UNIUNEA EUROPEANĂ
Fondul Social European

GUVERNUL ROMÂNIEI
Ministerul Administraţiei şi Internelor

Inovaţie în administraţie
Programul Operaţional "Dezvoltarea Capacităţii Administrative"

Proiectul "Creşterea capacităţii administraţiei publice de a gestiona procesele de recrutare, selecţie şi evaluare a funcţionarilor publici în contextul creşterii gradului de responsabilizare a administraţiei publice privind gestionarea funcţiei publice" cod SMIS 35032
Proiect cofinanţat din Fondul Social European prin Programul Operaţional Dezvoltarea Capacităţii Administrative

MODUL 1

„MANAGEMENTUL FUNCŢIEI PUBLICE"

TEHNOLOGIA INFORMAŢIEI ÎN MANAGEMENTUL FUNCŢIEI PUBLICE

Manualul participantului

Aprilie 2012

Acest manual a fost realizat în cadrul proiectului "Creşterea capacităţii administraţiei publice de a gestiona procesele de recrutare, selecţie şi evaluare a funcţionarilor publici în contextul creşterii gradului de responsabilizare a administraţiei publice privind gestionarea funcţiei publice" cod SMIS 35032

Agenţia Naţională a Funcţionarilor Publici
Operator de date cu caracter personal înregistrat la A.N.S.P.D.C.P. sub nr.19986

Cuprins

Tehnologia informaţiei în managementul funcţiei publice

1 Concepte de bază în utilizarea tehnologiei informaţiei

1.1 Internetul

Internetul îşi are originea într-un proiect militar desfăşurat de guvernul USA prin intermediul ARPA-NET.

În anii 1960, guvernul SUA, ca răspuns la succesul Uniunii Sovietice referitor la primul satelit, a înfiinţat ARPANet (Advance Research Projects Agency Network), însărcinată cu dezvoltarea unei reţele de comunicaţii computerizate, care să ramina disponibilă în condiţiile în care 80% dintre infrastructura sa ar fi fost afectată de un atac nuclear.

Reţeaua a legat în primă instanţă patru calculatoare aflate la Universitatea California din LA, Institutul de Cercetari Stanford, Universitatea California din Santa Barbara şi Univesritatea din Utah şi a folosit tehnologia comutarii de pachete.

Ulterior, în anii ’70, acestei reţele s-au adaugat diverse alte noduri de la universitati din SUA cât şi din Europa (Norvegia şi Londra).

În anul 1975, reţeaua a fost declarată oficial ca şi funcţională iar în anul 1983 ea s-a scindat în reţeaua militară MILNET şi partea civilă de reţea.

În cadrul reţelei, în anul 1972 a fost implementat serviciul de poştă electronică (email) iar la scurt timp s-a dezvoltat protocolul TELNET, utilizat pentru conectarea la calculatoare de la distanţă. În acelaşi an a aparut şi protocolul FTP (File Transfer Protocol), ce permite transferul fişierelor între calculatoare.

Abia în anul 1989, o echipă de la Laboratorul European de Fizică a Particulelor - CERN a propus conceptul de legare a documentelor prin *hypertext.* Astfel s-a născut conceptul de World Wide Web.

În anul 1993 a aparut primul browser web grafic, Mosaic – predecesorul Netscape Navigator.

Există diferite tipuri de rețele, dintre care cele mai importante sunt:

- wide area network (WAN) un calculator dintr-o anumită rețea comunică cu un alt calculator aflat la o distanță foarte mare (chiar în altă țară).
- local area network (LAN) calculatoarele sunt localizate foarte aproape unele de altele, în aceeași clădire, sau birou.

Internetul poate fi definit ca o multitudine de calculatoare conectate în rețea, extrapolând o reuniune de rețele de calculatoare fără a exista un raport de subordonare.

Odată cu apariția aplicațiilor de navigare web, Internetul s-a dezvoltat rapid devenind astfel cea mai mare rețea mondială de calculatoare.

Conectarea la Internet se realizează prin mai multe metode:

- dial-up – utilizând liniile telefonice și modem-urile
- network – utilizând cablu UTP
- CATV – utilizând cablu coaxial tv
- ADSL – utilizând fibra optică sau cupru
- Wireless – utilizând rețele radio

1.2 Funcţionarea World Wide Web

WWW utilizează principiul de lucru în rețea de tipul client-server.

Partea de client este deservită de browserele web. Când se introduce adresa URL (Uniform Resource Locator) în browser, acesta efectuează o cerere HTTP (Protocol de Transfer Hyper-Text) către calculatorul care deţine acea adresa (acest calculator poarta denumirea de server web).

La primirea cererii, serverul de web, returneaza pagina solicitata, într-o forma pe care browserul o poate interpreta.

1.3 Pagina Web

O pagină web reprezintă, de regulă, o colecţie de text, imagini, animaţii, etc. În general, fiecare pagină este un fişier separat pe serverul de web. Un site web este compus dintr-o colecţie de pagini web separate care sunt gestionate de un program denumit server de web

1.4 Serverele Web

Un server de Web este folosit cu două înţelesuri. Unul dintre ele se referă la programul care primeşte cererile HTTP şi prezintă pagina Web solicitată, într-un format pe care îl poate afişa browserul de Web. Se pot aminti între serverele de Web, programe precum Microsoft – IIS, Apache – Web Server.

Pe de altă parte, termenul este utilizat pentru a desemna calculatorul (maşina fizică) pe care rulează programul serverului de Web.

1.5 Browsere Web

Un browser web este un program instalat pe calculatorul persoanei care navighează pe web şi are ca rol interpretarea şi afisarea paginilor Web.

Primul browser grafic a fost Mosaic, produs de NCSA (National Center for Supercomputing Applications). A fost urmat de Netscape Navigator.

În ziua de astăzi, putem aminti urmatoarele browsere web: Microsoft Internet Explorer, Mozilla Firefox, Opera, Google Chrome, Safari (produs de Apple).

1.6 Definirea şi înţelegerea termenilor: HTML, HTTP, URL, Hyperlink

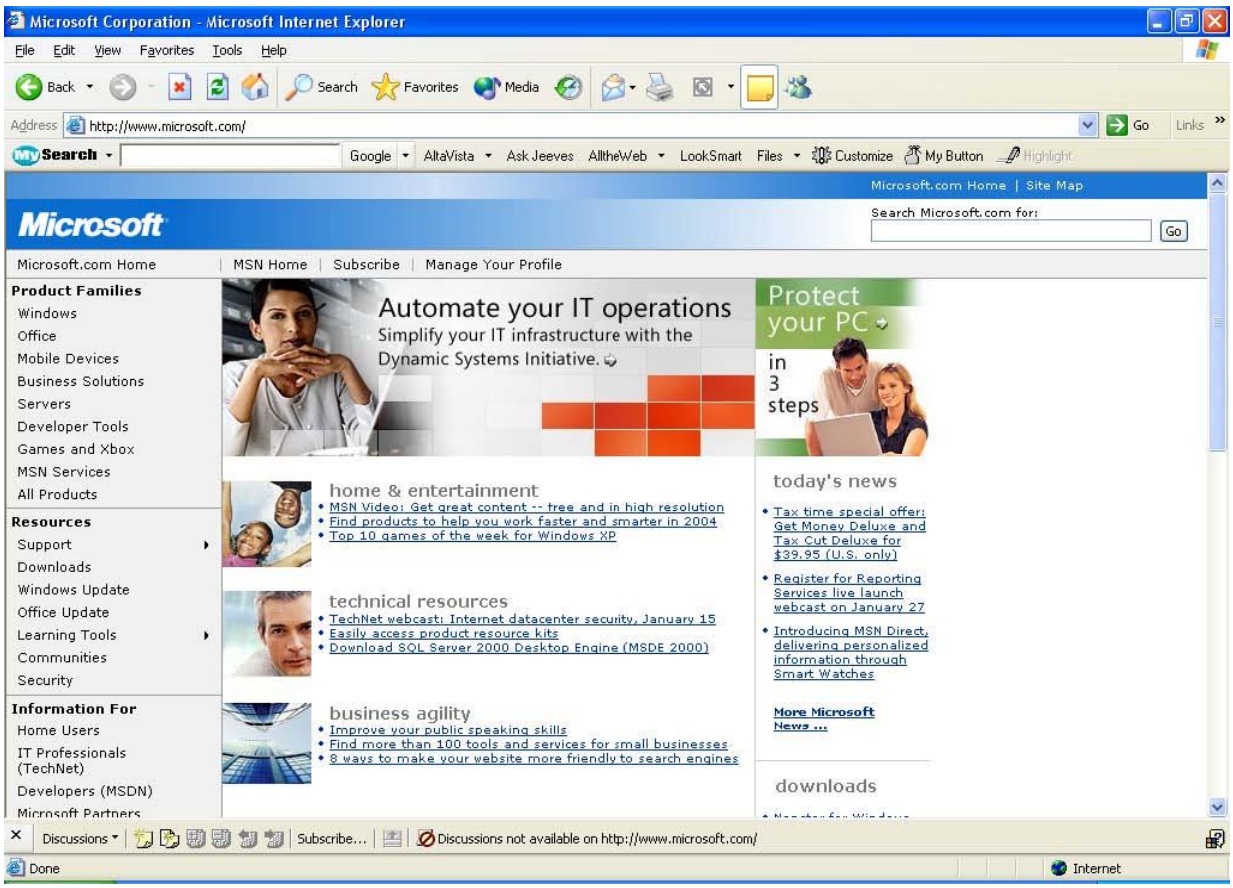
Hypertext Markup Language (HTML) este un limbaj cu ajutorul căruia se scriu pagini web pentru WWW.

Limbajul HTML îi permite textului să includă diferite fonturi, diferite imagini grafice şi legături. Acesta oferă o metodă de prezentare a textului, imaginilor, sunetelor şi filmelor ce sunt legate într-un mod nesecvenţial.

Hyperlink este o adresă într-o pagina Web, care face legătura spre altă pagină web (sau către alte tipuri de documente). Astfel, acesta lansează automat:

- Salt la o diferită parte a aceeaşi pagini;
- Salt la o diferită parte site-ului Web;
- Salt la o diferită pagină dintr-un diferit Web site;
- Activează o descărcare de fişiere;
- Lansează o aplicaţie video sau de sunet.

Poza de mai jos prezintă un fragment dintr-o pagină Web. Grupurile de text subliniate indică un hyperlink. Implicit linkurile sunt colorate în albastru.



Uniform Resource Locator (URL) identifică o resursă pe Internet ce oferă legături între două documente din WWW. Fiecare resursă din Internet are propria sa adresă de identificare sau un URL care specifică serverului unde să o găsească.

URL-ul este format din două părţi:

- Numele protocolului, cum ar fi: FTP şi HTTP.
- Numele domeniului.

  URL poate folosi diferite protocoale

Structura unei adrese de web

Calculatoarele comunică în rețea prin intermediul pachetelor de date. Un pachet este o informaţie logică ce cuprinde informaţii atât despre localizarea datelor, cât şi despre datele utilizatorului.

Orice calculator aflat în reţea are o adresa IP ce îi permite să fie identificat în mod unic în cadrul reţelei. Adresa IP este formată din clasa de rețea, adresa de reţea şi adresa calculatorului care primeşte mesajul.

Asemănător trimiterii unei scrisori, trebuie, în primul rând, cunoscut numele străzii (adresa de rețea) și apoi numărul unde se trimite scrisoarea (adresa calculatorului care primește mesajul).

Odată cu dezvoltarea Internetului nu a mai fost ușor de ținut evidența adreselor de rețea (IP-urilor) și a apărut termenul de DNS (Domain Name System) – care structurează sistemul de nume, al dispozitivelor din Internet, pe domenii subdomenii.

Exemplu de adresa ecdl.org.ro este reprezentată astfel: ecdl – subdomeniu în cadrul domeniului org; org – subdomeniu în cadrul domeniului ro.

Ca tipuri, cele mai cunoscute domenii sunt cele de țară (ro, de, fr, it, ch, uk, etc) și cele generice (com, edu, gov, net, org, etc).

Un protocol este un sistem de reguli şi proceduri ce guvernează comunicaţia între două sisteme deschise. Există o mulţime de protocoale dar condiţia pentru ca două dispozitive să poată schimba date între ele este ca ele să folosească acelaşi protocol.

Exista mai multe tipuri de protocoale:

- ***Protocoalele de aplicații*** – oferă schimbul de date între aplicațiile existente într-o rețea, ca de exemplu File Transfer Protocol (FTP) sau Simple Mail Transfer Protocol (SMTP).

File Transfer Protocol (FTP) este un proces ce permite schimbul de fişiere între 2 calculatoare.

