INSPECȚIA MUNCII

Nr.41/C.A.P./22.04.2021

ANUNT

Inspectia Muncii, cu sediul in Bucuresti, str. Matei Voievod, nr 14, sector 2, in calitate de autoritate contractanta, organizează o achizitie directă pentru:

1. Extindere valabilitate pachet licențe antivirus Bitdefender pentru un an.
2. servicii de asistență tehnică informatică pentru instalarea și configurarea noilor versiuni și verificarea și asigurarea securității informatice la nivelul rețelei locale Inspecției Muncii și inspectoratelor teritoriale de muncă.

în conformitate cu prevederile art. 7, alin (5) din Legea nr 98/2016 privind achizitiile publice si ale art. 43-46 din HG nr. 395/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achizitie publice /acordul-cadru din Legea nr. 98/2016 privind achizitiile publice, achizitie ce se va finaliza cu incheierea unui contract de servicii.

Obiectul achizitiei: extindere valabilitate pachet licențe antivirus Bitdefender pentru un an și servicii de asistență tehnică informatică pentru instalarea și configurarea noilor versiuni și verificarea și asigurarea securității informatice la nivelul rețelei locale Inspecției Muncii și inspectoratelor teritoriale de muncă.

1. Cod CPV: 48760000-3 - Pachet software de protecție antivirus
2. Cod CPV: 72611000-6 - Servicii de asistență tehnică informatică

Durata contractului : pentru extindere valabilitate pachet licențe antivirus Bitdefender un an de la data semnarii contractului,

pentru servicii de asistență tehnică informatică pentru instalarea și configurarea noilor versiuni și verificarea și asigurarea securității informatice la nivelul rețelei locale Inspecției Muncii și inspectoratelor teritoriale de muncă până la data de 31.12.2021 cu posibilitatea prelungirii pentru 4 luni conform prevederilor art.165 din HG 395/2016 cu completările și modificările ulterioare.

Str. Matei Voievod, nr. 14, Sector 2, București
Tel.: +4 021 302 70 31; fax: +4 021 252 00 97
comunicare@inspectiamuncii.ro
www.inspectiamuncii.ro

INSPECȚIA MUNCII

3. Valoarea estimata:

- pentru extindere valabilitate pachet licențe antivirus Bitdefender pentru un an pentru un număr de 2100 licențe : 92.437 lei fără TVA
- pentru servicii de asistență tehnică informatică pentru instalarea și configurarea noilor versiuni și verificarea și asigurarea securității informatice la nivelul rețelei locale Inspecției Muncii și inspectoratelor teritoriale de muncă: 18.488 lei fără TVA sau 27.732 lei în cazul prelungirii contractului pentru 4 luni conform prevederilor art.165 din HG 395/2016 cu completările și modificările ulterioare

4. Sursa de finantare : bugetul de stat
5. Criteriul de atribuire: pretul cel mai scazut.
6. Modul de elaborare a ofertei: conform caietului de sarcini anexat. Ofertele care nu indeplinesc in totalitate cerintele cuprinse in caietul de sarcini sau valoarea totala depaseste valoarea estimata a achizitiei, vor fi respinse.

   Pretul ofertei este ferm, nu se accepta actualizarea pretului.

   Limba de redactare a ofertei: romana
7. Perioada de valabilitate a ofertei: 30 zile de la termenul limita de depunere a ofertei.
8. Modul de transmitere a ofertelor:
   - la adresa autoritatii contractante amintita mai sus, cu adresa de inaintare sau,
   - la adresa de e-mail : cristian.tache@inspectiamuncii.ro sau
   - postare in catalogul de produse si servicii disponibil in SEAP, la adresa www.e-licitatie.ro si confirmarea postarii la adresa de email de mai sus.
9. Data limita pentru depunerea ofertelor : 26.04.2021, ora 12,00 . Ofertele depuse dupa aceasta data nu se iau in considerare.
10. Informatii suplimentare pot fi solicitate de la Cristian Tache , telefon 0755. 037.377, e-mail : cristian.tache@inspectiamuncii.ro

Str. Matei Voievod, nr. 14, Sector 2, București
Tel.: +4 021 302 70 31; fax: +4 021 252 00 97
comunicare@inspectiamuncii.ro
www.inspectiamuncii.ro

DOCUMENTAȚIE DE ATRIBUIRE

DENUMIRE CONTRACT: FURNIZARE PRODUSE

OBIECTUL CONTRACTULUI: LICENTE ANTIVIRUS - PRELUNGIRE VALABILITATE PENTRU UN AN, INCLUSIV PRESTARI SERVICII ANTIVIRUS

Cod CPV - PRINCIPAL : 48761000-0 Pachete software antivirus

SECUNDAR: 72611000-6 Servicii de asistenta tehnica informatica

Documentația de atribuire cuprinde:

Secțiunea I- Fișa de date a achiziției;
Secțiunea II- Caietul de sarcini;
Secțiunea III - Formulare
Secțiunea IV-Model de contract

Str. Matei Voievod, nr. 14, Sector 2, București
Tel.: +4 021 302 70 31; fax: +4 021 252 00 97
comunicare@inspectiamuncii.ro
www.inspectiamuncii.ro

INSPECŢIA MUNCII

SECŢIUNEA I
FIŞA DE DATE A ACHIZIŢIEI

SECŢIUNEA I: AUTORITATEA CONTRACTANTĂ

I.1) DENUMIRE, ADRESĂ ŞI PUNCT(E) DE CONTACT

Denumire oficială: **INSPECŢIA MUNCII**		
Adresă: **Str. Matei Voievod, Nr. 14**		
Localitate:**Bucureşti**	Cod poştal:021455	Ţara:**România**
Punct(e) de contact: **În atenţia D-lui Cristian Tache**	**Telefon: +04 021/302.72.14**	
E-mail: cristian.tache@inspectiamuncii.ro	**Fax: +04 021/302.70.50**	
Adresa/ele de internet (dacă este cazul): Adresa sediului principal al autorităţii contractante (URL): www.inspectiamuncii.ro Adresa profilului cumpărătorului (URL): www.e-licitatie.ro		

Număr zile până la care se pot solicita clarificări înainte de data limită de depunere a ofertelor/candidaturilor : 3

I.2) TIPUL AUTORITĂŢII CONTRACTANTE ŞI ACTIVITATEA PRINCIPALĂ (ACTIVITĂŢILE PRINCIPALE)

■ **Minister sau orice altă autoritate naţională sau federală, inclusiv subdiviziunile regionale sau locale ale acestora** □ Agenţie/birou naţional sau federal □ Colectivitate teritorială □ Agenţie/birou regional sau local □ Organism de drept public □Instituţie/agenţie europeană sau organizaţie europeană □ Altele (precizaţi): ————————	■ **Servicii publice generale** □ Apărare □ Ordine şi siguranţă publică □ Mediu □ Afaceri economice şi financiare □ Sănătate □ Construcţii şi amenajări teritoriale □ Protecţie socială □ Recreere, cultură şi religie □ Educaţie □ Altele (precizaţi):
Autoritatea contractantă acţionează în numele altor autorităţi contractante	

da □ nu ■

SECȚIUNEA II: OBIECTUL CONTRACTULUI

II.1) DESCRIERE

II.1.1) Denumirea dată contractului/concursului/proiectului de autoritatea contractantă/entitatea contractantă

FURNIZARE PRODUSE (PRELUNGIRE VALABILITATE PACHETE LICENTE ANTIVIRUS PENTRU UN AN) SI PRESTARI SERVICII ANTIVIRUS

II.1.2) Tipul contractului şi locul de executare a lucrărilor, de livrare a produselor sau de prestare a serviciilor

a)Lucrări □	b) Produse ■	c) Servicii ■
Executare □ Proiectare şi executare □ Executarea, prin orice mijloace, a unei lucrări, conform cerinţelor specificate de autoritatea contractantă □	Cumpărare □ Leasing □ Închiriere □ Închiriere cu opţiune de cumpărare □ O combinaţie între acestea □	**Categoria serviciilor:**
Locul principal de executare	Locul principal de livrare: **Bucuresti** Cod NUTS **RO321**	Locul principal de prestare

II.1.3) Procedura implică

Un contract de achiziţii publice ■

Punerea în aplicare a unui sistem de achiziţie dinamic (SAD) □

Încheierea unui acord-cadru □

II.1.5) Descrierea succintă a contractului sau a achiziţiei/achiziţiilor: FURNIZARE PRODUSE - (PRELUNGIRE VALABILITATE PACHETE LICENTE ANTIVIRUS PENTRU UN AN) SI PRESTARI SERVICII ANTIVIRUS

II.1.6) Clasificare CPV (vocabularul comun privind achiziţiile)

PRINCIPAL : 48761000-0 Pachete software antivirus

SECUNDAR: 72611000-6 Servicii de asistenta tehnica informatica

II.1.7) Contractul intră sub incidenţa acordului privind contractele de achiziţii publice da □ **nu** ■

II.1.8) Împărţire în loturi da □ **nu** ■

II.1.9) **Vor fi acceptate variante** (oferte alternative) da □ **nu** ■

II.2) CANTITATEA SAU DOMENIUL CONTRACTULUI

II.2.1) Cantitatea totală sau domeniul

Cantitate totală estimată : conform caietului de sarcini

Valoarea estimată fără TVA: este între 110.925 lei și 120.169lei din care :

92.437 lei pentru furnizare produse (prelungire valabilitate pachete licențe antivirus)

Între 18.488 și 27.732 pentru furnizare de servicii antivirus

Valoarea minima a intervalului reprezinta valoarea estimata a prezentei proceduri (in functie de care se vor elabora si evalua ofertele), iar valoarea maxima reprezinta valoarea estimata ce contine si valoarea posibilelor suplimentari pt.4 luni conf. art.165 din HG 395/2016

II.2.2) Opțiuni da ■ nu □

Prestarea serviciilor antivirus poate fi prelungit conform art. 165 din H.G. nr. 395/2016, cu maxim 4 luni.

