

PROCEDIMENTO N.º 2203000496

**AQUISIÇÃO DE SOLUÇÃO FIREWALL EM FORMATO APPLIANCE,
SOFTWARE DE PREVENÇÃO AVANÇADA DE AMEAÇAS E
SERVIÇOS DE SUPORTE TÉCNICO
CADERNO DE ENCARGOS**

CADERNO DE ENCARGOS

Cláusula 1.ª

Objeto

1. O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual que tem por objeto a aquisição de uma solução *firewall* em formato *appliance*, composta por dois chassis, bem como licenças de *software* de prevenção avançada de ameaças e serviços de suporte técnico, para cada chassis, adequados à solução fornecida.
2. A contratação visa proteger as redes e o tráfego de e para o *data center*, bem como as redes dos serviços administrativos da Faculdade de Ciências da Universidade de Lisboa.

Cláusula 2.ª

Contrato

O contrato, a reduzir a escrito, é composto pelo respetivo clausulado contratual e seu(s) anexo(s), integrando igualmente os elementos elencados nas disposições aplicáveis do Código dos Contratos Públicos (CCP).

Cláusula 3.ª

Obrigações do adjudicatário

Sem prejuízo de outras obrigações previstas na legislação aplicável e no presente caderno de encargos, da celebração do contrato decorrem para o adjudicatário as seguintes obrigações principais:

- a) Fornecer à entidade adjudicante uma solução *firewall*, composta por dois chassis, em conformidade com as especificações técnicas fixadas no Anexo ao presente caderno de encargos, de que faz parte integrante;
- b) Fornecer à entidade adjudicante 2 (duas) licenças de *software* de prevenção avançada de ameaças, uma para cada chassis, com prazo de duração de 3 (três) anos cada;

- c) Fornecer à entidade adjudicante serviços de suporte técnico 365x24x7, com tempo de resposta garantido, atualizações de *software* proativas, melhorias e correções de falhas, adequados à solução *firewall* fornecida, durante 3 (três) anos.

Cláusula 4.ª

Prazos e local de execução

1. A entrega dos bens deve ocorrer no prazo máximo de 180 (cento e oitenta) dias a contar da data de assinatura do contrato.
2. As licenças de *software* de prevenção avançada de ameaças e os serviços de suporte técnico são válidos por um período de 3 (três) anos a contar da data da sua ativação pela entidade adjudicante.
3. A entidade adjudicante dispõe de 90 (noventa) dias a contar da data de aceitação dos bens para proceder à ativação referida no número anterior.
4. O local de entrega dos bens é a Faculdade de Ciências da Universidade de Lisboa, com morada no Campo Grande, 1749-016 Lisboa.

Cláusula 5.ª

Operacionalidade dos bens

1. Os bens devem ser entregues em perfeitas condições de serem utilizados para os fins a que se destinam e dotados de todo o material de apoio necessário ao seu normal funcionamento.
2. O adjudicatário é responsável perante a entidade adjudicante por qualquer defeito ou discrepância que existam no momento em que os bens objeto do contrato lhe são entregues.

Cláusula 6.ª

Preço base e preço contratual

1. O preço base do procedimento é 132.000,00 € (cento e trinta e dois mil euros), montante máximo que a entidade adjudicante se dispõe a pagar pela execução de todas as prestações que constituem o objeto do contrato a celebrar.

2. Na fixação do preço base foram tidos em consideração os preços dos três orçamentos obtidos através da consulta preliminar ao mercado.
3. O preço base inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante, nomeadamente, despesas de transporte, armazenamento, entrega, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.
4. O preço contratual é o preço a pagar, pela entidade adjudicante, em resultado da proposta adjudicada, pela execução de todas as prestações que constituem o objeto do contrato.
5. Ao preço contratual acresce o IVA à taxa legal em vigor.

