



Instituto Nacional de
Investigação Agrária e
Veterinária, I.P.

CONTRATO Nº 70/2022/INIAV

Aquisição de Firewall - PRC 667/GCA/2022

Entre:

O Instituto Nacional de Investigação Agrária e Veterinária, I.P. (INIAV IP), serviço público dotado de autonomia administrativa e financeira, sedado na Av. da República, Quinta do Marquês, 2780-157 Oeiras, pessoa coletiva n.º 510 345 271, representado neste ato pelo seu Conselho Diretivo, como primeiro outorgante

e

A PARADADOS – Instalações de Rede Informática, Lda., com sede na Rua Luís de Camões, Lote 12, Loja, 2605-806 Casal de Cambra, matriculada na Conservatória do Registo Comercial de Sintra, sob o número único de matrícula e de identificação fiscal n.º 503 336 386, neste ato representada por João Paulo Perú Pires, na qualidade de representante legal da empresa, com poderes bastantes para outorgar o presente contrato, conforme documento comprovativo exibido, como segundo outorgante.

Considerando que:

- (i) O INIAV IP promoveu um procedimento de aquisição por Consulta Prévia ao abrigo do disposto na alínea c) do n.º 1 do Art.º 20.º do Código dos contratos Públicos (daqui em adiante designado por CCP) para Aquisição de Firewall, autorizado por despacho do Conselho Diretivo do INIAV IP em 19/10/2022, exarado na Decisão de Contratar e de Autorização de Despesa nº 780/GCA/2022, com despesa suportada pela Fonte de Financiamento 513, na Rubrica de Classificação Económica D.07.01.07 B0A0, com o cabimento n.º 3398 referente ao ano de 2022.
- (ii) O segundo outorgante apresentou proposta respondendo às exigências e especificidades do procedimento mencionado em (i);
- (iii) Nesta sequência, a “Aquisição de Firewall” foi adjudicada ao segundo outorgante nos termos do Despacho do Conselho Diretivo do INIAV IP de 13/12/2022, exarado sobre a informação de adjudicação



Instituto Nacional de
Investigação Agrária e
Veterinária, I.P.

Nº 973/GCA/2022, que também aprovou a minuta de contrato a celebrar, tendo sido objeto do compromisso n.º 4482.

É de boa-fé, livremente celebrado e reciprocamente aceite o presente contrato que se rege pelas cláusulas seguintes:

Cláusula 1.ª

Objeto do Contrato

O presente procedimento de Consulta Prévia tem por objeto a Aquisição de firewall, nos termos e condições, do Convite e do Caderno de Encargos, com as quantidades previstas no Anexo A do Caderno de Encargos, o qual é parte integrante.

Cláusula 2.ª

Entidade Adjudicante

A entidade adjudicante é o Instituto Nacional de Investigação Agrária e Veterinária I.P. (INIAV), com o NIPC 510 345 271, sedado na Av. da República, S/N, Quinta do Marquês, 2780-157 Oeiras, e com o Telefone 214 403 500.

Cláusula 3.ª

Contrato

1. O contrato é composto pelo respetivo clausulão e os seus anexos.
2. O contrato integra ainda os seguintes elementos:
 - a) Os suprimentos dos erros e das omissões do Caderno de Encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
 - b) Os esclarecimentos e as retificações relativos ao Caderno de Encargos;
 - c) O Caderno de Encargos, caso seja considerado relevante;
 - d) A proposta adjudicada;
 - e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
3. Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual aí são indicados.
4. Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do Caderno de Encargos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo



Instituto Nacional de
Investigação Agrária e
Veterinária, I.P.

99.º do Código dos Contratos Públicos e aceites pelo adjudicatário, nos termos do disposto no artigo 101.º desse mesmo diploma legal.

Cláusula 4.ª

Duração e execução do contrato

1. O contrato produzirá efeitos após a sua assinatura mantendo-se em vigor até 31 de dezembro de 2022, sem possibilidade de renovação ou prorrogação.
2. A execução do contrato corresponderá aos fornecimentos efetivamente efetuados no prazo estabelecido no ponto anterior, solicitados apenas pelo Gestor de Contrato ou pelo seu suplente e no cumprimento das quantidades e condições mencionadas no Mapa de Quantidades do Caderno de Encargos.

