

Software Requirements Specification

For

**Sistem informatic pentru gestiunea
inspectoratului de poliție**

Prepared by Foamete Constantin-Dan & Glavă Ștefan Alexandru

27.03.2024

Cuprins

Introducere

- 1.1 Scop
- 1.2 Convenții Document
- 1.3 Publicul Țintă și Sugestii de Lectură
- 1.4 Domeniul de Aplicare a Produsului
- 1.5 Referințe

Descrierea Generală

- 2.1 Perspectiva Produsului
- 2.2 Funcțiile Produsului
- 2.3 Clase și Caracteristici ale Utilizatorilor
- 2.4 Mediu de Operare
- 2.5 Constrângeri de Design și Implementare
- 2.6 Documentație Utilizator
- 2.7 Premize și Dependințe

Cerințe pentru Interfețele Externe

- 3.1 Interfețe Utilizator
- 3.2 Interfețe Hardware
- 3.3 Interfețe Software
- 3.4 Interfețe de Comunicare

Caracteristici ale Sistemului

- 4.1 Gestionarea Bazelor de Date a Criminaliștilor
- 4.2 Monitorizarea și Raportarea Incidentelor

Alte Cerințe Non-funcționale

- 5.1 Cerințe de Performanță
- 5.2 Cerințe de Siguranță
- 5.3 Cerințe de Securitate
- 5.4 Atribute de Calitate a Software-ului
- 5.5 Reguli de Afaceri

1. Introducere

1.1 Scop

Scopul acestui document este să stabilească cerințele și specificațiile pentru un sistem informatic care să gestioneze activitățile Inspectoratului de Poliție. Acesta va servi drept ghid pentru proiectarea și implementarea sistemului, asigurând că toate părțile implicate înțeleg obiectivele și cerințele esențiale.

1.2 Convenții Document

Acest SRS (Software Requirements Specification) respectă următoarele standarde și convenții tipografice:

Priorități: Fiecare cerință este însoțită de o prioritate, indicând importanța relativă a cerinței. Prioritățile sunt definite în următoarea manieră:

Prioritatea 1 (P1): Cerințe critice, esențiale pentru funcționarea de bază a sistemului sau pentru îndeplinirea scopului principal.

Prioritatea 2 (P2): Cerințe importante, dar nu vitale pentru funcționarea de bază.

Prioritatea 3 (P3): Cerințe opționale sau dorințe pentru îmbunătățiri viitoare.

Stil și Formatare: Cerințele esențiale sunt evidențiate folosind formatarea textului:

Boldat: Utilizat pentru a evidenția titlurile, subtitlurile și cerințele critice.

Referințe și Note de subsol: Atunci când este necesar, vor fi incluse referințe sau note de subsol pentru a oferi clarificări suplimentare sau pentru a indica sursele de informații.

Coerență și Consistență: Cerințele sunt structurate și formulate într-un mod coerent și consistent, pentru a facilita înțelegerea și implementarea lor.

Prin urmarea acestor standarde și convenții, se asigură că documentul este bine structurat, ușor de înțeles și că fiecare cerință este clară și prioritarizată în mod corespunzător, pentru a ghida eficient procesul de dezvoltare a sistemului.

1.3 Publicul Țintă și Sugestii de Lectură

Acest SRS este destinat echipei de dezvoltare, managerilor de proiect și utilizatorilor finali implicați în proiectul sistemului informatic pentru Inspectoratul de Poliție. Utilizatorii finali ar trebui să se concentreze pe "Manualul Utilizatorului" pentru a înțelege cum să interacționeze cu sistemul. Echipa de dezvoltare ar beneficia de "Documentația Tehnică a Sistemului" pentru detalii tehnice și de implementare. Este recomandat să consulte "Regulamentele și Legislația Relevantă" pentru a înțelege

cerințele legale. Studiile de caz și exemplele practice pot oferi inspirație și înțelegere suplimentară pentru toți cei implicați.

1.4 Domeniul de Aplicare a Produsului

Sistemul informatic dezvoltat are ca domeniu de aplicare gestionarea eficientă a activităților Inspectoratului de Poliție, incluzând:

- Gestiunea personalului, cazurilor și dosarelor
- Monitorizarea infrastructurii și echipamentelor
- Generarea de rapoarte și analize statistice
- Asigurarea securității și confidențialității datelor.

