Universitatea Tehnică a Moldovei

Facultatea *Calculatoare, Informatică şi Microelectronică*

Specialitatea *Tehnologii Informaţionale*

Raport

Tema:*"Sistem de management al securitatii informationale"*

Disciplina: "Tehnici de securitate informationala"

A efectuat: Student grupa TI-231 FR Apareci Aurica

Chişinău 2025

Cuprins

Introducere

1.1 Contextul standardului ISO/IEC 27001

Protejarea informațiilor a devenit o prioritate esențială pentru orice organizație, indiferent de dimensiune sau domeniu de activitate. Standardul internațional ISO/IEC 27001 oferă un cadru recunoscut la nivel global pentru implementarea, menținerea și îmbunătățirea unui Sistem de Management al Securității Informației (SMSI).

Acest standard stabilește cerințele pentru identificarea riscurilor informaționale, implementarea controalelor adecvate și evaluarea continuă a eficienței măsurilor de protecție. ISO/IEC 27001 nu se referă doar la aspectele tehnice ale securității, ci și la aspectele organizaționale și umane, promovând o abordare holistică asupra gestionării riscurilor legate de informații. Adoptarea acestui standard ajută organizațiile să reducă semnificativ expunerea la incidente de securitate, să respecte reglementările în vigoare și să câștige încrederea clienților și partenerilor prin asigurarea confidențialității, integrității și disponibilității datelor.

1.2 Scopul lucrării

Scopul lucrării este de a simula procesul de implementare a unui sistem de securitate informațională în conformitate cu cerințele standardului ISO/IEC 27001 într-o **organizație virtuală**, denumită **DataVault.** Această simulare urmărește să:

- Evidențieze importanța gestionării proactive a riscurilor de securitate;
- Identifice și clasifice activele informaționale;
- Evalueze potențialele amenințări și riscurile asociate;
- Propună măsuri de control corespunzătoare pentru reducerea riscurilor;
- Elaboreze o politică formală de securitate;
- Dezvolte o aplicație software cu interfață grafică pentru sprijinirea activităților descrise.

Prin această abordare integrată, se urmărește dobândirea unei înțelegeri aplicate a proceselor de management al securității informației și dezvoltarea competențelor practice în aplicarea standardelor internaționale.

1.3 Metodologia de analiză a securității informaționale

Analiza securității informaționale în cadrul acestei lucrări a fost realizată în mai mulți pași succesivi, urmând o metodologie inspirată de cerințele ISO/IEC 27001 și completată de bune practici din domeniul securității cibernetice:

1. Identificarea și clasificarea activelor informaționale pe categorii (informații, software, hardware);

2. Determinarea amenințărilor și vulnerabilităților care pot afecta aceste active;
3. Evaluarea riscurilor printr-o metodă calitativă, utilizând o matrice care ia în considerare probabilitatea și impactul fiecărei amenințări;
4. Stabilirea și aplicarea controalelor de securitate recomandate de ISO/IEC 27001 – Anexa A;
5. Redactarea politicii de securitate pentru organizație, în acord cu scopurile și obiectivele sale;
6. Proiectarea unei aplicații software cu GUI care să permită gestionarea activelor, riscurilor și controalelor într-un mod practic și centralizat.

Această metodologie permite o înțelegere completă a modului în care poate fi gestionat securizat un mediu informațional, simulând condițiile reale întâlnite într-o organizație modernă.

Prezentarea organizației

2.1 Denumirea și domeniul de activitate

Organizația virtuală analizată în cadrul acestei lucrări poartă denumirea DataVault și activează în domeniul tehnologiei informației, având ca obiect principal de activitate furnizarea de servicii cloud pentru stocarea, criptarea și backup-ul datelor.

DataVault oferă o platformă SaaS (Software as a Service) care permite companiilor mici și mijlocii să-și securizeze datele critice prin soluții automatizate de backup criptat, sincronizare în cloud și restaurare rapidă în caz de incidente. Serviciile se adresează în special organizațiilor care nu dispun de infrastructură IT proprie robustă, dar care doresc să-și asigure continuitatea operațională și conformitatea cu reglementările privind protecția datelor (ex. GDPR).

2.2 Structura organizațională

Organizația are o structură ierarhică funcțională care permite o delimitare clară a responsabilităților și o comunicare eficientă între nivelurile de conducere și execuție. Atribuțiile fiecărui compartiment sunt bine definite, astfel încât activitățile să se desfășoare coerent și controlat în contextul cerințelor de securitate informațională.

Denumire departament	Descriere	Numar angajati
IT & dezvoltare software	responsabil de dezvoltarea și întreținerea aplicației DataVault;	20
infrastructură și rețea	gestionează infrastructura serverelor, conexiunile VPN, firewall-ul și politicile de securitate la nivel de rețea;	10
suport clienți	oferă asistență tehnică și operațională pentru utilizatorii platformei;	8
juridic și conformitate	se ocupă de aspectele legale și de respectarea reglementărilor privind securitatea datelor;	4
financiar/resurse umane	gestionează procesele administrative, salariale și de recrutare;	5

management executiv	stabileşte direcţiile strategice ale companiei şi supervizează implementarea politicilor de guvernanţă şi securitate.	5

Această organizare permite o bună coordonare între echipe şi o alocare eficientă a resurselor pentru asigurarea securităţii informaţionale. DataVault are în total 52 de angajaţi distribuiţi pe departamente după cum sunt indicati in tabelul de mai sus.

Identificarea activelor informaționale

În cadrul oricărei organizații, activele informaționale reprezintă elemente esențiale pentru desfășurarea activităților curente, iar protejarea acestora este o componentă critică a managementului securității informației. Conform standardului ISO/IEC 27001, activele trebuie identificate, clasificate și protejate în funcție de valoarea lor pentru organizație și de impactul potențial al compromiterii lor. Mai jos este prezentată clasificarea activelor principale ale organizației DataVault.

