

## ARHITECTURA TEHNICĂ A SISTEMULUI

pentru

platforma integrata de servicii electronice ce trebuie implementată în cadrul proiectului „Soluții informatice integrate pentru simplificarea furnizării serviciilor către cetățeni și mediul de afaceri și optimizarea procedurilor administrative la nivelul Municipiului Râmnicu-Sărat”, Cod SMIS 129270

SIPOCA 647  
SMIS 129270

Proiect finanțat  
din POCA

Remis spre rambursare  
către AM POCA



## Cuprins

<b>1. Controlul documentului.....</b>	<b>3</b>
1.1. Aprobare finala .....	3
1.2. Lista de distribuție a documentului.....	4
1.3. Documente referință .....	4
1.4. Scopul documentului.....	4
<b>2. Arhitectura sistemului informatic .....</b>	<b>6</b>
2.1 Definiții, principii și constrângeri pentru arhitectura sistemului .....	6
2.2 Arhitectura logică a sistemului .....	7
2.2.1 Componente aplicative.....	8
2.2.2 Componenta de gestiune a bazei de date .....	9
2.3 Arhitectura fizică a sistemului .....	9
2.4 Managementul utilizatorilor si accesul la sistem.....	12
2.5 Securitatea sistemului informatic .....	12
2.6 Securitatea logică.....	14
2.6.1 Controlul Accesului Logic.....	14
2.6.2 Jurnalizare, monitorizare, auditare.....	14
2.7 Confidențialitatea datelor.....	15
2.8 Backup.....	15

**SIPOCA 647  
SMIS 129270**

**Proiect finanțat  
din POCA**

**Remis spre rambursare  
cătore AM POCA**





- activități de analiză a documentelor: structurile de organizare, Regulamente de Organizare și Funcționare, Nomenclator Arhivistic, procedurilor operaționale și de sistem
- A fost elaborată concepția de implementare a serviciilor electronice în cadrul proiectului, susținută printr-o prezentare în data de 02.09.2019, la sediul Primăriei Municipiului Râmnicu Sărat
- au fost desfășurate interviuri în perioada 02-25 Septembrie 2019 cu personalul cheie al beneficiarului din diferite unități organizatorice, după cum urmează:
  - o Compartiment informare și relații publice
  - o Serviciul Urbanism
  - o Compartiment contencios administrativ și juridic
  - o Compartiment administrare patrimoniu
  - o Compartiment registru agricol
  - o Compartiment arhivă
  - o Direcția asistență socială
  - o Compartiment încasare, constatare, debitare și amenzi persoane fizice
  - o Compartiment impozite și taxe locale, persoane juridice și executări silit
  - o Compartiment spațiu locativ
  - o Compartiment Informatizare

Proiect finanțat  
din POCARemis spre rambursare  
către AM POCA

S-au investigat în mod specific următoarele:

- cerințele funcționale ale platformei rezultate din analiza proceselor existente la nivelul instituției;
- cerințele non-funcționale ale platformei orientate pe aspecte referitoare la parametrii descriptivi de funcționare optimă a sistemului, precum interfețele utilizator, eficiența operațiunilor, acces și securitate, disponibilitate, robustețe, etc;
- modul de securizare a platformei și integrarea acesteia în cadrul sistemului informatic actual al instituției
- Nevoile utilizatorilor care se referă la interfețe, personalizare, utilizare facilă, disponibilitate





## 2. Arhitectura sistemului informatic

### 2.1 Definiții, principii și constrângeri pentru arhitectura sistemului

**Remis spre rambursare  
către AM POCA**

Prin arhitectura sistemului informatic înțelegem structurile, mecanismele și interfețele utilizate, precum și comunicarea între părțile componente. Arhitectura de sistem descrie viziunea fizică și logică a sistemului propus, relevă modul în care sistemul va fi construit, definește modul în care vor fi utilizate diferite concepte, cât și aspecte vizând posibilitatea dezvoltării viitoare a sistemului.