II.3) DURATA CONTRACTULUI SAU TERMENUL PENTRU FINALIZARE

De la data atribuirii contractului pana la 31.12.2021 .

II.4) AJUSTAREA PREȚULUI CONTRACTULUI

II.4.1. Ajustarea prețului contractului da □ nu ■

SECȚIUNEA III: INFORMAȚII JURIDICE, ECONOMICE, FINANCIARE ȘI TEHNICE

III.1) CONDIȚII REFERITOARE LA CONTRACT

III.1.1) Depozite valorice și garanții solicitate

III.1.1.b) Garanție de bună execuție da ■ **nu** □

Cuantumul garantiei de buna executie exprimata procentual este de 5% din pretul contractului, fara T.V.A. si se constituie in termen de 5 zile de la data inregistrarii contractului.

Modul de constituire: conform art.40 alin 1. din HG 395/2016.

III.1.2) Principalele modalități de finanțare și plată și/sau trimitere la dispozițiile relevante:

buget de stat

III.1.3) Forma juridică pe care o va lua grupul de operatori economici căruia i se atribuie contractul

conform art. 53 din Legea nr. 98/2016

III.1.4) Executarea contractului este supusă altor condiții speciale (*după caz*) da □ **nu** ■

III.1.5. Legislația aplicabilă

a) Legea nr. 98/2016 privind achizitiile publice, cu modificarile si completarile ulterioare

b) Hotărârea Guvernului nr. 395/2016 pentru aprobarea Normelor de aplicare a prevederilor referitoare la atribuirea contractelor de achiziție publică/acordului-cadru, cu modificarile si completarile ulterioare

- legislatie site www.anap.ro

III.2) CONDIȚII DE PARTICIPARE

III.2.1) Situația personală a operatorilor economici, inclusiv cerințele referitoare la înscrierea în registrul comerțului sau al profesiei

III.2.1.a) Situația personală a candidatului sau ofertantului:

Informații și formalități necesare pentru evaluarea respectării cerințelor

- Declarație privind neîncadrarea în art. 164 din Legea nr. 98/2016 - se va completa formularul nr. 1 din Secțiunea Formulare
- Declarație privind neîncadrarea în art. 165 din Legea nr 98/2016 - se va completa formularul nr. 2 din Secțiunea Formulare
- Declarație privind neîncadrarea în prevederile art. 167 din Legea 98/2016: se va completa formularul nr. 3 din Secțiunea Formulare
- Declaratie privind propunerea de contract formularul nr.7 din sectiunea formulare
- Declaratia privind securitatea si sanatatea in munca formularul nr.8 din sectiunea formulare.

Persoanele ce dețin funcții de decizie în cadrul autorității contractante, în ceea ce privește organizarea, derularea și finalizarea procedurii de atribuire sunt : Dantes Nicolae BRATU -Inspector General de Stat, Anisoara Alexandrescu -Director Economic, Luminița Mariana Corneci- Director - Directia Legislație, Contencios Administrativ, Cristian Tache - consilier, Dan Cornel Mitran - sef serviciu Informatica, Olimpiada Plugaru - expert IT, Ramona Elena Barna - expert IT, Victor Rotaru - expert IT, Luminita Tucmuruz - control financiar preventiv

III.2.2) Capacitatea economică și financiară

Informații și/sau nivel(uri) minim(e) necesare pentru evaluarea respectării cerințelor menționate	Modalitatea de îndeplinire
Fișa de informații generale	Se va completa formularul nr. 4 din secțiunea Formulare

III.2.3.a) Capacitatea tehnică şi/sau profesională	
Informaţii şi/sau nivel(uri) minim(e) necesare pentru evaluarea respectării cerinţelor menţionate	Modalitatea de îndeplinire
Declaraţie privind lista principalelor prestari de servicii în ultimii 3 ani	Se va prezenta formularul nr. 5 din Secţiunea Formulare Cerinţă minimă: Existenţa a cel puţin unui contract similar a cărui valoare este de 30% (33.300 lei) din valoarea estimată a prezentului contract. Prin contract similar se înţelege un contract al carui obiect a fost furnizarea de licente antivirus.
Recomandari din partea altor beneficiari	1. Prezentarea a minim 1 scrisoare de recomandare din care să rezulte modalitatea de îndeplinire a contractelor similare.
Informatii privind privind subcontractorii	1. Se va completa formularul nr. 9 din sectiunea formulare
III.2.3.b.) Standarde de asigurare a calităţii şi de protecţie a mediului	
Informaţii şi/sau nivel(uri) minim(e) necesare pentru evaluarea respectării cerinţelor menţionate	Modalitatea de îndeplinire
Certificate emise de organisme independente care atestă respectarea standardelor de asigurare a calităţii	Prestatorul să fie certificat conform grupei de standarde ISO 9001:2001 sau echivalent şi vor fi prezentate certificate doveditoare (copii semnate şi ştampilate cu menţiunea conform cu originalul)
III.2.4) Contracte rezervate	da □ **nu** ■

III.3) CONDIŢII SPECIFICE PENTRU CONTRACTELE DE SERVICII

III.3.1) Prestarea serviciilor în cauză este rezervată unei anumite profesii	da □ **nu** ■
III.3.2) Persoanele juridice au obligaţia să indice numele şi calificările profesionale ale membrilor personalului responsabili pentru prestarea serviciilor respective	da □ **nu** ■

SECȚIUNEA IV: PROCEDURĂ

IV.1) PROCEDURA

IV.1.1) Tipul procedurii şi modalitatea de desfăşurare
IV.1.1.a) Modalitatea de desfăşurare a procedurii de atribuire:achiziţie directă. **Depunerea ofertelor direct la sediul Inspectiei Muncii din str. Matei Voievod nr.14, sector 2 Bucuresti - Registratura sau pot fi transmise la adresa de e-mail cristian.tache@inspectiamuncii.ro sau pe fax la numarul 021.302.70.50**
IV.1.1.b) Tipul procedurii: Achizitie directa

IV.2) CRITERII DE ATRIBUIRE

IV.2.1) Preţul cel mai scăzut
IV.2.2) Se va organiza o licitaţie electronică da □ **nu** ■

IV.3) INFORMAŢII ADMINISTRATIVE

IV.3.1) Număr de referinţă atribuit dosarului de autoritatea contractantă : IM 37
IV.3.6) Limba sau limbile în care poate fi redactată oferta/candidatura/proiectul sau cererea de participare Română
Moneda în care se transmite oferta oferta financiară : RON
IV.3.7) Perioada minimă pe parcursul căreia ofertantul trebuie să îşi menţină oferta 90 de zile de la termenul limită de primire a ofertelor :

IV.4. PREZENTAREA OFERTEI

IV.4.1. Modul de prezentare a propunerii tehnice
Propunerea tehnică va fi în concordanţă cu specificaţiile caietului de sarcini
IV.4.2. Modul de prezentare a propunerii financiare
Ofertantul va prezenta oferta financiară conform Formularului nr. 6 din secţiunea Formulare.
IV.4.3. Modul de prezentare a ofertei
Adresa la care se depun ofertele: sediul Inspectiei Muncii din str. Matei Voievod nr. 14, sector 2 Bucuresti
Data limită pentru depunerea ofertelor : 26.04.2021 ora 14,00

INSPECȚIA MUNCII

Caiet de Sarcini - Prestare Servicii Asistență Antivirus

PRECIZĂRI INTRODUCTIVE

Inspecția Muncii deține un pachet de licență antivirus Bitdefender. Se dorește extinderea valabilității acestui pachet pentru o perioadă de un an, pentru cantitățile de mai jos, și achiziționarea de servicii de asistență tehnică informatică pentru instalarea și configurarea noilor versiuni și verificarea și asigurarea securității informatice la nivelul rețelei locale Inspecției Muncii și inspectoratelor teritoriale de muncă.