3.1 Clasificarea activelor

3.1.1 Informația

Informația reprezintă cel mai valoros activ pentru *DataVault,* deoarece întreaga activitate a organizației se bazează pe procesarea, stocarea și protejarea unor volume mari de date sensibile. Compania gestionează informații esențiale atât din surse interne, cât și externe, iar compromiterea acestora ar putea avea un impact sever asupra reputației, continuității operaționale și conformității legale. Datele clienților, în special cele salvate prin soluțiile de backup criptat, trebuie păstrate în condiții stricte de confidențialitate și integritate. Principalele active informaționale identificate includ:

- Baza de date a clienților (nume, emailuri, date de facturare);
- Fișiere de backup stocate în cloud (date criptate ale clienților);
- Documentație tehnică a platformei și procese interne;
- Date privind incidentele de securitate raportate;
- Credențiale și chei de criptare.

Aceste date necesită măsuri speciale de protecție pentru a asigura **confidențialitatea, integritatea și disponibilitatea** lor.

3.1.2 Software

Software-ul utilizat și dezvoltat de DataVault este fundamental pentru furnizarea serviciilor cloud și pentru menținerea infrastructurii organizației. Active software relevante:

- Aplicația principală DataVault (frontend + backend);
- API-ul de interacțiune cu serviciile de backup și criptare;
- Sistemul intern de ticketing și CRM;
- Soluții software pentru autentificare și monitorizare acces (ex. IdentityServer, Grafana);
- Sisteme de operare și licențe software utilizate pe servere și stațiile de lucru.

Securitatea acestor componente software este vitală pentru prevenirea exploatării vulnerabilităților sau a accesului neautorizat.

3.1.3 Hardware

Activele hardware formează infrastructura fizică esențială pentru funcționarea zilnică, dezvoltarea și întreținerea serviciilor oferite de DataVault. Fără aceste echipamente, procesele critice ale organizației, precum rularea aplicației, testarea noilor funcționalități sau operarea sistemelor de backup, nu ar putea fi realizate în condiții de siguranță și eficiență. În plus, fiabilitatea hardware-ului contribuie direct la menținerea disponibilității serviciilor cloud și la reducerea timpilor de întrerupere în caz de incidente tehnice. Activele hardware identificate includ:

- Servere fizice pentru testare și dezvoltare;
- Laptopuri și stații de lucru ale angajaților;
- Echipamente de stocare de tip NAS (Network Attached Storage);
- UPS-uri și sisteme de protecție electrică;
- Echipamente de backup local pentru medii critice.

Acestea trebuie protejate atât împotriva defecțiunilor, cât și a riscurilor fizice precum furtul sau accesul neautorizat în spațiile tehnice.

3.1.4 Rețea

Infrastructura de rețea este esențială pentru asigurarea conectivității continue, rapide și securizate între toate componentele sistemelor informatice utilizate de DataVault. Având în vedere că platforma companiei operează în regim cloud și deservește clienți prin internet, rețeaua trebuie să fie performantă, fiabilă și protejată împotriva atacurilor cibernetice. Orice întrerupere, vulnerabilitate sau breșă la nivel de rețea poate duce la compromiterea confidențialității datelor sau la întreruperea serviciilor esențiale. Active de rețea includ:

- VPN-ul intern utilizat pentru acces de la distanță;
- Routere, switch-uri și firewall-uri dedicate;
- Soluții de monitorizare a traficului de rețea;
- Politici și reguli de segmentare a rețelei interne;
- Loguri și jurnale de rețea.

Integritatea și confidențialitatea traficului de rețea sunt esențiale pentru prevenirea atacurilor precum interceptarea datelor sau compromiterea infrastructurii interne.

Identificarea amenințărilor de securitate

Securitatea informațională presupune nu doar protejarea activelor, ci și identificarea și înțelegerea riscurilor potențiale la care acestea sunt expuse. Amenințările pot avea origini interne sau externe și pot afecta confidențialitatea, integritatea sau disponibilitatea informațiilor și sistemelor. Pentru organizația DataVault, aceste riscuri sunt semnificative având în vedere natura serviciilor oferite și tipul de date gestionate.

4.1 Amenințări interne și externe

Amenințările interne sunt generate de acțiuni sau neglijențe ale persoanelor din interiorul organizației, precum angajații, colaboratorii sau chiar contractanții temporari. Aceste amenințări pot fi intenționate, în cazul unor acțiuni rău-voitoare (ex: sustragerea de date), sau neintenționate, ca urmare a lipsei de instruire sau a erorilor umane. Chiar dacă nu sunt la fel de mediatizate ca atacurile externe, amenințările interne sunt adesea mai periculoase, deoarece provin de la persoane care au deja acces legitim la sistemele organizației.

Un exemplu relevant îl constituie accesul neautorizat la date confidențiale de către angajați care nu au nevoie de aceste informații pentru desfășurarea atribuțiilor de serviciu. În lipsa unor politici clare de control al accesului și a unei monitorizări corespunzătoare, aceste situații pot trece neobservate.

De asemenea, erorile umane în configurarea sistemelor, modificarea parametrilor de rețea sau procesarea datelor pot duce la breșe de securitate involuntare. Lipsa instruirii continue în domeniul securității cibernetice determină comportamente necorespunzătoare, precum folosirea parolelor slabe, accesarea linkurilor nesigure sau partajarea datelor prin canale nesecurizate. Neglijența în manipularea echipamentelor, precum pierderea unui laptop necriptat sau lăsarea accesului deschis în rețea, reprezintă un alt tip de risc intern. La fel, utilizarea de software nesigur sau nelicențiat în scop personal poate introduce vulnerabilități în sistem, fie prin malware, fie prin lipsa actualizărilor de securitate.

