



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

**António José  
Gameiro  
Marques**

Digitally signed by  
António José Gameiro  
Marques  
Date: 2021.11.22 18:16:52  
Z

## **CADERNO DE ENCARGOS**

**AQUISIÇÃO DE NOVO CLUSTER DE FIREWALL PARA PROTEÇÃO DA  
INFRAESTRUTURA CYBER RANGE DO CERT.PT**



## **CADERNO DE ENCARGOS**

### **PARTE I**

#### **Cláusula 1**

##### **Objeto**

O presente Caderno de Encargos compreende as cláusulas na sequência do procedimento pré-contratual que tem por objeto a “aquisição de novo cluster de firewall para proteção da infraestrutura Cyber Range do CERT.PT”, de acordo com as Cláusulas Técnicas descritas no Anexo I da parte II do Caderno de Encargos.

#### **Cláusula 2**

##### **Definições**

Para efeitos do presente Caderno de Encargos, adotam-se as seguintes definições:

CCP – Códigos dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, na redação atual;

Contrato – contrato a celebrar entre a entidade adjudicante e o adjudicatário nos termos do presente caderno de encargos;

Órgão competente para a decisão de contratar – Exmo. Diretor Geral do Gabinete Nacional de Segurança, António Gameiro Marques;

Entidade Adjudicante – Presidência de Conselho de Ministros – Gabinete Nacional de Segurança / Centro Nacional de Cibersegurança;

Entidade Adjudicatária – entidade a quem se adjudica a execução do contrato.

#### **Cláusula 3**

##### **Forma e documentos contratuais**

1. Fazem parte integrante do contrato os seguintes documentos:
  - a) Os suprimimentos dos erros e 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 presente caderno de encargos;
  - d) A proposta adjudicada;
  - e) Os esclarecimentos à proposta adjudicada prestados pela Entidade Adjudicatária.
2. Em caso de divergência entre os documentos referidos no n.º 1, a prevalência é determinada pela ordem que nele se dispõe.
3. Em caso de divergência entre os documentos referidos no n.º 1 e o clausulado do contrato, prevalecem os primeiros, salvo quanto aos ajustamentos ao conteúdo do contrato propostos pelo órgão competente para a decisão de contratar e aceites pela Entidade Adjudicatária.



#### **Cláusula 4**

##### **Local de Prestação dos Serviços**

A prestação do serviço, objeto deste procedimento, deverá ser efetuada nos locais e nas formas que sejam acordadas entre as partes para cada uma das atividades, sendo que, sempre seja acordada a prestação de serviços de forma presencial estes serão prestados nas instalações da Entidade Adjudicante, sita na Rua da Junqueira Nº 69, 1300-342 Lisboa.

#### **Cláusula 5**

##### **Prazo e vigência do contrato**

A prestação de serviços a realizar no âmbito do contrato deverá ser executada com início e final definidos nas Cláusulas Técnicas descritas no Anexo I da parte II do presente Caderno de Encargos, sem prejuízo das obrigações acessórias que devem perdurar para além da cessação do contrato.

#### **Cláusula 6**

##### **Preço base e preço contratual**

1. Nos termos e para os efeitos, de acordo com o art.º 47 do CCP, o preço base do procedimento é fixado em 18.100,00 € (dezoito mil e cem) acrescido de IVA à taxa legal em vigor.
2. O preço base do procedimento constitui o limite máximo suscetível de ser apresentado nas propostas concorrentes, constituindo a sua violação causa de exclusão dessa proposta.

#### **Cláusula 7**

##### **Pagamento e condições de pagamento**

1. Face ao preço contratual, e considerando o prazo de vigência do contrato a celebrar, será realizado um pagamento do valor total contratual com entrada em vigor do contrato.
2. As quantias devidas pelo GNS/CNCS serão pagas no prazo de 30 dias após a receção da fatura e vencimento da obrigação respetiva.
3. Para os efeitos do número anterior, a obrigação considera-se vencida após a aceitação, pelo GNS/CNCS.
4. Desde que devidamente emitida e observado o disposto no n.º 1, a fatura é paga através de transferência bancária.
5. Nas condições de pagamento a apresentar pelos concorrentes não podem ser propostos adiantamentos.