Ofertanții trebuie să răspundă la toate cerințele cuprinse în cererea tehnică și să detalieze în propunerea sa tehnică modalitatea în care soluția îndeplinește această cerință. În cazul în care soluția prezentată nu oferă informații complete sau nu îndeplinește cerințele solicitate, comisia de evaluare are dreptul să declare soluția ca fiind necorespunzătoare.

Producătorul aplicațiilor software antivirus trebuie să fie certificat tehnic conform grupei de standarde ISO 9001:2001 pentru producție de software și vor fi prezentate certificate doveditoare. Acestea trebuie să fie emise de către o autoritate competentă din țara de origine a producătorului.

Prestatorul serviciilor de protecție antivirus trebuie să fie certificat tehnic conform grupei de standarde ISO 9001:2001 și ISO 27001:2013 și vor fi prezentate certificate doveditoare.

Ofertanții trebuie să fie certificați și autorizați de către producătorul aplicațiilor software antivirus ce vor fi utilizate pentru prestarea serviciilor ce fac obiectul prezentului caiet de sarcini și vor prezenta documente doveditoare.

Soluțiile și aplicațiile software antivirus folosite de prestatorul de servicii pentru protecția stațiilor de lucru și a serverelor fizice și virtuale trebuie sa fie parte integrantă a unei soluții de administrare centralizată, în vederea monitorizării facile de care beneficiar.

Ofertanții vor include în ofertă toate cheltuielile: transport la sediul beneficiarului a personalului de intervenție, manoperele aferente, taxele și orice alte cheltuieli legate de prestarea serviciilor și de configurarea echipamentelor prevăzute în prezenta cerere de ofertă.

Soluțiile și aplicațiile antivirus pentru securitate a datelor trebuie să fie disponibilă pentru livrare și instalare de către furnizor pe toate sistemele beneficiarului în 5 zile de la semnarea contractului, pentru a nu exista perioade lungi de timp în care sistemele și serverele nu sunt protejate împotriva amenințărilor.

1. OBIECTIVE GENERALE

Extinderea valabilității pachetului de licență antivirus trebuie să asigure protecția împotriva atacurilor virușilor informatici și a altor categorii de programe de aceeași natură (troieni, malware, ransomware, spyware, etc.), pentru toate resursele din rețeaua locală a Inspecției Muncii și inspectoratelor teritoriale de muncă, în conformitate cu Anexa 1 și cantitățile de mai jos.

Oferta va fi întocmită pentru protejarea a:

- 2.100 stații de lucru și conturile de e-mail echivalente;

Str. Matei Voievod, nr. 14, Sector 2, București
Tel.: +4 021 302 70 31; fax: +4 021 252 00 97
comunicare@inspectiamuncii.ro
www.inspectiamuncii.ro

- 1 mediu virtual și 150 servere de fișiere sau echivalente.

Autoritatea contractantă își rezervă dreptul de a modifica pe durata contractului în plus sau în minus, în cuantum de 10%, valorile de mai sus.

Servicii de asistență tehnică informatică care fac obiectul cererii de ofertă trebuie să asigure protecția rețelei informatice a Inspecției Muncii și a inspectoratelor teritoriale de muncă.

În acest scop extinderea valabilității pachetului de licență antivirus și serviciile antivirus ofertate, vor acoperi toate componentele rețelei IM și ITM și vor răspunde integral cerințelor exprimate în prezentul caiet de sarcini.

CARACTERISTICI GENERALE ALE PRODUSULUI

Produsul este o platformă integrată pentru managementul securității, gândită ca o soluție modulară. Produsul conține următoarele module:

- O consolă de management care asigură funcționalități de administrare.
- Protecție antimalware pentru stații fizice, laptop-uri și servere.
- Protecție antimalware pentru medii virtualizate.
- Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android.
- Controlul dispozitivelor, controlul accesului la Internet, filtrarea traficului prin modul de tip firewall pentru mașinile fizice și virtuale.
- Protecție și securitate pentru serverele email.

A. CONSOLA DE MANAGEMENT

1. Instalare și configurare:

1. Pachetul de instalare va fi livrat ca o mașină virtuală bazată pe sistem de operare Linux (ce nu necesită licențe adiționale) securizat care conține toate rolurile sau serviciile necesare. Imaginea de tip template se va putea importa în:
   a. VMware vSphere
   b. Citrix XenServer
   c. Microsoft Hyper-V
   d. Red Hat Enterprise Virtualization
   e. KVM

2. Consola de management se livrează cu o bază de date inclusă.
3. Soluția va fi scalabilă, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași mașină virtuală.
4. Mașinile de scanare pentru mediile virtuale VMware se instalează la distanță prin task din consola de management, iar pentru alte platforme se descarcă separat din interfața web a produsului.

5. Rolurile principale trebuie să fie cel puțin similare cu: Server cu bază de date, Server de comunicație, Server de actualizare, Server de Web.
6. Soluția va include adițional și un modul de balansare (load balancer) pentru cazurile în care mai multe mașini virtuale ale componentei de management sunt instalate cu același rol (pentru Load Balancing și performanță).
7. Soluția va include un mecanism de configurare a disponibilitații pentru Serverul cu baze de date (clustering pentru redundanță). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe mașini virtuale.

2. Cerințe generale:

1. Interfața consolei de management va fi și în limba română.
2. Interfața clientului de securitate, care se instalează pe stații și servere, va fi și în limba română.
3. Manualul de instalare a produsului va fi și în limba română.
4. Manualul de administrare a produsului va fi și în limba română.
5. Soluția va include un modul de update server prin care se asigură actualizarea de produs și a semnăturilor.
6. Soluția va permite activarea/dezactivarea actualizărilor de produs/semnături.
7. Soluția permite stabilirea actualizării automate a consolei de management prin stabilirea recurenței zilnice, săptămânale sau lunare, dar și prin stabilirea intervalului orar în care acesta se va actualiza. De asemenea, soluția va permite și trimiterea unei alerte de ne-funcționalitate, cu 30 de minute înainte de actualizare.
8. Pentru o mai bună urmărire a actualizărilor consolei de management, soluția va permite vizualizarea unui jurnal de modificări în care sunt precizate istoric:
    a. versiunea consolei de management
    b. data versiunii
    c. funcții noi și îmbunătățiri
    d. probleme rezolvate
    e. probleme cunoscute
9. Notificările - prezente în interfața, notificările necitite sunt evidențiate, trimise către una sau mai multe adrese de email, alertează administratorul în cazul unor probleme majore: licențiere, detecție viruși, actualizări de produs disponibile).
10. Soluția va permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware.
11. Soluția va permite instalarea serviciului de SMNP prin care se pot raporta stările de funcționare a mașinilor din cadrul componentei de management.

3. Panou de monitorizare și raportare (Dashboard):

1. Rapoartele din panoul de monitorizare vor putea fi configurate specificând numele raportului, tipul raportului și opțiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul după care o stație de lucru este considerată neactualizată).
2. Panoul central va conține rapoarte pentru toate modulele suportate.
3. Rapoartele din panoul central de comandă vor permite: adăugarea altor rapoarte, ștergerea lor și rearanjarea.

4. Inventarierea rețelei - managementul securității

1. Soluția se va integra cu domenii Active Directory multiple, VMware vCenter și va importa inventarul acestor platforme.
2. Pentru integrarea cu Active Directory, se va putea defini și intervalul de timp de sincronizare și va efectua sincronizarea.
3. Se permite descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, KVM.
4. Se permite descoperirea stațiilor stații fizice neintegrate în Active Directory/ Workgroup cu ajutorul Network Discovery.
5. Soluția va oferi opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP.
6. Soluția va permite instalarea la distanță sau manual a clienților antimalware pe mașini fizice și virtuale.
7. Soluția va permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice și virtuale.
8. Soluția va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanță pentru clientul antimalware.
9. Soluția va oferi posibilitatea de repornire a mașinilor fizice de la distanță.
10. Soluția va oferi informații detaliate despre fiecare task și se sesizează daca task-ul s-a finalizat sau nu cu succes.
11. Soluția va permite configurarea centralizată a clienților antimalware prin intermediul politicilor.
12. Politicile se pot aplica per Active Directory, user, computere și în funcție de locația fizică a acestora.
13. Se vor oferi în consola de management informații detaliate ale obiectelor din consolă: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizări, Versiunea produsului, Versiunea de semnături.
14. Clientul antivirus trebuie să fie capabil să facă actualizări din locații diferite, în funcție de rețeaua din care face parte (rețeaua poate fi identificată prin: DNS, Gateway, MAC, IP, etc.)
15. Soluția va permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare.