Amenințările externe, în schimb, sunt generate de factori din afara organizației și includ în principal atacuri cibernetice deliberate. Acestea pot lua forme diverse, cum ar fi phishing-ul, prin care atacatorii încearcă să obțină credențiale sensibile de la angajați, sau ransomware-ul, care criptează datele și solicită răscumpărări pentru deblocare.

Una dintre cele mai frecvente amenințări externe este interceptarea traficului de rețea prin atacuri de tip Man-in-the-Middle, mai ales în absența criptării corespunzătoare a comunicațiilor. În același timp, furtul fizic al echipamentelor – cum ar fi laptopurile cu acces la sisteme critice – poate duce la scurgerea de date sensibile, mai ales dacă dispozitivele nu sunt protejate prin criptare și autentificare dublă.

O altă categorie de riscuri externe este reprezentată de exploatarea vulnerabilităților software – de exemplu, în aplicațiile web sau API-urile oferite de platforma DataVault. Aceste vulnerabilități pot fi folosite de atacatori pentru a executa cod malițios, a accesa baze de date sau a compromite conturile utilizatorilor. Nu în ultimul rând, accesul neautorizat la infrastructura cloud, cauzat de setări greșite, parole compromise sau lipsa autentificării multifactor, poate permite intruși să obțină control asupra unor resurse critice ale companiei.

4.2 Corespondența între active și amenințări

Pentru a putea evalua în mod eficient riscurile de securitate, este esențial să se stabilească o legătură directă între activele informaționale identificate și posibilele amenințări la care acestea sunt expuse. Această corespondență permite înțelegerea modului în care fiecare activ poate fi afectat de incidente de securitate și oferă un cadru clar pentru prioritizarea măsurilor de protecție. În continuare, este prezentat un tabel care asociază principalele categorii de active din cadrul organizației cu cele mai relevante tipuri de amenințări identificate în procesul de analiză.

Activ	**Amenințări asociate**
Informație	Exfiltrare de date, acces neautorizat, pierdere accidentală, atacuri de tip phishing
Software	Exploatarea vulnerabilităților (XSS, CSRF, injection), actualizări întârziate
Hardware	Furt fizic, defecțiuni hardware, pierderi cauzate de întreruperi de curent
Rețea	Atacuri DoS/DDoS, interceptarea traficului, configurări greșite, atacuri brute force

Identificarea clară a relației dintre active și amenințările potențiale constituie o bază solidă pentru evaluarea riscurilor, întrucât permite concentrarea eforturilor de securitate asupra elementelor critice. Această abordare ajută organizația să își prioritizeze resursele și să implementeze controale specifice, adaptate fiecărui tip de activ și contextului său operațional. În etapa următoare, pe baza acestei corespondențe, se va realiza analiza nivelului de risc asociat fiecărui scenariu, utilizând o metodă calitativă de evaluare.

Evaluarea riscurilor de securitate informațională

Evaluarea riscurilor reprezintă un pas esențial în cadrul procesului de management al securității informaționale, fiind necesară pentru a identifica și măsura impactul potențial al diferitelor amenințări asupra activelor organizației. Scopul acestei etape este de a determina nivelul de expunere la risc și de a sprijini luarea deciziilor privind implementarea controalelor adecvate. În această lucrare, se aplică o metodă calitativă de evaluare, adaptată la specificul organizației virtuale DataVault.

5.1 Metodologia de evaluare (calitativă / cantitativă)

Metoda calitativă de evaluare a riscurilor reprezintă o abordare accesibilă și eficientă pentru identificarea și clasificarea riscurilor de securitate informațională, în special în contexte în care nu sunt disponibile date numerice exacte sau în care se dorește o analiză inițială rapidă. Această metodă presupune estimarea subiectivă a probabilității de apariție a unei amenințări, precum și a impactului potențial pe care aceasta l-ar putea avea asupra unui activ informațional critic.

Cele două variabile utilizate — probabilitatea și impactul — sunt evaluate pe o scală calitativă simplificată, formată din trei niveluri:

- *Probabilitate*: Scăzută (posibilitate redusă de apariție), Medie (posibilitate realistă în contextul actual), Ridicată (șanse mari de manifestare pe termen scurt sau mediu);
- *Impact*: Scăzut (consecințe minore, reversibile), Mediu (afectare parțială a serviciilor sau a datelor), Ridicat (pierderi semnificative, afectare operațională sau reputațională gravă).

Această metodă nu implică calcule matematice sau modele statistice complexe, ci se bazează pe judecăți de valoare argumentate, experiență profesională, cunoștințe despre contextul organizațional și istoricul incidentelor. Evaluatorii folosesc observații directe, consultări cu personalul cheie și revizuirea documentației pentru a aloca un nivel de probabilitate și unul de impact fiecărei amenințări identificate.

Prin combinarea acestor două dimensiuni, se obține o clasificare a riscurilor în patru categorii:

Risc redus – necesită doar monitorizare ocazională;

Risc moderat – necesită măsuri de control planificate;

Risc semnificativ – necesită intervenție activă și monitorizare continuă;

Risc critic – impune acțiuni imediate și controale stricte pentru a evita compromiterea activelor.

5.2 Matricea riscurilor

Pentru a facilita înțelegerea și compararea riscurilor, se utilizează o matrice de risc care combină cele două dimensiuni fundamentale: probabilitatea de apariție a unei amenințări și impactul asupra activului afectat. Matricea are o structură de tip 3x3, unde fiecare celulă reflectă un nivel de risc estimat, oferind astfel un instrument vizual clar pentru luarea deciziilor în materie de securitate.

