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: MBW.MD

ABORDAREA TEHNICĂ A PROIECTULUI

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

Cuprins

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

1. STANDARDE UTILIZATE LA ELABORARE PORTALULUI:

Proiectarea sistemului informațional va îndeplini cerințele de compatibilitate şi accesibilitate în concordanță cu specificațiile naționale precum si cele internaționale, precum ar fi W3C (World Wide Web Consortium, 5 Mai 1999) şi 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 procedeelor tehnologice în cadrul proiectului:

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

1.2. UTILIZAREA APLICAȚIILOR OPEN SOURCE

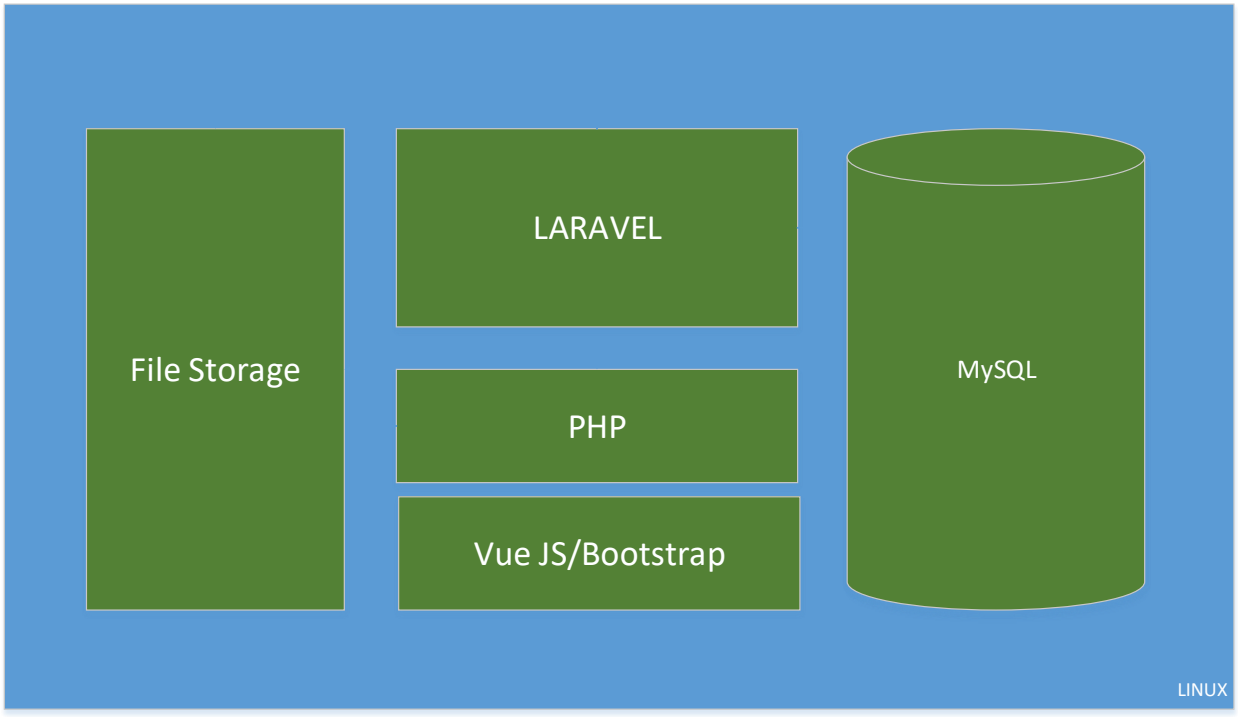
- Laravel 5.x;
- Unix (CentOS 6 latest)
- nGinx
- Java Script

1.3. UTILIZAREA BAZEI DE DATE

MySQL

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

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 interfației 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 cotat la nivelul pieței internationale. 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 testeri, pregătită prin experiența proprie, să ofere soluții reale problemelor pe care le punctează dezvoltatorii.

2.2. LISTA MODULE INTERNE

Nr	Lista module	Scurta descriere
1.	Dashboard	Vizualizarea grafica a diferitor tipuri de informație si acces rapid la aceasta din prima pagina
2.	Modulul designer de slider	Posibilitate de plasare si modificare slider din backoffice
3.	Modulul de căutare	Posibilitate de căutare rapida a diferitor date conform principiilor stabilite
4.	Modulul de gestiune profiluri si 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 si statice nelimitat

2.3. COMPONENTE EXTERNE

Nr	**Lista module**	**Scurta descriere**
10.	Zona de autentificare	Componente de autentificare in sistem
11.	Restabilire parola	Posibilitate de a reseta parola de acces la sistem integrata cu mail server
12.	Cabinet personal	Zona grafica prin intermediul căruia utilizatorii

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

	Date personale	vor avea acces la informații prestabilite in sistem.
13.		
14.	Integrarare 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 sl 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;
- Cappcha
- 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;