La proiectarea, realizarea și implementarea Platformei Integrate de servicii electronice trebuie să se țină cont de următoarele principii generale:

- Principiul legalității: care presupune crearea și exploatarea sistemului informatic în conformitate cu legislația națională în vigoare și a normelor și standardelor internaționale recunoscute în domeniu;
- Principiul divizării arhitecturii pe nivele: constă în proiectarea independentă a componentelor sistemului în conformitate cu standardele de interfață dintre nivele;
- Principiul arhitecturii bazate pe servicii (SOA): constă în distribuirea funcționalității aplicației în unități mai mici, distincte - numite servicii - care pot fi distribuite într-o rețea și pot fi utilizate împreună pentru a crea aplicații destinate implementării funcțiilor de business ale sistemului informatic.
- Principiul datelor sigure: stipulează introducerea datelor în sistem doar prin canalele autorizate și autentificate;
- Principiul securității informaționale: presupune asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate și eficiență pentru protecția datelor de pierderi, alterări, deteriorări și de acces nesancționat.
- Principiul transparenței: presupune proiectarea și realizarea conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informatice și de telecomunicații;
- Principiul expansibilității: stipulează posibilitatea extinderii și completării sistemului informatic cu noi funcții sau îmbunătățirea celor existente;
- Principiul scalabilității: presupune asigurarea unei performanțe constante a soluției informatice la creșterea volumului de date și a solicitării sistemului informatic;



- Principiul simplității și comodității utilizării: presupune proiectarea și realizarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor sistemului, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție;
- Principiul integrității, plenitudinii și veridicității datelor: presupune implementarea mecanismelor care permit păstrarea conținutului și interpretării univoce a datelor în condițiile unor influențe accidentale și eliminării fenomenelor de denaturare sau lichidare accidentală a acestora, furnizarea unui volum de date suficient executării funcțiilor de business al sistemului informatic și asigurarea unui grad înalt de corespundere a datelor cu starea reală a obiectelor pe care le reprezintă și care fac parte dintr-un sector concret al sistemului informatic.

În particular, pentru arhitectura sistemului informatic se insistă asupra respectării următoarelor principii primordiale:

- implementarea unei soluții centralizate client-server, WEB based, cu acces autorizat la interfață și date, utilizand componente software mature, de tip COTS, cu drept de proprietate perpetuu;
- asigurarea unei securități adecvate a sistemului informatic pentru a proteja informația și subsistemele componente împotriva utilizării lor neautorizate sau a divulgării informației cu caracter personal sau a celei cu accesibilitate limitată;
- recunoașterea informației ca patrimoniu și gestionarea ei adecvată;
- dezvoltarea și implementarea sistemului informatic oferind posibilitatea reutilizării lor pentru alte procese sau în perspectiva asigurării posibilității de dezvoltare de noi funcționalități;
- asigurarea capacității de restabilire în urma dezastrelor (asigurarea securității fizice și logice) ca parte componentă a planului de implementare.