5. Politici:

1. Soluția va permite configurarea setărilor antimalware prin intermediul politicilor din consola de management.
2. Politica va conține opțiuni specifice de activare/dezactivare și configurare a funcționalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web,controlul dispozitivelor, power user.
3. Soluția permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale.
4. Clientul antivirus va putea fi configurat de la distanță prin aplicarea unei singure politici ce include setări pentru toate modulele.
5. Posibilitatea ca politica să poată fi schimbată automat în funcție de:

a. User-ul logat pe stație
b. IP sau clasa de IP a stației
c. Gateway-ul alocat
d. DNS serverul alocat
e. Clientul este/nu este în aceeași rețea cu infrastructura de management
f. Tipul rețelei (LAN, wireless).

6. Rapoarte:

1. Soluția va conține rapoarte care prezintă statusul mașinilor client din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.
2. Rapoartele programate pot fi trimise către un număr nelimitat de adrese de email (nu este nevoie să aibă un cont în consola de management).
3. Soluția va permite vizualizarea rapoartelor curente programate de administrator.
4. Soluția va permite exportarea rapoartelor în format .pdf și detaliile ca format .csv.

7. Carantina:

1. Soluția va permite restaurarea fișierelor aflate în carantină în locația originală sau într-o cale sau locație configurabilă.
2. Permite descărcarea fișierelor aflate în carantină doar pentru mașinile virtuale protejate prin modulul mediilor virtuale integrate cu VMware vShield.
3. Carantina va fi locală, pe fiecare stație administrată și va fi administrată, fie local, fie din consola de management.

8. Utilizatori:

1. Administrarea se va putea face pe bază de roluri.
2. Roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter sau rol personalizat.
   a. Administrator companie: administrează arhitectura consolei de management;
   b. Administrator rețea: administrează serviciile de securitate;
   c. Reporter: monitorizează și generează rapoarte.
3. Utilizatorii pot fi importați din Microsoft Active Directory sau creați în consola de management.
4. Se va permite configurarea detaliată a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări.
5. Se va permite deconectarea automată a oricărui tip de utilizator după un anumit timp pentru o protecție sporită a datelor afișate în consola de administrare. Acest interval se poate personaliza de administratorul soluției.

9. Log-uri:

1. Înregistrarea acțiunilor utilizatorilor.
2. Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator.
3. Se va permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune.

10. Actualizare:

1. Se permite definirea de locații de actualizare multiple.
2. Se permite activarea/dezactivarea actualizărilor de produs și semnături.
3. Se permite actualizarea produsului într-o rețea fără acces la Internet.
4. Orice client antivirus să poată fi configurat să livreze update-urile către alt client antivirus.
5. Soluția să dispună de un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat de pe internet, fără intervenția administratorului. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, Mac sau, poate descarcă pachetele pentru modul de scanare centralizată în mediile de virtualizare VMware, Hyper-V.
6. În cadrul serverului de actualizare, pentru o mai bună urmărire a actualizărilor pachetele pentru protecția stațiilor și serverelor sau a pachetelor pentru modul de scanare centralizată, să fie posibilă vizualizarea unui jurnal de modificări în care sunt precizate istoric:
    a. versiunea pachetului
    b. data versiunii
    c. funcții noi și îmbunătățiri
    d. probleme rezolvate
    e. probleme cunoscute
7. Soluția va permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare va include 2 tipuri de actualizări de produs:
    a. Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei.
    b. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc.).
8. Soluția va permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management.

11. Certificate:

1. Accesul la consola de management să se facă prin HTTPS.
2. Serverul web, din consola centrală de management trebuie să permită importarea de certificate digitale eliberate de o autoritate de certificare autorizată sau proprie organizației.
3. Soluția permite afișarea în consola de management a informațiilor despre certificatele instalate: nume, autoritatea emitentă, data eliberării și data expirării certificatelor eliberate.

B. PROTECȚIE STAȚII ȘI SERVERE FIZICE/VIRTUALE

1. Caracteristici generale minimale și eliminatorii:

1. Pentru reducerea la minimum a consumului de resurse, soluția antimalware trebuie să permită instalarea personalizată a modulelor deținute (de exemplu, să permită instalarea

soluției antimalware fără modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall).

2. Pentru o mai bună protecție a stațiilor și serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigură protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor de lucru și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare.
3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware.
4. Pentru o mai bună protecție a stațiilor de lucru și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate).

2. Cerințe de sistem:

1. Sisteme de operare pentru stații de lucru: Windows 10, Windows 8, Windows 7, Windows Vista (SP1), Windows XP (SP3).
2. Sisteme de operare pentru servere: Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1.
3. Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai recent, Debian 5.0 sau mai recent.

3. Administrare și instalare la distanță (remote):

1. Înainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
2. Instalarea se va putea face în mai multe moduri:
   a. prin descărcarea directă a pachetului pe stația pe care se va face instalarea;
   b. prin instalarea la distanță, direct din consola de management.
3. Instalarea clienților la distanță în alte locații decât cele în care este instalată consola de management se va face prin intermediul unui client existent în locațiile respective de tip relay pentru a minimiza traficul în WAN.
4. În consolă vor fi disponibile informații despre fiecare stație de lucru: numele stației, IP, sistem de operare, module instalate, politica aplicată, informații despre actualizări, etc.
5. Din consolă se va putea trimite o singură politică pentru configurarea integrală a clientului de pe stații/servere.
6. Consola va include o secțiune, „Audit", unde se vor menționa toate acțiunile întreprinse fie de administratori fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare, etc.
7. Posibilitatea creării unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biți cat și pentru cele pe 64 de biți.
8. Posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), servere (fizice și/sau virtuale).
9. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.

10. Administratorul va putea creea grupuri sau chiar subgrupuri, unde va putea muta stațiile/serverele din rețea pentru cele care nu sunt integrate în domeniu.
11. Permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domeniu.

4. Caracteristici și funcționalități principale ale modulului antimalware:

1. Soluția permite administratorului să stabilească acțiunea luată de produsul Antimalware la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni:

    1. Acțiune implicită pentru fișiere infectate:
        i. interzice accesul
        ii. dezinfectează
        iii. ștergere
        iv. mută fișierele în carantină
        v. nici o acțiune

    2. Acțiune alternativă pentru fișierele infectate:
        i. interzice accesul
        ii. dezinfectează
        iii. ștergere
        iv. mută fișierele în carantină
    3. Acțiune implicită pentru fișierele suspecte:
        i. interzice accesul
        ii. ștergere
        iii. mută fișierele în carantină
        iv. nici o acțiune
    4. Acțiune alternativă pentru fișierele suspecte:
        i. interzice accesul
        ii. ștergere
        iii. mută fișierele în carantină
2. Scanarea automată în timp real va putea fi setată să nu scaneze arhive sau fișiere mai mari de o anumită dimensiune, mărimea fișierelor putând fi definită de administratorul soluției.
3. Definirea până la 16 nivele de profunzime pentru scanarea în arhive.
4. Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă.
5. Scanarea oricărui suport de stocare a informației (CD-uri, hard disk-uri externe, unități partajate etc.). De asemenea, se va putea anula scanarea în cazul în care sunt detectate unități care au informații stocate mai mari de o anumită dimensiune configurabilă.
6. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP.
7. Configurarea căilor ce urmează a fi scanate la cerere.

8. Clienții antimalware pentru workstation să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese.
9. Posibilitatea de a testa semnăturile și update-urile de produs înainte de a fi lansate în producție (stageing).
10. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware.
11. Posibilitatea de a configura scanările programate astfel încât să se execute cu prioritate redusă.
12. Produsul antimalware poate fi configurat să folosească scanarea în cloud, și parțial scanarea locală. Pentru stațiile ce nu au suficiente resurse hardware, scanarea se poate face cu o mașină de scanare instalată în rețea.
13. Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:
    - Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având toate semnăturile și motoarele stocate local.
    - Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud și, parțial, semnături locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală.
    - Scanarea centralizată în Cloud-ul privat, cu o amprentă redusă, necesitând un server de securitate pentru scanare. În acest caz, nu se stochează local nici o semnătură, iar scanarea este transferată către serverul de securitate.
    - Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare locală (motoare full).
    - Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare hibrid (cloud public cu motoare light).
14. Pentru o protecție sporită, soluția antimalware trebuie sa aibă 3 tipuri de detecție: bazată pe semnături, bazată pe comportamentul fișierelor și bazată pe monitorizarea proceselor.
15. Pentru o protecție sporită, soluția antimalware trebuie sa poată scana paginile HTTPS.
16. Pentru o mai bună gestionare a antimalware instalat pe stații, produsul va include opțiunea de setare a unei parole pentru protecția la dezinstalare.
17. Pentru siguranța utilizatorului, clientul va include un modul de antiphishing.
18. Soluția oferă protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată.
19. Pe mașinile virtuale parte a unui pool instalarea clientului antimalware se face doar pe mașină de tip template, după care se recompune pool-ul de mașini virtuale.