Cláusula 7.ª

Condições de pagamento

1. A quantia devida pela entidade adjudicante deve ser paga no prazo de 30 dias após a receção pela mesma das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva.
2. Em caso de discordância por parte da entidade adjudicante quanto aos valores indicados nas faturas, deve esta comunicar, por escrito, ao adjudicatário, os respetivos fundamentos, ficando o adjudicatário obrigado a prestar os esclarecimentos necessários ou a proceder à emissão de nova fatura corrigida.
3. O não pagamento dos valores contestados pela entidade adjudicante não vence juros de mora nem justifica a suspensão das obrigações contratuais do adjudicatário, devendo, no entanto, a entidade adjudicante proceder ao pagamento da importância não contestada.
4. Desde que devidamente emitidas e observado o disposto nos n.ºs 1 e 2, as faturas são pagas através de transferência bancária para a instituição de crédito indicada pelo adjudicatário.
5. No caso de suspensão da execução do contrato e independentemente da causa da suspensão, os pagamentos ao adjudicatário serão automaticamente suspensos por igual período.
6. Na eventualidade de atraso nos pagamentos, dentro dos prazos contratual e legalmente previstos, a entidade adjudicante encontra-se sujeita às consequências que, nos termos da

lei, advêm desses atrasos, nomeadamente as previstas nos n.ºs 3 e 4 do artigo 5.º, no n.º 2 do artigo 9.º e no n.º 3 do artigo 8.º, todos da Lei dos Compromissos e Pagamentos em Atraso, constantes da Lei n.º 8/2012, de 21 de fevereiro, e, ainda, os previstos no artigo 326.º do CCP.

Cláusula 8.ª

Gestor do contrato

1. A execução do contrato será permanentemente acompanhada pelo gestor do contrato designado pela entidade adjudicante.
2. No exercício das suas funções, o gestor pode acompanhar, examinar e verificar, presencialmente, a execução do contrato pelo adjudicatário.
3. Caso o gestor do contrato detete desvios, defeitos ou outras anomalias na execução do contrato, determina ao adjudicatário que adote as medidas que, em cada caso, se revelem adequadas à correção dos mesmos.
4. O desempenho das funções de acompanhamento e fiscalização do modo de execução do contrato não exime o adjudicatário de responsabilidade por qualquer incumprimento ou cumprimento defeituoso das suas obrigações.

Cláusula 9.ª

Tratamento de dados

1. O adjudicatário obriga-se a tratar todos os dados pessoais a que tiver acesso, de acordo com o previsto no Regulamento Geral de Proteção de Dados Pessoais (RGPD), aprovado pelo Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.
2. O adjudicatário obriga-se a não divulgar quaisquer informações e documentação, técnica e não técnica, comercial ou outra, relativa à entidade adjudicante, de que venha a ter conhecimento ao abrigo ou em relação com a execução do contrato.
3. O adjudicatário obriga-se também a não utilizar as informações obtidas para fins alheios à execução do contrato.

4. O adjudicatário obriga-se a remover e destruir no termo final do prazo contratual todo e qualquer registo, em papel ou eletrónico, que contenha dados ou informações referentes ou obtidas na execução do contrato e que a entidade adjudicante lhe indique para esse efeito.

Cláusula 10.ª

Sanções contratuais de natureza pecuniária

1. Pelo incumprimento de quaisquer obrigações emergentes do contrato, por causa imputável ao adjudicatário, poderá a entidade adjudicante aplicar-lhe uma sanção no valor de 1‰ (um por mil) do preço contratual.
2. Nos casos em que as obrigações impliquem o cumprimento de um prazo, será aplicada a sanção pecuniária fixada no número anterior por cada dia de atraso.
3. O valor acumulado das sanções previstas no número anterior não pode exceder o limite máximo de 20% do preço contratual.
4. Nos casos em que seja atingido o limite de 20% e a entidade adjudicante decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30%.

Cláusula 11.ª

Força maior

1. Não podem ser impostas penalidades ao adjudicatário, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.
2. Podem constituir força maior, quando se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.

3. Não constituem força maior, designadamente:

- a) Circunstâncias que não constituam força maior para os subcontratados do adjudicatário, na parte em que intervenham;
- b) Greves ou conflitos laborais limitados às sociedades do adjudicatário ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
- c) Determinações governamentais, administrativas ou judiciais de natureza sancionatória, ou de outra forma resultantes do incumprimento pelo adjudicatário de deveres ou ónus que sobre ele recaiam;
- d) Manifestações populares devidas ao incumprimento pelo adjudicatário de normas legais;
- e) Incêndios ou inundações com origem nas instalações do adjudicatário cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
- f) Avarias nos sistemas informáticos ou mecânicos do adjudicatário não devidas a sabotagem;
- g) Eventos que estejam ou devam estar cobertos por seguros.