1.5 Referințe

<https://www.geeksforgeeks.org/>

<https://www.wikipedia.org/>

<https://stackoverflow.com/>

<https://www.w3schools.com/>

2. Descrierea Generală

2.1 Perspectiva Produsului

Sistemul informatic va fi integrat în infrastructura existentă a Inspectoratului de Poliție, având o interfață utilizator prietenoasă și intuitivă. Va fi proiectat pentru a fi scalabil și flexibil, asigurând securitatea și confidențialitatea datelor. Suportul tehnic și mentenanța vor fi disponibile pentru a menține funcționalitatea sistemului pe termen lung.

2.2 Funcțiile Produsului

Sistemul informatic va include următoarele funcționalități principale:

1. Gestiunea Personalului: Permite înregistrarea și gestionarea datelor angajaților, inclusiv informații personale și istoricul de angajare.
2. Gestiunea Cazurilor și Dosarelor: Facilitează înregistrarea și monitorizarea cazurilor deschise de către Inspectoratul de Poliție, inclusiv stadiul de desfășurare.
3. Generarea de Rapoarte: Furnizează facilități pentru generarea de rapoarte privind activitățile și performanța Inspectoratului de Poliție.

Aceste funcționalități esențiale vor acoperi necesitățile de bază ale instituției, contribuind la eficientizarea proceselor interne și la gestionarea eficace a activităților specifice.

2.3 Clase și Caracteristici ale Utilizatorilor

Utilizatorii sistemului pot fi împărțiți în următoarele clase și au următoarele caracteristici:

1. Administratori:

- **Descriere:** Administratorii sunt responsabili cu configurarea și gestionarea generală a sistemului.
- **Caracteristici:**
 - Acces complet la toate funcționalitățile sistemului.
 - Capacitatea de a crea, modifica și șterge conturi de utilizator.
 - Autoritate pentru configurarea și gestionarea drepturilor de acces.

2. Ofițeri de Poliție:

- **Descriere:** Ofițerii de poliție sunt utilizatori de zi cu zi ai sistemului, implicați în gestionarea cazurilor și a dosarelor.
- **Caracteristici:**
 - Acces la funcționalitățile relevante pentru înregistrarea și actualizarea cazurilor.
 - Capacitatea de a accesa și a actualiza datele personale și informațiile legate de cazuri.

3. Personal Administrativ:

- **Descriere:** Personalul administrativ poate fi implicat în gestionarea resurselor umane sau a altor aspecte administrative ale sistemului.
- **Caracteristici:**
 - Acces la funcționalități specifice de gestionare a resurselor umane sau a altor activități administrative.
 - Capacitatea de a accesa rapoarte și date statistice relevante.

4. Utilizatori Externi:

- **Descriere:** Utilizatori externi pot fi parteneri instituționali sau alte părți interesate care au nevoie de acces limitat la anumite informații sau funcționalități ale sistemului.
- **Caracteristici:**
 - Acces limitat la funcționalități și date specifice, conform nevoilor și permisiunilor acordate.

2.4 Mediu de Operare

Sistemul va funcționa într-un mediu de operare tipic birourilor, inclusiv în rețele locale sau cloud, în funcție de infrastructura existentă și preferințele instituției.

Caracteristicile mediului de operare includ:

1. **Platformă Hardware:** Sistemul va fi accesibil pe calculatoare și dispozitive mobile utilizate în cadrul Inspectoratului de Poliție, asigurând compatibilitatea cu diverse configurații hardware.
2. **Sistem de Operare:** Va fi compatibil cu sistemele de operare comune, cum ar fi Windows, macOS și Linux, pentru a asigura accesibilitatea și interoperabilitatea cu diferitele medii de lucru.
3. **Conectivitate la Rețea:** Accesul la rețele locale sau la internet va fi necesar pentru conectarea la serverele sistemului și pentru actualizările de software.
4. **Securitate:** Se vor implementa măsuri adecvate de securitate pentru protejarea datelor și a accesului la sistem, inclusiv autentificare în două pași și criptare a datelor.
5. **Interfață Utilizator:** Interfața sistemului va fi compatibilă cu diferitele medii de afișare, asigurându-se că este optimizată pentru utilizare pe desktopuri, laptopuri și dispozitive mobile.

2.5 Constrângeri de Design și Implementare

Această secțiune va include descrierea oricăror elemente sau probleme care vor limita opțiunile disponibile pentru dezvoltatori.

