echipamentului conectat la reţea este utilizată ca o metodă de autentificare a conexiunilor.
8.4.3. Entitatea asigură că tot traficul de intrare în reţeaua corporativă şi de ieşire din reţea 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 reţelelor WiFi în cadrul entităţii se controlează într-un mod strict. Accesul la reţelele WiFi se autorizează în mod corespunzător. Utilizarea protocolului WEP în cadrul reţelelor WiFi trebuie evitată.
8.4.6. Conexiunea la distanţă a utilizatorilor prin intermediul reţelelor publice se autorizează în mod corespunzător. Entitatea asigură că soluţii eficiente de securitate sunt utilizate pentru autentificarea nominală a utilizatorilor, limitarea accesului la resursele necesare şi asigurarea confidenţialităţii comunicaţiilor.
8.4.7. Entitatea asigură că utilizatorii serviciilor în reţea ale entităţii au acces doar la serviciile pentru care au fost autorizaţi în mod specific.
8.4.8. Entitatea asigură că accesul la interfeţele de administrare pentru echipamentele de reţea 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 staţiile utilizatorilor şi pe servere doar pentru utilizatorii autorizaţi.
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, aplicaţiile 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 staţiile 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 necesităţilor de serviciu. Instalarea şi rularea utilitarelor de sistem nu trebuie să fie permisă.
8.5.6. Entitatea asigură că utilizarea aplicaţiilor şi serviciilor de sistem care asigură dirijarea la distanţă a staţiilor de lucru este limitată şi strict monitorizată.
8.5.7. Instalarea de aplicaţii program pe staţiile de lucru ale utilizatorilor se efectuează doar de persoanele responsabile.

8.6. Accesul la aplicaţii şi informaţii
Obiectiv: să prevină accesul neautorizat la informaţia deţinută în sistemele de aplicaţii.

8.6.1. Accesul la funcţiile sistemelor de aplicaţii şi informaţia din sisteme se restricţionează în conformitate cu politica de control al accesului stabilită în entitate.
8.6.2. Entitatea asigură că sistemele de aplicaţii dispun de măsuri de protecţie suficiente şi eficiente în scopul limitării accesului doar pentru utilizatorii autentificaţi şi doar în limita drepturilor autorizate.

IX. Achiziţionarea, dezvoltarea şi mentenanţă sistemelor de aplicaţii

9.1. Cerinţele de securitate pentru sistemele aplicative
Obiectiv: să asigure că cerinţele de securitate sunt considerate la planificarea, elaborarea, implementarea şi modificarea sistemelor de aplicaţii.

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

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

9.2.1. Datele de intrare ale aplicaţiilor se validează pentru a se asigura că aceste date sunt corecte şi corespunzătoare.
9.2.2. În cadrul aplicaţiilor se implementează verificări de validare pentru a detecta orice modificare a informaţiei prin procesare eronată sau prin acte deliberate.
9.2.3. Entitatea asigură că cerinţele pentru integritatea mesajelor electronice în cadrul aplicaţiilor sunt stabilite şi măsuri de securitate corespunzătoare sunt identificate şi implementate.
9.2.4. Datele de ieşire din cadrul aplicaţiilor se validează pentru a se asigura că procesarea informaţiei stocate este corectă.
9.2.5. Toate activităţile 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 aplicaţii.

9.3.1. Entitatea asigură că toate modificările aferente mediului de operare pentru sistemele de aplicaţii sunt strict controlate. Orice modificare în prealabil se testează şi se autorizează.
9.3.2. Mediile de operare pentru sistemele de aplicaţii critice se izolează de alte medii, pentru a evita

compromiterea securităţii lor în rezultatul compromiterii securităţii sistemelor mai puţin critice.
9.3.3. Entitatea asigură că accesul la codurile sursă ale sistemelor de aplicaţii este strict limitat.
9.3.4. Fişierele de configuraţie ale sistemelor de aplicaţie se protejează corespunzător. Parolele existente în fişierele de configuraţie se criptează.

9.4. Securitatea în procesul de dezvoltare şi de suport
Obiectiv: să menţină securitatea sistemelor de aplicaţii.

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

X. Managementul incidentelor de securitate a informaţiei

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

10.1.1. Entitatea stabileşte o procedură formală privind managementul incidentelor de securitate a informaţiei.
10.1.2. Pentru raportarea în timp util a incidentelor de securitate a informaţiei, entitatea asigură un singur punct de contact pentru toţi angajaţii săi, contractanţii şi utilizatorii terţi la care aceştia vor fi instruiţi să raporteze cât mai curând orice incident sau problemă legată de utilizarea sistemelor şi tehnologiilor entităţii.
10.1.3. Toţi angajaţii, contractanţii şi utilizatorii terţi ai sistemelor şi serviciilor informaţionale se instruiesc pentru a raporta orice vulnerabilitate de securitate observată sau suspectată în cadrul sistemelor sau a serviciilor.