4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.

5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante de força maior.

Cláusula 12.ª

Resolução do contrato por parte da entidade adjudicante

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, a entidade adjudicante pode resolver o contrato, a título sancionatório, no caso de o adjudicatário violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, designadamente, no caso de atraso, total ou parcial, na prestação dos serviços objeto do contrato superior a 7 (sete) dias

ou declaração escrita do adjudicatário de que o atraso em determinada prestação excederá esse prazo.

2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao adjudicatário e não implica a repetição das prestações já realizadas pelo mesmo nos termos previstos no presente caderno de encargos, a menos que tal seja expressamente determinado pela entidade adjudicante.

Cláusula 13.ª

Resolução do contrato por parte do adjudicatário

1. O adjudicatário pode resolver o contrato com os fundamentos e nos termos previstos no artigo 332.º do CCP.
2. A resolução do contrato pelo adjudicatário não determina a repetição das prestações já realizadas, cessando, porém, todas as obrigações do adjudicatário previstas no contrato, com exceção daquelas a que se refere o artigo 444.º do CCP.

Cláusula 14.ª

Subcontratação e cessão da posição contratual

Não é permitida a subcontratação nem a cessão da posição contratual sem a autorização prévia e por escrito da entidade adjudicante, nos termos do CCP.

Cláusula 15.ª

Comunicações

1. Sem prejuízo de poderem vir a ser acordadas outras regras, quaisquer comunicações entre a entidade adjudicante e o adjudicatário devem ser efetuadas através de carta registada com aviso de receção ou por correio eletrónico, para os seguintes contactos:

Contraente Público

Gestor do contrato: [*identificação*]

Morada: Campo Grande, 1749-016 Lisboa.

Correio eletrónico: [*endereço*]

PROCEDIMENTO N.º 2203000496

**AQUISIÇÃO DE SOLUÇÃO FIREWALL EM FORMATO APPLIANCE,
SOFTWARE DE PREVENÇÃO AVANÇADA DE AMEAÇAS E
SERVIÇOS DE SUPORTE TÉCNICO
CADERNO DE ENCARGOS**

Cocontratante

Pessoa de contacto: [identificação]

Morada: [endereço]

Correio eletrónico: [endereço]

2. Qualquer comunicação feita por carta registada é considerada recebida na data em que for assinado o aviso de receção ou, na falta dessa assinatura, na data indicada pelos serviços postais.
3. Qualquer comunicação feita por correio eletrónico é considerada recebida na data constante do respetivo recibo de receção.

Cláusula 16.ª

Contagem dos prazos

À contagem de prazos na fase de execução do contrato são aplicáveis as regras constantes do artigo 471.º do CCP.

Cláusula 17.ª

Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do tribunal administrativo de círculo de Lisboa, com renúncia expressa a qualquer outro.

Cláusula 18.ª

Direito aplicável e natureza do contrato

O contrato rege-se pelo direito português e tem natureza administrativa.

ANEXO

ESPECIFICAÇÕES TÉCNICAS

A Faculdade de Ciências da Universidade de Lisboa pretende com este procedimento adquirir uma solução de anteparas de segurança, vulgo *firewall*, para a sua rede. Pretende-se que a solução proposta seja em formato *appliance*, composta por dois chassis que irão operar em redundância e alta disponibilidade.

A solução terá de ser capaz de identificar um elevado número de ataques diferenciados e tentativas de intrusão na rede e nos sistemas informáticos existentes na Faculdade. Além da deteção de tentativas de ataques com base em padrões de tráfego ou assinaturas conhecidas pretende-se que a solução proposta tenha também a capacidade de usar métodos de inteligência artificial como “*Machine Learning*” para mitigar novas técnicas de intrusão na rede ainda antes destas já estarem identificadas e referenciadas em assinaturas.

