



RTSolutions

S.C. “Rețele Terestre” S.R.L., str. Mitropolit G. Bănulescu-Bodoni 59/B, of. 825, tel/fax (+373) 22 101 777, e-mail: office@rts.md

ELABORAREA PAGINII WEB: Monitorul.md

ABORDAREA TEHNICĂ A PROIECTULUI



Cuprins

1. STANDARDE UTILIZATE LA ELABORARE PORTALULUI:	3
1.1. COMPONENTELE TEHNICE	3
1.2. UTILIZAREA APLICAȚIILOR OPEN SOURCE	3
1.3. UTILIZAREA BAZEI DE DATE	3
2.3. COMPONENTE EXTERNE	6
3. CERINTE FUNCTIONALE:	6
4. CERINȚE DE SECURITATE	9
5. MACHETAREA	11
6. SERVERUL, PLATFORMA	11
7. LOGURILE ȘI GOOGLE ANALYTICS, YANDEX METRICA	13

1. STANDARDE UTILIZATE LA ELABORARE PORTALULUI:

Proiectarea sistemului informațional va îndeplini cerințele de compatibilitate și accesibilitate în concordanță cu specificațiile naționale precum și cele internaționale, precum ar fi W3C (World Wide Web Consortium, 5 Mai 1999) și recomandările WAI (Web Accessibility Initiative), acceptate la nivel mondial drept standarde internaționale în domeniul accesibilității web.

Toate browser-ele de Internet (Internet Explorer 11, Edge, Firefox, Chrome) cu toate versiunile acestora, dar nu mai vechi de 2 ani trebuie să poată afișa corect conținutul site-ului.

1.1. COMPONENTELE TEHNICE

Utilizarea procedeeleor tehnologice în cadrul proiectului:

- PHP 7,2;
- Bootstrap 4 (responsive design);
- HTML;
- CSS;

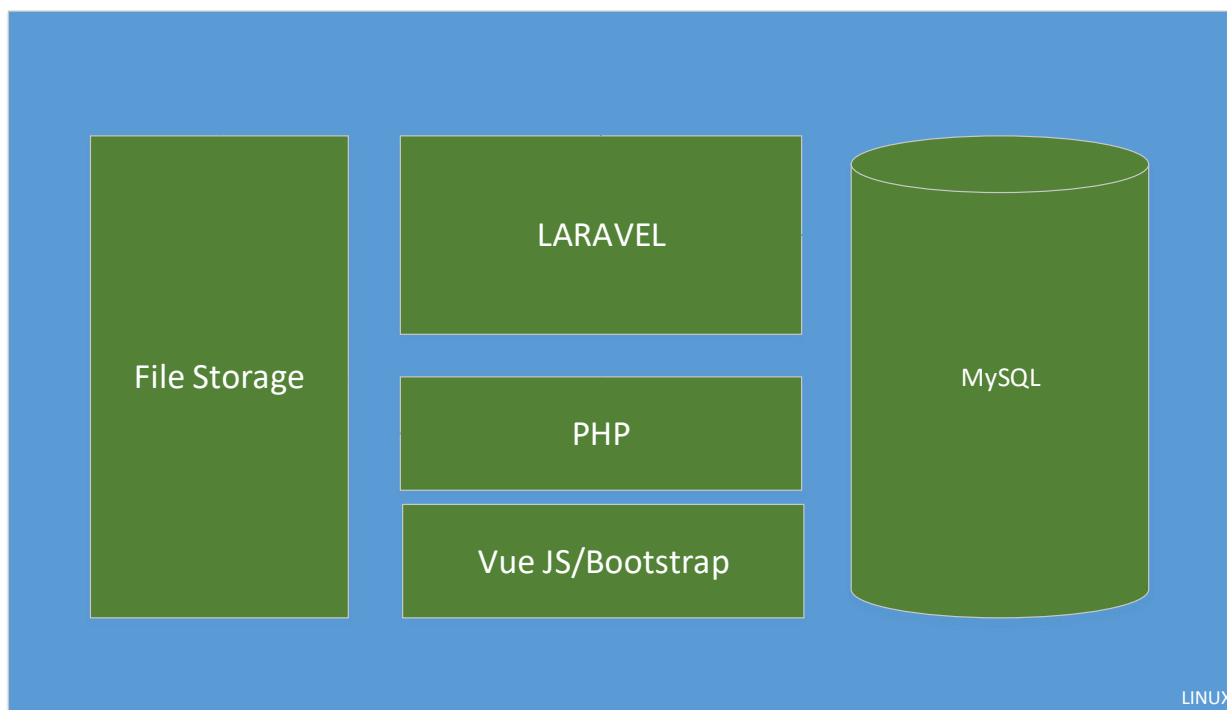
1.2. UTILIZAREA APLICAȚIILOR OPEN SOURCE