10.2. Reacţiunea la incidentele de securitate
Obiectiv: să asigure reacţiunea corespunzătoare la incidentele de securitate.

10.2.1. Entitatea asigură că responsabilităţile şi procedurile de reacţiune la incidentele de securitate sunt explicit stabilite în cadrul entităţii, pentru a asigura un răspuns rapid, eficient şi sistematic la incidentele de securitate a informaţiei.
10.2.2. Probele aferente incidentelor de securitate se colectează şi păstrează în condiţii de siguranţă în scopul investigării incidentelor şi asigurării suportului în cazul eventualelor acţiuni legale legate de incidentele petrecute.
10.2.3. Entitatea asigură un proces de analiză a incidentelor de securitate şi învăţarea din acestea, pentru a nu admite repetarea incidentelor similare.
10.2.4. Entitatea asigură înregistrarea, documentarea completă şi raportarea incidentelor de securitate.

XI. Managementul continuităţii activităţii

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

entităţii.

11.1.1. Entitatea defineşte şi implementează un proces complex de planificare a continuităţii activităţii şi restabilire a sistemelor TI în situaţii de incident.
11.1.2. Entitatea elaborează, testează, aprobă şi menţine în stare actuală un plan de continuitate a afacerii şi de restabilire în situaţii de incident.
11.1.3. Planul de continuitate a afacerii se elaborează în baza unei analize la impact asupra proceselor de activitate ale entităţii provocat de riscurile de securitate a informaţiei.
11.1.4. Planul de continuitate a afacerii se revizuieşte cel puţin anual.

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

11.2.1. Cerinţele afacerii pentru nivelul de continuitate şi restabilire a sistemelor şi serviciilor TI se stabilesc şi se aprobă în cadrul entităţii (ex. timpul de restabilire, momentul restabilirii datelor, etc).
11.2.2. Entitatea asigură proceduri documentate de restabilire a sistemelor şi serviciilor critice conform necesităţilor 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 toţi angajaţii antrenaţi în procesul de restabilire sunt conştienţi de acţiunile efectuate.
11.2.4. Entitatea asigură un local de rezervă şi infrastructura necesară pentru restabilirea sistemelor şi serviciilor critice în situaţii de incident major.
11.2.5. Entitatea asigură că localul de rezervă nu este expus aceloraşi riscuri precum localul de bază şi dispune de capacităţile necesare pentru susţinerea procesului de restabilire.

XII. Conformitatea

12.1. Conformitatea cu cerinţele legale şi regulatorii
Obiectiv: să evite încălcarea actelor normative ce ţin de securitatea informaţiei.

12.1.1. Entitatea identifică şi este la curent cu toate modificările aferente actelor normative aplicabile în sfera securităţii informaţiei.
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 protecţia corespunzătoare a datelor cu caracter personal în conformitate cu actele normative. Considerate trebuie să fie atât datele personale ale clienţilor, cât şi datele angajaţilor entităţii.

XIII. Securitatea datelor de carduri bancare

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

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

XIV. Auditul intern al securităţii informaţiei

14.1. Planificarea şi organizarea auditului
Obiectiv: să asigure organizarea şi planificarea eficientă a auditului intern al securităţii informaţiei.

14.1.1. Entitatea asigură că auditorii interni TI sunt independenţi în raport cu responsabilităţile operaţionale 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 puţin o dată în trei ani. Suplimentar, se asigură că audite ale eficienţei şi eficacităţii proceselor TI importante sunt efectuate.
14.1.4. Auditul intern al SMSI al entităţii se efectuează cel puţin anual.

Vezi și

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

Sursa URL:
https://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] https://bnm.md/ro/search?hashtags[0]=securitatea informației [4] https://bnm.md/ro/search?hashtags[0]=confidențialitate [5] https://bnm.md/ro/search?hashtags[0]=integritatea informației [6] https://bnm.md/ro/search?hashtags[0]=risc de securitate a informației [7] https://bnm.md/ro/search?hashtags[0]=sistem informatic