A solução proposta tem também de ser capaz de inspecionar todo o tráfego até a camada 7 do modelo OSI (*Open System Interconnection*) e assim identificar a aplicação responsável pelo tráfego inspecionado, bem como implementar políticas de rede baseadas na aplicação que gerou o tráfego inspecionado.

A solução a fornecer deve ser composta por 2 (dois) chassis, devendo cada um deles conter os seguintes números mínimos de portas com os seguintes formatos e largura de banda:

- a) 8 portas 1G/2.5G/5G/10G em formato nativo UTP;
- b) 12 portas 1G/10G em formato SFP/SFP+;
- c) 4 portas 25G em formato SFP28;
- d) 4 portas 40G/100G em formato QSFP+/QSFP28.

Um requisito muito importante será a capacidade de envio de registo de eventos, normalmente denominados por “log”, para servidores remotos, e em formato customizado. Os logs terão de poder ser identificados por etiquetas que correspondem ao syslogtag na aplicação rsyslog e terá de obedecer às características especificadas para o campo “TAG” no RFC 3164. A identificação do tipo de log terá de permitir diferenciar na “TAG” se a mensagem de log corresponde a uma mensagem referente à aplicação de uma regra de *firewall*, a uma mensagem referente a um evento do sistema da *firewall*, a uma mensagem referente ao motor de deteção de vulnerabilidades e/ou intrusão, a uma mensagem referente a filtros de url, e a uma mensagem referente à análise de ficheiros e/ou conteúdos, sendo que essa análise foi executada na *cloud* ou outro sistema externo à *firewall*.

A solução proposta deve incluir suporte para uma API XML que, com a devida autenticação, aceite e responda aos seguintes pedidos através de um simples GET em https:

- a) Pedidos de obtenção da tabela de arp e *neighbors* ipv6;
- b) Pedidos de obtenção de um relatório ou lista com os endereços locais mais atacados;
- c) Pedidos de obtenção de um relatório ou lista com os endereços externos que efetuaram mais ataques num determinado intervalo de tempo;
- d) Pedidos de obtenção de informação de CVE constantes numa determinada assinatura;
- e) Pedidos de obtenção de informações de descrições, referências, *urls* e outras informações relevantes constantes numa determinada assinatura;
- f) Pedidos de obtenção da configuração atual da *firewall*.

Características técnicas exigidas:

1. Mínimo 8 portas 1G/2.5G/5G/10G em formato nativo UTP;
2. Mínimo 12 portas 1G/10G em formato SFP/SFP+;
3. Mínimo 4 portas 25G em formato SFP28;
4. Mínimo 4 portas 40G/100G em formato QSFP+/QSFP28;
5. Porta de gestão do tipo “*Out-of-band Ethernet*” em formato SFP;

6. Duas portas 1G em formato SFP dedicadas para *setup* de alta disponibilidade;
7. Porta 40G em formato QSFP+ dedicada para *setup* de alta disponibilidade;
8. Porta consola serie em formato Rj-45 e em formato micro USB;
9. Mínimo espaço de armazenamento de 480GB em formato SSD;
10. Formato *rack* com máximo de 2U's de altura;
11. Refrigeração com entrada de ar fresco no sentido frente para trás;
12. Duas fontes AC redundantes de potência máxima 760 *Watt* por fonte;
13. Capacidade de funcionamento entre os 0º C e 50º C e entre 10% e 70% de humidade relativa;
14. Dissipação máxima de calor de 1640 BTU/hora;
15. Período médio entre falhas de funcionamento superior a 190000 horas;
16. Gestão/administração através de interface web, linha de comandos e API XML;
17. Suporte para diferentes perfis de administração e gestão da *firewall*, com diferentes níveis de privilégio;
18. Suporte à visualização e validação de alterações à configuração antes de serem aplicadas;
19. Capacidade de armazenar diferentes versões de configuração da *firewall*;
20. Capacidade de hierarquizar as políticas de segurança e a criação de políticas globais à configuração;
21. Suporte para SNMP;
22. Suporte para envio de *logs* para um servidor remoto de Syslog;
23. Suporte para a criação de políticas baseadas em utilizadores e grupos de utilizadores;
24. Suporte à integração com diretório da Microsoft (Active Directory);
25. Suporte para *logs* em formato syslog com informação de login e logout de utilizadores;
26. Suporte para identificação de utilizadores em portal próprio de autenticação através de métodos seguros como Kerberos, NTLM e SAML;
27. Suporte para identificação de utilizadores a partir dos seguintes métodos: LDAP, Captive Portal, VPN, NACs (XML e API), Syslog, Terminal Services, XFF Headers, Server Monitoring, e client probing;