Cláusula 5.ª

Local e prazo de entrega

1. Os bens devem ser entregues no INIAV, IP – Avenida da República, Quinta do Marquês, 2780-157 Oeiras – Departamento de Logística e Sistemas de Informação (DLSI) – A/C
2. O fornecimento total dos bens deve acontecer de uma só vez e prazo máximo de 5 dias úteis após o envio da Nota de Encomenda pelo Gestor de Contrato ou pelo seu suplente, no local mencionado no ponto anterior.

Cláusula 6.ª

Preço Contratual e condições de pagamento

1. O preço máximo que o INIAV se dispõe a pagar pelo referido contrato é de € 25.900,00 (vinte e cinco mil e novecentos euros), ao qual acrescerá o IVA respetivo no momento da faturação.
2. Este preço inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, nomeadamente os relativos ao transporte e manuseamento dos bens objeto do contrato para o respetivo local de entrega, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.
3. As quantias devidas pelo INIAV, respeitantes aos fornecimentos efetivamente feitos, devem ser pagas no prazo máximo de 60 dias após a receção das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva.
4. Para efeitos do número anterior, a obrigação considera-se vencida com a assinatura dos autos de receção correspondentes aos fornecimentos efetivamente feitos.
5. Cada fatura deve obrigatoriamente detalhar a informação referente ao:

- Produto fornecido;



Instituto Nacional de
Investigação Agrária e
Veterinária, I.P.

- Preços unitários e totais de cada produto;
- IVA por produto e IVA total;
- Números de Compromisso e Procedimento, bem como N.º de Contrato;

6. Em caso de discordância por parte do INIAV, quanto aos valores indicados na fatura, devem estas ser comunicadas ao fornecedor, por escrito, os respetivos fundamentos, ficando o fornecedor obrigado a prestar os esclarecimentos necessários e/ou proceder à emissão da respetiva nota de crédito.
7. As faturas referentes a cada entrega devem ser enviadas para o email compras.gca@iniav.pt ou através do Portal da Fatura Eletrónica na Administração Pública – FE-AP, até 5 dias úteis após cada entrega.
8. O INIAV reserva-se ao direito de não aceitar faturas emitidas depois do término do contrato e/ou sem Nota de Encomenda ou com Nota de Encomenda efetuada por pessoa diferente do Gestor de Contrato ou do seu suplente.

Cláusula 7.ª

Requisitos do fornecimento dos bens

1. O fornecimento total dos bens deve acontecer de uma só vez e prazo máximo de 5 (cinco) dias úteis, após o envio da Nota de Encomenda pelo Gestor de Contrato ou pelo seu suplente, no local mencionado na Cláusula 5ª.
2. Caso o prazo não possa ser cumprido, por motivos imputáveis ao fornecedor, este obriga-se a informar o INIAV, no prazo máximo de 12 (doze) horas, indicando a data prevista para o fornecimento solicitado.
3. O fornecedor obriga-se a disponibilizar, simultaneamente com a entrega dos bens objeto do contrato, todos os documentos em língua portuguesa, que sejam necessários para a boa utilização, função ou funcionamento daqueles, bem como, os manuais de utilização, bulas, fichas técnicas, certificados de qualidade e todos aqueles necessários, que forem solicitados para verificação de conformidade com os equipamentos existentes (sempre que aplicável).
4. É aplicável, com as necessárias adaptações, o disposto na lei que disciplina aspetos relativos à venda de bens de consumo e das garantias a ela relativas, no que respeita à conformidade dos bens.
5. O fornecedor é responsável perante o INIAV por qualquer deformação ou discrepância dos bens fornecidos objeto do contrato que exista no momento em que os bens lhe são entregues.
6. Todas as despesas e custos com o transporte dos bens, objeto do contrato, para o local de entrega são da responsabilidade do fornecedor.