FTP suportă diferite comenzi ce permit transferul bidirecţional de fişiere binare şi ASCII între diferite calculatoare. Acest protocol este instalat împreună cu utilităţile oferite de TCP/IP.

Simple Mail Transfer Protocol (SMTP) este un protocol TCP/IP folosit la transmiterea mailului.

- ***Protocoalele de transport*** – ca de exemplu Transport Control Protocol (TCP) asigură transmiterea corectă a datelor între două dispozitive.

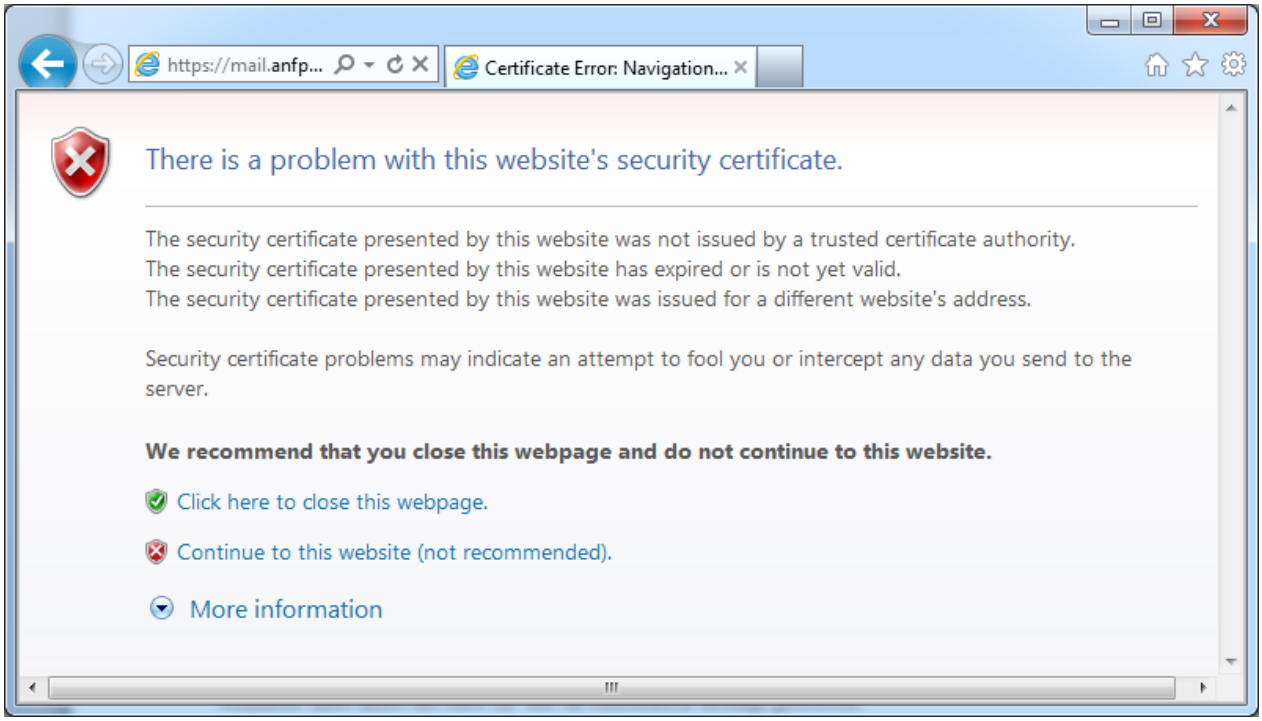
- ***Protocoale de rețea*** **–** ca de exemplu Internet Protocol (IP)

Transport Control Protocol/Internet Protocol (TCP/IP) este un protocol standard folosit pentru a comunica în Internet.

HyperText Transport Protocol (HTTP) este un protocol prin care paginile WWW sunt transferate prin reţea. Este folosit atât de client (browser) cât şi de serverul web.

HyperText Transport Protocol Secure (HTTPS) este un protocol prin care paginile WWW sunt transferate prin reţea în formă criptată. Este folosit pentru a asigura confidenţialitatea datelor aflate în tranzit între client (browser) şi serverul de web.

HTTPS este în acelaşi timp o metodă de autentificare a server-ului web care îl foloseşte, prin intermediul aşa-numitelor "certificate digitale" - o colecţie de date pe care un browser o solicită server-ului pentru a putea începe transferul criptat; dacă certificatul este emis de o autoritate de certificare înregistrată (de exemplu VeriSign), browser-ul poate fi sigur că server-ul cu care comunică este chiar cel pentru care a fost emis certificatul. La accesarea unei pagini web prin protocolul https se poate observa simbolul unui lacăt – care indică modul de accesare securizat. Dacă certificatul utilzat a fost emis local, identificarea serverului nu mai este posibilă dar fluxul de comunicaţii între client (browser) şi server este criptat asigurând confidenţialitatea. Situaţiile în care un server de web foloseşte certificate emise local sunt de regulă limitate (ex. o instituţie işi genereză propriul certificat pentru a cripta informaţiile între serverul de web folosit pentru accesarea web-mail şi browsere). Ca regulă generală, dacă nu ne aflăm într-o situaţie din cele care formează excepţii, nu trebuie continuată navigarea pe o pagină web a carei originalitate nu poate fi identificată prin certificat. În cazul unui certificat ce nu poate fi validat de către nici o autoritate de certificare din baza de date a browserului, când folosim browserul Internet Explorer, bara de adrese va fi colorată cu roşu, iar în partea dreaptă apare mesajul „Certificate Error”.



2 Introducere în securitatea sistemelor informatice şi tranzacţiilor web

2.1 Evoluţia securităţii reţelelor şi sistemelor informatice

2.1.1 Conceptul de securitate

Securitatea sistemelor informatice nu este un simplu concept; este un adevărat proces extins, ce implică instrumente, tehnologii, protocoale şi dispozitive hardware, în vederea securizării datelor şi prevenirii atacurilor informatice.

Soluţii pentru securitatea reţelelor au existat încă din anii `60, însă abia la începutul anilor 2000 se poate vorbi despre o maturizare a soluţiilor disponibile.

Scopul securităţii sistemelor şi reţelelor informatice este acela de a încerca prevenirea atacurilor şi în acelaşi timp reducerea consecinţelor, în momentul în care acestea se întîmplă. Contiunitatea desfăşurării normale a operaţiilor instituţiilor sau companiilor reprezintă un alt aspect de avut în vedere atunci când vorbim de securitate.

Conceptul de site web protejat și calculator protejat

Riscuri în folosirea unui card de credit pe Internet

- Utilizarea cărţilor de credit pentru a cumpară diferite produse de pe Internet trebuie făcută cu grijă deoarece exista pericolul de a fi făcut public contul cardului utilizat şi banii ar putea fi utilizaţi de alte personae neautorizate.
- Trebuie utilizate cu atenție site-urile web de plată on-line sau alte site-uri care solicită date cu caracter personal, deoarece acestea ar putea fi utilizate de persoane rău intenționate în vederea săvârșirii unor infracțiuni sau fraude.

Unele site-uri oferă posibilitatea păstrării confidenţialităţii datelor. De aceea, pentru a avea acces la date va trebui ca utilizatorul sa aibă un nume de utilizator (Username) şi o parolă. Cu aceste date utilizatorul va avea acces la datele din contul lui. Exemplu de site web protejat este orice site de mail (gmail, yahoo mail, etc).

Pe același principiu trebuie restricționat și accesul în cadrul unei rețele de calculatoare. Astfel, accesarea informațiilor în această situație trebuie făcută pe baza unor permisiuni alocate pe grupuri de utilizatori care sunt identificate în politicile de securitate. Un utilizator se identifică, ca fiind membru al unui grup prin introducerea username-ului și a parolei.

Securitatea datelor reprezintă un element foarte important atunci când se lucrează cu date confidenţiale.

Există diferite modalităţi de protejare a datelor:

- Accesul fizic la calculator este restricţionat.
- Adoptarea unei politici de parolare corespunzătoare
- Trebuie să se respecte politica de confidențialitate a parolei
- Stabilirea drepturilor pe care le are fiecare utilizator
- Copierea datelor în mod regulat
- Folosirea programelor de securitate tip firewall
- Folosirea programelor antivirus
- Criptarea fişierelor la care se lucrează

Reguli referitoare la autentificarea utilizatorilor

Identificarea unui utilizator la o resursă informatică se recomandă a fi efectuată cel puțin pe baza numelui de utilizator şi a parolei. Acestea trebuie să fie de o anumită complexitate, ca de exemplu:

- Să fie de minim 9 caractere;
- Să conţină minim o cifră;
- Să conţină minim un caracter special;
- Să conţină minim o literă mare şi o literă mică;
- Nu trebuie să conţină denumirea utilizatorului sau părţi din aceasta;
- Durata de valabilitate a parolei să fie de 180 zile calendaristice, perioadă după care aceasta expiră şi va fi solicitată automat, de către sistem, o nouă parolă la momentul expirării.

Parola şi numele de utilizator sunt confidenţiale fiind nerecomantată comunicarea acestora unei terţe persoane, indiferent de poziţia acelei persoane într-o organizație.

Aspecte legale – Copyright

Copyright-ul este o modalitate legală de protejare a lucrărilor cu condiţia ca
aceste lucrări să aibă o formă tangibilă (adică se pot vedea, auzi sau atinge).
Drepturi de utilizare specifice aplicaţiilor software:

- Programele open source - garantează accesul tuturor utilizatorilor la codul-sursă;
- Freeware – programe care pot fi totuşi difuzate gratis de către autor, care îşi păstrează drepturile de autor;
- Licenţele – acordă dreptul de folosire nu şi drept de comercializare sau distribuţie;
- Shareware - acele aplicaţii sau programe care pot fi achiziţionate direct de la persoana care le-a creat.

2.1.2 Justificarea securităţii sistemelor informaţionale

Securitatea sistemelor informaţionale este strâns legată de termenul de „hacker”, care în ziua de astăzi este folosit în sens greşit – dar acceptat ca atare, pentru a desemna o persoană ce atacă reţele sau sisteme de calcul, animată de intenţii negative. Acestea au ca scop fie urmărirea unui folos material, răzbunarea, interese politice sau o anumită doctrină, recunoaşterea valorii în rândul unei comunităţi, etc. În orice caz, termenul de *„hacker”* desemnează în realitate o persoană care are cunoştinţe extinse despre sistemele de calcul şi reţele şi duce în acelaşi timp un proces continuu de auto-instruire şi perfecţionare.

Termenul corect pentru a descrie o persoană cu intenţii negative este cel de *„cracker”*.

Cracking-ul a inceput încă din anii `60 prin **Phone Freaks.** Phone Freaker-ii erau persoane care generau sunete de o anumită frecvenţă folosind un fluier – imitând în acest fel un ton de dialing în reţeaua publică de telefonie, pentru a opera apeluri telefonice gratuite. Acest fenomen a durat până în jurul anilor `80.

Odată cu evoluţia sistemelor şi reţelelor au evoluat şi metodele de cracking iar în anii 80, odată cu introducerea modemurilor a apărut şi conceptul de **Wardialing.** Acest tip de atac presupune utilizarea unor programe ce scaneză automat numere de telefon dintr-o anumită regiune pentru a căuta computere conectate şi faxuri. În momentul în care acestea sunt descoperite, un program de spart parole este lansat pentru a obţine accesul.

Wardriving-ul apare în anii 90 şi presupune obţinerea de acces neautorizat exploatând tehnologia wireless şi Access Pointurile. Într-un atac wardrive un cracker utilizează un laptop şi un vehicul pentru a scana reţelele wireless dintr-o anumită zonă. După identificarea potenţialelor reţele ţintă sunt utilizate programe de spart parole sau chiar programe de spart algoritmi de criptare, în vederea obţinerii accesului neautorizat asupra sistemelor personale sau ale instituţiilor.

Termenul de ***Malware*** reprezintă orice formă de software periculos, care poate prelua controlul asupra PC-ului și produce daune sau cel puțin comportări stânjenitoare. În această categorie se încadrează virușii, spam-urile, phishing-ul, wormii, caii troieni, etc.

Viruşii sunt programe software maliţioase care se ataşează de alte programe legitime sau fişiere executabile pentru a executa anumite funcţii nedorite, pe sistemele utilizatorilor, fără ştirea acestora.

Mulţi viruşi necesită activarea de către utilizatori şi pot să rămână în stare de hibernare până la o anumită dată. Când se activează, viruşii pot căuta pe disc alte fişiere executabile pentru a le infecta. Viruşii pot să fie inofensivi (ex. virus care afişează o anumită poză pe ecran) sau pot să fie distructivi (ex. ştergerea tututot informaţiilor de pe calculator). Ei se pot de asemenea programa ca să îşi producă mutaţii în cod pentru a nu fi detectaţi de programele anti-virus. Viruşii se transmit prin intermediul stickurilor USB, CD/DVD, hard diskuri portabile, fişiere partajate în reţea sau email. Răsapândirea prin email este cea mai comună formă de propagare în zilele noastre.