28. Suporte à criação de zonas constituídas por vários interfaces e criação de políticas baseadas em zonas;
29. Suporte à criação de políticas com várias zonas de origem e/ou várias zonas de destino;
30. Suporte à criação de políticas baseadas em aplicações e capacidade de reconhecimento no mínimo de 2400 aplicações;
31. Capacidade de aplicar e/ou criar exceções à aplicação de qualquer das funcionalidades de inspeção (IPS, antivírus, etc) ao tráfego de determinada aplicação;
32. Suporte para agrupar aplicações por categorias de forma que as políticas de segurança sejam aplicadas por categorias de aplicações;
33. Suporte à criação de regras de QoS baseadas em aplicações;
34. Suporte à aplicação de perfis de proteção com base em identificadores de categoria e risco para cada vulnerabilidade;
35. Suporte para referências CVE na identificação das vulnerabilidades detetadas;
36. Suporte para a conversão e importação de assinaturas de Snort e Suricata;
37. Suporte à identificação e bloqueio de ligações C&C (*Command and Control*) desconhecidas em tempo real e através de métodos baseados em *machine learning*;
38. Suporte à análise de ficheiros executáveis desconhecidos e scripts do tipo *powershell* desconhecidos através de métodos de *machine learning* e bloqueio em caso de potencial ameaça sem recurso a técnicas de *sandboxing*;
39. Suporte para mecanismos de DNS *Sinkhole*;
40. Suporte para o bloqueio de transferência de ficheiros localizados em URLs categorizados como inseguros;
41. Suporte para o bloqueio de ligações através da verificação de assinaturas independente do porto de origem ou destino usado na ligação;
42. Suporte contra a exfiltração de dados;
43. Capacidade para processar tráfego do tipo appmix em *firewall* a uma taxa superior ou igual a 36Gbps identificando a aplicação que gera o tráfego e registando todo o tráfego em syslog;

44. Capacidade para processar tráfego do tipo appmix em *firewall* e *full inspection* a uma taxa superior ou igual a 22Gbps identificando a aplicação que gera o tráfego, registando todo o tráfego em syslog, em simultâneo com antivirus e antispyware;
45. Capacidade para processar tráfego IPSec a uma taxa igual ou superior a 21Gbps;
46. Capacidade para processar 4 milhões de sessões em simultâneo e estabelecer 246 mil novas sessões por segundo;
47. Capacidade para processar políticas de prevenção ou deteção de intrusões sem adicionar uma latência superior a 1ms em cada ligação de rede;
48. Suporte para funcionamento em L3, L2, TAP ou *virtual wire* quer seja tráfego IPv4 ou IPv6;
49. Suporte para *relay* de DHCP;
50. Suporte para *routing* estático;
51. Suporte para OSPFv2 e OSPFv3;
52. Suporte para BGP;
53. Suporte para RIP;
54. Suporte para *policy-based forwarding* baseado no endereço/rede de origem;
55. Suporte para *policy-based forwarding* baseado no utilizador ou grupo do utilizador;
56. Suporte para *policy-based forwarding* baseado na aplicação;
57. Suporte para PPPoE;
58. Suporte para Multicast PIM Sparse Mode;
59. Suporte para Multicast PIM Source Specific Mode;
60. Suporte para IGMP v1, v2 e v3;
61. Suporte para IKEv1 e IKEv2 através de pré-shared key e certificados;
62. Suporte para TLS 1.3;
63. Suporte para 802.1Q (4094 vlan ids);
64. Suporte para 802.3ad/802.1ax;
65. Suporte para alta disponibilidade em modo ativo/ativo e ativo/passivo.