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

- 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 sa 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 aplicatie a persoanelor neautorizate sau de pe stații din afara sistemului, utilizatorii trebuie instruiti 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 administrătorilor sau utilizatorilor privilegiați [ex: backup, fișiere de configurare, fișiere de sistem, registri, instălari, update-uri];

- Politica parolelor [lungime, complexitate, valabilitate, numar de încercari nereușite] trebuie să poată fi aplicată unitar de catre administratorii de sistem tuturor utilizatorilor aplicației.
- Aplicația va loga informațiile importante din activitatea utilizatorilor pentru a permite administratorilor investigații de tip „cine-ce-unde-cand" a executat operațiuni în aplicație. Furnizorul soluției website-ului, trebuie să cunoască complexitatea logurilor

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

astfel încît să poată identifica în cadrul investigațiilor „cine-ce-unde-cînd" a executat operațiuni specifice aplicației cu un istoric de minim 1 an.

- Serverul web accesat de către utilizatorii aplicației trebuie să fie protejat si 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 sa 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 informția 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 nesancționate a informației;
- Asigurarea integrității fizice a informației;
- Autentificarea și autorizarea, dirijarea accesului, înregistrarea acțiunilor.

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

- Soluția web va fi implementată astfel incat sa respecte legislatia privind protectia datelor persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date.
- Avînd în vedere importanța datelor prelucrate, este esențială implementarea și respectarea celor trei principii fundamentale ale securitatii 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 sa fie protejate înpotriva incercărilor deliberate sau accidentale de acces neautorizat la datele pe care aceasta le gestioneaza. Designul solutiei de securitate trebuie sa fie astfel conceput incat sa asigure securitatea si confidentialitatea atat a datelor personale ale utilizatorilor, dar si a continutului si functionalitatilor aplicatiei, astfel incat utilizatorii sa acceseze doar acele secțiuni și conținut care le este permis prin apartenența la un profil sau machete de securitate.
- Soluția de securitate va fi configurată astfel încît:
  - Să nu permita persoanelor neautorizate modificarea sau alterarea semnatica a informatiilor din sistem;
  - Să asigure consistența datelor si sa permita identificarea sursei datelor initiale si a persoanelor care au accesat sau au inregistrat aceste date in sistem;
  - Să asigure securizarea / protecția datelor vehiculate pe mai multe niveluri: la nivel de acces in rețea, la nivel de aplicație și la nivel de bază de date.
- Paginile web trebuie să fie configurate încît 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 urmatoarele caracteristici:

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

- Soluția trebuie să autentifice toate activitățile realizate, incluzînd operațiunile administrative și activitatea administratorilor. Întregistrarea 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 sa ia in considerare cel puțin: locația din care se realizeaza 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 reufza accesul precum și să poată solicita modificarea metodei de autentificare a utilizatorului;
- Soluția trebuie să asigure stabilirea exactă a operațiunilor permise fiecarui utilizator;
- Credențialele de acces ale utilizatorilor la aplicație trebuie să fie unice în sistem și vor putea fi genereate 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 dupa ce acestea au fost utilizate și / sau la intervale regulate. De asemenea, soluția trebuie să asigure personalizarea politicilor aferente compozitiei 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 constrîngerile privind prelucrarea datelor, sistemului informatic trebuie sa se respecte urmatoarele reguli aferente:
    - Confidențialitate - asigurarea protecției datelor înpotriva acceselor neautorizate.
    - Integritate - asigurarea protecției, exactității și completitudinii datelor și a soluțiilor fumizate 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/infomații.

5. MACHETAREA

- Web site-ul trebuie va fi 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 vizualizate la un monitor cu o rezoluţie minimă de 1024 x 768 px fără scroll orizontal. Cu toate acestea, design-ul va fi conceput automat dimensionabil pentru rezoluţiile superioare celei standard.
- Elementele click’abile trebuie să fie dinamice, adică să reacţioneze (prin mişcare 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 atît în performanțiă cît 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 si 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 producţie.

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;

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

- Posibilitatea de filtrare a conținutului site-ului, a fişierelor şi a directoarelor pentru care se doreşte 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: Apache

La etapa de elaborare, site-ul va fi plasat pe serverul Executorului, la care va avea acces şi Beneficiarul pentru a testa şi a încărca conţinutul.
După finisarea lucrărilor, Executorul va asigura transferul site-ul şi bazei de date pe serverul ales de către Beneficiar.

În cadrul paginii – web a proiectului wineofmoldova.com informaţia va fi prezentată şi stocată în format **Unicod (UTF-8)**, lucru care va permite stocarea în baza de date a informaţiei în orice versiune lingvistică. Conţinutul paginii – web şi, de asemenea, facilităţile de administrare vor fi realizate în limbile română, engleză şi rusă cu folosirea caracterelor latine, chirilice şi diacriticele româneşti (ş, ţ, ă, î, â).

Cerințe referitor la performanța site-ului:

- Timpul mediu de încarcare 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 încît, 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.

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