Acestea pot include:

- Politici corporatiste sau reglementări legale care trebuie respectate în cadrul proiectului.
- Limitări hardware, cum ar fi cerințele de timp sau de memorie.
- Interfețe către alte aplicații sau sisteme cu care sistemul trebuie să interacționeze.
- Tehnologii, instrumente și baze de date specifice care trebuie utilizate în cadrul proiectului.
- Operațiuni paralele care trebuie să fie luate în considerare în proiectare și implementare.
- Cerințe de limbaj de programare sau protocoale de comunicare.

- Considerații de securitate care trebuie luate în considerare în proiectare și implementare.
- Convenții de design sau standarde de programare, în special dacă organizația clientului va fi responsabilă pentru întreținerea software-ului livrat.

Aceste constrângeri vor influența direcția și abordarea proiectului, precum și opțiunile tehnice și de proiectare disponibile pentru echipa de dezvoltare.

2.6 Documentație Utilizator

Prezentare PPT - demo

2.7 Premize și Dependințe

Premisele și dependențele includ:

- **Componente de la Terți:** Utilizarea unor componente de la terți sau a unor soluții comerciale pentru anumite funcționalități poate afecta planificarea și implementarea proiectului. Este important să se țină cont de disponibilitatea acestor componente și de posibilele limitări sau restricții asociate cu utilizarea lor.
- **Mediul de Dezvoltare și de Operare:** Factori legați de mediul de dezvoltare și de operare, cum ar fi sistemul de operare, versiunea limbajului de programare sau infrastructura de rețea, ar putea afecta implementarea și performanța sistemului. Este esențial să se asigure compatibilitatea și adecvarea mediului de lucru pentru nevoile proiectului.
- **Constrângeri Tehnice sau de Resurse:** Limitările tehnice sau de resurse, cum ar fi capacitățile hardware sau restricțiile de timp și buget, pot influența planificarea și implementarea proiectului. Este important să se evalueze și să se gestioneze aceste constrângeri în mod corespunzător.

3. Cerințe pentru Interfețele Externe

3.1 Interfețe Utilizator

Interfața utilizatorului (UI) este componenta principală a sistemului informatic, care facilitează interacțiunea utilizatorilor cu funcționalitățile și datele sistemului.

Caracteristicile cheie ale interfeței utilizatorului includ:

1. **Design Intuitiv:** Interfața utilizatorului va fi proiectată pentru a fi intuitivă și ușor de utilizat, astfel încât utilizatorii să poată naviga și interacționa cu sistemul fără dificultăți.

2. **Aspect Coerent și Plăcut:** Va fi aplicat un design coerent și plăcut, cu utilizarea culorilor și elementelor vizuale în concordanță cu identitatea vizuală a Inspectoratului de Poliție.
3. **Navigare Simplă și Eficientă:** Elementele de navigare vor fi clar structurate și organizate, pentru a permite utilizatorilor să găsească rapid și ușor funcționalitățile și informațiile de care au nevoie.

3.2 Interfețe Hardware

Interfețele hardware incluse în cadrul proiectului nostru pentru gestionarea Inspectoratului de Poliție sunt următoarele:

1. **Imprimante:** Vor fi utilizate pentru imprimarea diferitelor documente și rapoarte generate de sistem, cum ar fi rapoarte de activitate, fișe de identificare sau alte documente relevante pentru activitățile desfășurate de Inspectoratul de Poliție. Imprimantele trebuie să fie compatibile cu sistemul și să ofere o calitate ridicată a imprimării pentru a asigura claritatea și profesionalismul
2. **Faxuri:** În anumite situații, comunicarea prin fax poate fi încă necesară pentru schimbul rapid și sigur al informațiilor între Inspectoratul de Poliție și alte instituții sau părți interesate. Astfel, sistemul trebuie să ofere suport pentru trimiterea și primirea de faxuri, fie prin intermediul echipamentelor fizice, fie prin integrarea cu servicii de fax online.

3.3 Interfețe Software

Interfețele software reprezintă punctele de interacțiune între diversele componente ale sistemului informatic. În cadrul proiectului nostru pentru gestionarea Inspectoratului de Poliție, se vor dezvolta și implementa mai multe interfețe software pentru a asigura funcționarea corectă și integrarea adecvată a sistemului. Acestea pot include:

1. **Interfața Utilizator (UI):** Interfața prin care utilizatorii interacționează direct cu sistemul. Aceasta poate fi sub formă de aplicație web, aplicație desktop sau aplicație mobilă, și va oferi funcționalități precum gestionarea cazurilor, raportarea incidentelor, și accesul la rapoarte și statistici.
2. **Baze de Date și Sisteme de Gestionare a Bazelor de Date (DBMS):** Interfețele pentru bazele de date și pentru sistemele de gestionare a bazelor de date vor fi utilizate pentru a permite stocarea, accesarea și gestionarea eficientă a datelor necesare funcționării sistemului.