REPÚBLICA
PORTUGUESA

AGRICULTURA
E ALIMENTAÇÃO

Avenida da República, Quinta do Marquês, 2780-157 Oeiras
Tel.: 214 403 500 | Fax: 214 403 666
geral@iniav.pt | www.inia.pt



Cláusula 8.ª

Incumprimento Contratual e aplicabilidade de Sanções

1. Em caso de incumprimento contratual por parte do fornecedor e nos termos previstos na lei, poderá o INIAV IP, resolver o contrato a título sancionatório e/ou aplicar as sanções previstas na lei e no Caderno de Encargos.
2. A resolução do contrato não prejudica o direito de indemnização, nos termos da referida norma legal.

Cláusula 9.ª

Cessão da Posição Contratual e Subcontratação

O adjudicatário não poderá ceder a sua posição contratual ou proceder à subcontratação sem autorização do INIAV IP.

Cláusula 10.ª

Caução

Nos termos do n.º 2 do artigo 88.º do Código dos Contratos Públicos não é exigível a prestação de caução.

Cláusula 11.ª

Gestor de Contrato

De modo a acompanhar permanentemente a execução do contrato, será designado como Gestor do Contrato _____ ausência do Gestor, as funções de Gestor de Contrato serão asseguradas pela pessoa que o substituir no momento.

Cláusula 12.ª

Dever de Sigilo

1. O adjudicatário compromete-se a garantir o sigilo sobre todas as informações de natureza profissional consideradas, pelo INIAV, como confidenciais (documentação técnica e não técnica, comercial ou outra), bem como a demais informações privadas ou de propriedade do INIAV, resultante da sua atividade, e das quais possa vir a ter conhecimento, ao abrigo ou em relação com a execução do Contrato a celebrar.
2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem ser objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do Contrato a celebrar.
3. Excluem-se do dever de sigilo previsto a informação e a documentação que sejam comprovadamente do domínio público à data da respetiva obtenção pelo prestador de serviços ou que este seja legalmente



obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Cláusula 13.ª

Casos Fortuitos ou de Força Maior

1. Nenhuma das partes incorrerá em responsabilidade se, por caso fortuito ou de força maior, designadamente, em caso de greves ou de outros conflitos coletivos de trabalho, for impedida de cumprir as obrigações assumidas no contrato.
2. A parte que invocar caso fortuito ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para restabelecer a situação.

Cláusula 14.ª

Patentes, licenças e marcas registadas

São da responsabilidade do adjudicatário quaisquer encargos decorrentes da obtenção ou utilização, no âmbito do contrato, de patentes, licenças ou marcas registadas.

Cláusula 15.ª

Foro Competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Judicial da Comarca de Oeiras, com expressa renúncia a qualquer outro.

Cláusula 16.ª

Legislação Aplicável

Ao presente contrato aplicar-se-á o disposto nos documentos contratuais, o disposto no Código dos Contratos Públicos, bem como as demais disposições legais inerentes à natureza do serviço a contratar e legislação específica.