Impact \ Probabilitate	Scăzută	Medie	Ridicată
Ridicat	Moderat	Semnificativ	**Critic**
Mediu	Redus	Moderat	Semnificativ
Scăzut	Redus	Redus	Moderat

5.3 Nivelurile de risc identificate

Pe baza corespondenței dintre active și amenințări, precum și folosind matricea prezentată anterior, au fost identificate următoarele niveluri de risc pentru DataVault:

Activ	Amenințare	Probabilitate	Impact	Nivel de risc
Informație	Exfiltrare de date	Ridicată	Ridicat	**Critic**
Software	Vulnerabilități de tip injection	Medie	Ridicat	**Semnificativ**
Hardware	Defecțiuni hardware	Scăzută	Mediu	**Moderat**
Rețea	Interceptarea traficului (MitM)	Medie	Mediu	**Semnificativ**
Informație	Pierdere accidentală	Medie	Ridicat	**Semnificativ**
Rețea	Atac DoS/DDoS	Scăzută	Ridicat	**Semnificativ**
Hardware	Furt fizic al laptopului	Medie	Mediu	**Semnificativ**

Această evaluare permite luarea unor decizii informate cu privire la prioritizarea controalelor de securitate, în funcție de nivelul de risc asociat fiecărui activ și scenariu.

Controale de securitate implementate

Implementarea controalelor de securitate reprezintă etapa în care organizația aplică măsuri concrete pentru a reduce nivelul de risc identificat anterior. Aceste controale trebuie alese în mod justificat, documentate și adaptate la specificul fiecărui activ. În cadrul organizației virtuale DataVault, măsurile de securitate sunt aliniate cu standardul ISO/IEC 27001 și sunt structurate în trei categorii: tehnice, administrative și fizice.

6.1 Selectarea măsurilor conform ISO 27001

Standardul ISO/IEC 27001:2022 reprezintă un cadru internațional recunoscut pentru implementarea unui sistem de management al securității informației (SMSI), iar *Anexa A* a acestui standard oferă un set detaliat de 93 de controale de securitate. Aceste controale sunt organizate în patru categorii tematice majore, reflectând o abordare cuprinzătoare asupra protejării informațiilor și infrastructurii organizaționale:
Controale organizaționale – vizează stabilirea politicilor, definirea rolurilor, responsabilităților și structurilor de guvernanță privind securitatea informației;

- Controale tehnologice – se referă la protecția activelor prin mijloace tehnice, cum ar fi criptarea, autentificarea, monitorizarea și controlul accesului;
- Controale fizice – au ca scop protejarea mediului fizic și a echipamentelor împotriva accesului neautorizat sau deteriorării;
- Controale legale și contractuale – asigură conformitatea cu legislația în vigoare, reglementările naționale și cerințele contractuale impuse de terți.

În cadrul organizației *DataVault*, selecția controalelor s-a realizat în mod rațional și justificat, ținând cont de riscurile identificate anterior, de resursele disponibile și de nivelul de maturitate al sistemului IT. S-a urmărit aplicarea principiului proporționalității, prin care fiecărui risc i se atribuie un control care să ofere protecție eficientă fără a supradimensiona sau subestima măsura necesară.
Printre controalele selectate și implementate în cadrul sistemului de securitate al DataVault se numără:

A.5.1 – Politici de securitate a informației: stabilește cadrul general pentru adoptarea, comunicarea și revizuirea politicilor de securitate;

A.6.1 – Managementul resurselor și al rolurilor: definește clar responsabilitățile individuale pentru protejarea informațiilor;

A.8.1 – Controlul accesului logic: asigură că accesul la activele informaționale este acordat doar persoanelor autorizate, conform principiului minimului privilegiu;

A.9.1 – Criptarea informației: impune utilizarea de metode criptografice sigure pentru protejarea datelor atât în repaus, cât și în tranzit;

A.12.6 – Managementul vulnerabilităților tehnice: presupune identificarea, evaluarea și remedierea vulnerabilităților în software și infrastructură;

A.13.1 – Securitatea rețelei: garantează implementarea unor măsuri de protecție și monitorizare pentru rețeaua internă și externă a companiei.

Fiecare dintre aceste controale este documentat, auditat periodic și adaptat la nevoile specifice ale organizației, contribuind activ la reducerea riscurilor și la asigurarea unui mediu operațional sigur și conform cu bunele practici internaționale.

6.2 Descrierea controalelor tehnice, administrative și fizice

Pentru o protecție eficientă a activelor informaționale, organizația DataVault a adoptat o abordare stratificată a securității, implementând controale tehnice, administrative și fizice. Acestea se completează reciproc și oferă o apărare în profunzime, reducând riscurile legate de acces neautorizat, pierdere de date, incidente cibernetice și deficiențe operaționale.

Controale tehnice

Controalele tehnice sunt cele implementate la nivelul sistemelor informatice, rețelelor și aplicațiilor. Ele asigură protecție automatizată și permanentă împotriva amenințărilor digitale și a erorilor umane, și sunt esențiale pentru menținerea integrității și confidențialității informațiilor procesate de DataVault. Printre principalele măsuri tehnice implementate se regăsesc:

- **Criptarea datelor** în tranzit și în repaus, folosind algoritmi avansați (TLS 1.3, AES-256), aplicabilă atât fișierelor clienților, cât și bazelor de date interne;
- **Autentificare multifactor (MFA)** obligatorie pentru accesul la platformele interne și conturile privilegiate;
- **Controlul accesului pe bază de roluri (RBAC)**, care limitează accesul utilizatorilor doar la informațiile strict necesare;
- **Sisteme de detecție a intruziunilor (IDS)** și firewall-uri inteligente (WAF) care filtrează traficul malițios și previn atacurile de tip injection;
- **Monitorizare și jurnalizare continuă** a activității în infrastructură, cu alerte automate la comportamente anormale;
- **Soluții de backup automatizat și replicare a datelor** în locații geografice diferite.