#### **Cláusula 8**

##### **Caução**

Não é exigida a prestação de caução dado que o preço contratual é inferior a € 500.000,00 (quinhentos mil euros), nos termos da alínea a) do n.º 2 do Art.º 88.º do Código dos Contratos Públicos.



## **Cláusula 9**

### **Dever de sigilo e confidencialidade**

1. Informação Confidencial é, para os efeitos restritos deste contrato, toda a informação revelada no âmbito dos projetos, seja sob qualquer forma (incluindo, mas não se limitando a, revelações feitas por escrito, oralmente ou sob a forma de amostras, modelos, programas de computador ou qualquer outra forma) pela Entidade Adjudicante para os fins ou em conexão com o objeto do Acordo.
2. No âmbito do presente contrato, serão realizados vários projetos com natureza e classificação diferentes, obrigando a realização de acordos de confidencialidade respetivos entre a Entidade Adjudicante e Entidade Adjudicatária.
3. A Entidade Adjudicatária deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à entidade adjudicante, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.
4. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
5. Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo adjudicatário 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.
6. O dever de sigilo a que alude os números anteriores mantém-se em vigor para além do termo de vigência, inicial ou que venha a ser acordado, sob pena de o adquirente dos serviços instaurar a competente ação judicial para efeitos de justa indemnização, em especial quando dessa revelação de informação venha a resultar dano ou prejuízo para a imagem do GNS/CNCS ou para os terceiros com os quais mantenha relações institucionais ou comerciais, caso em que a violação de quaisquer deveres legais a que o adjudicatário se encontre vinculado no âmbito da sua atividade, designadamente, os relativos à proteção de segredos comerciais ou outros conexos, será comunicada às autoridades administrativas e criminais competentes, para os devidos efeitos.
7. A Entidade Adjudicatária, para além de guardar sigilo, deve também garantir total confidencialidade sobre todos os assuntos constantes do objeto do presente caderno de encargos, e tratar como confidencial toda a informação e documentação a que tenha acesso no âmbito da sua execução, sendo esta obrigação extensível a outras partes, colaboradores ou terceiros que as mesmas envolvam, mesmo depois do término do presente contrato.

## **Cláusula 10**

### **Proteção de Dados Pessoais**

1. Qualquer acesso que a Entidade Adjudicatária venha a ter relativamente a qualquer dado pessoal apenas pode ocorrer para os fins constantes do presente caderno de encargos, e nos termos da legislação aplicável à proteção de dados pessoais.
2. A Entidade Adjudicatária não pode proceder à reprodução, gravação, cópia ou divulgação dos dados pessoais para outros fins que não constem no presente documento, comprometendo-se ainda ao seguinte:



- a. Respeitar integralmente o disposto na legislação europeia e nacional aplicável à proteção de dados pessoais e em qualquer outra legislação que a substitua e/ou venha a ser aplicável a esta matéria;
  - b. Cumprir rigorosamente as instruções do caderno de encargos no que diz respeito ao acesso, registo, transmissão ou qualquer outra operação de tratamento de dados pessoais;
  - c. Tratar os dados pessoais de forma lícita e com respeito pelo princípio da boa-fé, utilizando-os exclusivamente para as finalidades a que se reporta o Contrato, não podendo ser posteriormente tratados de forma incompatível com tais finalidades;
  - d. Implementar medidas técnicas e organizativas para proteger os dados contra destruição accidental ou ilícita, perda accidental, alterações, difusão ou acesso não autorizados, e contra qualquer outra forma de tratamento ilícito dos mesmos dados pessoais.
3. Se quaisquer dados se perderem ou forem danificados no âmbito da execução do Contrato, por causas imputáveis à Entidade Adjudicatária, esta compromete-se a adotar as medidas que forem necessárias com vista à recuperação dos dados, sem quaisquer custos adicionais.
  4. Prestar à Entidade Adjudicante toda a colaboração de que esta careça para esclarecer qualquer questão relacionada com o tratamento de dados pessoais efetuado ao abrigo do contrato e manter a Entidade Adjudicante informada em relação ao tratamento de dados pessoais, obrigando-se a comunicar de imediato qualquer situação que possa afetar o tratamento dos dados em causa ou que de algum modo possa dar origem ao incumprimento das disposições legais em matéria de proteção de dados pessoais ou dos termos do instrumento de legalização concedido pela Comissão Nacional de Proteção de Dados ao GNS.
  5. A obrigação de sigilo prevista na presente cláusula mantém-se mesmo após a cessação do presente contrato, independentemente do motivo por que ocorra.