Wormii (Worms) sunt programe software maliţioase ce prezintă o periculozitate sporită. Aceştia se înmulţesc singuri, exploatând diverse vulnerabilităţi existente în reţea. De regulă, wormii îincetinesc până la blocare calculatoarele infectate sau reţelele în care se propagă. Dacă un virus necesită un program care să îl ruleze, wormii se pot rula ei înşişi, fără participarea utilizatorilor şi se pot transmite singuri prin intermediul reţelelor. De exemplu SQL Slammer Worm în Ianuarie 2003 a blocat 250 000 de gazde din Internet în interval de 30 de minute de la lansare.

Caii Troieni (Trojan Horses) reprezintă software maliţios care derulează operaţiuni dăunătoare deghizat sub o funcţionalitate utilă. Un virus sau un worm poate căra un cal troian. Acesta conţine cod ce exploateză privilegiile utilizatorului sub care rulează. Jocurile de calculator accesate online pot avea deseori ataşat un cal troian. În momentul în care jocul este executat, acesta funcţionează conform aşteptărilor utilizatorului însă în subsidiar şi troianul rulează şi continuă să ruleze chiar şi după ce jocul a fost închis. Odată instalaţi, aceştia pot cauza distrugeri imediate, pot să deschidă o uşă de acces de la distanţă în sistem pentru a fi utilizată de atacatori sau pot executa anumite sarcini, după cum au fost instruiţi. Caii troieni care urmăresc acţiuni specifice sunt greu detectaţi.

Troienii pot fi transmişi prin diferite metode: ataşamente email, programe freeware, instalări fizice, canale de chat IRC, websiteuri infectate, etc.

De cele mai multe ori, caii troieni fac (şi) “keystroke logging”; captează tot ceea ce utilizatorul introduce de la tastatură, capturând în acest fel nume de utilizatori, parole, detalii ale unor carduri bancare, etc şi le salvează într-un fişier ascuns care este trimis ulterior atacatorului.

2.1.3 Prevenirea infecţiilor cu viruşi, wormi şi troieni

Modalitatea de bază pentru prevenirea infecţiilor cu viruşi şi cai troieni o reprezintă programele anti-virus. Acestea previn infecţiile şi răspândirea de software maliţios. Pentru a fi eficiente, aceste programe trebuiesc actualizate permanent iar la anumite intervale precis stabilite trebuiesc realizate scanări exhaustive ale tuturor hard discurilor/partiţiilor din calculatoare. Printre producătorii de software anti-virus amintim Symantec, Computer Associates, McAfee, Trend Micro, etc. Protecţia anti-virus nu este totală şi nu previne pătrunderea de soft maliţios în reţele, doar protejează gazdele de infecţii.

Întrucît wormii sunt bazaţi mai mult pe vulnerabilităţi existente şi exploatabile prin reţele, detecţia şi eliminarea acestora este mai complicate şi necesită mai multe operatii şi experienta. Procesul de inlaturare a unei infectii cu wormi se deruleaza in 4 etape:

- **Izolarea** presupune restringerea infectiei doar la zonele de retea/gazdele deja infectate. Programele firewall pot ajuta in limitarea raspindirii.

- **Inocularea** are ca scop protejarea sistemelor care nu au fost inca infectate prin aplicarea de software “patch” oferit de producatorul softului care a creat vunlnerabilitatea prin care se propaga wormul.

- **Carantina –** presupune izolarea sistemelor infectate prin decuplarea acestora de la retea şi pregatirea pentru faza de inlaturare a infectiei.

- **Eradicarea –** presupune eliminarea wormului prin terminarea procesului acestuia, indepartarea fisierelor şi cheilor de registri create şi aplicarea softului “patch”. In cazul in care infectia este raspindita şi severa se impune reinstalarea sistemului de operare

Trebuie avuta in vedere necesitatea instalarii tuturor updateurilor de securitate pe care producatorii de software le scot pe piata, pentru a reduce posibilitatea infectiilor.

Programele software firewall instalate local pot ajuta la prevenirea intrării wormilor in sistem sau pot ajuta in fazele de eliminare ale acestora

2.1.4 Organizaţii care activează în domeniul securităţii informatice

Pentru o mai bună gestiune a acestei probleme, au fost create organizaţii pentru securitatea reţelelor cu scopul de a forma comunităţi de profesionişti în acest domeniu. Rolul acestor organizaţii este de a elabora standarde şi de a pune la dispoziţie mijloacele necesare cooperării între specialişti. Următoarele organizaţii aparţin domeniului securităţii informatice (lista nu este exhaustiva, doar exemplificativă):

- SysAdmin, Audit, Network, Security (SANS) Institute – a fost înfiinţată in 1989 ca şi organizaţie de învăţământ şi cercetare ce pune accent pe instruirea şi certificarea de profesionişti in domeniul securităţii sistemelor informatice şi al reţelelor.

- Computer Emergency Response Team (CERT) – a fost fondata in cadrul Universităţii Carnegie Mellon din SUA ca şi parte a Software Engineering Institute (SEI). Scopul acesteia este de a lucra cu comunităţi din Internet pentru a detecta şi rezolva incidentele de securitate. Are un spectru de activitate in cinci domenii: siguranţa software (software assurance), sisteme informatice sigure (secure systems), securitate organizaţională (organizational security), răspuns coordonat (coordinated response) şi educaţie/pregătire (education/training).

- International Information Systems Security Certification Consortium (ISC^2) – are scop educaţional şi de certificare pentru dezvoltarea de profesionişti in securitatea sistemelor informaţionale in peste 135 de tari. Oferă 4 certificări de securitate: Systems Security Certified Practicioner (SSCP), Certified Secure Software Lifecycle Professional (CCSLP), Certification and Accreditation Professional (CAP), Certified Information Systems Security Professional (CISP).

2.1.5 Semnatura digitală

Certificatul digital

Odată cu dezvoltarea reţelei Internet, a apărut necesitatea autentificării unor documente în format electronic transmise în reţea. Dezvoltarea sistemelor de plată non-cash, a comerţului electronic, a telefoniei mobile şi în general, a mijloacelor de transmisii de date care necesită criptare sau autentificare a condus la crearea unei noi situaţii juridice.

Certificatele digitale:

- Reprezintă o colecție de date pe care un browser o solicită server-ului pentru a putea începe transferul criptat.
- Este emis de terți de încredere și oferă un mecanism cu ajutorul căruia se câștigă o încredere mai mare în legatură cu autenticitatea unui document electronic.
- Sunt declaraţii semnate digital cu referire la o anumită cheie publică, certificatul fiind semnat de emitentul său. Atunci când se eliberează un certificat digital, emitentul atestă validitatea legăturilor dintre cheia publică şi informaţiile referitoare la identitatea celor care o accesează.

Semnatura digitală este un algoritm matematic folosit pentru a demonstra autenticitatea unui mesaj sau document digital.

Pentru a putea sa isi atinga scopul, semnatura digitala trebuie sa aiba urmatoarele caracteristici:

- Autentificarea semnatarului (trebuie sa existe imposibilitatea virtuala ca altcineva sa poata avea aceeasi semnatura)
- Autentificarea documentului (in acelasi mod cum nu se poate inlocui o pagina semnata manual, sa nu existe posibilitatea modificarii sau alterarii continutului semnat)

Pentru intelegerea modului in care o semnatura digitala functioneaza, este necesara explicarea termenilor urmatori:

- **Algoritm criptografic –** este un algoritm matematic ce permite transformarea datelor din text clar in text cifrat pe de o parte (operatiune denumita criptare) cit si transformarea unui text cifrat in text clar (operatiune denumita decriptare) pe baza unor *chei*.

- **Sistem criptografic simetric –** foloseste aceeasi cheie (privata-secreta) atit pentru operatiunea de criptare cit si pentru operatiunea de decriptare. Exemple de algoritmi de criptare simetrica: DES, 3DES, AES, etc

- **Sistem criptografic asimetric –** foloseste o cheie pentru criptare si o alta cheie pentru decriptare. Cheia folosita pentru criptare este publica (oricine poate cripta cu ea) in timp ce chiea folosita pentru decriptare este privata (doar destinatarul poate decripta ceea ce a fost criptat cu cheia publica). Trebuie evidentiat faptul ca o cheie publica este strins legata de cheia privata pereche. Desi cheia publica este derivata din cea privata, forta algoritmului sta in aceea ca din cheia publica nu se poate reconstitui cheia privata. Criptarea asimetrica are o complexitate foarte mare, lucru care duce la imposibilitatea folosirii ei in mod rentabil pe blocuri mari de date si din aceste motive, cele mai dese intrebuintari sunt:

    - *distribuirea cheilor secrete pentru sistemele criptografice simetrice prin medii nesigure (ex SSL pentru HTTPS)*

- *semnatura electronica a unor continuturi digitale, in vederea autentificarii originii acestora*

Exemple de algoritmi de criptare asimetrică: DH, El Gamal, RSA, etc.

Asa precum am vazut, semnatura digitala se realizeaza prin 2 chei ce formeaza o pereche (o cheie privata si o cheie publica derivata). Cheia privata este folosita doar de semnatar pentru a-si semna documentele. Din aceste considerente, pentru a se realiza finalitatea de siguranta a semnaturii digitale, este necesar sa se ia toate masurile necesare pentru pastrarea confidentialitatii si integritatii cheii private. De multe ori, cheile private sunt distribuite detinatorilor pe un suport electronic distinct (token USB, smart card, etc) iar pentru accesarea acesteia trebuie introdus un cod PIN.

In ceea ce priveste cheia publica, legatura acesteia cu titularul cheii private (deci al semnatarului) se face pe baza certificatului digital. Acest lucru este necesar deoarece trebuie validata identitatea persoanei care semneaza.

Procesul de semnare a unui document electronic are urmatoarele etape:

- documentul de semnat si cheia privata a semnatarului intra in algoritmul de calcul al semnaturii digitale
- semnatura rezultata din pasul anterior este grupata cu documentul semnat si este trimisa destinatarului (in aceasta faza este inclusa si cheia publica a semnatarului, care urmeaza a valida semnatura odata ajuns fisierul la destinatar)

Procesul de verificare a semnaturii, odata primit documentul, comporta urmatoarele etape:

- documentul (odata pe PC-ul destinatarului) este despachetat impreuna cu semnatura si cheia publica
- este folosit un algoritm de verificare a documentului si semnaturii iar daca cele doua corespund, inseamna ca documentul are o forta juridica egala cu cea a unui document semnat de mina.

Sistemele de semnatura digitala utilizeaza, in realitate, 2 procese distincte pentru a-si indeplini scopul (avem de-a face in realitate cu 2 mecanisme individuale, unul dintre ele fiind angrenat pentru prevenirea modificarilor/alterarii intre sursa si destinatie iar celalalt avind rol de identificator unic al semnatarului):

- pentru integritate se pot folosi algoritmii: MD5, SHA1 sau RIPEM-160

- pentru autentificare se pot folosi algoritmii: RSA si DSA

3 Portalul de management al funcţiilor publice şi al funcţionarilor publici

3.1 Prezentarea generală a portalului

Utilitatea portalului

Portalul este special conceput pentru a asigura şi facilita managementul funcţiilor publice şi al funcţionarilor publici într-o manieră transparentă şi în timp real. Totodată portalul reprezintă şi un instrument de comunicare eficient între compartimentele de resurse umane din cadrul instituţiilor publice şi Agenţia Naţională a Funcţionarilor Publici (ANFP). Astfel, s-a realizat transpunerea, în mare măsură, a operaţiilor de management al funcţiilor publice dintr-o diversitate de modalităţi de lucru într-un mod unitar şi centralizat. Se intenţionează eliminarea, pe cât posibil, a corespondenţei pe suport de hârtie şi realizarea, aproape în totalitate, a gestionarii electronice a funcţiei publice prin intermediul portalului şi al sistemului integrat de management al funcţiilor publice.

Accesarea portalului şi transferul informaţiilor

Portalul este accesibil de la orice staţie conectată la Internet la adresa https://www.anfp.gov.ro. Fiecare instituţie publică desemnează un responsabil care va asigura permanent legătura cu ANFP. Responsabilul din partea instituţiei publice, după autentificarea pe portal (pe baza datelor transmise de către ANFP) are la îndemână o serie de funcţionalităţi prin intermediul cărora poate iniţia operaţii specifice managementului funcţiei publice şi al funcţionarilor publici. Astfel, instituţiile publice pot iniţia modificări la structura proprie a funcţiilor publice, acestea urmând a fi validate sau nu de către reprezentanţii ANFP, existând o comunicare permanentă a stadiului operaţiilor iniţiate.