Controale administrative

Controalele administrative vizează procesele, politicile și responsabilitățile organizaționale. Ele stabilesc cadrul de guvernanță și definesc modul în care angajații, colaboratorii și partenerii trebuie să gestioneze informațiile și să reacționeze în fața riscurilor. Măsurile administrative adoptate includ:

- **Politici oficiale de securitate a informației**, aprobate de conducere și comunicate întregului personal;
- **Reguli documentate de control al accesului, clasificare a informațiilor și manipulare a datelor sensibile**;
- **Atribuirea clară a responsabilităților legate de securitate** în cadrul fiecărui departament;
- **Programe de instruire periodică** pentru angajați privind bunele practici, recunoașterea atacurilor de tip phishing și protejarea echipamentelor mobile;
- **Procese de audit intern** și evaluare a conformității cu politicile de securitate;
- **Proceduri clare de răspuns la incidente**, cu scenarii predefinite pentru intervenție și notificare a părților afectate.

Controale fizice

Controalele fizice asigură protejarea infrastructurii hardware și a spațiilor critice împotriva accesului neautorizat, vandalismului, furtului sau dezastrelor naturale. Deși DataVault este o companie orientată către cloud, aceasta deține și administrează echipamente esențiale în centre proprii sau colocalizate.
Măsurile fizice implementate sunt:

- **Acces controlat în zonele tehnice**, cu badge-uri electronice, camere de supraveghere (CCTV) și înregistrare a accesului;
- **Echipamente server montate în rackuri securizate**, cu blocare fizică și senzori de temperatură/umiditate;
- **Utilizarea de UPS-uri și generatoare de rezervă**, pentru a preveni întreruperile cauzate de pene de curent;
- **Restricționarea accesului vizitatorilor și personalului neautorizat** în sălile tehnice;
- **Politici privind echipamentele mobile**, care prevăd utilizarea exclusivă a dispozitivelor aprobate și criptarea obligatorie a acestora.

Prin aplicarea combinată a acestor trei tipuri de controale, DataVault asigură o acoperire completă a vectorilor de risc, contribuind la menținerea unui sistem de securitate robust, aliniat cerințelor internaționale și așteptărilor clienților.

6.3 Plan de tratament al riscurilor

După evaluarea riscurilor și identificarea nivelurilor acestora, următorul pas în cadrul sistemului de management al securității informației constă în elaborarea unui plan de tratament al riscurilor. Scopul acestui plan este de a reduce riscurile la un nivel acceptabil prin aplicarea unor controale corespunzătoare, în concordanță cu natura amenințărilor, valoarea activelor și resursele disponibile. Planul include o serie de elemente esențiale:

Riscul identificat – descrierea clară a riscului evaluat;

Controlul aplicat – măsura de securitate aleasă pentru tratarea riscului;

Standardul de referință – codul controlului din Anexa A a ISO/IEC 27001;

Responsabilul desemnat – persoana sau echipa responsabilă de implementare;

Termenul de implementare – limita de timp stabilită pentru aplicarea controlului;

Statusul – stadiul în care se află măsura (planificat, în curs, implementat);

Nivelul de risc rezidual – nivelul de risc estimat după aplicarea măsurii.

Această abordare sistematică permite urmărirea progresului în aplicarea măsurilor și evaluarea eficienței acestora în reducerea riscurilor. Un fragment ilustrativ din planul de tratament pentru DataVault este prezentat mai jos:

Riscul identificat	Control aplicat	Cod ISO	Responsabil	Termen	Status	Risc rezidual
Exfiltrare date clienți	Criptare + MFA	A.8.28	IT Manager	30 zile	Implementat	Redus
Exploatarea vulnerabilităților web	Audit cod + WAF	A.12.1	Dev Lead	60 zile	În curs	Moderat
Furt fizic echipamente mobile	Politici MDM + criptare disc	A.7.7	Admin Sistem	45 zile	Planificat	Redus
Interceptarea traficului rețelei	VPN criptat + IDS	A.13.1	Inginer Rețea	20 zile	Implementat	Redus

Planul este revizuit periodic de către echipa de securitate și aprobat de conducerea organizației. În cazul apariției unor incidente, a modificării structurii organizaționale sau a evaluărilor externe (ex. audituri), planul este actualizat pentru a reflecta realitatea operațională și a asigura o protecție continuă și relevantă.

Politica de securitate a informației

Politica de securitate a informației reprezintă documentul fundamental care stabilește cadrul de referință pentru protejarea activelor informaționale ale organizației. Aceasta reflectă angajamentul conducerii de a asigura confidențialitatea, integritatea și disponibilitatea informațiilor și definește regulile generale privind comportamentul acceptabil, măsurile de protecție și mecanismele de monitorizare.

7.1 Principii generale și obiective

Politica de securitate a informației a organizației se bazează pe următoarele principii fundamentale:

Confidențialitatea – asigurarea că informațiile sensibile sunt accesibile doar persoanelor autorizate;

Integritatea – menținerea acurateței completitudinii datelor/sistemelor;

Disponibilitatea – garantarea accesului la informații și sisteme atunci când este necesar.