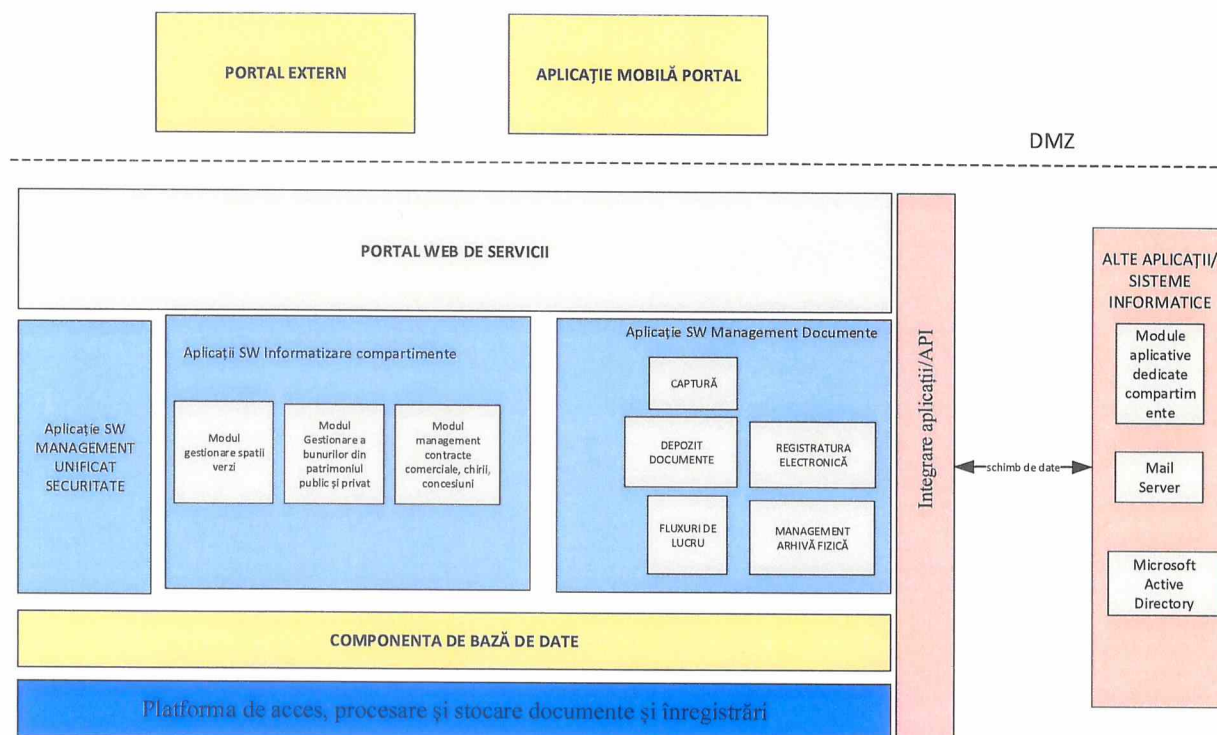
Soluția tehnică pentru sistemul informatic propus va include un singur mediu, utilizat inițial pentru dezvoltare/testare și instruire și ulterior pentru producție.

22 Arhitectura logică a sistemului  
SIPOCA 647  
SMIS 129270

Proiect finanțat  
din POCA

Remis spre rambursare  
către AM POCA

CONFORM CU  
ORIGINALUL  
Municipalitatea Râmnicu Sărat



**SIPOCA 647  
SMIS 129270**

**Fig. 1 Arhitectura logica a sistemului**

**Remis spre rambursare  
către AM POCA**

**Proiect finanțat  
din POCA**

### 2.2.1 Componente aplicative

Platforma integrată include următoarele componente:

- Portal web de servicii pentru cetățeni și mediul de afaceri, prevăzut cu o componentă de Portal Extern și Aplicație Mobilă
- Aplicație software de management a documentelor, cu următoarele module funcționale:
  - Depozit documente electronice
  - registratură electronică
  - captură a documentelor
  - fluxuri de lucru
  - management arhivă fizică de documente
- Aplicații software informatizare compartimente:
  - Modul Registrul spațiilor verzi
  - Modul gestionare a bunurilor din patrimoniul public și privat
  - Modul management contracte comerciale, chirii, concesiuni



- Aplicație software pentru monitorizare evenimente de securitate

### 2.2.2 Componenta de gestiune a bazei de date

Soluția de gestiune a bazei de date asigură necesarul de persistență operațională pentru componentele Platformei Integrate.