GeoTrust
Website Profile
Website identity confirmed

Domain: https://www.anfp.gov.ro
Name: AGENTIA NATIONALA A FUNCTIONARILOR PUBLICI
Address: Str. Eforie Nr. 5 , Bucuresti 050036 RO
Telephone:

Site Security Confirmed
The following SSL certificate has been issued for secure communications

Serial Number: 2695
Validity Period: 9-Nov-2011 to 11-Dec-2013

SSL certificates from GeoTrust® are the ultimate online security and trust solution delivering both 256-bit encryption and the True Site™ trust mark providing third-party website identity validation.

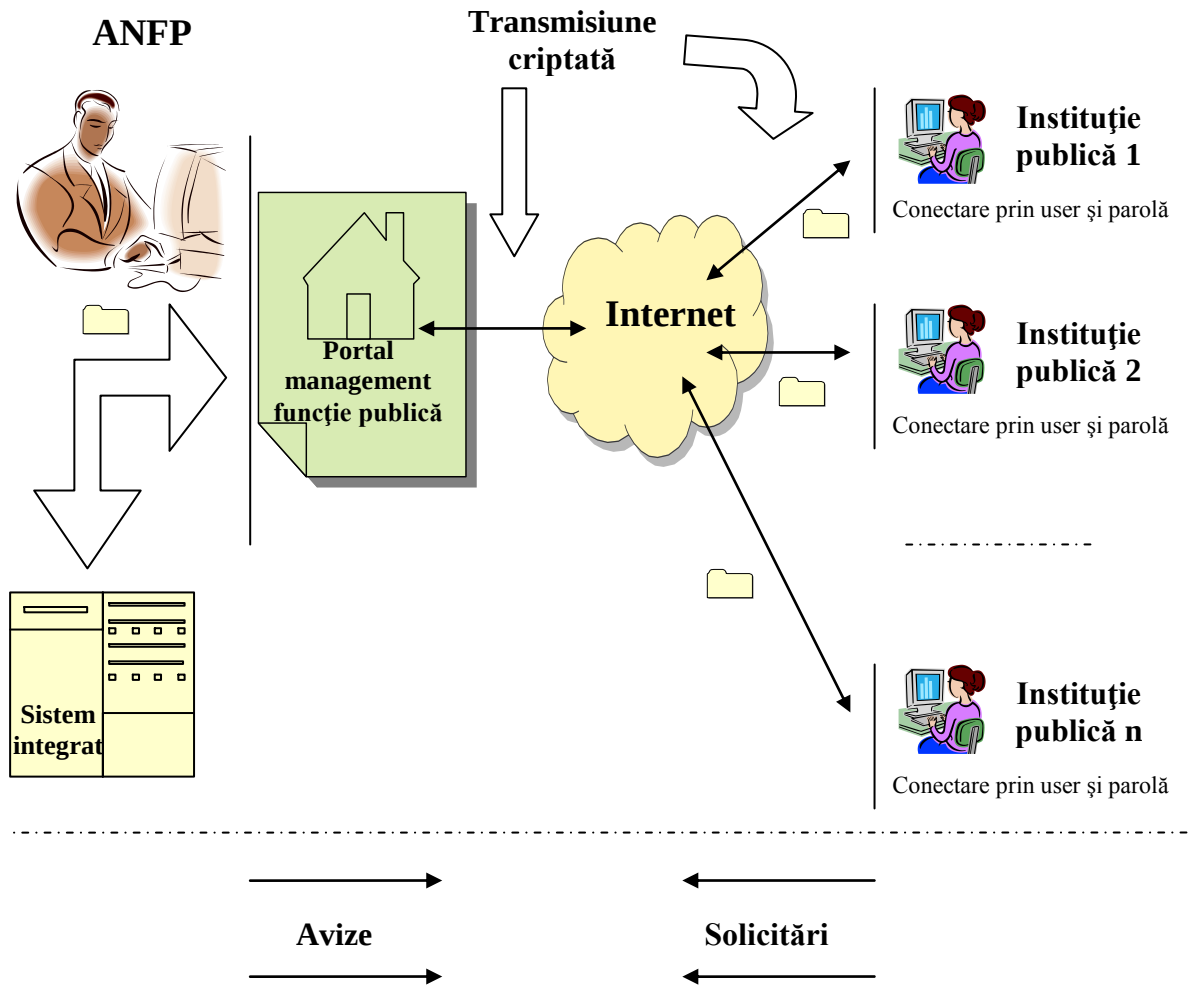
The presence of SSL means you can rest assured that communications (e.g. credit card numbers) between your browser and this site's web servers are private and secure when the SSL session is activated.

True Site is subject to the Relying Party Agreement.

Please visit GeoTrust for more information about Internet trust services.

Prin utilizarea unui certificat SSL, portalul de management al funcţiilor publice şi al funcţionarilor publici asigura transmiterea criptată a datelor dintre instituţiile publice şi ANFP. Această măsură de securitate face imposibilă interceptarea datelor transmise între reprezentanţii instituţiilor publice şi ANFP.

Reprezentarea schematică a funcţionării portalului

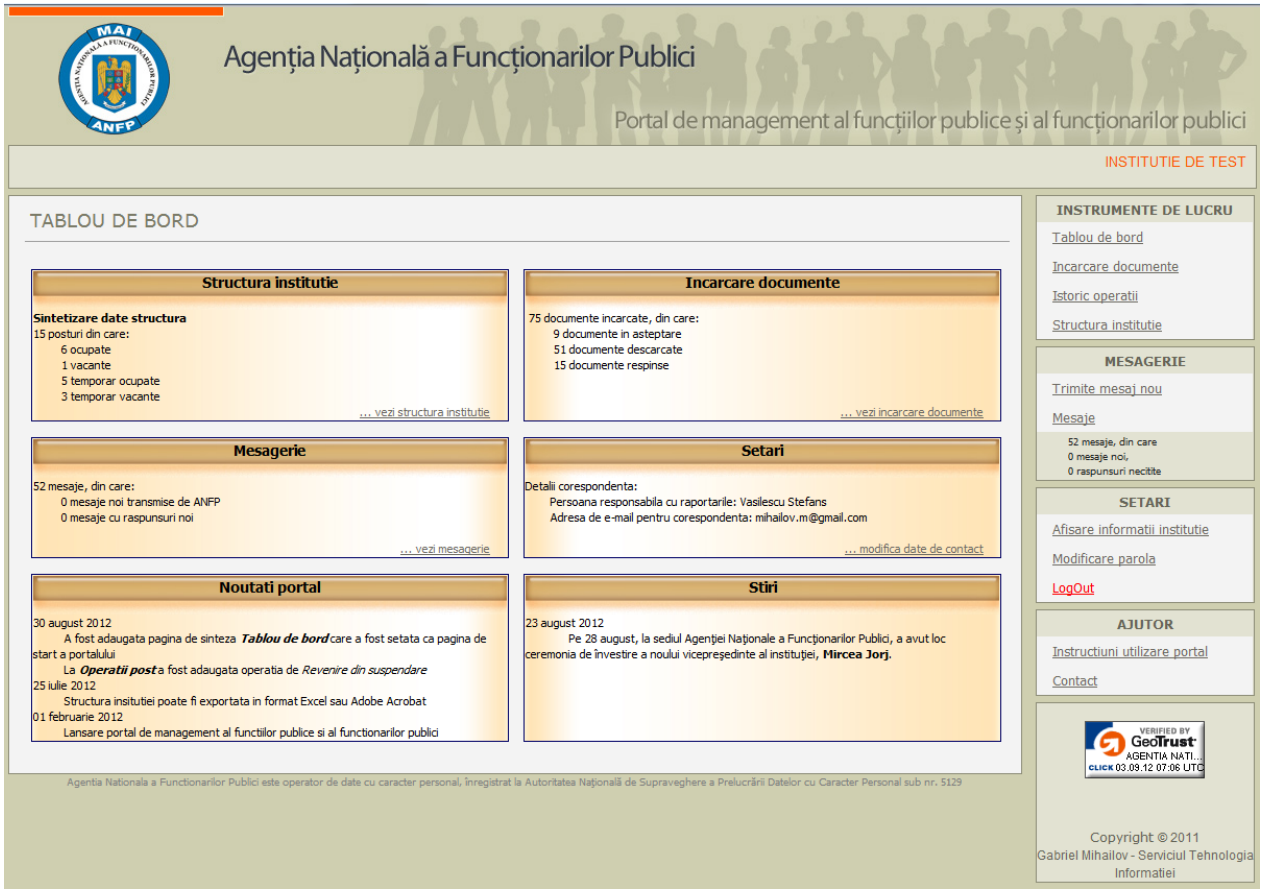


3.2 Utilizarea portalului şi funcţionalităţile acestuia

Fiecare instituţie publică are desemnat un reprezentant responsabil cu gestionarea funcţiilor publice prin intermediul portalului. ANFP transmite parolele pe format hârtie către autorităţile şi instituţiile publice centrale precum şi pentru serviciile deconcentrate ale acestora (acolo unde este

cazul). Accesul se face prin intermediul unui utilizator şi a unei parole ştiute doar de reprezentantul desemnat. Reprezentantul desemnat poate schimba oricând parola de acces sau, în cazul în care nu o mai ştie, poate solicita reprezentantului ANFP resetarea parolei.

La introducerea parolei primite de la ANFP se va deschide o fereastra unde se va solicita schimbarea parolei. Persoana desemnata din cadrul autorităţii sau instituţiei publice va introduce o nouă parolă, care trebuie sa îndeplinească următoarele condiţii: minim 9 caractere, să conţină litere, cifre şi caractere speciale. Noua parolă va fi cunoscută doar de către persoanele desemnate în acest sens de conducerea instituţiei respective, întrucât asigură accesul la contul web al portalului care conţine structura instituţiei, iar deţinătorul parolei poate opera o serie de modificări în structură. Precizăm că ANFP nu are acces la noua parolă introdusă de către utilizator, astfel încât responsabilitatea gestionării acesteia revine integral instituţiei publice.



La lansarea portalului (după introducerea parolei) se deschide o pagină in care sunt sintetizate principalele informaţii vehiculate în portal.

Transmisia informaţiilor dintre instituţie şi ANFP nu poate fi interceptată, aceasta fiind criptată.

Principalele funcţionalităţi puse la dispoziţie prin intermediul portalului sunt:

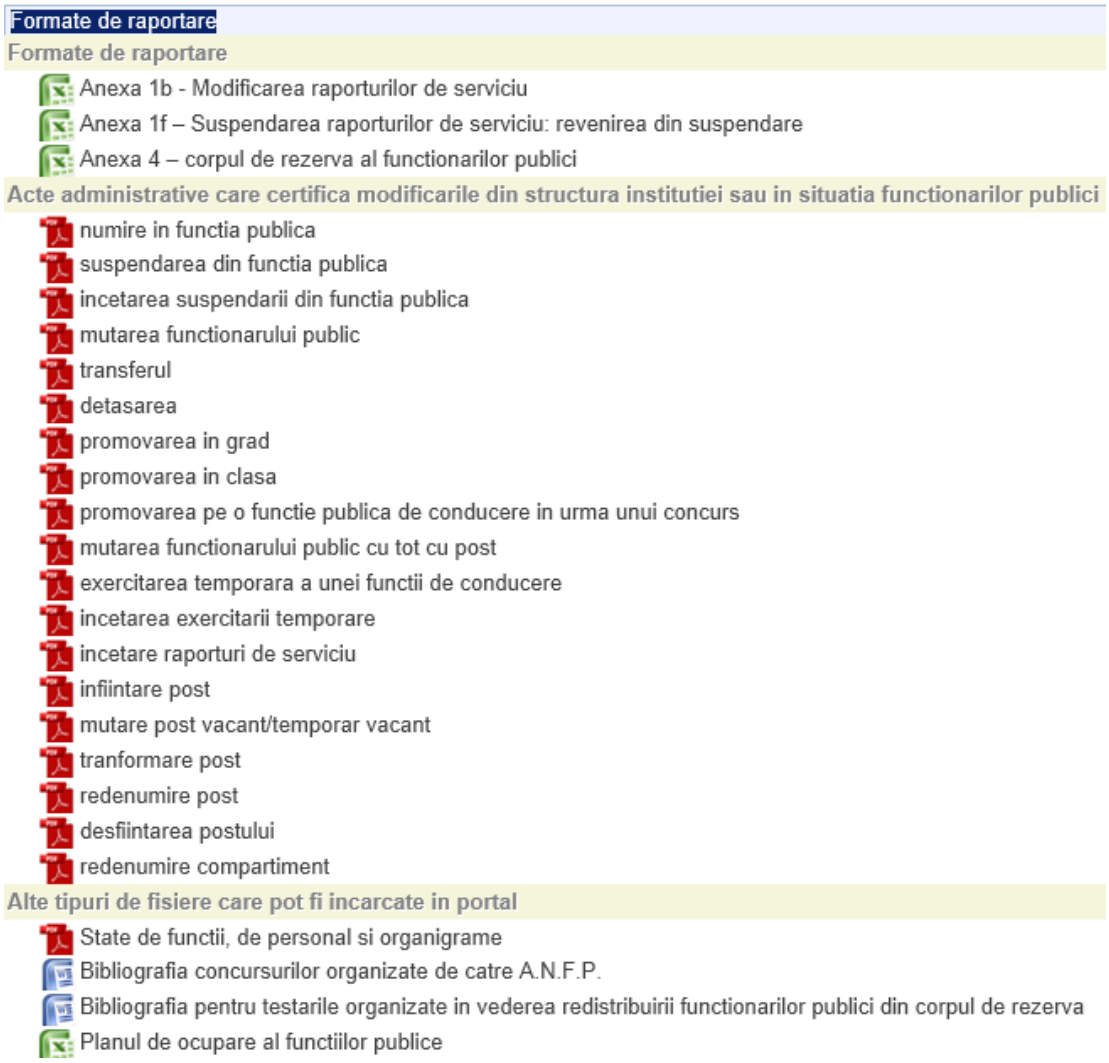
- Încărcare documente
- Istoric operaţii
- Structură instituţie
- Mesagerie
- Setări

Aceste funcţionalităţi sunt accesibile apelând opţiunile amplasate pe partea dreaptă în cadrul Portal-ului după cum se observă şi în figura alăturată.