- Laravel 5.x;
- Unix (CentOS 6 latest)
- nGinx
- Java Script

1.3. UTILIZAREA BAZEI DE DATE

MySQL 5,7

2. ARHITECTURA SERVER



2.1. PLATFORMA LARAVEL

Laravel Framwork – propunem la necesitate utilizare aceasta platforma datorita scalabilității acesteia si posibilitatii crearii diferitor sisteme informationale, indiferent de nivelul de complexitate al acesteia. Datorita posibilităților sale aceasta platforma a devenit **numărul 1 in lume** <https://coderseye.com/best-php-frameworks-for-web-developers/>

Definit ca un limbaj de programare Open Source, Laravel a câștigat prin simplitatea și facilitatea interfaței prezentate un număr mare de programatori. Considerat nu doar simplu de instalat și folosit, ci și elegant, Laravel prezintă acea doză de atractivitate care poate încânta ochiul tehnic al dezvoltatorului web, care își dorește să creeze layout-uri aspectuoase. Este vorba despre o revoluționare a tot ceea ce înseamnă, de ani buni, PHP și Wordpress (în ceea ce privește blogurile specializate).

Laravel rezolvă una dintre cele mai întâlnite probleme ale dezvoltatorilor: aceea a livrării rapide a unui produs validat și bine cotate la nivelul pieței internaționale. Extrem de importantă este și dezvoltarea unui produs care să exprime profesionalism, seriozitate sau care să convingă consumatorii să treacă la următoarea etapă, aceea a achiziției.

Toate aceste probleme par a fi facil rezolvate de o soluție Open Source, cunoscută în rândul programatorilor sub numele de Laravel. Ușurința în folosirea Laravel este consolidată și de manualul de utilizare, complet și extrem de bine documentat.

De asemenea, în jurul acestui framework s-a construit o comunitate puternică de dezvoltatori și tester, pregătită prin experiența proprie, să ofere soluții reale problemelor pe care le puntează dezvoltatorii.

2.2. LISTA MODULE INTERNE

Nr	Lista module	Scurta descriere
1.	Dashboard	Vizualizarea grafica a diferitor tipuri de informație și acces rapid la aceasta din prima pagina
2.	Modulul designer de slider	Posibilitate de plasare și modificare slider din backoffice
3.	Modulul de căutare	Posibilitate de căutare rapidă a diferitor date conform principiilor stabilite
4.	Modulul de gestiune profiluri și roluri	Modul de gestiune
5.	Modulul de gestiune a permisiunilor	Modul de gestiune
6.	Modulul de gestiune a utilizatorilor	Modul de gestiune
7.	Modulul de gestiune a log-urilor interne	Modul de vizualizare
8.	Modulul de gestiune a log-urilor externe	Modul de vizualizare
9.	Modul de gestiune noutati/articole	Modul va oferi posibilitate de creare a paginilor dinamice și statice nelimitat
10.	Modulul de suport lingvistic	Modul de suport lingvistic (pagini, publicații) cu posibilitatea de a efectua modificări prin intermediul panoului administrativ
11.	Modul setari	
12.	Modul de bannere	Plasarea și gestionarea publicitatii
13.	Publicarea modulelor și vizualizarea fișierelor pdf + flexpaper / flux	Modul de upload și/sau generare PDF

14.	Modul de produs	Comercializare abonamente electronice
15.	Modul de notificare prin e-mail	Transmitere de mesaje in format email
16.	Modul de statistica/Zilnic/Saptaminal/Lunar/Anual	Abonamente comercializare in dependenta de tip al acestuia
17.	Transfer al bazei de date	Migrarea continutului din portal vechi in cel nou
18.	Sistem de plati electronice mPay	Integrare cu sistemul de plati electronice
19.	Reîmprospătarea designului site-urilor existent	pagini de site + cont de utilizator) + aducerea designului mobil
20.	Responsive design	Aplicarea designului catre toate pagini

2.3. COMPONENTE EXTERNE

Nr	Lista module	Scurta descriere
21.	Zona de autorizare	Componente de autentificare in sistem
22.	Restabilire parola	Posibilitate de a reseta parola de acces la sistem integrata cu mail server
23.	Cabinet personal Date personale	Zona grafica prin intermediul căruia utilizatorii vor avea acces la informații prestabilite in sistem.
24.		
25.	Integrare Social Media	Posibilitate de efectuare share prin intermediul butoanelor SMM

3. CERINTE FUNCTIONALE:

3.1.1. AUTENTIFICARE

Business procesul de autentificare pe portalul dedicat raportări unde va introduce login si parola. Autentificarea se va efectua prin credențialele oferite de către administratorul sistemului la activarea contului. Ulterior, utilizatorul are posibilitate sa-si modifice singur parola. Exista cerințe de complexitate privind setarea parolei, precum lungimea si caracterele utilizate. Administratorul SI are posibilitatea de a dezactiva si reactiva ulterior conturile utilizatorilor.