Cláusula 17.ª

Proteção de Dados Pessoais

1. O adjudicatário obriga-se a cumprir o disposto em todas as disposições legais aplicáveis em matéria de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados, no sentido conferido pela:
 - Lei n.º 58/2019, de 8 de agosto, a qual assegura a execução, na ordem jurídica interna, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (RGPD), de 27 de abril de 2016;
 - Lei n.º 59/2019, de 8 de agosto, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016;
 - Resolução do Conselho de Ministros n.º 41/2018 de 22 de março de 2018, que fixa as orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação e as procedimentos a adotar, bem como a restante legislação nacional e comunitária aplicável em matéria de privacidade, em relação a todos os dados pessoais a que aceda no âmbito ou para efeitos da prestação de Serviços, nomeadamente:
2. As partes reconhecem e aceitam que, relativamente a todos os dados pessoais a que o adjudicatário tiver acesso ou lhe forem transmitidos pelo INIAV para efeitos da prestação de Serviços:
 - a) O INIAV atuará na qualidade de responsável pelo tratamento dos dados (tal como definido na Lei n.º 59/2019, de 8 de agosto), determinando as finalidades e os termos do tratamento desses dados pelo adjudicatário;
 - b) O adjudicatário atuará na qualidade de entidade subcontratante (tal como definido na Lei n.º 59/2019, de 8 de agosto), tratando os dados pessoais em estrita observância das instruções do responsável pelo tratamento desses dados;
 - c) Entende-se, para este efeito, que tratamento de dados pessoais são as operações, com ou sem recurso a meios automatizados, efetuadas sobre os dados pessoais dos clientes, trabalhadores, colaboradores e prestadores de serviços do INIAV, incluindo a recolha, o registo, a organização, o armazenamento, a adaptação ou a alteração, a recuperação, a consulta, a utilização, a divulgação, a transferência e/ou a disponibilização a terceiros, o alinhamento, a combinação, o bloqueamento, o apagamento e a destruição dos dados anteriormente referidos;
3. O adjudicatário compromete-se, designadamente, a não copiar, reproduzir, adaptar, modificar, alterar, apagar, destruir, difundir, transmitir, divulgar ou, por qualquer outra pessoa, colocar à disposição de terceiros os dados pessoais a que tiver acesso ou lhe forem transmitidos pela responsável dos tratamentos



de dados ao abrigo do Contrato, sem que para tal tenha sido expressamente instruído, por escrito, por aquele responsável ou pelos titulares dos dados, no exercício dos seus respetivos direitos.

4. Sem prejuízo das demais obrigações previstas no Caderno de Encargos, o adjudicatário obriga-se a cumprir rigorosamente o disposto na legislação aplicável em matéria de tratamento de dados pessoais e nomeadamente a:
- a) Tratá-los apenas de acordo com as instruções do INIAV, única e exclusivamente, para efeitos da prestação de Serviços, cumprindo-se as obrigações estatuídas sobre proteção de dados;
 - b) Prestar ao INIAV toda a colaboração de que este careça para esclarecer qualquer questão relacionada com o tratamento de dados pessoais efetuado ao abrigo do Contrato a celebrar e manter o INIAV informado em relação ao tratamento de dados pessoais;
 - c) Prestar assistência ao INIAV, tendo em conta a natureza do tratamento e a informação ao seu dispor, no sentido de assegurar as obrigações referentes à notificação de violações de dados pessoais, designadamente através da comunicação sempre que possível até 72 horas subsequentes ao conhecimento (da ocorrência) de qualquer violação de dados pessoais que ocorra, prestando ainda colaboração ao INIAV na adoção de medidas de resposta ao incidente, na investigação do mesmo e na elaboração das notificações que se mostrem necessárias, nos termos da Lei n.º 59/2019, de 8 de agosto;
 - d) Autorizar a divulgação do Contrato a celebrar à CNPD, enquanto autoridade de controlo nacional, bem como os elementos com ele relacionado, caso tal seja exigido;
 - e) Colaborar com o INIAV tendo em conta a natureza do tratamento e, na medida do possível, adotar as medidas técnicas e organizativas referidas nesta Cláusula, onde se incluem a anonimização ou a pseudonimização aos dados pessoais para reduzir os riscos para os titulares de dados em questão, não excluindo outras eventuais medidas de proteção de dados, e permitindo-se que estas cumpram a sua obrigação de dar resposta aos pedidos dos titulares dos dados, tendo em vista o exercício, por estes, dos seus direitos nos termos da Lei n.º 59/2019, de 8 de agosto;
 - f) Consoante a escolha do INIAV ou do titular eliminar ou devolver os dados pessoais no momento da cessação do Contrato, apagando quaisquer cópias existentes, exceto se a conservação ou a transmissão dos dados for exigida por lei;
 - g) Manter registos das atividades de tratamento de dados realizadas em nome do INIAV, ao abrigo do Contrato, segundo os requisitos previstos na Lei n.º 59/2019, de 8 de agosto;
 - h) Cumprir todas as demais disposições legais no que respeita ao registo, transmissão ou qualquer outra operação de tratamento de dados pessoais previstos na Lei n.º 59/2019, de 8 de agosto;
 - i) Não os transferir para fora do Espaço Económico Europeu, sem o consentimento prévio, por escrito, do responsável pelo tratamento dos dados;
 - j) Disponibilizar ao responsável pelo tratamento dos dados todas as informações necessárias para



demonstrar o cumprimento das obrigações previstas na Lei n.º 59/2019, de 8 de agosto, facilitar e contribuir para as auditorias, inclusive as inspeções conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado;