5. Firewall:

1. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
2. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.
3. Posibilitatea de a defini rețele de încredere pentru mașina destinație.
4. Să existe predefinite minim 10 seturi de reguli.

6. Carantina:

1. Produsul antimalware să permită trimiterea automată a fișierelor din carantină către laboratoarele antimalware ale producătorului.
2. Trimiterea conținutului carantinei va putea fi expediat în mod automat, la un interval definit de administrator.
3. Produsul antimalware să permită ștergerea automată a fișierelor aflate în carantină mai vechi de o anumită perioadă, pentru a nu încărca inutil spațiul de stocare.
4. Posibilitatea de a restaura un fișier din carantină în locația lui originală.
5. Modulul de carantină va permite rescanarea obiectelor după fiecare actualizare de semnături.

7. Protecția datelor:

1. Produsul permite blocarea datelor confidențiale (pin-ul cardului, cont bancar, etc.) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.

8. Controlul conținutului:

1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularități:
   a. Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini.
   b. Permite blocarea accesului la Internet pe intervale orare.
   c. Permite blocarea paginilor de internet care conțin anumite cuvinte cheie.
   d. Permite controlul accesului numai la anumite pagini de internet specificate de administrator;
   e. Permite blocarea accesului la anumite aplicații definite de administrator;
   f. Permite restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violență, pornografie, etc.).

9. Controlul dispozitivelor:

1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.
2. Modulul va permite controlul următoarelor tipuri de dispozitive:
   a. Bluetooth Devices
   b. CDROM Devices
   c. Floppy Disk Drives
   d. Security Policies 153
   e. IEEE 1284.4
   f. IEEE 1394
   g. Imaging Devices
   h. Modems

i. Tape Drives
j. Windows Portable
k. COM/LPT Ports
l. SCSI/SAS RAID
m. Printers
n. Network Adapters
o. Wireless Network Adapters
p. Internal and External Storage

3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client.

4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

10. Power User:

1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului.
2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa și modifica setările clientului antimalware dintr-o consolă disponibilă local pe mașina client.
3. Administratorul va putea suprascrie din consolă setările aplicate de utilizatorii Power User.

11. Actualizare:

1. Posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizare).
2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).
3. Actualizarea pentru locațiile remote prin intermediul unui client antimalware care are și rol de server de actualizare.

C. PROTECȚIE ȘI SECURITATE PENTRU DISPOZITIVELE MOBILE

1. Cerințe minime de sistem:

- Telefoane cu sistem de operare iOS 5 sau mai recent: Apple iPhone și tablete iPad
- Telefoane și tablete cu sistem de operare Android 2.2 sau mai recent.

2. Caracteristici:

1. Permite asocierea unui dispozitiv cu un utilizator din Active Directory.
2. Instalarea se face prin trimiterea unui email către utilizator cu detaliile de instalare.
3. Activarea dispozitivului mobil în consola de management să se facă prin scanarea unui cod QR.
4. Pachetele de instalare se vor putea descărca de pe Apple App Store și Google Play.
5. Se vor putea întreprinde următoarele acțiuni:

a. Blocarea dispozitivului;
b. Deblocarea dispozitivului;
c. Ștergerea datelor și revenirea la setările din fabrică;

d. Localizarea dispozitivului;
e. Scanarea dispozitivului(doar pentru cele cu sistem de operare Android);
f. Criptarea memoriei dispozitivului(doar pentru cele cu sistem de operare (Android).

6. Consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel încât utilizatorul să aibă acces total asupra lui (rooted or jailbroken devices).

D. ANTIMALWARE, ANTISPAM ȘI FILTRARE DE CONȚINUT PENTRU SERVERE EMAIL LINUX

1. Produsul va oferi protecție antimalware, antispam și antiphishing, precum și filtrare de atașamente și conținut.
2. Actualizarea motoarelor și semnăturilor antimalware trebuie să poată fi făcută automat la un interval de maxim 1 ora, precum și la cerere.
3. Administratorul va putea defini o acțiune secundară (ștergere sau plasare în carantină) pentru cazul în care dezinfectarea unui mesaj eșuează.
4. În afara de detecția pe bază de semnături, modulul de protecție antimalware va trebui să includă și scanare euristică comportamentală, prin simularea unui calculator virtual în interiorul căruia sunt rulate și analizate aplicații cu potențial periculos, pentru a proteja sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă.
5. Modulul antimalware trebuie să permită configurarea de acțiuni separate pentru fișierele suspecte.
6. Produsul va oferi protecție anti-phishing, care să detecteze tentativele de copiere a infățișării și conținutului mesajelor autentice în vederea păcălirii destinatarului acestora pentru obținerea ilegală de date confidențiale.
7. Produsul va oferi protecție antispam, cu o bază de semnaturi actualizabila prin internet.
8. Modulul antispam trebuie sa includă un filtru URL cu o bază de adrese URL cunoscute a fi folosite în mesaje spam sau phishing, precum și un filtru de caractere pentru detectarea automată a mesajelor scrise cu caractere chirilice sau asiatice.
9. Modulul antispam trebuie să includă un filtru euristic și un serviciu/filtru online pentru imbunătățirea protecției împotriva valurilor de spam nou apărute.
10. Produsul va oferi opțiuni multiple de acțiune la identificarea unui mesaj spam: ștergere, plasarea în carantina sau marcarea subiectului ca spam.
11. Produsul va permite configurarea unei liste de adrese sau domenii email considerate sigure, ale căror emailuri vor fi permise automat de către modulul antispam. Produsul va permite configurarea unei liste de adrese sau domenii email cunoscute pentru trimiterea de mesaje spam, care vor fi detectate în mod automat de către modulul antispam.
12. Produsul va permite configurarea de reguli de filtrare de conținut pe bază de cuvinte cheie și expresii regulate, precum și configurarea de reguli de filtrare a atașamentelor email în funcție de tip, nume și mărime.
13. Produsul va oferi acțiuni specifice pentru mesajele de conțin obiecte protejate prin parola (ignorare, ștergere sau plasare în carantină).
14. Produsul va permite configurarea de reguli de filtrare specifice pentru anumite grupuri de utilizatori.
15. Pentru ușurința accesului la setări, produsul va avea consola de administrare web. Consola web va permite crearea de conturi de administrator diferite.

16. Produsul va înregistra evenimentele privind funcționarea și activitatea de scanare în fișiere log
17. Produsul va permite configurarea dimensiunii fișierelor log și ștergerea automată a logurilor mai vechi de un număr de zile definit de administrator.
18. Produsul va permite trimiterea de alerte pe mail către administrator în cazul detecțiilor de viruși, spam și conținut.
19. Produsul va notifica administratorul în momentul în care va detecta o actualizare disponibilă pe serverele producătorului antivirus.
20. Produsul va oferi statistici și grafice privind activitatea de scanare (inclusiv numărul de mesaje scanate și detecții de viruși și spam).
21. Suport SNMP pentru trimiterea mesajelor de tip alertă.
22. Produsul trebuie să fi primit certificare VBSpam/VBSpam+ în fiecare dintre ultimele 12 teste VBSpam, cu o rată medie de detecție de peste 99.8%".