### 2.3 Arhitectura fizică a sistemului

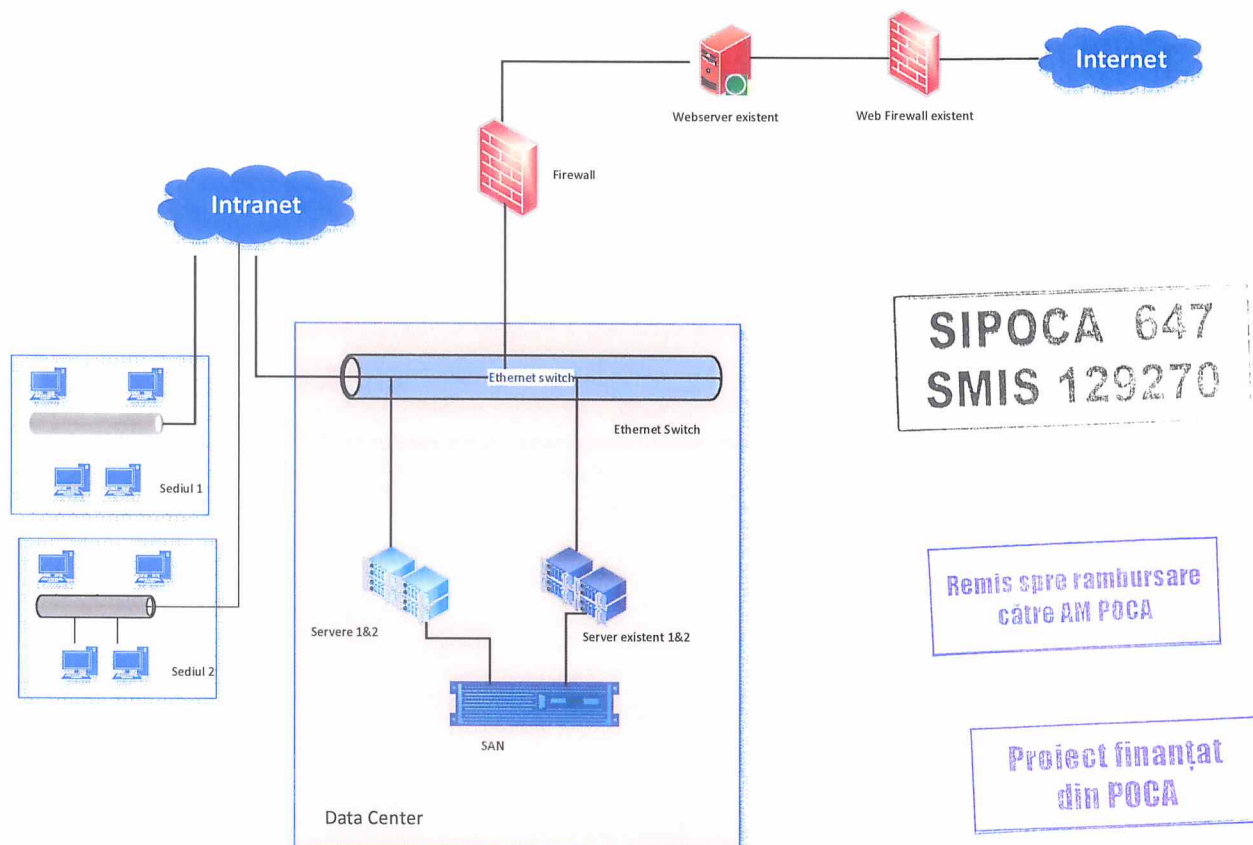


Fig. 2 Arhitectura fizica a sistemului

Arhitectura sistemului va respecta următoarele constrângeri:

- Arhitectura va permite organizarea unui DMZ în care să fie instalată, pe un server existent, o componentă a Portalului Web de servicii, ce va asigura accesul utilizatorilor externi (cetățeni) de pe calculatoare prin intermediul web sau de pe dispozitivele mobile de tip smartphone prin intermediul aplicațiilor mobile.
- Arhitectura permite funcționarea în regim de înaltă disponibilitate, atât pentru componentele critice (Portal Web de servicii, Aplicație software de management

documente și sistemul de bază de date), cât și pentru echipamentele de procesare și stocare din compunerea sistemului propus.

- Soluția tehnică propusă va utiliza un mediu virtualizat integral
- Înalta disponibilitate a sistemului va fi asigurată la nivel fizic, prin propunerea unor echipamente redundante pentru procesare, cât și prin faptul că echipamentele propuse prezintă redundanță funcțională la nivelul componentelor interne cum ar fi: procesoare, memorie RAM, HDD-uri, plăci de rețea LAN/SAN, surse de alimentare etc.
- la defectarea unuia din servere, aplicațiile vor continua să ruleze pe celelalte servere fără ca utilizatorii să sesizeze întreruperi ale serviciului;
- sistemul de stocare propus asigură redundanță necesară pentru protecția datelor fiind prevăzut cu controlere redundante, porturi FC redundante pe fiecare controller, porturi pentru management local și la distanță redundante, surse de alimentare redundante și ventilatoare redundante
- legăturile dintre servere și rețeaua Intranet se va realiza prin conectarea serverelor în Switch-ul ce va fi livrat în cadrul proiectului și prin conectarea acestuia cu ruter-ul existent ce asigură rutarea în cadrul rețelei Intranet a instituției.
- legăturile dintre servere livrate în proiect și sistemul de stocare se vor face exclusiv prin legături de mare viteză;
- legăturile dintre serverele existente și sistemul de stocare se vor face exclusiv prin legături Gigabit Ethernet. Sistemul de stocare va fi echipat cu interfețele necesare acestor conexiuni;
- sistemul de stocare va fi împărțit în volume separate pentru fiecare mașină virtuală, având capacitatea și nivelul RAID adecvat pentru fiecare tip de mașină (ex. baza de date, server aplicații, etc);
- legătura de date dintre infrastructură și internet se va realiza exclusiv prin intermediul firewall-ului și va fi protejată de acestea;
- pentru asigurarea unui nivel adecvat al securității informaționale soluția informatică livrată trebuie să permită realizarea de conexiuni securizate între terminalele utilizatorilor și serverul de aplicație pentru asigurarea siguranței informației expediate (prin intermediul sesiunilor SSL).