- k) Assegurar que o pessoal autorizado a tratar dados pessoais assume um compromisso de confidencialidade, e que conhece, e se compromete a cumprir todas as obrigações aqui previstas.
- 5. O adjudicatário obriga-se a pôr em prática as medidas técnicas e organizativas necessárias à proteção dos dados pessoais tratados por conta do INIAV contra a respetiva destruição, accidental ou ilícita, a perda accidental, a alteração, a difusão ou o acesso não autorizado, bem como contra qualquer outra forma de tratamento ilícito dos mesmos dados pessoais.
- 6. As medidas a que se refere o número anterior devem garantir um nível de segurança adequado em relação aos riscos que o tratamento de dados apresenta, à natureza dos dados a proteger e aos riscos, de probabilidade e gravidade variável para os direitos e liberdades das pessoas singulares.
- 7. O adjudicatário concorda com o acesso aos dados pessoais tratados ao abrigo do Contrato a celebrar será estritamente limitado ao pessoal que necessitar de ter acesso aos mesmos para efeitos de cumprimento das obrigações aqui assumidas pelo adjudicatário.
- 8. O adjudicatário obriga-se a comunicar ao responsável pelo tratamento dos dados qualquer situação que possa afetar o tratamento dos dados pessoais ou de algum modo dar origem ao incumprimento das disposições legais em matéria de proteção de dados, devendo ainda tomar todas as medidas necessárias e ao seu alcance para a fazer cessar de imediato.
- 9. O adjudicatário será responsável por qualquer prejuízo em que o INIAV vier a incorrer em consequência do tratamento, por si ou pelo seu pessoal, de dados pessoais ou em violação das normas legais aplicáveis e ao disposto no Contrato a celebrar, quando tal violação seja imputável ao adjudicatário e solidária com o pessoal no âmbito do serviço prestado, quando a violação seja imputável à atuação destes últimos.
- 10. O adjudicatário, fica autorizado a recorrer à subcontratação de um terceiro para colaboração na prestação de Serviços, obrigando-se, porém, a assegurar que o mesmo cumprirá o disposto na legislação aplicável, devendo tal obrigação constar de contrato escrito que, para o efeito, se obriga a celebrar com esse terceiro, e bem assim assegurando-se o cumprimento das obrigações decorrentes (tal como definido na Lei n.º 59/2019, de 8 de agosto) e demais legislação aplicável relativa a Dados Pessoais, vinculando suas ações à essência, natureza e finalidades da presente disposição contratual, no estrito cumprimento do dever de sigilo e de confidencialidade.
- 11. O adjudicatário, sempre que o INIAV receber um pedido de acesso ou retificação de dados pessoais ou uma oposição ao seu tratamento por parte dos seus titulares dos dados, deverá prestar assistência ao responsável pelo tratamento dos dados através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares, tendo em vista o

Cláusula 18ª

Especificações Técnicas

Tabelas de Conformidade - 6600 PLUS SNBT	
Nº Linha	Requisito
	Firewall
1	Application Control
2	URL Filtering
3	Antivirus
4	Web Filtering
5	Anti-spam e Email Security
6	Anti Bot
7	Identity Awareness
8	VPN IPSEC
9	VPN SSL
10	IPS
11	Instalação em modo Router e modo Transparente
12	Instâncias Virtuais de Firewall com gestão independente: 2
	Networking
13	Suporte Múltiplos Links WAN - Redundância
14	Suporte Múltiplos Links WAN - Balanceamento de carga
15	Routing baseado em políticas
16	Rotas Estáticas
17	IPv6
18	802.1q- VLAN Tagging
19	DHCP Relay e DHCP Server
20	Spanning-Tree (802.1d)
21	Suporte 802.3.ad e também LACP – Agregação de Links (Activo-Activo ou Activo-Passivo)
22	Suporte de Dead Gateway Detection
23	Job Scheduler
24	Suporte TOS/DiffServ
25	Suporte para Virtual Switch