SERVICII

Servicii prestate pe durata contractului
Sistemul antivirus trebuie să fie în mod obligatoriu însoțit de următoarele servicii pentru perioada contractată:

1. Instalarea și configurarea în întreaga rețea a Inspecției Muncii a celor mai recente versiuni ale produselor ofertate și a cheilor de licență aferente acestora.
2. Posibilitatea prestatorului de a răspunde unor solicitări cu privire la incidente provocate de către atacurile virușilor în termen de 24 ore prin intervenție în locațiile beneficiarului fizic sau de la distanță.
3. Ofertantul trebuie să asigure intervenții periodice, on site la sediul central al Inspecției Muncii cu frecvență săptămânală pentru verificarea și dezinfecția rețelei locale de calculatoare.
4. Ofertantul trebuie să asigure intervenții periodice, remote la sediul inspectoratelor teritoriale de muncă cuprinse în anexa nr. 1, cu frecvență lunară, pentru verificarea și dezinfecția rețelei locale de calculatoare.
5. Ofertantul trebuie să asigure intervenții la cerere, în situații critice, on site, la sediul Inspecției Muncii și ITM București pentru evenimente critice în maximum 4 ore de la primirea solicitării.
6. Ofertantul trebuie să asigure intervenții la cerere, în situații critice, on site, la sediul celorlalte inspectorate teritoriale de muncă cuprinse în anexa nr.1 pentru evenimente critice în maximum 8 ore de la primirea solicitării. Intervențiile la cerere vor fi în limita de o intervenție/lună calendaristică.
7. Fiecare intervenție periodică din orice locație IM și ITM se va finaliza prin completarea unei fișe de intervenție în care vor fi consemnate activitățile efectuate. Fișa de intervenție va fi semnata de către persoana care a efectuat intervenția și de către un reprezentant desemnat al beneficiarului. Fișele de intervenție vor certifica prestarea serviciilor și vor condiționa plata lunară a acestora. Modelul fișei de intervenție precum și procedura de solicitare a intervențiilor la cerere vor fi stabilite de comun acord între beneficiarul și prestatorul serviciilor, în momentul contractării.

8. Ofertantul trebuie să asigure asistență și suport tehnic în limba română prin telefon, e-mail și chat non-stop 24h/zi, 7 zile/săptămână, pentru perioada de derulare a contractului. Modalitatea de asigurare a asistenței și a suportului tehnic pentru diagnoză și rezolvarea problemelor va fi on line sau telefonic, după caz.

   Serviciile vor fi implementate în rețeaua IM și ITM pentru o perioadă cuprinsă între data încheierii contractului și 31.12.2021, facturabile lunar, cu posibilitatea de prelungire a contractului cu o perioadă de maxim 4 luni conform prevederilor art. 6, alin. 3 lit. d din H.G. 925/2006, cu modificările și completările ulterioare.

LIVRABILE:

- kit-urile de instalare ale produselor cu interfața în limba româna,
- certificate de licență,
- documentația produsului în limba română.

Str. Matei Voievod, nr. 14, Sector 2, București
Tel.: +4 021 302 70 31; fax: +4 021 252 00 97
comunicare@inspectiamuncii.ro
www.inspectiamuncii.ro

INSPECȚIA MUNCII

ANEXA 1 la CONTRACT DE FURNIZARE PRODUSE ȘI SERVICII nr.

Nr crt	Denumirea produsului	Denumire producator	Cant. u.m.
0	1	2	3
1	GravityZone Security for Endpoints Physical Workstations, valabilitate 1 an	Bitdefender SRL	2.100,00
2	GravityZone Security for Mail Servers, valabilitate 1 an	Bitdefender SRL	2.100,00
3	GravityZone Security for Endpoints Physical Servers, valabilitate 1 an	Bitdefender SRL	150,00
4	GravityZone Security for Virtual Environments (VS) , valabilitate 1 an	Bitdefender SRL	1,00
5	Servicii antivirus, valabilitate 1 luna		8,00

ANEXA 2

SERVICII:	
1.	Furnizorul va asigura instalarea și configurarea în întreaga rețea a Inspecției Muncii a celor mai recente versiuni ale produselor ofertate și a cheilor de licență aferente acestora.
2.	Furnizorul va răspunde unor solicitări cu privire la incidente provocate de către atacurile virușilor în termen de 24 ore prin intervenție în locațiile beneficiarului fizic sau de la distanță.
3.	Furnizorul va asigura intervenții periodice, on site la sediul central al Inspecției Muncii cu frecvență săptămânală pentru verificarea și dezinfecția rețelei locale de calculatoare.
4.	Furnizorul va asigura intervenții periodice, remote la sediul inspectoratelor teritoriale de muncă cuprinse în anexa nr. 1 la Caietul de sarcini, cu frecvență lunară, pentru verificarea și dezinfecția rețelei locale de calculatoare.
5.	Furnizorul va asigura intervenții la cerere, în situații critice, on site, la sediul Inspecției Muncii și ITM București pentru evenimente critice în maximum 4 ore de la primirea solicitării.
6.	Furnizorul trebuie să asigure intervenții la cerere, în situații critice, on site, la sediul celorlalte inspectorate teritoriale de muncă cuprinse în anexa nr.1 la Caietul de sarcini, pentru evenimente critice în maximum 8 ore de la primirea solicitării. Intervențiile la cerere vor fi în limita la o intervenție/lună calendaristică.
7.	Fiecare intervenție periodică din orice locație IM și ITM se va finaliza prin completarea unei fișe de intervenție în care vor fi consemnate activitățile efectuate. Fișa de intervenție va fi semnata de către persoana care a efectuat intervenția și de către un reprezentant desemnat al beneficiarului. Fișele de intervenție vor certifica prestarea serviciilor și vor condiționa plata lunara a acestora.
8.	Furnizorul va trebui să asigure asistență și suport tehnic în limba română prin telefon, e-mail și chat non-stop 24h/zi, 7 zile/săptămână, pentru perioada de derulare a contractului. Modalitatea de asigurare a asistenței și a suportului tehnic pentru diagnoza și rezolvarea problemelor va fi on line sau telefonic, după caz.

Str. Matei Voievod, nr. 14, Sector 2, București
Tel.: +4 021 302 70 31; fax: +4 021 252 00 97
comunicare@inspectiamuncii.ro

INSPECȚIA MUNCII

ANEXA 3- LOCAȚII la CONTRACT DE FURNIZARE PRODUSE ȘI SERVICII nr

Locațiile pentru care se prestează serviciile antivirus și datele de contact

Nr. crt.	Organizatia	Adresa mail
1	ITM Alba	informatica@itmalba.ro
2	ITM Arad	informatica@itmarad.ro
3	ITM Arges	informatica@itmarges.ro
4	ITM Bacau	informatica@itmbacau.ro
5	ITM Bihor	informatica@itmbihor.ro
6	ITM Bistrita-Nasaud	informatica@itmbistrita.ro
7	ITM Botosani	informatica@itmbotosani.ro
8	ITM Braila	informatica@itmbraila.ro
9	ITM Brasov	informatica@itmbrasov.ro
10	ITM Bucuresti	informatica@itmbucuresti.ro
11	ITM Buzau	informatica@itmbuzau.ro
12	ITM Calarasi	informatica@itmcalarasi.ro
13	ITM Caras-Severin	informatica@itmcaras.ro
14	ITM Cluj	informatica@itmcluj.ro
15	ITM Constanta	informatica@itmconstanta.ro
16	ITM Covasna	informatica@itmcovasna.ro
17	ITM Dambovita	informatica@itmdambovita.ro
18	ITM Dolj	informatica@itmdolj.ro
19	ITM Galati	informatica@itmgalati.ro
20	ITM Giurgiu	informatica@itmgiurgiu.ro
21	ITM Gorj	informatica@itmgorj.ro
22	ITM Harghita	informatica@itmharghita.ro
23	ITM Hunedoara	informatica@itmhunedoara.ro
24	ITM Ialomita	informatica@itmialomita.ro
25	ITM Iasi	informatica@itmiasi.ro
26	ITM Ilfov	informatica@itmilfov.ro
27	ITM Maramures	informatica@itmmaramures.ro
28	ITM Mehedinti	informatica@itmmehedinti.ro
29	ITM Mures	informatica@itmmures.ro
30	ITM Neamt	informatica@itmneamt.ro
31	ITM Olt	informatica@itmolt.ro
32	ITM Prahova	informatica@itmprahova.ro
33	ITM Salaj	informatica@itmsalaj.ro
34	ITM Satu Mare	informatica@itmsatumare.ro
35	ITM Sibiu	informatica@itmsibiu.ro

Str. Matei Voievod, nr. 14, Sector 2, București
Tel.: +4 021 302 70 31; fax: +4 021 252 00 97
comunicare@inspectiamuncii.ro
www.inspectiamuncii.ro

36	ITM Suceava	informatica@itmsuceava.ro
37	ITM Teleorman	informatica@itmteleorman.ro
38	ITM Timis	informatica@itmtimis.ro
39	ITM Tulcea	informatica@itmtulcea.ro
40	ITM Valcea	informatica@itmvalcea.ro
41	ITM Vaslui	informatica@itmvaslui.ro
42	ITM Vrancea	informatica@itmvrancea.ro
43	Inspectia Muncii	iminformatica@inspectiamuncii.ro
44	Revista Obiectiv	iminformatica@inspectiamuncii.ro

FORMULARE

OPERATOR ECONOMIC

_____

(denumirea/numele)