sesiunilor SSL)

**SIPOCA 647**  
**SMIS 129270**

Remis spre rambursare  
către AM POCA

Proiect finanțat  
din POCA



- sistemul trebuie sa fie scalabil, atat din punct de vedere hardware (adaugare de nuclee de procesare, memorie RAM sau discuri), software (adaugare de noi utilizatori) dar si din punct de vedere business (adaugare de noi functionalitati);

Platforma integrată va include o platforma de acces, procesare și stocare documente și înregistrări compusă din cel puțin urmatoarele componente hardware:

Nr.	Descriere	Cantitate
1	Server	2
2	Sistem de stocare centralizata de tip Unified	1
3	Rack cu UPS	1
4	Switch	1
5	Firewall	1

Remis spre rambursare  
către AM POCA

SIPOCA 647  
SMIS 129270

Proiect finanțat  
din POCA

Dimensionarea componentelor va trebui sa asigure configurarea a minim 8 mașini virtuale cu minimul de resurse de procesare dupa cum urmează:

Componenta	Numar minim de noduri	Disponibilitate minima	Numar core-uri minime pe nod
Portal web	2	Cluster Activ	12
Aplicație software de management documente	2	Cluster Activ	12
SGBD	2	Cluster Activ-Pasiv	8
Aplicații software pentru informatizare activități compartimente	1		10
Aplicație monitorizare evenimente de securitate	1		4



Componentele de balansare a cererilor pentru clusterelor aplicative ale Portalului Web și Aplicației software de management documente vor putea fi instalate în mașini virtuale pe unul din serverele existente în infrastructura actuală a beneficiarului. Mașinile virtuale ce vor fi puse la dispoziție sunt echipate cu sistem de operare de tip Windows Server.

**Remis spre rambursare  
cătore AM POCA**

## 2.4 Managementul utilizatorilor și accesul la sistem

Pentru asigurarea managementului utilizatorilor și accesului la sistem, se vor avea în vedere următoarele:

- identificarea în mod unic a fiecărui utilizator intern în sistem prin crearea de conturi unice și personalizate de acces;
- gestionarea centralizată și unitară a accesului utilizatorilor în sistem prin autorizarea utilizatorului doar la componentele și modulele funcționale ale sistemului conform cu drepturile de acces și atribuțiile specifice;
- accesul la sistem se va putea realiza doar prin autentificarea utilizatorilor.

## 2.5 Securitatea sistemului informatic

Formularea cerintelor de securitate are drept scop definirea cadrului general de securitate prin care sa se asigure confidentialitatea, integritatea și disponibilitatea informațiilor stocate, procesate sau transmise prin sistemele de comunicații și informatice, destinate operationalizării sistemului.

Arhitectura platformei integrate trebuie să respecte reglementările legale privind GDPR ca și principiu de bază. În acest sens, securitatea datelor prelucrate de sistemul informatic, inclusiv din punct de vedere al comunicațiilor, dintre entitățile participante în sistem trebuie să fie conforma normelor legale.

Platforma integrată trebuie să asigure mecanisme de protecție împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le gestionează. Soluția de securitate trebuie să asigure securitatea și confidentialitatea datelor cu caracter personal existente în bazele de date. Astfel, utilizatorii vor putea accesa numai acele secțiuni și acel conținut care le sunt permise prin apartenența la un profil sau la o macheta de securitate.

Soluția de securitate va fi configurată astfel încât:





IOT.