26	Suporte para Virtual Routers
	Networking em IPv6
27	Rotas estáticas
28	RIPv6
29	BGP4+
30	OSPFv3
31	DNS
32	Endereçamento de interfaces
33	IPv6 Tunnel sobre IPv4
34	IPv4 tunnel sobre IPv6
35	Packet e network sniffing
36	NAT
37	Troubleshooting específico IPv6
	Protocolos de Routing
38	OSPF
39	BGP
40	RIP
41	IGMP
42	PIM SM
43	PIM DM
	Performance
44	Throughput: 32 Gbps (pacotes UDP 1518 byte)
45	Conexões Concorrentes: 4 Milhões
46	Novas sessões por segundo: 116.000
47	Nº de Portas 10/100/1000 em RJ45 (cobre) = 8
48	Nº de Portas 10 Gbit/s em fibra SFP+ = 4 + 4 x SFP+ SR Transceivers
49	Nº Vlans >=1024
50	NGFW (IPS+Application Control): 6.2 Gbps
51	Threat Prevention: 3.7 Gbps
52	Nº de power units = 2
53	Deve incluir porta de LOM
	Features
54	Appliance física
55	Suporte Clustering (Activo-Activo e Activo-Passivo)
47	Suporte Clustering com mais de 2 membros num cluster
58	Suporte Clustering com diferentes versões de software



59	Firewall Aplicacional (Detecção em tempo real de protocolos dinâmicos) ex: FTP, SIP, H323, etc..
60	Detecção/Bloqueio de Serviços como P2P, Instant Messaging por aplicação (voz, vídeo ou file sharing)
61	Suporte para controlo de acesso de pelo menos 150 serviços/protocolos predefinidos
62	Comunicação entre a Gateway e a Management deve ser encriptada e autenticada com certificados PKI
63	NAT de Aplicações Tempo Real
64	PAT
65	NAT/PAT baseado em regras
66	Permitir autenticação de serviços
67	Integração com Active Directory
68	Integração com LDAP
69	Base de dados local de utilizadores
70	2 factor authentication: Com tokens físicos, Soft tokens, SMS e e-mail
71	Reputação de Clientes
72	Solução tem que suportar proxy de HTTP & HTTPS
73	Endpoint Control
	VPN
74	VPN Throughput >= 4.9 Gbps
75	Suporte de IKEv1 e IKEv2
76	Tem que suportar criptograficamente 3DES e AES-256 para IKE Phase I e II IKEv2
77	Tem que suportar pelo menos os seguintes grupos de Diffie-Hellman: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit)
78	IKE Phase2 – Encriptação de Dados (DES, 3DES, AES-128, AES-192, AES-256,e NULL)
79	IKE Phase2 - Suporte Integridade dos Dados (MD5, SHA1, SHA256, SHA384, SHA512 e NULL)
80	Suporte de VPNs Site to Site – Full Mesh (all to all) ou Star (Remote to center).
81	Suporte de IKE com PKI e pre-shared Secret
82	Aprovisionamento automático de VPNs site-to-site
83	Gestão automática de túneis IPSec de backup
84	Suporte routing dinâmico em VPN IPSec
85	Cliente VPN (Windows XP, MacOS, iOS, Android)
86	Suporte de One-Time Password para VPN sem recurso a terceiros fabricantes ou servidores adicionais
87	Criptografia (3DES, IKE, AES)
88	Aplicação de políticas e restrições de acesso por utilizador ou por grupo de utilizadores
89	Single Sign On VPN
	Application Control e URL Filtering
90	Actualização de assinaturas automática
91	Reconhecimento de aplicações >=4000