- 3. Interfețe de Securitate și Autentificare:** Pentru gestionarea securității sistemului, vor fi dezvoltate interfețe specializate pentru autentificare, autorizare și gestionarea accesului la diferitele funcționalități și date ale sistemului.

3.4 Interfețe de Comunicare

Interfețele de comunicare planificate pentru proiectul nostru de gestionare a Inspectoratului de Poliție vor include:

- 1. Email și Notificări:** Serviciile de email vor fi utilizate pentru trimiterea și primirea de mesaje între utilizatori sau către alte sisteme. De asemenea, notificările vor fi implementate pentru a alerta utilizatorii cu privire la evenimente sau acțiuni importante în cadrul sistemului.
- 2. Bază de Date Comună:** Se va implementa o bază de date comună pentru a facilita schimbul de date și informații între diversele componente ale sistemului și alte sisteme externe. Această bază de date va fi utilizată pentru stocarea și accesul la informații relevante pentru gestionarea eficientă a activităților Inspectoratului de Poliție, precum și pentru a permite integrarea și interoperabilitatea cu alte sisteme.

4. Caracteristici ale Sistemului

4.1 Caracteristica Sistemului: Gestiunea Cazurilor

3.1.1 Descriere și Prioritate

Această caracteristică permite înregistrarea, monitorizarea și gestionarea cazurilor deschise de către Inspectoratul de Poliție. Este considerată de prioritate ridicată, având în vedere importanța centrală a acestui proces pentru funcționarea corectă a instituției.

4.1.2 Secvențe Stimul/Răspuns

- Utilizatorul accesează interfața de gestionare a cazurilor și începe înregistrarea unui nou caz.
- Sistemul solicită informații relevante despre cazul nou înregistrat.
- Utilizatorul furnizează detaliile necesare, inclusiv informații despre reclamant, tipul incidentului și alte informații relevante.
- Sistemul validează și stochează informațiile introduse.
- Utilizatorul primește confirmarea înregistrării cu succes a cazului.

4.1.3 Cerințe Funcționale

REQ-1: Înregistrarea cazurilor cu un formular structurat.
REQ-2: Validarea datelor introduse pentru coerență.
REQ-3: Categorizarea și prioritizarea automată a cazurilor.
REQ-4: Monitorizarea și actualizarea stadiului cazurilor.
REQ-5: Notificări pentru modificările cazurilor.
REQ-6: Asignare automată a unui număr unic pentru fiecare caz.
REQ-7: Posibilitatea de a atașa fișiere relevante la fiecare caz.
REQ-8: Funcționalitate de căutare și filtrare a cazurilor.
REQ-9: Sistem de auditare pentru monitorizarea modificărilor cazurilor.
REQ-10: Generare automată a rapoartelor periodice despre cazuri.
REQ-11: Posibilitatea de a atașa comentarii la fiecare caz.
REQ-12: Exportul datelor cazurilor în format CSV sau Excel.
REQ-13: Asignarea unui investigator pentru fiecare caz.
REQ-14: Integrare cu servicii de hărți pentru vizualizarea geografică a cazurilor.
REQ-15: Sistem de notificări automat pentru termenele limită ale cazurilor.
REQ-16: Atribuirea priorității cazurilor pentru optimizarea resurselor.
REQ-17: Căutare avansată pentru găsirea rapidă a cazurilor relevante.
REQ-18: Funcționalitate de raportare a cazurilor rezolvate și nerezolvate.
REQ-19: Asignarea de echipe de lucru pentru cazurile complexe.
REQ-20: Integrare cu servicii de calendarizare pentru gestionarea termenelor limită.

4.2 Caracteristica Sistemului: Generarea Rapoartelor

4.2.1 Descriere și Prioritate

Această caracteristică permite utilizatorilor să genereze rapoarte detaliate și analize statistice privind activitățile Inspectoratului de Poliție. Deoarece rapoartele sunt esențiale pentru evaluarea performanței și pentru luarea deciziilor informate, această caracteristică are prioritate înaltă.