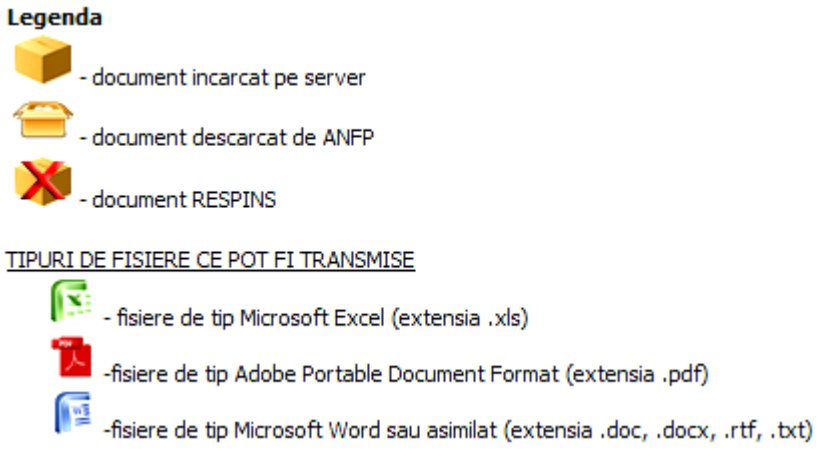
3.2.1 Încărcare documente

Primul instrument de lucru din meniul aflat în partea dreaptă a portalului îl reprezintă opţiunea „Încărcare documente”. Accesarea acestei opţiuni va duce la deschiderea ferestrei denumite *Gestiune documente raportare*. Din lista derulantă a ferestrei se va selecta tipul raportării, conform figurii de mai jos, care urmează să fie transmis. De asemenea, pot fi încărcate şi alte tipuri de documente ca de exemplu: acte administrative în format pdf. care certifică modificările din structura instituţiei, documente în format Word, documente cu semnătură electronică, alte tipuri de documente. Documente ce pot fi încărcate pe Portal, după cum se observă în figura de mai jos, sunt de împărţite în trei categorii: „Formate de raportare”, „Acte administrative care certifică modificările din structura instituţiei sau în situaţia funcţionarilor publici” şi „Alte tipuri de fişiere”. Această metodă de transmitere a fişierelor de către instituţiile publice către ANFP este mult mai sigură şi eficientă decât metodele utilizate anterior (email, fax, corespondenţă, etc.) având la bază următoarele avantaje:

- Prin utilizarea unui certificat SSL, transmiterea fişierelor este criptată şi acestea nu pot fi interceptate
- Existenţa unui cont de utilizator pentru fiecare instituţie certifică faptul că documentul are ca expeditor instituţia respectivă
- Poate fi transmisă, către ANFP, corespondenţă în format electronic şi semnată electronic (dacă instituţia dispune de semnătură electronică) timpul transmiterii fiind foarte mic
- Documentele transmise prin intermediul Portal-ului sunt preluate de responsabilii ANFP în cel mai scurt timp, acestea fiind vizibile în sistemul integrat imediat ce acestea au fost upload-ate de către responsabilii instituţiilor
- In orice moment responsabilul instituţiei poate vedea istoricul documentelor/raportărilor transmise către ANFP şi status-ul acestora
- Prin utilizarea acestei soluţii informatice se reduce semnificativ timpul prelucrării documentelor şi costul transmiterii acestora (faţă de poştă, fax, etc.)



După selectarea tipului de document, se va selecta fişierul ce urmează a fi încărcat cu ajutorul butonului *Browse*, iar încărcarea fişierului se va face prin utilizarea butonului *Încărcare fişier pe server*, după completarea descrierii fişierului respective în cadrul rubricii cu această destinaţie. Descrierea fişierului trebuie sa aibă minim 15 caractere. În cadrul aceleiaşi ferestre vor fi afişate documentele încărcate, iar tipul raportării, descrierea, nume fişier, dimensiune fişier şi data încărcării se completează automat în urma încărcării fişierelor de către utilizator şi a introducerii descrierii acestora. Coloana Observaţii va afişa observaţiile transmise de către responsabilul cu instituţia din cadrul ANFP la recepţionarea fişierului. Coloana *Stare* va indica dacă fişierul a fost deschis, dacă nu a fost deschis, sau dacă a fost respins de către responsabilul din Agenţie, lucru descris în legenda din partea de jos a ferestrei după cum se observă şi în legenda de mai jos.



3.2.2 *Istoric operaţii*

Prin intermediul acestei opţiuni utilizatorul va putea vizualiza istoricul operaţiunilor efectuate în contul web al instituţiei, lucru ce îi va permite utilizatorului monitorizarea permanentă a accesării şi utilizării contului de web, evitând astfel eventualele încercări de acces neautorizat.

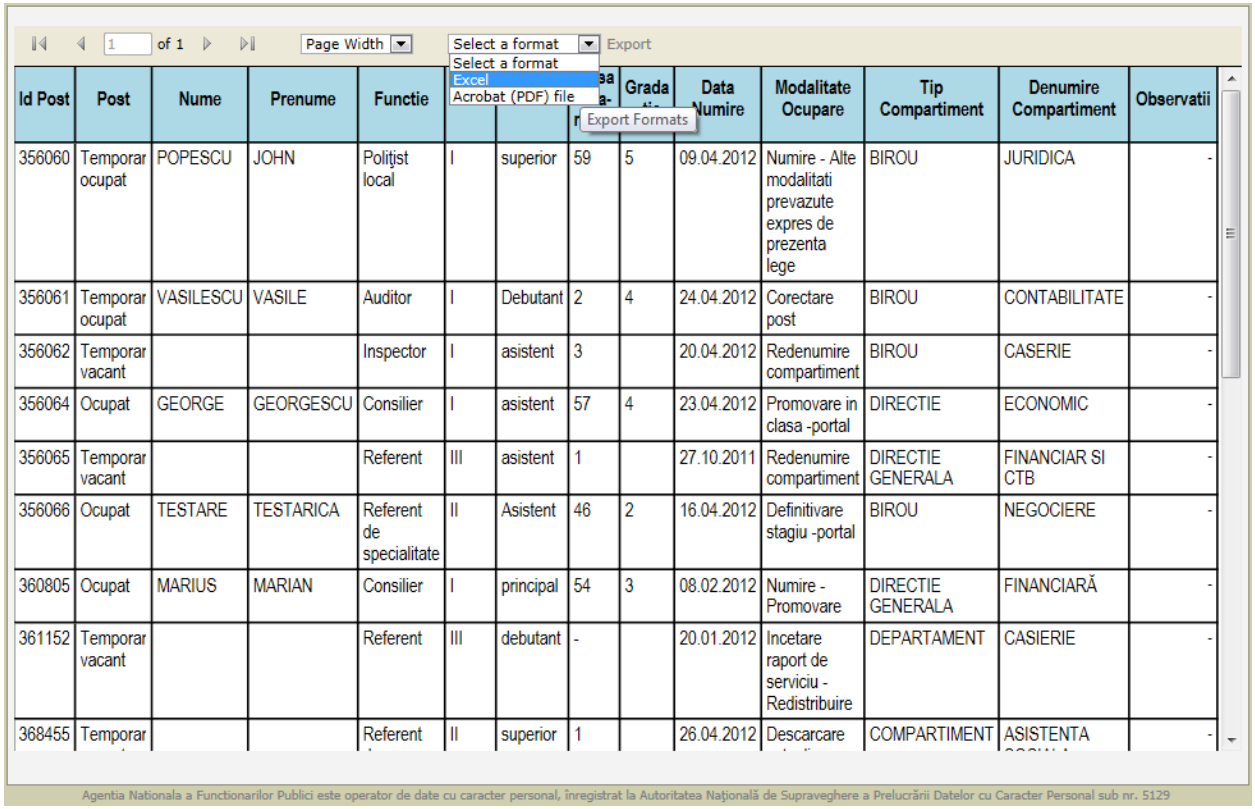
3.2.3 *Structură instituţie*

Prin accesarea acestei opţiuni se va deschide o fereastră care va afişa structura instituţiei, în forma în care aceasta există în baza de date a Agenţiei, cu excepţia coloanei care conţine CNP – ul (în scopul protejării datelor cu caracter personal).

În partea de jos a paginii Structură instituție se regăsește o caseta în care se face sinteza structurii instituției după cum se afișează în imagine:

De asemenea dacă se dorește prelucrarea datelor existente în structura instituției acestea pot fi exportate într-un document Excel acesând butonul Raport structura institutie aflat în pagina Structura instituție

Prin apelarea butonului Raport structura institutie se generează un raport ce poate fi exportat şi salvat în format excel pentru o prelucrare ulterioară sau în PDF pentru pastrarea datelor şi imprimare.



Id Post	Post	Nume	Prenume	Functie					Grada	Data Numire	Modalitate Ocupare	Tip Compartiment	Denumire Compartiment	Observatii
356060	Temporar ocupat	POPESCU	JOHN	Poliţist local	I	superior	59	5		09.04.2012	Numire - Alte modalitati prevazute expres de prezenta lege	BIROU	JURIDICA	-
356061	Temporar ocupat	VASILESCU	VASILE	Auditor	I	Debutant	2	4		24.04.2012	Corectare post	BIROU	CONTABILITATE	-
356062	Temporar vacant			Inspector	I	asistent	3			20.04.2012	Redenumire compartiment	BIROU	CASERIE	-
356064	Ocupat	GEORGE	GEORGESCU	Consilier	I	asistent	57	4		23.04.2012	Promovare in clasa -portal	DIRECTIE	ECONOMIC	-
356065	Temporar vacant			Referent	III	asistent	1			27.10.2011	Redenumire compartiment	DIRECTIE GENERALA	FINANCIAR SI CTB	-
356066	Ocupat	TESTARE	TESTARICA	Referent de specialitate	II	Asistent	46	2		16.04.2012	Definitivare stagiu -portal	BIROU	NEGOCIERE	-
360805	Ocupat	MARIUS	MARIAN	Consilier	I	principal	54	3		08.02.2012	Numire - Promovare	DIRECTIE GENERALA	FINANCIARĂ	-
361152	Temporar vacant			Referent	III	debutant	-			20.01.2012	Incetare raport de serviciu - Redistribuire	DEPARTAMENT	CASIERIE	-
368455	Temporar			Referent	II	superior	1			26.04.2012	Descarcare	COMPARTIMENT	ASISTENTA	-

În vederea efectuării unei operaţiuni asupra unui post din structura de funcţii publice de către utilizator, se va accesa din coloana Operaţii butonul *Detalii* din cadrul casetei corespunzătoare postului respectiv. Accesarea va deschide o fereastră numită *Operaţii post selectat*. Din caseta *Operaţii post* a ferestrei prezentate în imaginea de mai jos, utilizatorul va selecta, dintre operaţiunile disponibile, pe cea pe care doreşte să o efectueze şi va completa în acest scop formularul care se va deschide în fereastră. După realizarea operaţiei de modificare se va folosi butonul afişat în partea de jos a formularului pentru introducerea modificării în structură.