TECHNOLOGY  
TALORS

SMIS 129270

Proiect finanțat  
din POCA

Remis spre rambursare  
câtre AM POCA

- sa nu permita persoanelor neautorizate sa modifice sau sa altereze informatiile din sistem;
- sa nu permita persoanelor neautorizate sa acceseze sistemul;
- sa asigure integritatea si autenticitatea datelor si sa permita identificarea sursei datelor initiale si a persoanelor care au accesat sau au inregistrat aceste date in sistem;
- sa asigure trasabilitatea actiunilor utilizatorilor si operatiunilor efectuate in sistem;
- nu va exista posibilitatea de acces pentru persoanele dintr-un mediu extern la date dintr-un mediu considerat intern;
- informatiile private care se transmit vor fi criptate pana la livrare, astfel incat sa nu poata fi interceptate si utilizate;
- informatiile vor putea fi protejate integral si in permanenta pentru acces neautorizat;
- grupurile de utilizatori vor putea fi setate pentru diferite niveluri de acces in sistem;
- sistemul va permite controlul complet al accesului utilizatorilor la aplicatii prin inregistrarea orei si datei la care a fost executata fiecare tranzactie, precum si identitatea utilizatorului care a initiat-o;
- va oferi posibilitatea de blocare facila si selectiva a utilizatorilor;
- va asigura securitatea tuturor interfetelor sistemului informatic prevenind accesul utilizatorilor neautorizati la sistem;
- nu va permite utilizatorilor obisnuiti accesul la datele din baza de date decat prin intermediul functiilor incluse in sistemul informatic (ecrane dedicate);
- in caz de avarii vor exista inregistrate suficiente informatii de diagnosticare pentru a ajuta la identificarea si solutionarea problemei.
- Accesul la date trebuie sa se faca doar prin intermediul serviciilor oferite de componentele informatice, pe baza drepturilor detinute de catre utilizatori, accesul direct la datele din tabele nefiind permis. De asemenea, accesul trebuie sa fie reglementat prin politicile de securitate, aferente fiecarui tip de utilizator.

Sistemul trebuie sa includa mecanisme pentru asigurarea urmatoarelor servicii de securitate:

- confidentialitatea, care asigura ca datele sunt accesibile, vizibile sau disponibile doar utilizatorilor autorizati atat pentru datele stocate cat si pentru cele care tranziteaza sistemul;
- integritatea, care asigura nealterarea datelor sau distrugerea acestora de catre o actiune neautorizata;





- Înregistrarea în jurnal a autentificărilor cu succes (dată, oră, adresa IP)
- Înregistrarea în jurnal a autentificărilor fără succes (dată, oră, adresa IP)
- Aceste jurnale vor fi disponibile în aplicație pentru vizualizare de către administratorii sistemului.

## 2.7 Confidențialitatea datelor

În cadrul proiectului se vor respecta următoarele principii:

- că urmează abordarea **confidențialității prin concepție** pentru a asigura securitatea modulelor și a infrastructurii lor complete;
- că respectă cerințele și obligațiile juridice privind **protecția și confidențialitatea datelor** recunoscând riscurile la adresa confidențialității care reies din analiza și prelucrarea avansată a datelor.

## 2.8 Backup

Backup-ul datelor din Platforma Integrată se va realiza cu ajutorul unei aplicații dedicate ce va fi livrată în cadrul proiectului și care va asigura backup la nivelul serverelor din componerea Platformei.

Aceasta va permite programarea operațiunilor de back-up (atat integral cat si incremental) precum și verificarea integrității datelor din fișierele rezultate. Back-up-urile rezultate vor putea fi folosite imediat oricand pentru a porni un sistem in pericol ca si o masina virtuala cu acces la toate datele din sistemul respectiv, salvate la ultimul back-up, fara a fi necesara restaurarea partitiei rezervate de sistemul de operare sau restaurarea generala, operatiuni cu durata ridicata de timp. Realizarea back-up-ului va include toate componentele serverelor: sistemul de operare, aplicatiile, serviciile, configurarile si setarile specifice precum si toate celelalte date.

SIPOCA 647  
SMIS 129270

Proiect finanțat  
din POCA

Remis spre rambursare  
către AM POCA