4.2.2 Secvențe Stimul/Răspuns

- Utilizatorul accesează interfața de generare a rapoartelor și selectează tipul de raport dorit.
- Sistemul solicită parametrii și criteriile de filtrare pentru raportul selectat.
- Utilizatorul furnizează criteriile de filtrare și confirmă generarea raportului.
- Sistemul procesează datele și generează raportul conform specificațiilor utilizatorului.
- Utilizatorul primește raportul generat și poate să-l descarce sau să-l imprime.

4.2.3 Cerințe Funcționale

- REQ-20:** Generarea rapoartelor diverse și personalizabile.
- REQ-21:** Filtrarea și specificarea parametrilor pentru rapoarte.
- REQ-22:** Generarea rapoartelor în formate ușor de utilizat.
- REQ-23:** Personalizarea conținutului și aspectului rapoartelor.
- REQ-24:** Asigurarea securității datelor rapoartelor.
- REQ-25:** Programare automată pentru generarea rapoartelor.
- REQ-26:** Exportul rapoartelor în diferite formate de fișiere.
- REQ-27:** Partajarea rapoartelor cu utilizatorii relevanți.
- REQ-28:** Salvarea setărilor preferate pentru generarea rapoartelor.
- REQ-29:** Trimiterea automată a rapoartelor către adresele specificate.
- REQ-30:** Programarea rapoartelor personalizate pe baza unui șablon.
- REQ-31:** Implementarea de grafice și diagrame în rapoartele generate.
- REQ-32:** Exportul rapoartelor direct într-o bază de date externă.
- REQ-33:** Compararea datelor între diferite perioade în rapoartele analitice.
- REQ-34:** Programarea rapoartelor automate să fie trimise într-un folder specific.

4.3 Caracteristica Sistemului: Gestiunea Personalului

4.3.1 Descriere și Prioritate

Această caracteristică permite înregistrarea și gestionarea datelor angajaților din cadrul Inspectoratului de Poliție, inclusiv informații personale, detalii de contact și istoricul de angajare. Fiind esențială pentru gestionarea resurselor umane și a organizației, această caracteristică are prioritate înaltă.

4.3.2 Secvențe Stimul/Răspuns

- Utilizatorul accesează interfața de gestionare a personalului și selectează opțiunea de înregistrare a unui nou angajat.
- Sistemul solicită informațiile necesare despre angajat, cum ar fi numele, poziția și detalii de contact.
- Utilizatorul introduce informațiile despre angajat și confirmă înregistrarea.
- Sistemul validează datele și le stochează în baza de date a personalului.
- Utilizatorul primește confirmarea înregistrării cu succes a noului angajat.

4.3.3 Cerințe Funcționale

- REQ-35:** Înregistrarea datelor de bază ale angajaților.
- REQ-36:** Gestionarea detaliilor de contact ale angajaților.
- REQ-37:** Înregistrarea istoricului de angajare al fiecărui angajat.
- REQ-38:** Gestionarea permiselor și documentelor angajaților.
- REQ-39:** Asigurarea securității datelor personale ale angajaților.
- REQ-40:** Asocierea de privilegii specifice pentru fiecare angajat.
- REQ-41:** Gestionarea evaluărilor de performanță și a feedback-ului angajaților.

REQ-42: Monitorizarea concediilor și absențelor angajaților.
REQ-43: Gestionarea training-urilor și a dezvoltării profesionale.
REQ-44: Actualizarea eficientă a informațiilor de contact ale angajaților.
REQ-45: Gestionarea eficientă a permiselor și licențelor angajaților.
REQ-46: Înregistrarea obiectivelor și realizărilor individuale ale angajaților.
REQ-48: Notificări pentru evaluările periodice ale performanței angajaților.
REQ-49: Atașarea documentelor de identificare și certificări la profilurile angajaților.
REQ-50: Implementarea unui chat intern pentru comunicarea rapidă între angajați și departamente.

5. Alte Cerințe Non-funcționale

5.1 Cerințe de Performanță

Pentru a asigura funcționarea optimă a produsului în diverse circumstanțe, sunt stabilite următoarele cerințe de performanță:

1. **Timp de Răspuns Rapid:** Sistemul trebuie să ofere un timp de răspuns mediu sub 2 secunde pentru majoritatea operațiunilor de bază, cum ar fi accesarea informațiilor despre un caz sau generarea unui raport standard. Această cerință este esențială pentru a asigura o experiență utilizator fluidă și eficientă.
2. **Scalabilitate:** Sistemul trebuie să fie capabil să gestioneze o creștere semnificativă a numărului de utilizatori și a volumului de date fără a afecta semnificativ performanța. Aceasta este crucială pentru a asigura funcționarea adecvată a sistemului în timpul perioadelor de vârf sau a creșterii neașteptate a utilizării.
3. **Fiabilitate și Disponibilitate:** Sistemul trebuie să fie disponibil 24/7 și să ofere o fiabilitate ridicată, cu un uptime de cel puțin 99.9%. Astfel, se asigură accesibilitatea continuă a funcționalităților sistemului și evitarea timpilor de inactivitate care ar putea afecta operațiunile Inspectoratului de Poliție.
4. **Performanță a Interfeței Utilizator:** Interfața utilizatorului trebuie să ofere o experiență responsivă și plăcută, cu o încărcare rapidă a paginilor și a elementelor grafice. Aceasta contribuie la creșterea eficienței utilizatorilor și la îmbunătățirea satisfacției acestora în utilizarea sistemului.
5. **Eficiența Utilizării Resurselor:** Sistemul trebuie să utilizeze resursele hardware și software în mod eficient, minimizând consumul de memorie și de capacitate de procesare. Aceasta contribuie la reducerea costurilor de întreținere și la maximizarea performanței sistemului.

5.2 Cerințe de Siguranță

Pentru a asigura utilizarea sigură a produsului și pentru a preveni orice pierderi, daune sau vătămări care ar putea rezulta din utilizarea acestuia, sunt stabilite următoarele cerințe de siguranță:

1. **Protecția Datelor Sensibile:** Sistemul trebuie să implementeze măsuri solide de securitate și criptare pentru protejarea datelor sensibile, cum ar fi informațiile personale ale angajaților sau ale cetățenilor, pentru a preveni accesul neautorizat sau scurgerile de informații.
2. **Autentificare și Autorizare Riguroasă:** Accesul la funcționalitățile sensibile ale sistemului, precum înregistrarea și gestionarea cazurilor sau a datelor personale, trebuie să fie restricționat și controlat strict prin autentificare și autorizare adecvată, pentru a preveni utilizarea neautorizată sau abuzul.

5.3 Cerințe de Securitate

Sunt stabilite următoarele cerințe de securitate pentru a proteja utilizatorii și datele utilizate sau create de produs:

1. **Controlul Accesului:** Sistemul trebuie să ofere mecanisme de control al accesului pentru a asigura că doar utilizatorii autorizați au permisiunea de a accesa anumite funcționalități sau date sensibile. Aceasta include implementarea unor niveluri adecvate de autentificare și autorizare a utilizatorilor.
2. **Confidențialitatea Datelor:** Toate datele sensibile sau personale stocate în cadrul sistemului trebuie să fie protejate împotriva accesului neautorizat și a divulgării. Se vor utiliza tehnici de criptare adecvate pentru a asigura confidențialitatea datelor în timpul stocării și transmiterii acestora.
3. **Integritatea Datelor:** Sistemul trebuie să garanteze integritatea datelor, prevenind modificările neautorizate sau frauduloase asupra acestora. Se vor implementa mecanisme de verificare și validare a datelor pentru a asigura că acestea rămân autentice și nealterate.

5.4 Atributele Calității Software

În cadrul proiectului, sunt stabilite următoarele atribute ale calității software, care vor fi importante atât pentru clienți, cât și pentru dezvoltatori:

1. **Ușurința în Utilizare:** Interfața utilizatorului trebuie să fie intuitivă și ușor de navigat, pentru a facilita utilizarea fără efort a sistemului. Se urmărește ca utilizatorii să poată accesa rapid funcționalitățile dorite și să își îndeplinească sarcinile fără dificultate.
2. **Fiabilitatea și Stabilitatea:** Sistemul trebuie să fie stabil și să funcționeze fără erori sau întreruperi frecvente. Se dorește ca produsul să ofere o experiență fiabilă și consistentă utilizatorilor săi.
3. **Mentenabilitatea și Extensibilitatea:** Codul și arhitectura sistemului trebuie să fie ușor de întreținut și de extins în viitor. Se urmărește ca dezvoltatorii să poată efectua modificări și actualizări fără a afecta funcționalitățile existente și fără a introduce erori noi.
4. **Securitatea și Protecția Datelor:** Sistemul trebuie să fie protejat împotriva amenințărilor de securitate și să asigure confidențialitatea și integritatea datelor utilizatorilor. Se pun accent pe implementarea unor măsuri solide de securitate pentru a preveni accesul neautorizat sau divulgarea informațiilor sensibile.