Obiectivele majore ale politicii sunt:

- Prevenirea pierderilor de date sau a accesului neautorizat;
- Asigurarea unui cadru clar pentru tratarea riscurilor de securitate;
- Conformitatea cu standardele internaționale (ISO/IEC 27001) și reglementările legale;

Promovarea unei culturi organizaționale orientate spre securitate și responsabilitate digitală.

7.2 Responsabilități și roluri

Pentru aplicarea eficientă a politicii, sunt definite roluri și responsabilități clare în cadrul organizației:

Conducerea executivă (CEO, CIO) – aprobă politica și susține resursele necesare implementării;

Responsabilul cu securitatea informației (CISO) – coordonează aplicarea măsurilor de securitate, gestionează incidentele și supraveghează revizuirea periodică a politicii;

Managerii de departamente – implementează controalele de securitate în aria lor de responsabilitate și asigură instruirea echipei;

Angajații și colaboratorii – respectă politicile și procedurile, raportează prompt orice incident;

Departamentul IT – gestionează controalele tehnice, actualizările de securitate, backup-urile și integritatea infrastructurii.

Toate responsabilitățile sunt comunicate oficial și sunt însoțite de instruiri și proceduri practice.

7.3 Măsuri pentru conformitate și monitorizare

Pentru ca politica de securitate a informației să fie aplicată în mod eficient și consecvent, este esențial ca organizația să implementeze un sistem riguros de monitorizare, verificare și corectare. Aceste

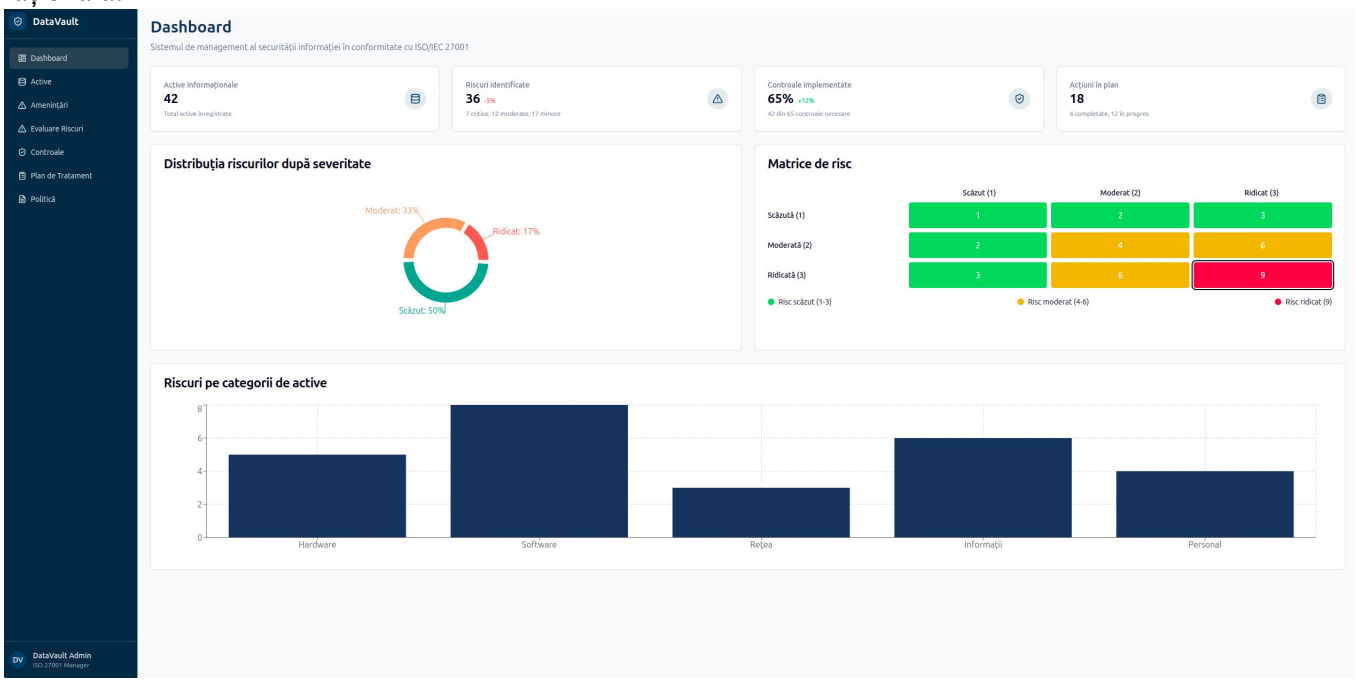
măsuri asigură nu doar conformitatea cu cerințele interne și externe, ci și capacitatea organizației de a reacționa proactiv la modificările mediului de risc. Prin monitorizarea continuă a proceselor, audituri periodice, instruirea angajaților și analizarea incidentelor, DataVault menține un nivel ridicat de control operațional și o îmbunătățire constantă a sistemului de management al securității informației (SMSI). În continuare sunt prezentate principalele mecanisme de conformitate aplicate.

- Audituri interne anuale privind aplicarea politicilor și eficiența controalelor de securitate;
- Verificări periodice ale drepturilor de acces și ale jurnalelelor de activitate în sisteme;
- Formări și testări periodice pentru personal, inclusiv simulări de phishing sau incidente;
- Evaluări de risc actualizate semestrial sau la modificări majore în infrastructură;
- Raportări regulate către conducere privind incidentele de securitate, statusul implementării măsurilor și planurile de îmbunătățire;
- Documentarea tuturor incidentelor, analizarea cauzelor și aplicarea de măsuri corective.

Prin aceste mecanisme, DataVault asigură nu doar conformitatea cu standardul ISO/IEC 27001, ci și o îmbunătățire continuă a sistemului său de management al securității informației (SMSI).