## **Cláusula 11**

### **Resolução por parte do contraente público**

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, o GNS pode resolver o contrato, a título sancionatório, no caso de o adjudicatário violar de forma grosseira ou negligente ou de modo grave ou reiterado qualquer uma das obrigações que lhe incumbem.
2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao adjudicatário.

## **Cláusula 12**

### **Cessão da posição contratual e subcontratação**

1. A Entidade Adjudicatária não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato sem autorização da entidade adjudicante.
2. A Entidade Adjudicatária não pode subcontratar total ou parcialmente os serviços incluídos no mesmo sem autorização prévia da entidade adjudicante
3. Para efeitos da autorização prevista no número anterior, deve:
  - a) Ser apresentada pelo cessionário ou pela entidade subcontratada toda a documentação exigida ao adjudicatário no presente concurso;
  - b) A entidade adjudicante deverá apreciar, designadamente, se o cessionário ou a entidade subcontratada não se encontra em nenhuma das situações previstas no artigo 55º do CCP,



PRESIDÊNCIA DO CONSELHO DE MINISTROS  
**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, na sua redação atual, e se tem capacidade técnica e financeira para assegurar o exato e pontual cumprimento do contrato.

### **Cláusula 13**

#### **Responsabilidade e Obrigações principais da Entidade Adjudicatária**

1. A Entidade Adjudicatária responde pelos danos que causar à entidade contratante em razão do incumprimento culposo das obrigações que sobre ele impendam.
2. A Entidade Adjudicatária responde ainda perante a entidade contratante pelos danos causados pelos atos e omissões de terceiros, por si empregues na execução de obrigações emergentes do contrato, como se tais atos ou omissões fossem praticados por aquele.
3. A Entidade Adjudicatária aceita e compromete-se a cumprir com as Obrigações de Segurança constantes da Cláusula 2ª da Parte II – Cláusulas Técnicas, do presente Caderno de Encargos.

### **Cláusula 14**

#### **Alterações ou aditamentos do contrato**

Qualquer alteração ou aditamento ao contrato, que não diga respeito a questões fundamentais do procedimento, apenas será válida se resultar de acordo de ambos os contraentes, reduzido a escrito e anexado ao contrato inicial.

### **Cláusula 15**

#### **Foro competente para resolução de litígios**

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo de Círculo de Lisboa, com expressa renúncia a qualquer outro.

### **Cláusula 16**

#### **Contagem dos Prazos**

Os prazos para a execução das atividades são acordados entre as partes na fase de planeamento da execução da atividade e são contados na forma e com as regras acordadas entre as partes.

### **Cláusula 17**

#### **Legislação aplicável**

O contrato é regulado pela legislação portuguesa.



PRESIDÊNCIA DO CONSELHO DE MINISTROS

**Gabinete Nacional de Segurança**

*Centro Nacional de Cibersegurança*

## **PARTE II – CLÁUSULAS TÉCNICAS**

### **Cláusula única**

#### **Especificações Técnicas**

As Especificações Técnicas são as que se indicam no Anexo I do presente Caderno de Encargos.