Formular 1

DECLARAŢIE PRIVIND NEÎNCADRAREA ÎN ART. 164 DIN LEGEA 98/2016

Subsemnatul _____, reprezentant împuternicit al _____, *(denumirea/numele şi sediul/adresa operatorului economic)* în calitate de _____ *(candidat/ofertant/ofertant asociat/terţ susţinător al candidatului/ofertantului* _____*)* declar pe propria răspundere, sub sancţiunea excluderii din procedură şi a sancţiunilor aplicate faptei de fals în acte publice, că nu mă aflu în situaţiile prevăzute la **art. 164 din Legea 98/2016** privind atribuirea contractelor de achiziţie publică, respectiv nu am fost condamnat prin hotărâre definitivă a unei instanţe judecătoreşti, pentru comiterea uneia dintre următoarele infracţiuni:

a) constituirea unui grup infracţional organizat, prevăzută de art. 367 din Legea nr. 286/2009 privind Codul penal, cu modificările şi completările ulterioare, sau de dispoziţiile corespunzătoare ale legislaţiei penale a statului în care respectivul operator economic a fost condamnat;

b) infracţiuni de corupţie, prevăzute de art. 289-294 din Legea nr. 286/2009, cu modificările şi completările ulterioare, şi infracţiuni asimilate infracţiunilor de corupţie prevăzute de art. 10-13 din Legea nr. 78/2000 pentru prevenirea, descoperirea şi sancţionarea faptelor de corupţie, cu modificările şi completările ulterioare, sau de dispoziţiile corespunzătoare ale legislaţiei penale a statului în care respectivul operator economic a fost condamnat;

c) infracţiuni împotriva intereselor financiare ale Uniunii Europene, prevăzute de art. 18^1 -18^5 din Legea nr. 78/2000, cu modificările şi completările ulterioare, sau de dispoziţiile corespunzătoare ale legislaţiei penale a statului în care respectivul operator economic a fost condamnat;

d) acte de terorism, prevăzute de art. 32-35 şi art. 37-38 din Legea nr. 535/2004 privind prevenirea şi combaterea terorismului, cu modificările şi completările ulterioare, sau de dispoziţiile corespunzătoare ale legislaţiei penale a statului în care respectivul operator economic a fost condamnat;

e) spălarea banilor, prevăzută de art. 29 din Legea nr. 656/2002 pentru prevenirea şi sancţionarea spălării banilor, precum şi pentru instituirea unor măsuri de prevenire şi combatere a finanţării terorismului, republicată, cu modificările ulterioare, sau finanţarea terorismului, prevăzută de art. 36 din Legea nr. 535/2004, cu modificările şi completările ulterioare, sau de dispoziţiile corespunzătoare ale legislaţiei penale a statului în care respectivul operator economic a fost condamnat;

f) traficul şi exploatarea persoanelor vulnerabile, prevăzute de art. 209-217 din Legea nr. 286/2009, cu modificările şi completările ulterioare, sau de dispoziţiile corespunzătoare ale legislaţiei penale a statului în care respectivul operator economic a fost condamnat;

g) fraudă, în sensul articolului 1 din Convenţia privind protejarea intereselor financiare ale Comunităţilor Europene din 27 noiembrie 1995.

De asemenea, declar pe propria răspundere, sub sancţiunea excluderii din procedură şi a sancţiunilor aplicate faptei de fals în acte publice, că nici un membru al organului de administrare, de conducere sau de supraveghere al societăţii sau cu putere de reprezentare, de decizie sau de control în cadrul acesteia nu face obiectul excluderii aşa cum este acesta definit la art. 164, alin (1) din Legea 98/2016.

Subsemnatul declar că informaţiile furnizate sunt complete şi corecte în fiecare detaliu şi înţeleg că autoritatea contractantă are dreptul de a solicita, în scopul verificării şi confirmării declaraţiilor orice documente doveditoare de care dispunem.

Înteleg că în cazul în care această declaraţie nu este conformă cu realitatea sunt pasibil de încălcarea prevederilor legislaţiei penale privind falsul în declaraţii.

Operator economic,

_____

(semnatura autorizată)

OPERATOR ECONOMIC

_____

(denumirea/numele)

Formular 2

DECLARAȚIE PRIVIND NEÎNCADRAREA ÎN ART. 165 ȘI 167 DIN LEGEA 98/2016

Subsemnatul _____, reprezentant împuternicit al _____, *(denumirea/numele și sediul/adresa operatorului economic)* în calitate de _____ *(candidat/ofertant/ofertant asociat/terț susținător al candidatului/ofertantului* _____) la procedura de _____ pentru achiziția de _____, cod CPV _____, la data de _____ organizată de _____ (denumirea autorității contractante), declar pe proprie răspundere că:

1. **Nu ne-am** încălcat obligațiile privind plata impozitelor, taxelor sau a contribuțiilor la bugetul general consolidat așa cum aceste obligații sunt definite de art. 165, alin. (1) și art. 166, alin. (2) din Legea 98/2016.
2. **Nu ne aflăm** în oricare dintre următoarele situații prevăzute de art. 167, alin (1) din Legea 98/2016, respectiv:

a) nu am încălcat obligațiile stabilite potrivit art. 51, iar autoritatea contractantă poate demonstra acest lucru prin orice mijloc de probă adecvat, cum ar fi decizii ale autorităților competente prin care se constată încălcarea acestor obligații;

b) nu ne aflăm în procedura insolvenței sau în lichidare, în supraveghere judiciară sau în încetarea activității;

c) nu am comis o abatere profesională gravă care ne pune în discuție integritatea, iar autoritatea contractantă poate demonstra acest lucru prin orice mijloc de probă adecvat, cum ar fi o decizie a unei instanțe judecătorești sau a unei autorități administrative;

d) nu am încheiat cu alți operatori economici acorduri care vizează denaturarea concurenței în cadrul sau în legătură cu procedura în cauză;

e) nu ne aflăm într-o situație de conflict de interese în cadrul sau în legătură cu procedura în cauză;

f) nu am participat anterioar la pregătirea procedurii de atribuire ceea ce a condus la o distorsionare a concurenței;

g) nu ne-am încălcat în mod grav sau repetat obligațiile principale ce ne reveneau în cadrul unui contract de achiziții publice, al unui contract de achiziții sectoriale sau al unui contract de concesiune încheiate anterior, iar aceste încălcări au dus la încetarea anticipată a respectivului contract, plata de daune-interese sau alte sancțiuni comparabile;

h) nu ne facem vinovați de declarații false în conținutul informațiilor transmise la solicitarea autorității contractante în scopul verificării absenței motivelor de excludere sau al îndeplinirii criteriilor de calificare și selecție, am prezentat aceste informații sau suntem în măsură să prezentăm documentele justificative solicitate;

i) nu am încercat să influențăm în mod nelegal procesul decizional al autorității contractante, să obținem informații confidențiale care ne-ar putea conferi avantaje nejustificate în cadrul procedurii de atribuire, nu am furnizat din neglijență informații eronate care pot avea o influență semnificativă asupra deciziilor autorității contractante privind excluderea din procedura de atribuire a unui operator economic, selectarea acestuia sau atribuirea contractului de achiziție publică/acordului-cadru către respectivul operator economic.

Subsemnatul declar că informațiile furnizate sunt complete și corecte în fiecare detaliu și înțeleg că autoritatea contractantă are dreptul de a solicita, în scopul verificării și confirmării declarațiilor orice documente doveditoare de care dispunem.

Înteleg că în cazul în care această declarație nu este conformă cu realitatea sunt pasibil de încălcarea prevederilor legislației penale privind falsul în declarații.

Operator economic,

_____

(semnătura autorizată)

OPERATOR ECONOMIC

_____

(denumirea/numele)

Formular 3

DECLARAŢIE PRIVIND EVITAREA CONFLICTULUI DE INTERESE POTRIVIT ART. 59 ŞI 60 DIN LEGEA 98/2016

1. Subsemnatul _____, reprezentant împuternicit al _____, *(denumirea/numele şi sediul/adresa operatorului economic)* în calitate de _____ *(candidat/ofertant/ofertant asociat/terţ susţinător al candidatului/ofertantului* _____) la procedura de _____, declar pe proprie răspundere, următoarele: cunoscând prevederile **art. 59 şi 60 din Legea nr. 98/2016** privind achiziţiile publice şi componenţa listei cu persoanele ce deţin funcţii de decizie în autoritatea contractantă cu privire la organizarea, derularea şi finalizarea procedurii de atribuire, declar că societatea noastră nu se află în situaţia de a fi exclusă din procedură.

Subsemnatul declar că informaţiile furnizate sunt complete şi corecte în fiecare detaliu şi înţeleg că autoritatea contractantă are dreptul de a solicita, în scopul verificării şi confirmării declaraţiilor, orice documente doveditoare de care dispun.