3.1.2. ROLURI

Sistemul va prevedea un set strict definit de roluri și drepturi.

Pentru toate rolurile:

- Autorizare pe site;
- Cppcha
- ieșirea din sistem.

Administratorul - Angajatul ONVV, cu drepturi depline de acces la sistem :

- Administrarea generală a site-ului: acces la setări pentru toate module.
- Gestionarea profilurilor utilizatorilor (vizualizarea, editare etc.);
- Vizualizarea, editarea conținutului a paginilor de conținut.;
- Vizualizarea, editarea, adăugarea noutăților.

User – utilizator (persoana juridică), cu acces exclusiv la partea client a sistemului

3.1.3. MANAGEMENTUL UTILIZATORILOR ȘI ACCESUL LA SISTEM

Pentru asigurarea managementului utilizatorilor (administratori de sistem si utilizatori web-aplicație) si accesului la website, se vor avea in vedere urmatoarele:

- identificarea in mod unic a fiecarui utilizator prin crearea de conturi unice si personalizate de acces;
- gestionarea centralizata si unitara a accesului utilizatorilor prin autorizarea utilizatorului doar la componentele si modulele aplicative ale website-ului conform cu drepturile de acces si atributiile specifice;
- accesul la orice componenta logica de website, se va putea realiza doar prin autentificarea utilizatorilor / administratorilor
- credentialele de acces la aplicatie pentru utilizatori vor fi obținute doar prin intermediul administratorilor;
- credențialele de acces la componentele de website vor fi limitate la nivelul administratorilor si utilizatorilor cu drepturi privilegiate [ex: administratori webserver, DNS, application, backup, fileserver, owner folder, user fileserver] si vor fi controlate într-un director distinct de cel al utilizatorilor aplicației.

3.1.4. AUTENTIFICARE

Procesul de autentificare va fi efectuat prin accesarea link-ului respectiv, unde în baza login-ului și parolei se vor autentifica în cabinetul personal.

Astfel :

- Mecanismul de autentificare al aplicației web, trebuie să respingă orice tentativă de acces la aplicație în situațiile în care:
 - Username-ul este greșit;
 - Parola este greșită;
 - Nu sunt îndeplinite simultan toate condițiile anterioare.
- Deși tehnic mecanismul de autentificare nu permite accesul la aplicație a persoanelor neautorizate sau de pe stații din afara sistemului, utilizatorii trebuie instruiți asupra securității și asupra faptului că nu trebuie să înstrăineze credențialele de acces.
- Credențialele de acces la aplicație ale utilizatorilor vor fi destinate exclusiv aplicației și nu vor putea fi utilizate pentru accesarea sau modificarea configurației sistemului și nici pentru accesul la resurse specifice administratorilor sau utilizatorilor privilegiați [ex: backup, fișiere de configurare, fișiere de sistem, registre, instalări, update-uri];
- Politica parolelor [lungime, complexitate, valabilitate, număr de încercări nereușite] trebuie să poată fi aplicată unitar de către administratorii de sistem tuturor utilizatorilor aplicației.
- Aplicația va loga informațiile importante din activitatea utilizatorilor pentru a permite administratorilor investigații de tip „cine-ce-unde-când” a executat operațiuni în aplicație. Furnizorul soluției website-ului, trebuie să cunoască complexitatea logurilor astfel încât să poată identifica în cadrul investigațiilor „cine-ce-unde-când” a executat operațiuni specifice aplicației cu un istoric de minim 1 an.
- Serverul web accesat de către utilizatorii aplicației trebuie să fie protejat și de firewall software. Pe serverul web nu se vor instala și nu vor rula componente sau servicii în afara celor destinate accesului web. Traficul prin protocol nesecurizat http trebuie să fie oprit.
- Utilizatorii nu vor avea acces la alte componente ale website-ului din centrul de date în afara aplicației web, pe portalul special destinat acesteia.