## **ANEXO I**

### **1. Objetivo**

O presente caderno de encargos tem por objetivo o fornecimento e instalação de 2 (dois) equipamentos firewall para proteção da infraestrutura de suporte à plataforma de Cyber Range do CERT.PT. Pretende-se que os equipamentos a fornecer garantam a existência de mecanismos de redundância e alta disponibilidade ao nível da proteção de perímetro e outras componentes de segurança da infraestrutura que irá suportar esta plataforma.

### **2. Âmbito**

O concorrente deverá, para além de outros serviços que julgue pertinente, incluir os seguintes serviços especializados:

- a) Levantamento e validação das condições e requisitos para a implementação da solução;
- b) O reconhecimento dos locais de instalação, salas e bastidores;
- c) A especificação da arquitetura funcional e tecnológica e identificação de componentes e tecnologia associados ao projeto global;
- d) O desenho da solução e elaboração dos esquemas lógicos de toda a solução;
- e) Quando aplicável, a migração das regras e políticas atualmente em produção;
- f) Verificação e confirmação da energia, cablagem e segurança;
- g) Instalação física e start-up de todos os equipamentos propostos;
- h) Instalação e start-up de todas as soluções propostas;
- i) Interligação de todos os equipamentos à rede de dados;
- j) Realização de testes de ensaio;
- k) Verificação da conformidade da instalação com as normas e regulamentos em vigor;
- l) Testes de funcionamento aos equipamentos e soluções;
- m) Testes de conectividade das ligações;
- n) Análise e implementações de otimizações decorrentes dos testes e ensaios;
- o) Simulação controlada de um restauro/reposição de serviços em caso de falha;

Enumeram-se de seguida os requisitos que a solução a fornecer deverá cumprir, no âmbito das diferentes componentes.

#### **2.1. Componente de Firewall**

##### **2.1.1. Firewall, networking e routing**

- a) Inspeção em profundidade detalhada de pacotes;
- b) Políticas baseadas em utilizador/grupo, Geo-IP, Serviço Internet (Exemplo: Windows Update) ou rede/IP;
- c) Políticas de acesso limitadas por tempo ou largura de banda;
- d) Aplicar política em redes ou por tipo de serviço;
- e) Políticas por LAN, WAN, DMZ, LOCAL, VPN e redes Wireless;
- f) Proteção contra ataques. Por exemplo, DoS e bloqueio de portscans;
- g) Suporte de proxy explícito;
- h) Balanceamento do link WAN: várias ligações à Internet;
- i) Verificação do estado da ligação automática, fail over automático;
- j) Inspeção de protocolos DNS, DHCP e NTP;
- k) Redundância de equipamentos de Firewall.



### **2.1.2. VPNs**

- a) Possibilidade de atuar como terminador de túneis VPN SSL e IPSec;
- b) VPN site-a-site: PFS, IPSec, AES / 3DES de 256 bits;
- c) Autenticação por certificados X.509 ou pre-shared key;
- d) Acesso remoto: SSL, IPsec, com suporte para 500 clientes Windows/ iPhone / iPad / Android;
- e) Possibilidade de instalação de cliente vpn SSL para Windows e sua respetiva configuração via portal de utilizador;
- f) Possibilidade de ligar à VPN antes do login no Windows.

### **2.1.3. Secure wireless**

Garantir a possibilidade de funcionamento como controlador AP, numa interface única e integrada, permitindo assim a configuração de políticas de segurança específicas para AP na Firewall.

### **2.1.4. Controlo e visibilidade aplicacional**

- a) A Firewall deverá classificar todo o tráfego em função da aplicação, de tal forma que se obtenha visibilidade da atividade em função da aplicação;
- b) Possibilidade de encaminhar o tráfego por caminhos alternativos (Policy Based Routing). Conseguir, por exemplo, que a Firewall desvie e diferencie as atividades corporativas e de negócio por um link ADSL diferente do link principal (rota por defeito);
- c) Reconhecer tráfego encriptado em HTTPS;
- d) Reconhecer aplicações em múltiplos portos;
- e) Permitir controlo de acesso a aplicações em função de utilizador da AD.