Înţeleg că în cazul în care această declaraţie nu este conformă cu realitatea sunt pasibil de încălcarea prevederilor legislaţiei penale privind falsul în declaraţii.

2. Subsemnatul _____ declar că voi informa imediat autoritatea contractantă dacă vor interveni modificări în prezenta declaraţie la orice punct pe parcursul derulării procedurii de atribuire a contractului de achiziţie publică sau, în cazul în care vom fi desemnaţi câştigători, pe parcursul derulării contractului de achiziţie publică, având în vedere şi prevederile **art. 61 din Legea nr. 98/2016**.

Subsemnatul declar că informaţiile furnizate sunt complete şi corecte în fiecare detaliu şi înţeleg că autoritatea contractantă are dreptul de a solicita, în scopul verificării şi confirmării declaraţiilor orice documente doveditoare de care dispunem.

Înteleg că în cazul în care această declaraţie nu este conformă cu realitatea sunt pasibil de încălcarea prevederilor legislaţiei penale privind falsul în declaraţii.

Operator economic,

_____

(semnatura autorizată)

Formular nr. 10

A se transmite pe hârtie cu antetul
ofertantului/operatorului economic

OFERTANT/OPERATOR ECONOMIC

_____
(denumirea/numele)

FORMULAR DE OFERTĂ

Către .....
(denumirea autorității contractante și adresa completă)
Domnilor,
1. Examinand invitația de participare transmisă de dvs. cu nr. ....., subsemnații, reprezentanți ai ofertantului

_____, ne oferim ca, în conformitate
(denumirea/numele ofertantului)
cu prevederile și cerintele cuprinse în documentația mai sus menționată, să prestăm _____ pentru suma de _____ lei
(denumirea serviciului) (suma în litere și în cifre)
reprezentând _____ lei, la care se adaugă taxa pe valoarea adaugată în valoare de
(suma în litere și în cifre)
_____ lei.
(suma în litere și în cifre)
2. Ne angajăm ca, în cazul în care oferta noastră este stabilită câștigătoare, să prestăm serviciile în graficul de timp stabilit.
3. Ne angajăm să menținem aceasta ofertă valabilă pentru o durată de _____ zile,
(durata în litere și cifre)
respectiv până la data de _____, și ea va rămâne obligatorie
(ziua/luna/anul)
pentru noi și poate fi acceptată oricând înainte de expirarea perioadei de valabilitate.
4. Până la încheierea și semnarea contractului de achiziție publică această oferta, împreună cu comunicarea transmisă de dumneavoastră, prin care oferta noastră este stabilită câștigătoare, vor constitui un contract angajant între noi.
5. Alături de oferta de bază:
|_| depunem ofertă alternativă, ale cărei detalii sunt prezentate într-un formular de ofertă separat, marcat în mod clar "alternativă";

|_| nu depunem ofertă alternativă.
(se bifează opțiunea corespunzătoare)
6. Înțelegem că nu sunteți obligați să acceptați oferta cu cel mai scăzut preț sau orice altă oferta pe care o puteți primi.

Data _____/_____/_____

_____, în calitate de _____, legal autorizat să (numele în clar al persoanei autorizate) (funcția)

semnez oferta pentru și în numele _____.
(denumirea/numele ofertantului)

Formularul nr. 4

Operator economic

_____

(denumirea/numele)

INFORMAŢII GENERALE

1. Denumirea/numele:
2. Codul fiscal:
3. Adresa sediului central:
4. Telefon:
   Fax:
   E-mail:
5. Certificatul de înmatriculare/înregistrare

_____

(numărul, data şi locul de înmatriculare/înregistrare)

6. Obiectul de activitate, pe domenii:

_____

(în conformitate cu prevederile din statutul propriu)

7. Birourile filialelor/sucursalelor locale, dacă este cazul:

_____

(adrese complete, telefon/fax, certificate de inmatriculare/inregistrare)

8. Principala piaţă a afacerilor:
9. Cifra de afaceri pe ultimii 3 ani:

Anul	Cifra de afaceri anuală anuală la 31 decembrie (mii lei)	Cifra de afaceri anuală la 31 decembrie (echivalent euro)
1.		
2.		
3.		
Media anuală:		

Data completării.....

Operator economic,

.....

(semnătură autorizată)

Formularul nr. 5

Operator economic

_____

(denumirea/numele)

DECLARAŢIE PRIVIND LISTA PRINCIPALELOR PRESTARI DE SERVICII ÎN ULTIMII 3 ANI

1. Subsemnatul, reprezentant împuternicit al _____ *(denumirea/numele candidatului/ofertantului)* şi *sediul/adresa*

declar pe propria răspundere, sub sancţiunile aplicate faptei de fals în acte publice, că datele prezentate în tabelul anexat sunt reale.

2. Subsemnatul declar că informaţiile furnizate sunt complete şi corecte în fiecare detaliu şi inteleg că autoritatea contractantă are dreptul de a solicita, în scopul verificării şi confirmării declaraţiilor, situaţiilor şi documentelor care însotesc oferta, orice informaţii suplimentare în scopul verificării datelor din prezenta declaratie.

3. Subsemnatul autorizez prin prezenta orice instituţie, societate comercială, bancă, alte persoane juridice să furnizeze informaţii reprezentanţilor autorizaţi ai autorităţii contractante _____ cu privire la orice aspect tehnic şi financiar în

(denumirea şi adresa autorităţii contractante)

legatură cu activitatea noastră.

4. Prezenta declaraţie este valabilă pana la data de _____

(se precizează data expirării perioadei de valabilitate a ofertei

Nr. Crt.	Denumirea şi obiectul contractului + Numărul şi data contractului	Codul CPV	Denumirea/numele beneficiarului /clientului + Adresa	Calitatea în contract*)	Preţul total al contractului (lei)	Preţul total al contractului (valuta**)	Natura si cantitatea (U.M.)	Perioada de livrare	Observaţii
0	1		2	3	4	5	6	7	8
1									
2									
.....									

Data completării.....

Operator economic,

.....

(semnătură autorizată)

)

*) Se precizează calitatea în care a participat la îndeplinirea contractului care poate fi de: contractant unic sau contractant conducator (lider de asociaţie); contractant asociat; subcontractant.

**)Se va preciza data de referinţă pentru stabilirea echivalentului în valută a contractului respectiv.

OPERATOR ECONOMIC
_____[ANTET]_____

Formularul nr. 8

DECLARATIE PRIVIND PROTECTIA MUNCII

Subsemnatul..... reprezentant imputernicit al _____,
(denumirea/numele si sediul/adresa operatorului economic)

declar pe propria raspundere, sub sanctiunea excluderii din procedura si a sanctiunilor aplicate faptei de fals in acte publice, ca vom respecta pe toata durata contractului, in cazul in care acesta ne va fi atribuit, regulile obligatorii referitoare la conditiile de munca si protectia muncii in vigoare la nivel national, in speta prevederile Legii 319/2006 privind securitatea si sanatatea in munca si orice alta reglementare care va aparea in perioada mentionata mai sus.

Data completarii: __/__/2016

Operator economic,

_____

(semnatura autorizata)

OPERATOR ECONOMIC
_____[ANTET]_____

Formularul nr. 9

DECLARATIE PRIVIND SUBCONTRACTANTII
(partea/partile din contract care sunt indeplinite de subcontractanti si specializarea acestora)

Subsemnatul(a) ..... (numele si prenumele), reprezentant imputernicit al ..... (denumirea/numele si sediul/adresa operatorului economic), declar pe propria raspundere, sub sanctiunile aplicate faptei de fals in acte publice, ca datele prezentate in tabelul anexat sunt reale.
Subsemnatul declar ca informatiile furnizate sunt complete si corecte in fiecare detaliu si inteleg ca autoritatea contractanta are dreptul de a solicita, in scopul verificarii si confirmarii declaratiilor, situatiilor si documentelor care insotesc oferta, orice informatii suplimentare in scopul verificarii datelor din prezenta declaratie.
Subsemnatul autorizez prin prezenta orice institutie, societate comerciala, banca, alte persoane juridice sa furnizeze informatii reprezentantilor autorizati ai ..... (denumirea si adresa autoritatii contractante) cu privire la orice aspect tehnic si financiar in legatura cu activitatea noastra.
Prezenta declaratie este valabila pana la data de ..... (se precizeaza data expirarii perioadei de valabilitate a candidatului)

Nr. crt.	Denumire subcontractant/ adresa/CUI	Specializare subcontractant	Partea/partile din contract ce urmeaza a fi subcontractate	Procentul din valoarea contractului reprezentat de lucrarile ce urmeaza a fi subcontractate	Acord subcontractor cu specimen de semnatura
...					

Data completarii: __/__/2016

Operator economic,

_____

(semnatura autorizata)