3.1.5. CĂUTAREA PE SITE

Căutare pe site ar trebui să fie activată în header-ul site-ului, făcând click pe iconița de căutare:

Apare câmp de introducere:

În acest câmp utilizatorul trebuie să introducă informația căutată și să facă click pe «Enter». După ce el trebuie să acceseze pagina cu rezultatele căutării. Rezultatele căutării sunt construite sub formă de listă, fiecare rând al listei poate fi de mai multe tipuri:

- ❖ Link -ul către noutăți (titlu, data);
- ❖ Link-ul către documente (numele documentului, tip fișier, dimensiunea fișierului);
- ❖ Link-ul către pagina de conținut a site-ului (titlu paginii).

4. CERINȚE DE SECURITATE

Prin securitate informațională se înțelege protejarea resurselor informaționale împotriva acțiunilor premeditate sau accidentale cu caracter natural sau artificial, care au ca rezultat cauzarea prejudiciului posesorilor și utilizatorilor sistemului.

Sarcinile de bază ale asigurării securității informaționale vor fi:

- Asigurarea confidențialității informației, adică prevenirea accesului la informație a persoanelor fără drepturi și împuterniciri corespunzătoare;
- Asigurarea integrității logice a informației, prevenirea introducerii, actualizării și nimicirii nesanctionate a informației;
- Asigurarea integrității fizice a informației;
- Autentificarea și autorizarea, dirijarea accesului, înregistrarea acțiunilor.
- Soluția web va fi implementată astfel încât să respecte legislația privind protecția datelor persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.
- Având în vedere importanța datelor prelucrate, este esențială implementarea și respectarea celor trei principii fundamentale ale securității informatice în funcționarea sistemului:
 - Confidențialitatea datelor vehiculate de către sistemul informatic;
 - Integritatea datelor, a sistemului în sine (configurații, setări, etc);
 - Disponibilitatea sistemului în orice condiții.
- Soluțiile web trebuie să fie protejate împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care aceasta le gestionează. Designul soluției de securitate trebuie să fie astfel conceput încât să asigure securitatea și confidențialitatea atât a datelor personale ale utilizatorilor, dar și a conținutului și funcționalităților aplicației, astfel încât utilizatorii să acceseze doar acele secțiuni și conținut care le este permis prin apartenența la un profil sau machetă de securitate.
- Soluția de securitate va fi configurată astfel încât:



- Să nu permita persoanelor neautorizate modificarea sau alterarea semnificației a informațiilor din sistem;
- Să asigure consistența datelor și să permită identificarea sursei datelor inițiale și a persoanelor care au accesat sau au înregistrat aceste date în sistem;
- Să asigure securizarea / protecția datelor vehiculate pe mai multe niveluri: la nivel de acces în rețea, la nivel de aplicație și la nivel de bază de date.
- Paginile web trebuie să fie configurate încât să ofere protecție pentru următoarele vulnerabilități:
 - Cross-site scripting;
 - Information leakage;
 - Predictable resource location;
 - SQL injection;
 - iFRAME injection;
 - Insufficient authentication;
 - Insufficient authorization;
 - Abuse of functionality;
 - Directory indexing;
 - HTTP response splitting;

Pentru a preveni riscurile asociate compromiterii credențialelor privilegiate [de administrator de sistem] se va implementa soluția de autentificare cu următoarele caracteristici:

- Soluția trebuie să autentifice toate activitățile realizate, incluzând operațiunile administrative și activitatea administratorilor. Întregirarea activității administratorilor trebuie să permită identificarea username-ului din sistemul informatic care a realizat respectiva activitate;
- Soluția trebuie să permită o analiză de risc asociată tentativei de login, analiza care trebuie să ia în considerare cel puțin: locația din care se realizează accesul, sistemele la care se solicită acces și device-urile de pe care se realizează solicitarea de acces iar în urma acestei analize să poată permite sau refuza accesul precum și să poată solicita modificarea metodei de autentificare a utilizatorului;
- Soluția trebuie să asigure stabilirea exactă a operațiunilor permise fiecărui utilizator;
- Credențialele de acces ale utilizatorilor la aplicație trebuie să fie unice în sistem și vor putea fi generate și gestionate doar de către administratorii de sistem; parolele de acces vor fi criptate;
- Soluția trebuie să asigure gestionarea parolelor pentru conturile privilegiate — inclusiv modificarea parolelor după ce acestea au fost utilizate și / sau la intervale



regulate. De asemenea, soluția trebuie să asigure personalizarea politicilor aferente compoziției parolelor precum și vizualizării parolelor;

- Soluția trebuie să asigure stabilirea exactă a operațiunilor permise fiecărui utilizator;
- Soluția trebuie să fie compatibilă cu certificatele SSL.
- Pentru asigurarea îndeplinirii cerințelor de securitate legate de constrângerile privind prelucrarea datelor, sistemului informatic trebuie să se respecte următoarele reguli aferente:
 - Confidențialitate - asigurarea protecției datelor împotriva acceselor neautorizate.
 - Integritate - asigurarea protecției, exactității și completitudinii datelor și a soluțiilor furnizate pentru stocarea și gestionarea acestora, dar și asigurarea împotriva manipulării frauduloase a datelor/informațiilor.
 - Asigurarea controlului centralizat al tuturor aspectelor legate de securitate (autentificare, autorizare, auditare etc.), bazat pe separarea clară între control și date/informații.