Operaţiile de modificare a postului – cu excepţia modificării gradaţiei şi a clasei de salarizare – se desfăşoară în patru etape după cum urmează:

1. Reprezentatul instituţiei (utilizatorul portalului) efectuează operaţia dorită

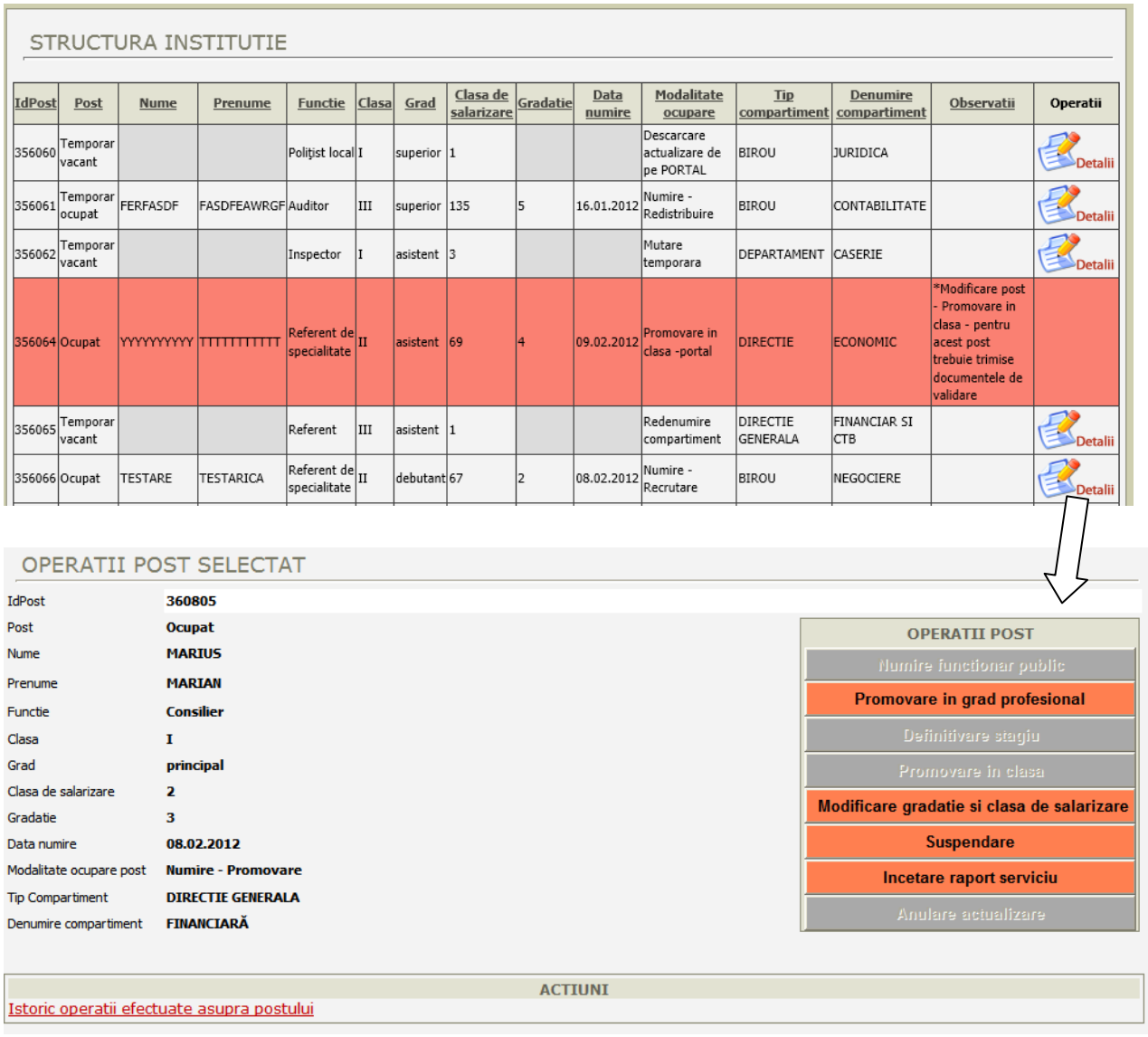
2. Reprezentantul ANFP verifică şi acceptă modificarea efectuată. Până în momentul în care modificarea este acceptată de către ANFP, reprezentantul instituţiei poate anula operaţia efectuată. Dacă operaţia a fost acceptată de către ANFP, aceasta va deveni vizibilă şi în structura instituţiei, postul afectat fiind

scos în evidenţă prin culoarea portocalie a fundalului. Dacă operaţia nu este acceptată de către ANFP ea va fi anulată iar instituţia în cauză va fi anunţată printr-un mesaj (vezi capitolul Mesagerie)

3. Pentru operaţia efectuată la etapa 1, reprezentatul instituţiei va încărca documentul (actul administrativ) aferent. Se va avea în vedere ca în descrierea documentului să fie menţionat identificatorul postului şi / sau numele funcţionarului public în cauză.

4. Reprezentantul ANFP va verifica actul administrativ şi va valida operaţia efectuată la etapa 1. Odată cu validarea operaţiei de actualizare a postului, modificarea devine definitivă.

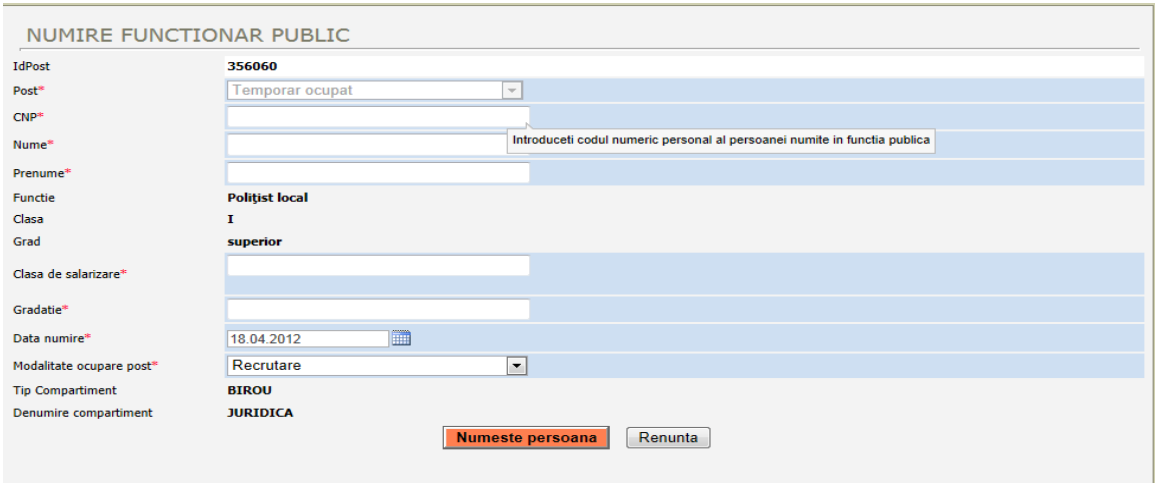
Trebuie menţionat faptul că odată începută o operaţie de actualizare a postului, nu mai poate fi operată o altă modificare decât după parcurgerea celor patru etape menţionate mai sus. De exemplu, pentru suspendarea unei persoane şi numirea unei alte persoane pe respectivul post, trebuie urmaţi cei patru paşi pentru operaţia de suspendare, după care vor fi efectuate din nou cele patru etape pentru numire.



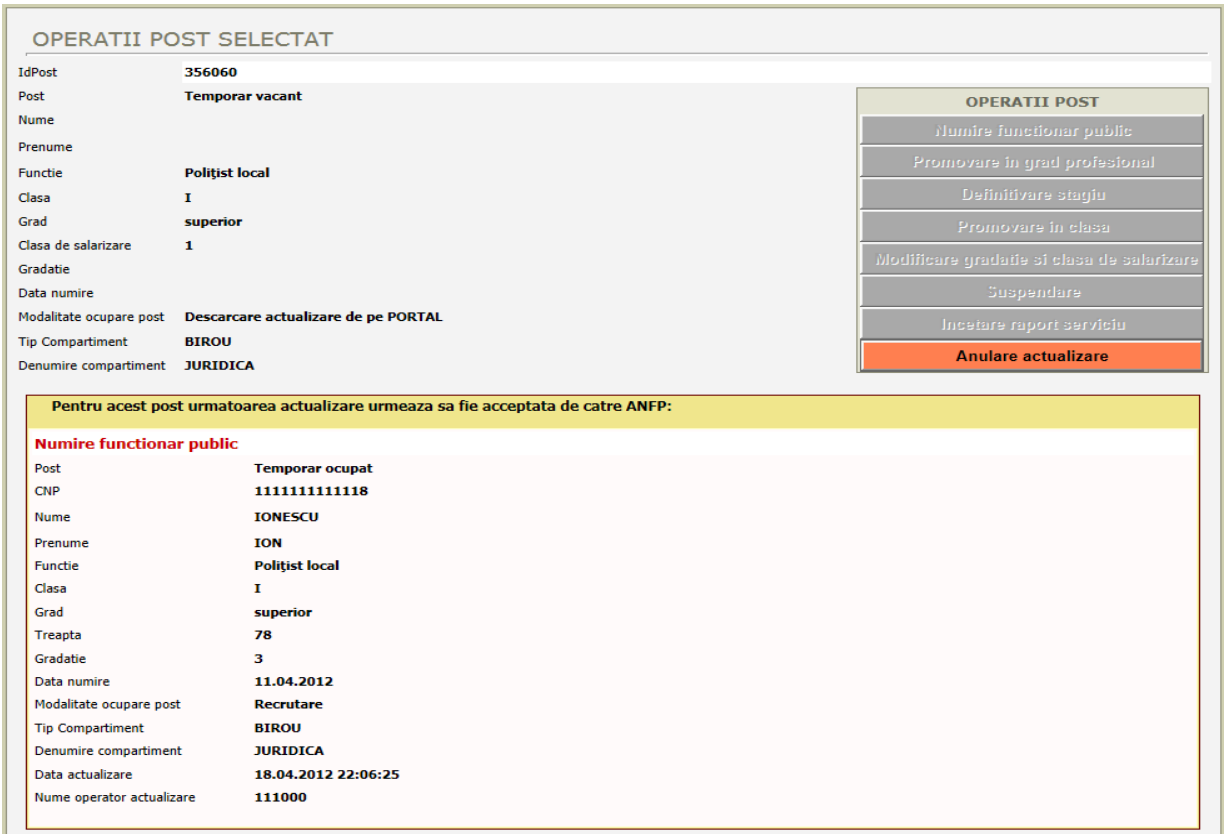
În funcţie de starea posturilor din cadrul unei structuri, din fereastra *Operaţii post selectat,* pot fi iniţiate operaţiile:

- Numire funcţionar public
- Promovare în grad profesional
- Definitivare stagiu
- Promovare în clasă
- Modificare gradaţie şi clasă de salarizare
- Suspendare
- Încetare raport serviciu

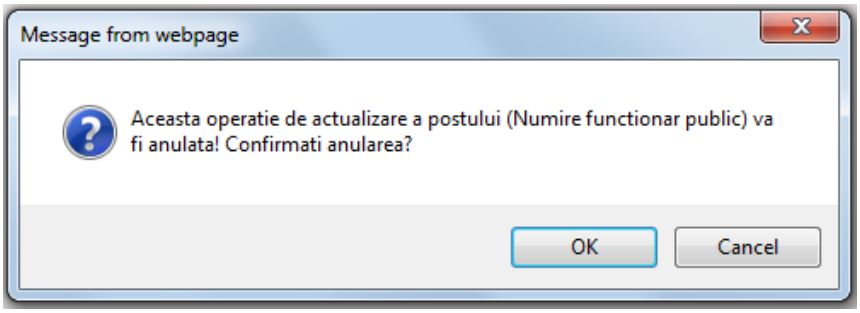
Numire funcţionar public



Butonul **Numire funcţionar public** este activ doar pentru posturile vacante sau temporar vacante. Pentru un post vacant nu poate fi făcută decât o numire definitivă iar pe un post temporar vacant nu poate fi făcută decât o numire temporară. Pentru a putea efectua numirea trebuie completate toate informaţiile solicitate. În cazul în care aceste informaţii lipsesc sau nu sunt corect completate, la apăsarea butonului **Numeşte persoana**, în dreptul casetelor de text în cauză vor fi afişate mesaje de eroare. În cazul în care toate informaţiile sunt corect completate, numirea este transmisă către ANFP după cum se observă în imaginea de mai jos.