92	Reconhecimento de widgets (sub aplicações dentro das principais Apps Web 2.0 >=250000 (ex: Farmville dentro do Facebook)
93	Solução tem que ter categorizado >= 200 milhões URLs e ter uma cobertura de mais do que 85% da Alexa's top 1Milhão de sites
94	Controlo por largura de banda de cada aplicação Web 2.0
95	Inspecção SSL
96	Criação de assinaturas personalizadas e privadas
97	Criação de regras pelo índice de criticidade de segurança da aplicação
98	Criação de regras pelo índice de popularidade da aplicação
99	Criação de regras pela categoria da aplicação
100	Criação de regras pela tecnologia da aplicação
101	Criação de regras pelo fabricante da aplicação
102	Controlo de utilizadores dentro de uma solução de VDI ou Terminal Services.
103	Inspeccionar o tráfego mesmo dentro de SSL encriptado. Tráfego tanto Inbound como Outbound
104	Alertar e questionar os utilizadores através de popups sobre a utilização das diferentes aplicações
	User Identity Acquisition
105	Aquisição da identidade dos users através de Microsoft Active Directory query (com base nos eventos de segurança)
106	Browser-based como método de autenticação de users que não pertencem ao domínio
107	Client agent dedicado para aquisição e report de identidades à Gateway
108	Suporte de terminal servers
109	Integração com directory services, IF-MAP e RADIUS
110	Impacto nos domain controllers deve ser menor de 3%
111	Suporte de terminal servers e citrix
112	Deve permitir identificação de users através de proxy (X-forwarded headers)
113	Identificação de users através de Microsoft Active Directory sem agente instalado nos domain controllers
114	Suporte de autenticação transparente via Kerberos para Single Sign On
115	Suporte para utilização de grupos LDAP
116	Partilha da identidade dos users entre diversas Gateways
117	Criação de Regras por Utilizador ou Grupo de Utilizador
118	Utilizadores que não pertencem a rede serem confrontados com um Captive Portal para os autenticar
119	Suporte para contas Guest com gestão independente
120	Identificação de dispositivos (incluindo Fabricante e SO)
121	Regras baseadas em dispositivos ou grupos de dispositivos
	IDS/IPS
122	Actualização de assinaturas automática



123	Largura de Banda do IPS >= 10.14 Gbps
124	Capacidade de criação de perfis para o IPS (existência de perfis pré-definidos) para serem utilizados imediatamente.
125	Capacidade de capturar tráfego na consola de gestão para protecções específicas.
126	Protecção contra Denial of Service
127	Funcionalidade de bypass em caso de carga excessiva
128	Regras de bloqueio automático por País
129	O IPS tem que ter a capacidade de importar e converter protecções de SNORT
130	O motor de IPS tem que ter mecanismos de detecção de assinaturas de exploits, anomalias protocolares, Controlos de aplicação e detecção comportamental.
131	Tem que existir protecções de SCADA no motor de IPS.
132	Suporte de motor de detecção de Antibot
133	Protocol Tunneling Recognition
134	Capacidade de criar perfis de protecção para apenas protecções cliente ou de servidores ou a combinação dos dois
	Anti-spam e Email Security
135	A solução deve ser conteúdo e linguagem agnóstica.
136	A solução deve ter classificação em tempo real e protecções baseadas em spam detectado que se baseia em padrões e não no conteúdo.
137	A solução deve incluir bloqueio de reputação de IP com base no serviço online com a finalidade de evitar falsos positivos.
	Anti-Bot e Anti-Vírus
138	A solução de Anti-Bot e Anti-Vírus deverá estar integrado na firewall de próxima geração.
139	Modulo de Anti-bot deve ser capaz de detectar e parar o comportamentos anómalos de rede.
140	Modulo Anti-Bot deve usar um mecanismo de detecção de multi-camadas , que inclui reputação de IPs , URLs e endereços de DNS e detectar padrões de comunicação de bots.
141	O Anti-Bot deve ser capaz de analisar as acções de bots.
142	Os modulos de Anti-Bot e Anti -Virus deve ser administrado a partir de uma consola central.
143	Anti-Bot e Anti-Virus deve ter uma correlação de eventos centralizado e mecanismo de reporting.
144	Aplicação de anti-vírus deve ser capaz de impedir o acesso a sites mal-intencionados
145	Modulo de anti-vírus deve ser capaz de inspecionar tráfego com criptografia SSL.
146	Anti-Bot e Anti-Virus deve ser ter atualizações em tempo real a partir de um serviço baseado na nuvem do fabricante.
147	Anti-Virus deve ser capaz de parar a entrada de ficheiros maliciosos.
148	Políticas anti-vírus e anti-bot devem ser geridas centralmente com uma política granular e eficaz.
	Sandblast - Protecção de ataques Zero-Day
149	Fabricante deve ter como opção a capacidade de proteger contra ataques de "Zero-Day" antes de proteções de