### **2.1.5. Navegação Web**

- a) Possibilidade de aplicar diferentes perfis de segurança (IPS. File Blocking, Spyware, Antivírus. etc.) ao tráfego de diferentes aplicações Web, incluindo quando as aplicações se servem do mesmo servidor Web (mesmo endereço IP, mesmo porto TCP);
- b) Proxy totalmente transparente para antimalware e web filtering;
- c) Proteção avançada contra ameaças ("sandbox");
- d) Detecção, bloqueio, rastreio, análise e resolução para proteção da organização contra-ataques de malware;
- e) Malware na Web, trojans e spyware em HTTP/S, FTP e e-mail baseado na Web;
- f) Regras e exceções personalizáveis.

### **2.1.6. Filtragem de Email**

- a) Detecção de Malware, trojans e spyware em tráfego de email, IMAP, POPe SMTP;
- b) Possibilidade de aplicar diferentes perfis de deteção e filtragem de email a regras específicas de firewall;



- c) Capacidade de análise de spam, recorrendo as seguintes técnicas: IP Address Check, URL Check, Detect Phishing URLs in Email, Email Checksum Check, Spam Submission;
- d) Capacidade de bloqueio de email recorrendo a black ou white lists.

#### **2.1.7. DLP e controlo de ficheiros**

- a) Controlo do movimento (upload/download) de ficheiros nas aplicações que suportaram a transferência de ficheiros (FTP, SMTP, POP3, HTTP, HTTPs, etc.);
- b) DLP: capacidade de procura de padrões como por exemplo cartões de crédito, bem como sequências concretas.

#### **2.1.8. Especificações**

O processamento deve ser adequado à tipologia da solução apresentada, garantindo:

- a) Redundância de equipamentos físicos;
- b) 16 interfaces GE RJ-45 (10/100/1000Base-T, fixos/nativos);
- c) 8 interfaces GE SFP+ (10/100/1000Base-T, fixos/nativos);
- d) 4 interfaces 10 GE SFP+ (10GB);
- e) Débito máximo Firewall superior a 25 Gbps com pacotes UDP 1518 byte;
- f) Débito Threat Protection 3 Gbps;
- g) Débito VPN IPSEC superior a 10 Gbps;
- h) Débito VPN SSL 2 Gbps;
- i) 3 milhões de sessões concorrentes;
- j) SSL inspection 4 Gbps;
- k) Aceleração do tráfego de Firewall, SSL e IPSEC por hardware;
- l) Aceleração de tráfego NGFW por hardware;
- m) O Equipamento deve ter a altura máxima de 1U;
- n) O equipamento não deve exceder um consumo de energia máximo de 125W, com fontes de alimentação redundantes;
- o) licenciamento para acesso remoto de 500 utilizadores, independentemente do formato (Portal, Mobile ou IPSEC);
- p) A Firewall deverá incorporar uma interface aberta (API) para possibilitar a integração da sua configuração e operação com outros sistemas;
- q) A API deverá ser aberta e documentada para possibilitar a integração do equipamento com outras aplicações. A API deverá permitir operações de leitura (receber dados estatísticos), operações de escrita (modificar a configuração) e alteração de objetos dinâmicos;
- r) Suporte SNMP para obtenção de valores e estados da plataforma de segurança.
- s) O equipamento deve deter as seguintes certificações: ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, IPv6.

### **3. Garantia e manutenção da solução a adquirir**

Todos os equipamentos a fornecer devem incluir a garantia do fabricante durante 3 (três) anos, incluindo suporte técnico prestado pelo mesmo ou por parceiro devidamente certificado no regime (support level) 24/7.