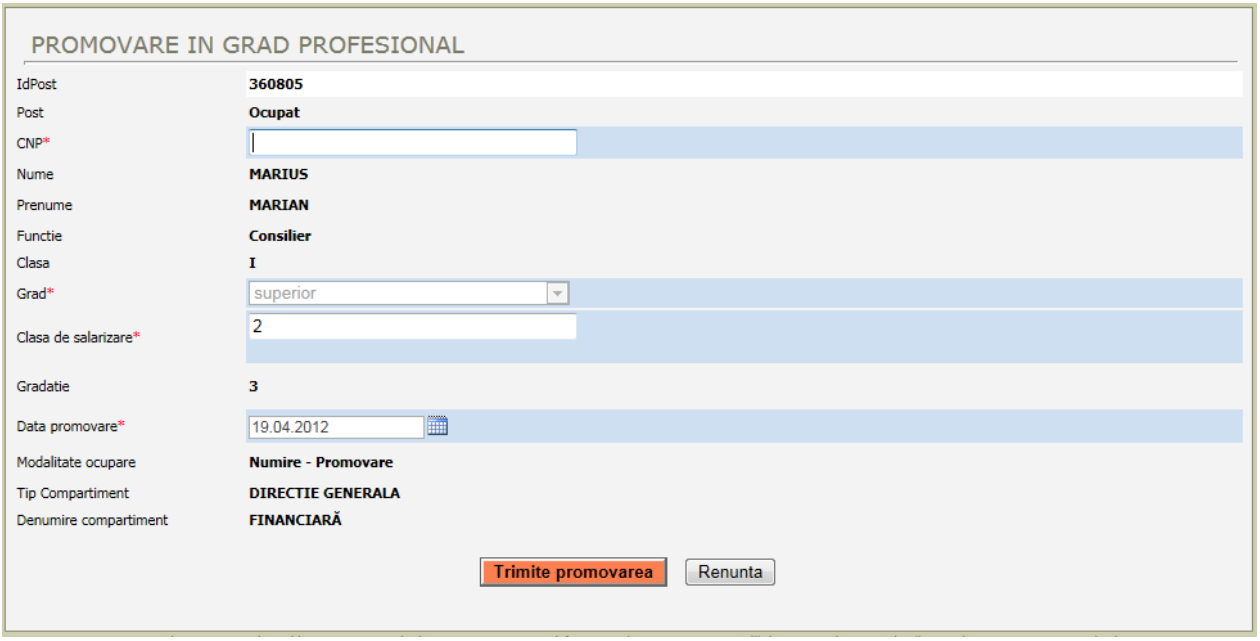
În situaţia unei erori, se va utiliza butonul *Anulare actualizare*. Acest buton poate fi accesat atât timp cât modificarea nu a fost preluată de către responsabilul din cadrul ANFP. În cazul accesării acestui buton, utilizatorului i se va cere confirmarea operaţiei de anulare.



După confirmarea operaţiei de anulare propunerea de numire va fi retrasă (nu va mai fi vizibilă pentru reprezentanţii ANFP) iar asupra postului respectiv vor putea fi efectuate alte operaţii de actualizare.

Promovare în grad profesional

Butonul **Promovare în grad profesional** devine activ doar în cazul posturilor ocupate definitiv ce au gradul profesional asistent sau principal.



În cazul promovării se va completa codul numeric personal al persoanei ce promovează, noua clasă de salarizare şi data de la care se face promovarea. Restul etapelor sunt similare cu cele a operaţiei de numire a funţionarilor publici.

Definitivare stagiu

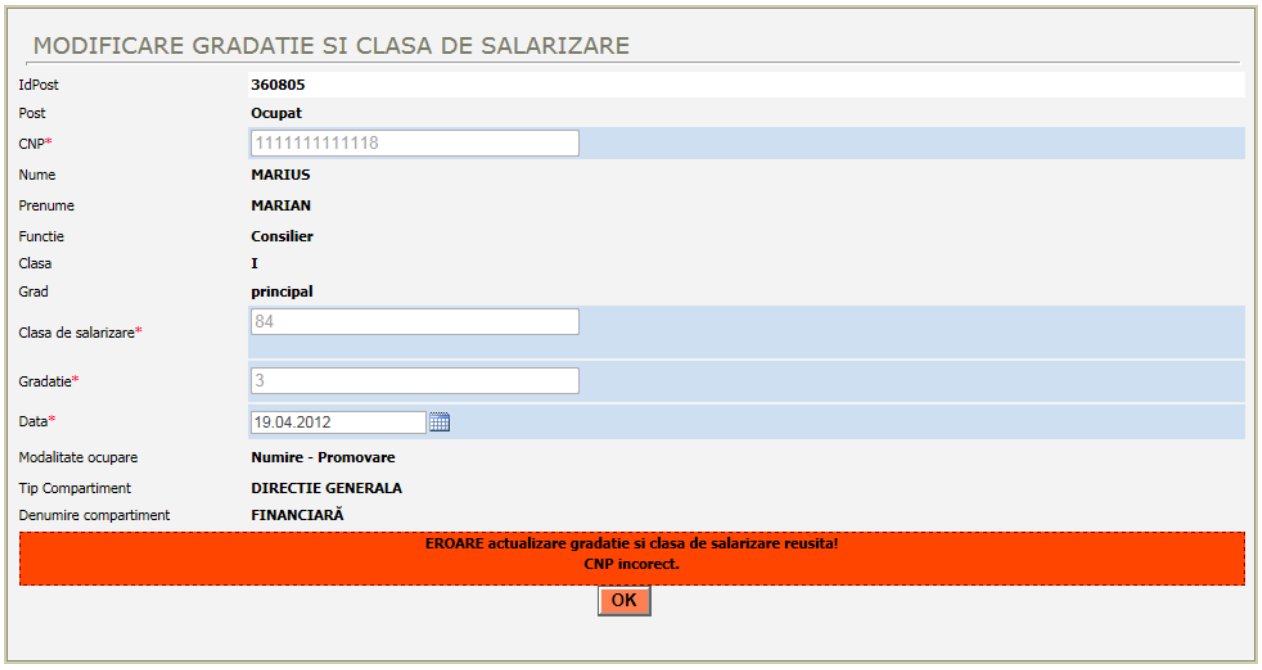
Operaţia de definitivare de stagiu este identică cu operaţia de promovare în grad profesional doar că se aplică posturilor ocupate definitiv ce au gradul profesional debutant.

Promovare în clasă

Promovarea în clasă este disponibilă doar pentru posturile ocupate definitiv de clasa II sau III. În funcţie de clasa în care promovează (din clasa II în clasa I şi din clasa III în clasa II sau I) vor fi disponibile liste de funcţii diferite corespunzătoare clasei selectate.

Modificare gradaţie şi clasă de salarizare

Operaţia de modificare a gradaţiei şi a clasei de salarizare este singura operaţie ce nu se desfăşoară în cei patru paşi descrişi mai sus. Pentru această operaţie se va realiza doar etapa 1 din procesul de modificare a postului, nemaifiind necesare etapele de acceptare şi de validare din partea ANFP şi nici încărcarea de documente justificative. Această acţiune va produce modificări direct în baza de date a sistemului integrat de management a funcţiei publice.



În cazul în care codul numeric personal introdus pentru persoana căreia i se modifică gradaţia sau clasa de salarizare nu coincide cu CNP-ul aferent acesteia din baza de date, va fi generată o eroare ilustrată mai sus.

Suspendare

Operaţia de suspendare va putea fi accesată pentru toate posturile ocupate definitiv sau temporar. Vor fi completate câmpurile corespunzătoare CNP-ului, data suspendării raportului de serviciu şi motivul suspendării.

Încetare raport serviciu

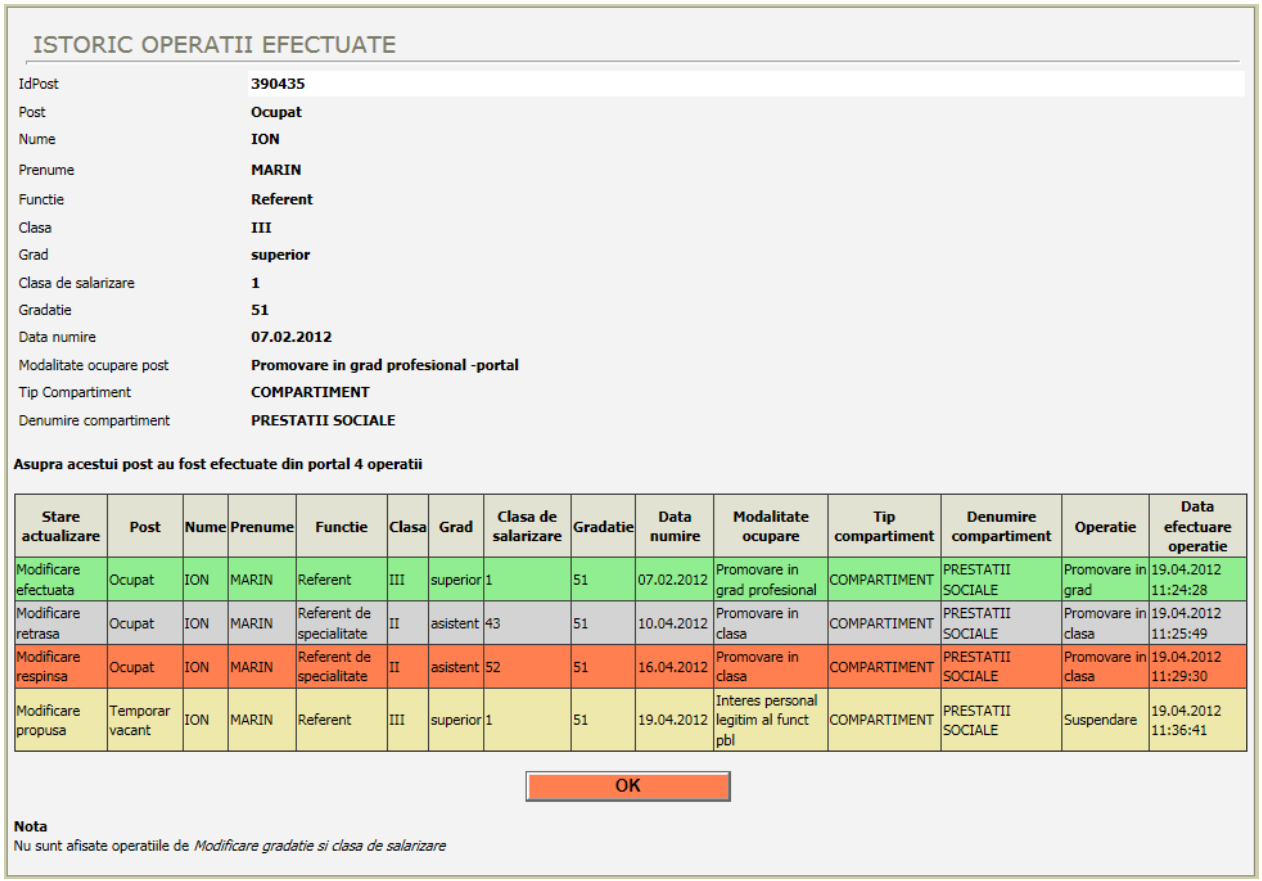
Operaţia de încetare a raportului de serviciu se realizează în mod similar cu operaţia de suspendare

Asupra posturilor aflate în curs de validare nu se por putea efectua nici un fel de operaţiuni, acestea fiind afişate în culoarea portocaliu.

În subsolul ferestrei „Operaţii post selectat” există două opţiuni:

- Istoric operaţii efectuate asupra postului - prin intermediul căreia pot fi vizualizate operaţiile efectuate asupra postului respectiv;
- Sancţiuni aplicate persoanei care ocupă postul - prin intermediul căreia pot fi raportate sancţiunile ocupantului postului în vederea gestionării cazierului administrativ.