	assinatura estáticos serem criados.
150	Fabricante deve ter como opção a capacidade de análise e detecção de malware em documentos comerciais, tais como Adobe PDFs e arquivos de MS Office , bem como EXE e arquivos Zip.
151	Fabricante deve ter como opção a capacidade de executar dentro do equipamento local ou num sistema na cloud do fabricante.
152	Fabricante deve ter como opção a capacidade de ter zero falsos positivos (não existencia de falsos positivos).
153	Fabricante deve ter como opção a capacidade de emular ataques contra vários ambientes do sistema operativos Windows, pelo menos : Windows XP, Windows 7, Windows 8
154	Fabricante deve ter como opção a capacidade de ser gerida centralmente.
155	Fabricante deve ter como opção a capacidade de aumentar a segurança através da partilha automática de informações novos ataques detectados com outras gateways gerando automaticamente as assinaturas para as bloquear noutros equipamentos.
156	Fabricante deve ter como opção a uma solução de sandboxing com a capacidade de inspecionar e bloquear ataques que passam via HTTPS sem o uso de dispositivos adicionais.
157	Fabricante deve ter como opção uma solução de sandboxing capaz de poder ser implementado inline, na nuvem, num equipamento out of band ou com um MTA - Mail Transfer Agent.
158	A solução de sandboxing deve combinar a validação/análise de ficheiros com Threat Extraction.
159	A solução de threat emulation deve ter como opção "Restrição Geo", restringindo a emulação a um país específico.
160	A solução deve ser flexível ao ponto de permitir manter o formato do ficheiro original e especificar o tipo de conteúdo a ser removido.
161	A solução de Threat Extraction deve disponibilizar, imediatamente, uma versão limpa do documento ao utilizador, dando acesso ao documento original apenas após análise e confirmação de que o documento não é malicioso
	Certificações
162	UL, CB, CE, TUV GS
163	FCC, CE, VCCI, RCM/C-Tick
164	RoHS, WEEE, REACH1, ISO140011
165	Mobile Access Blade for 200 concurrent connections
166	3 x CES STANDARD To Mobile Acces Blade 200
167	SmartEvent and SmartReporter blade for 5 gateways (Smart-1 & open server) 3 year subscription

ANEXO A
Mapa de Quantidades

Nº de Linha	Descrição	Quantidades
1	Firewall de nova geração.	1

Depois de confirmadas as formalidades inerentes à adjudicação, o contrato foi assinado pelos representantes de ambas as partes.

Feito em duplicado, no dia 16 de dezembro de 2022, ficando um exemplar em poder de cada uma das partes.

Primeiro Outorgante (*):

**Nuno
Canada**

Assinado de forma digital por Nuno Canada
DN: c=PT, title=Presidente do Conselho
Diretivo, ou=Instituto Nacional de
Investigação Agrária e Veterinária IP,
o=Instituto Nacional de Investigação Agrária
e Veterinária IP, cn=Nuno Canada
Dados: 2022.12.19 16:20:42 Z

Segundo Outorgante (*):

Assinado por: **JOÃO PAULO PERÚ PIRES**
Num. de Identificação:
Data: 2022.12.20 13:28:35+00'00'

Assinado por: **PATRÍCIA MÓNICA GUILHERME
TAVARES INÁCIO**
Num. de Identificação:
Data: 2022.12.19 17:58:20+00'00'



CARTÃO DE CIDADÃO
* * * *



CARTÃO DE CIDADÃO
* * * *

(*) Conselho Diretivo do INIAV, I.P.