5. MACHETAREA

- Web site-ul trebuie să fie corect vizualizat în următoarele browser-uri (versiunile actuale):
 - Internet Explorer;
 - Microsoft EDGE;
 - Chrome
 - FireFox;
 - Opera;
 - Safari.
- Site-ul va trece cu succes validarea pe <http://validator.w3.org>.
- Site-ul trebuie să fie vizualizat la un monitor cu o rezoluție minimă de 1024 x 768 px fără scroll orizontal. Cu toate acestea, design-ul va fi conceput automat dimensionabil pentru rezoluțiile superioare celei standard.
- Elementele click'abile trebuie să fie dinamice, adică să reacționeze (prin mișcare sau culoare) la hover, click.

6. SERVERUL, PLATFORMA

Baza de date:

Serverul de baze de date trebuie să aibă următoarele caracteristici:

- serverul de baze de date va fi scalabil atât în performanță cât și în capacitate. Va trebui să ofere posibilitatea de a mări capacitatea de stocare, la cerere;
- serverul de baze de date va fi ales de către prestator, fiind o varianta compatibilă cu serverele de baze de date MySQL;
- bazele de date vor fi compatibile cu standardele limbajului SQL;
- administratorul va avea posibilitatea de a administra conținutul informației, de a realiza copii de siguranță și a stoca și readuce informația din arhive;
- scalabil orizontal și vertical, cu model relațional integrat și suport Extensible Markup Language (XML);

Pe server se va menține facilitatea care îi permite beneficiarului crearea de copii de rezervă a bazei de date în producție.

Sistemul de backup al site-ului web pentru protejarea datelor trebuie să asigure:

- Posibilitatea de creare a unei copii de rezervă a întregului site;
- Posibilitatea restaurării site-ului pe baza copiei de rezervă;
- Posibilitatea de filtrare a conținutului site-ului, a fișierelor și a directoarelor pentru care se dorește crearea de copii de rezervă;
- Posibilitatea programării unui proces de backup automat.

Limbaj de programare: PHP. În site nu va fi utilizat flash. Toate elementele active vor fi elaborate pe CSS, Javascript, AJAX

Web Server: nGinx

La etapa de elaborare, site-ul va fi plasat pe serverul Executorului, la care va avea acces și Beneficiarul pentru a testa și a încărca conținutul.

După finisarea lucrărilor, Executorul va asigura transferul site-ului și bazei de date pe serverul ales de către Beneficiar.

În cadrul paginii – web a proiectului wineofmoldova.com informația va fi prezentată și stocată în format **Unicode (UTF-8)**, lucru care va permite stocarea în baza de date a informației în orice versiune lingvistică. Conținutul paginii – web și, de asemenea, facilitățile de administrare vor fi

realizate în limbile română, engleză și rusă cu folosirea caracterelor latine, chirilice și diacriticele românești (ș, ț, ă, î, â).

Cerințe referitor la performanța site-ului:

- Timpul mediu de încărcare a unei pagini: 2-3 secunde, în funcție de tipul de conexiune de care dispune utilizatorul;
- Indexarea cuvintelor cheie, titlului paginii, conținutului, titlurilor link-urilor pentru o mai bună performanță;
- Page Caching - să permită printr-un sistem de cache să rețină pagina astfel încât, dacă mai există o cerere pentru aceeași pagină, să o poată afișa mai repede.

7. LOGURILE ȘI GOOGLE ANALYTICS, YANDEX METRICA

- Fișierele log vor stoca datelor de accesare și gestiune a paginii web Wine of Moldova (conectare, citire date, erori, etc.). Fișierele log vor sta la baza mecanismului de extragere a statisticilor soluției informatice și asigurare a securității informației.
- La fel site-ul va fi integrat cu serviciul Google Analytics pentru oferirea informațiilor statistice de accesare a site-ului și a activității utilizatorilor.
- În cadrul serviciului Google Analytics vor fi definite raporate personalizate și tablouri de board după specificațiile beneficiarului.