Istoric operaţii efectuate asupra postului



ISTORIC OPERATII EFECTUATE

IdPost	**390435**
Post	**Ocupat**
Nume	**ION**
Prenume	**MARIN**
Functie	**Referent**
Clasa	**III**
Grad	**superior**
Clasa de salarizare	**1**
Gradatie	**51**
Data numire	**07.02.2012**
Modalitate ocupare post	**Promovare in grad profesional -portal**
Tip Compartiment	**COMPARTIMENT**
Denumire compartiment	**PRESTATII SOCIALE**

Asupra acestui post au fost efectuate din portal 4 operatii

Stare actualizare	Post	Nume	Prenume	Functie	Clasa	Grad	Clasa de salarizare	Gradatie	Data numire	Modalitate ocupare	Tip compartiment	Denumire compartiment	Operatie	Data efectuare operatie
Modificare efectuata	Ocupat	ION	MARIN	Referent	III	superior	1	51	07.02.2012	Promovare in grad profesional	COMPARTIMENT	PRESTATII SOCIALE	Promovare in grad	19.04.2012 11:24:28
Modificare retrasa	Ocupat	ION	MARIN	Referent de specialitate	II	asistent	43	51	10.04.2012	Promovare in clasa	COMPARTIMENT	PRESTATII SOCIALE	Promovare in clasa	19.04.2012 11:25:49
Modificare respinsa	Ocupat	ION	MARIN	Referent de specialitate	II	asistent	52	51	16.04.2012	Promovare in clasa	COMPARTIMENT	PRESTATII SOCIALE	Promovare in clasa	19.04.2012 11:29:30
Modificare propusa	Temporar vacant	ION	MARIN	Referent	III	superior	1	51	19.04.2012	Interes personal legitim al funct pbl	COMPARTIMENT	PRESTATII SOCIALE	Suspendare	19.04.2012 11:36:41

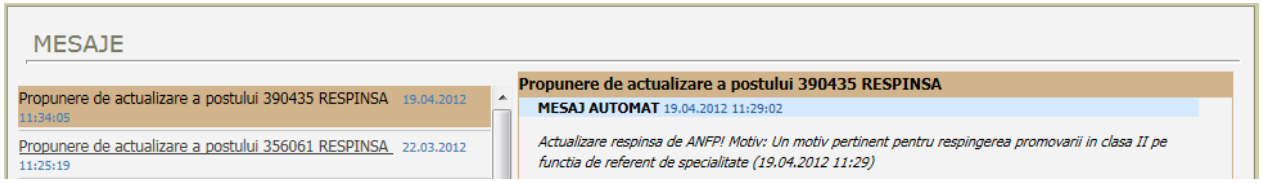
OK

Nota
Nu sunt afisate operatiile de *Modificare gradatie si clasa de salarizare*

În pagina de istoric operaţii sunt afişate toate modificările efectuate de pe portal (nu sunt afişate modificările de către ANFP în aplicaţia internă). Fiecare înregistrare este evidenţiată printr-o culoare în funcţie de starea acesteia:

- Verde pentru modificările acceptate de ANFP
- Gri pentru actualizările anulate de către instituţie prin intermediul portalului
- Portocaliu pentru actualizările respinse de către ANFP
- Galben pentru modificările de post ce nu au fost încă analizate de ANFP

În cazul în care o operaţie de actualizare a unui post a fost respinsă de către ANFP, în mod automat va fi transmis un mesaj pe portal în care se specifică idenitificatorul postului pentru care a fost respinsă actualizarea şi motivaţia respingerii acesteia.

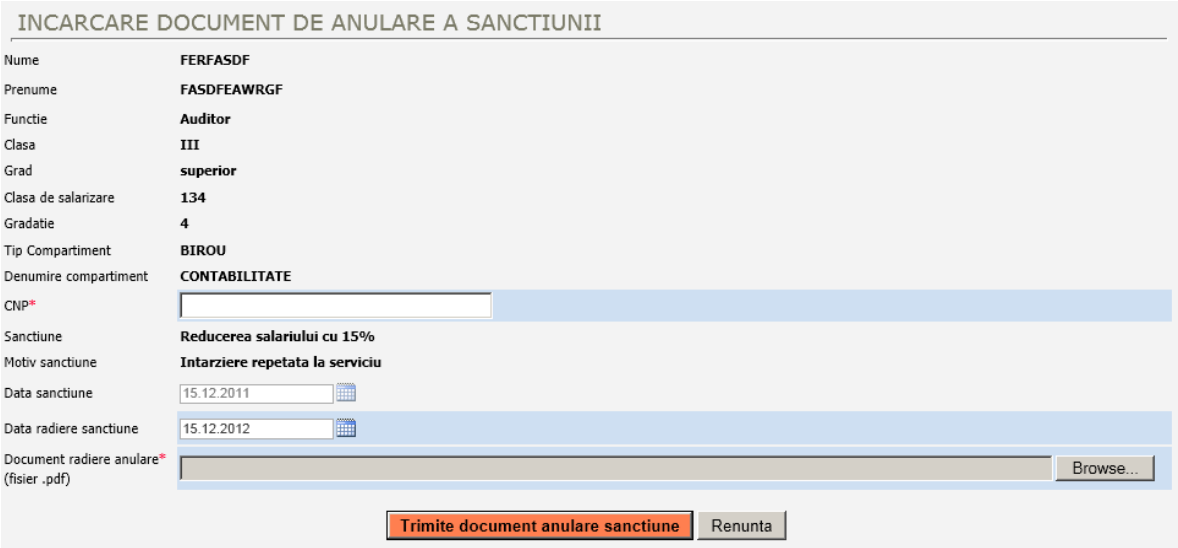


Adăugarea unei sancţiuni ocupantului postului selectat

- Din subsolul ferestrei „Operaţii post selectat" se alege opţiunea **Sancţiuni aplicate persoanei X**;

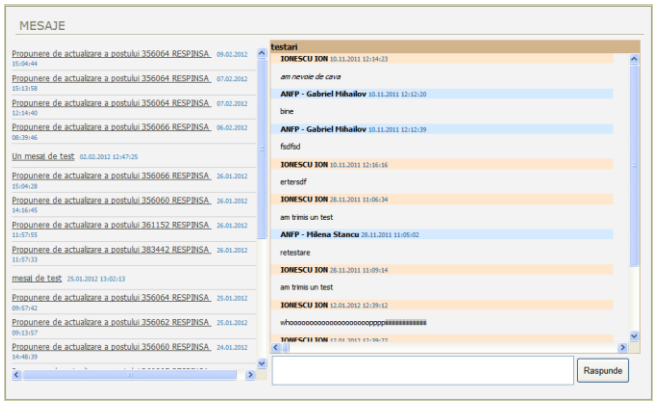
- Din fereastra de mai sus se alege butonul **Adaugă sancţiune** după care se deschide fereastra

- Sunt completate toate câmpurile şi se upload-ează obligatoriu documentul justificativ, după care se apasă butonul **Adaugă sancţiune**;
- După adăugarea unei sancţiuni, aceasta va fi validată sau nu de către ANFP;
- O sancţiune în vigoare poate fi anulată prin selectarea opţiunii „Anulează sancţiune” din dreptul sancţiunii, coloana „Acţiuni”. Prin selectarea acestei opţiuni se deschide pagina ilustrată mai jos



- După upload-ul documentelor justificative şi completarea câmpurilor obligatorii se iniţiază operaţia de anulare a sancţiunii;
- În final, această operaţie va fi validată sau nu de către ANFP.

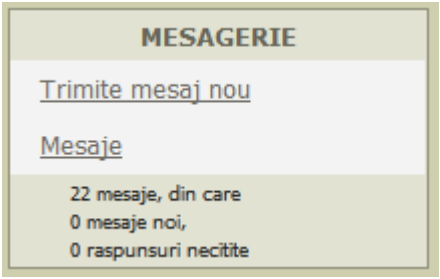
Mesagerie



Prin intermediul mesageriei portalului se pot transmite mesaje către responsabilul cu instituţia din cadrul Agenţiei şi se pot recepţiona mesaje de la acesta, prin accesarea opţiunilor *Trimite un mesaj nou*

şi *Mesaje*. Menţionăm că istoricul mesajelor se va păstra în portal, acesta neputând fi şters de către utilizator sau de către responsabilul ANFP.

Comunicarea se poate face aproape în timp real între responsabilii desemnaţi din cadrul instituţiilor şi reprezentanţii ANFP, fiind pus la dispoziţie, după cum se observă în figura de mai jos, un instrument de tip messenger.



3.2.4 Setări

Din cadrul acestui meniu, opţiunea *Afişare informaţii instituţie* poate fi utilizată de către utilizator pentru schimbarea responsabilului cu raportarea din cadrul instituţiei respective sau pentru modificarea datelor de contact ale acestuia. La prima accesare a portalului se vor actualiza datele de contact ale responsabilului desemnat din partea instituţiei publice.

Este foarte important ca aceste date să fie actualizate. Adresa de email joacă un rol foarte important în procesul de management al funcţiei publice, aceasta fiind utilizată de sistemul integrat din cadrul ANFP la notificarea responsabililor instituţiilor cu ocazia unor evenimente sau modificări referitoare la structura instituţiei sau la utilizarea Portalului. (de exemplu este înştiinţat că a fost resetată parola de acces şi datele persoanei de contact din cadrul ANFP cu care trebuie să ia legătura).

Meniul conţine opţiunea *Modificarea parolei*, opţiune care permite modificarea parolei de acces la Portal. Opţiunea *Logout,* din cadrul meniului, permite delogarea utilizatorului şi este recomandat a fi utilizată ori de câte ori utilizatorul nu mai utilizează Portal-ul.

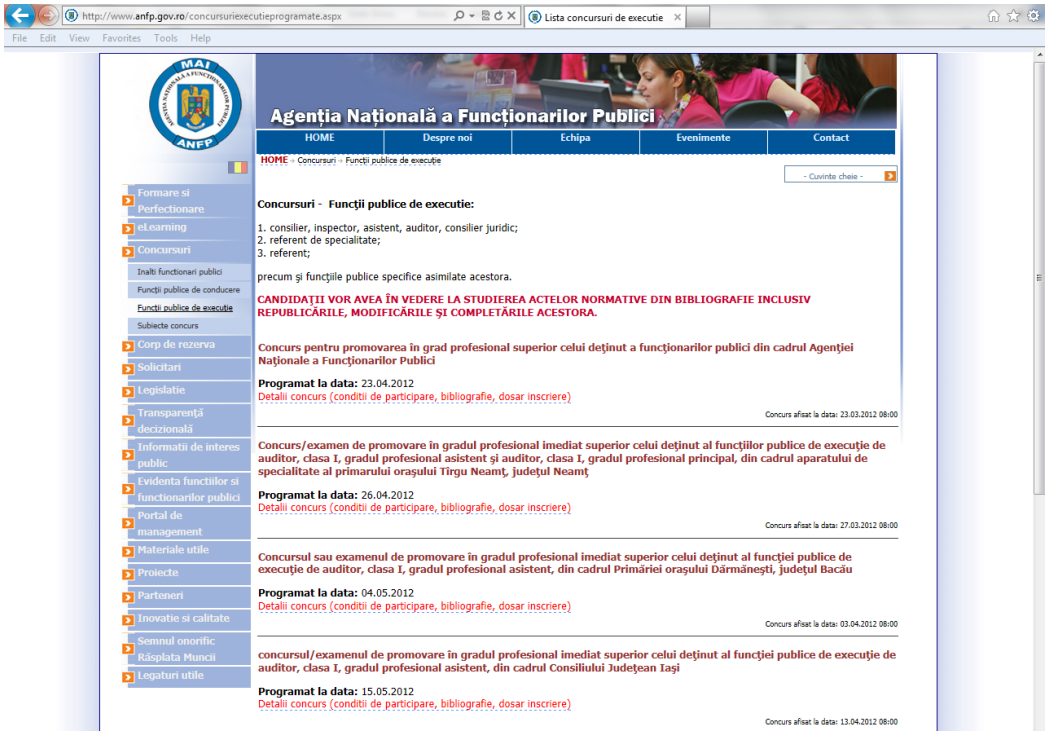
3.2.5 Ajutor

În cadrul acestei secţiuni sunt accesibile *Instrucţiunile de utilizare ale Portalului* şi datele de *Contact* ale responsabililor ANFP.

4 Gestiunea concursurilor pentru ocuparea funcţiilor publice în contextul utilizării tehnologiei informaticii

Prin intermediul sistemului informatic integrat sunt gestionate şi concursurile pentru ocuparea funcţiilor publice.

Odată validat, un concurs, acesta este afişat automat pe web site-ul ANFP (www.anfp.gov.ro)



Organizarea de către ANFP a probelor suplimentare de cunoştinţe în domeniul IT

Pentru concursurile organizate la sediul ANFP în cazul în care există probe suplimentare în domeniul IT, este utilizată platforma e-Learning a Agenţiei

Platforma e-Learning este utilizată doar în cazurile în care este prevăzută una din următoarele condiţii de participare la concurs:

- cunoştinţe în domeniul tehnologiei informaţiei - nivel de dificultate de bază
- cunoştinţe în domeniul tehnologiei informaţiei - nivel de dificultate mediu
- cunoştinţe în domeniul tehnologiei informaţiei - nivel de dificultate avansat

În cazul în care Angajatorul (instituţia publică) solicită cunoştinţe specifice în domeniul tehnologiei informaţiei (ex: programare într-un anumit limbaj, utilizarea unui anumit program informatic, grafică, prelucrare video, etc) acesta trebuie să asigure specialiştii IT în vederea organizării probei suplimentare de testare a cunoştinţelor în domeniul IT