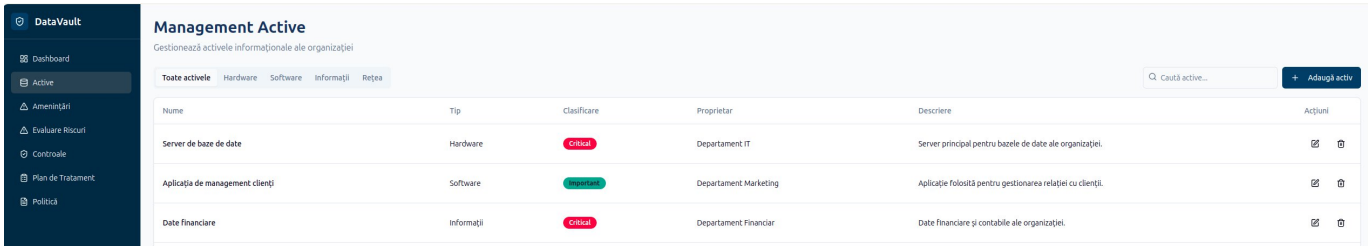
Aplicație software pentru suportul activităților

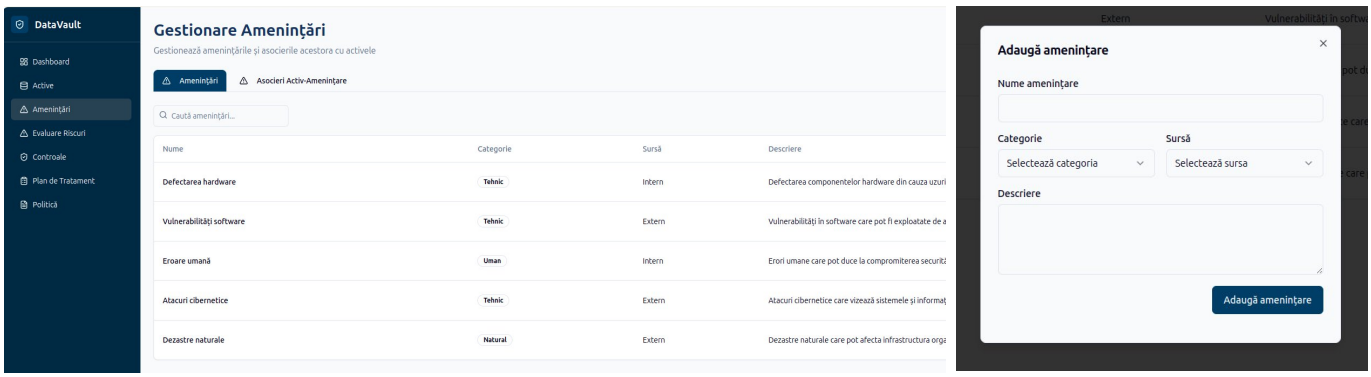
Pentru o mai bună înțelegere și vizualizare a procesului de implementare a măsurilor de securitate conform ISO/IEC 27001, a fost dezvoltată o interfață grafică dedicată. Această aplicație software are rolul de a centraliza activitățile realizate în cadrul studiului și de a facilita gestionarea activelor, evaluarea riscurilor și aplicarea controalelor de securitate. Prin utilizarea unei structuri vizuale clare și interactive, aplicația sprijină utilizatorii în urmărirea și documentarea fiecărui pas din procesul de securitate informațională.



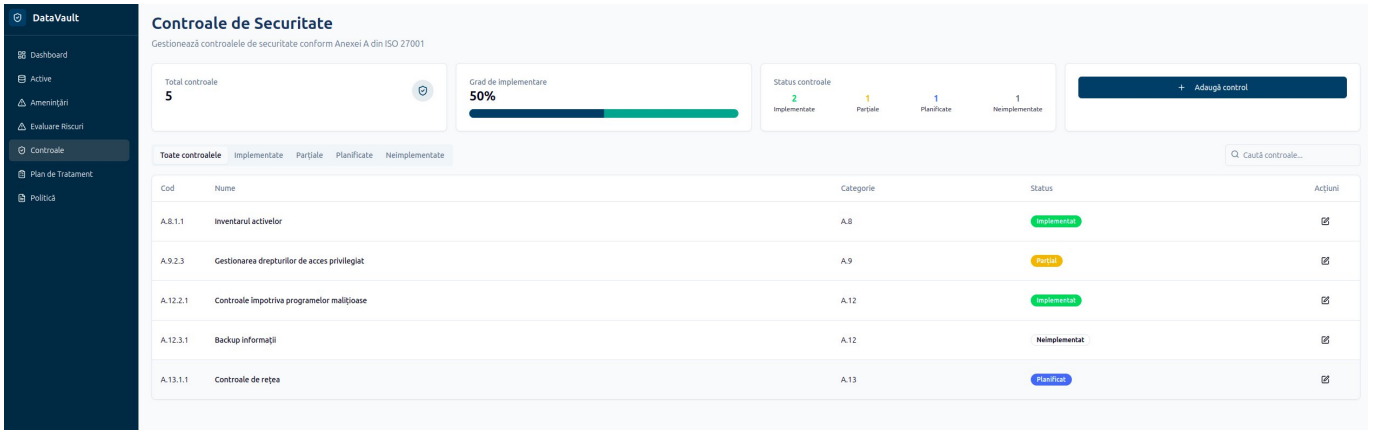
Principalele funcționalități includ:

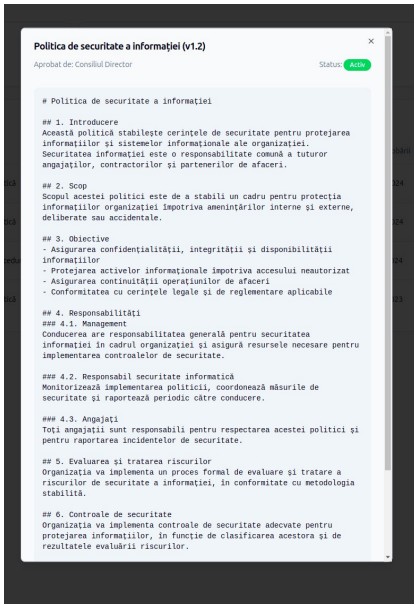
- Gestionarea activelor informaționale, cu clasificare pe categorii (informații, software, hardware);
- Asocierea amenințărilor specifice fiecărui activ, pe baza unei baze de date predefinite;

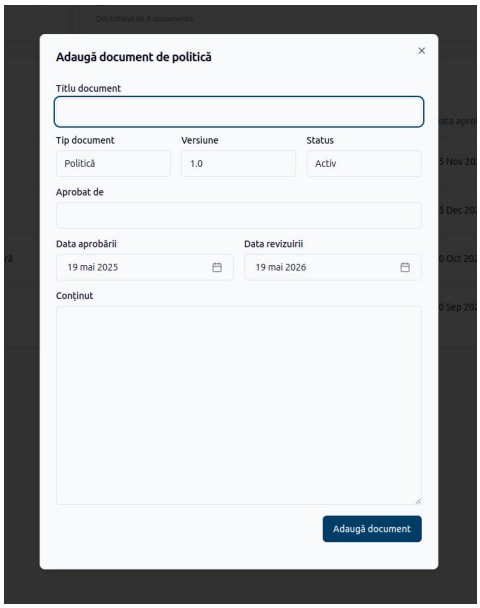


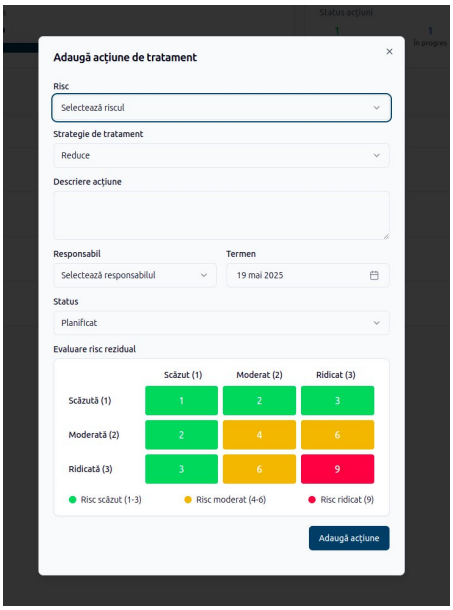


- Evaluarea riscurilor prin selectarea nivelurilor de probabilitate și impact și generarea automată a matricei de risc;
- Selectarea și atribuirea controalelor de securitate conform standardului;
- Crearea și actualizarea planului de tratament al riscurilor, cu alocarea responsabililor și urmărirea statusului;
- Administrarea politicii de securitate, cu opțiuni de revizuire periodică și export.









Aplicația este construită modular, cu o interfață intuitivă, orientată pe utilizator, optimizată pentru desktop și acces intern securizat.

Concluzii

Implementarea unui sistem de management al securității informației conform standardului ISO/IEC 27001 reprezintă un proces esențial pentru orice organizație care dorește să protejeze în mod eficient datele sale și să asigure continuitatea operațională. În cadrul acestui raport, s-a analizat aplicarea teoretică și practică a acestui standard în contextul unei organizații virtuale, DataVault, activă în domeniul serviciilor cloud.

Primul pas a constat în definirea structurii organizației și identificarea activelor informaționale esențiale. Acestea au fost clasificate în patru categorii principale: informații, software, hardware și rețea. Această clasificare a stat la baza întregului proces de analiză a riscurilor și a permis o abordare organizată și detaliată asupra măsurilor de protecție necesare.

În continuare, au fost identificate o serie de amenințări interne și externe care pot afecta securitatea activelor, de la erori umane și acces neautorizat până la atacuri cibernetice complexe. Asocierea acestor amenințări cu activele relevante a permis construirea unei viziuni clare asupra punctelor critice din organizație. Evaluarea riscurilor a fost realizată utilizând o metodă calitativă, bazată pe estimarea probabilității și a impactului fiecărei amenințări. Prin utilizarea unei matrice de risc simplificate, riscurile au fost clasificate în patru niveluri: redus, moderat, semnificativ și critic, ceea ce a permis prioritizarea tratamentului acestora în mod eficient.

Pe baza acestor riscuri, au fost selectate și implementate controale de securitate conform Anexei A din ISO/IEC 27001:2022. Acestea au fost structurate în trei categorii: tehnice, administrative și fizice, acoperind toate palierele necesare pentru un sistem de securitate complet. Măsurile au fost incluse într-un plan de tratament al riscurilor, monitorizat și actualizat periodic.

Pentru sprijinirea activităților descrise, s-a dezvoltat o aplicație software cu interfață grafică (GUI), care permite gestionarea activelor, evaluarea riscurilor, atribuirea controalelor și administrarea politicii de securitate într-un mod centralizat și intuitiv. Această aplicație aduce valoare practică proiectului, facilitând aplicarea standardului în contexte reale.

În concluzie, raportul demonstrează că un sistem de securitate informațională bine structurat, bazat pe standarde internaționale și susținut de instrumente digitale adecvate, poate asigura protejarea eficientă a datelor și proceselor critice. Modelul propus poate servi drept punct de referință pentru implementări reale în organizații similare, contribuind la consolidarea culturii de securitate și la reducerea riscurilor cibernetice.