



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

PROGRAMA DO CONCURSO

**Aquisição de Equipamento de Segurança para a Rede Alargada do
Governo Regional dos Açores**



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

ÍNDICE

Artigo 1.º Identificação e objeto do concurso	3
Artigo 2.º Entidade adjudicante	3
Artigo 3.º Órgão que tomou a decisão de contratar	3
Artigo 4.º Plataforma eletrónica de contratação	3
Artigo 5.º Esclarecimentos, retificações, erros e omissões	4
Artigo 6.º Prazo e modo de apresentação das propostas	4
Artigo 7.º Documentos que constituem as propostas	5
Artigo 8.º Apresentação de propostas variantes	6
Artigo 9.º Prazo mínimo da obrigação de manutenção das propostas	6
Artigo 10.º Critério de adjudicação	6
Artigo 11.º Documentos de habilitação	6
Artigo 12.º Caução	7
Artigo 13.º Agrupamentos	8
Artigo 14.º Despesas inerentes à celebração do contrato	8
Artigo 15.º Comunicações e notificações	8
Artigo 16.º Assinatura eletrónica e selos temporais	8
Artigo 17.º Legislação aplicável	9
Anexo I	10
Anexo II	11
Anexo III	24



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Artigo 1.º

Identificação e objeto do concurso

- 1 - O presente procedimento tem por objeto Aquisição de Equipamento de Segurança para a Rede Alargada do Governo Regional dos Açores, nos termos melhor definidos no caderno de encargos.
- 2 - O presente procedimento segue a tramitação do concurso público, nos termos do artigo 132.º a 154.º do Código dos Contratos Públicos (CCP), sendo designado por **Aquisição de Equipamento de Segurança para a Rede Alargada do Governo Regional dos Açores** ".

Artigo 2.º

Entidade adjudicante

A entidade adjudicante é a Região Autónoma dos Açores, através da Secretaria Regional das Obras Públicas e Comunicações (SROPC) – Direção Regional das Comunicações (DRCom), sita no Largo do Colégio, n.º 4, 9500-054 Ponta Delgada, telefone n.º (+351) 296 206 200 e correio eletrónico drcom-info@azores.gov.pt

Artigo 3.º

Órgão que tomou a decisão de contratar

A decisão de contratar foi tomada pela Secretária Regional das Obras Públicas e Comunicações a 22/09/2021.

Artigo 4.º

Plataforma eletrónica de contratação

- 1 - A participação no concurso depende de prévia inscrição, gratuita, na plataforma eletrónica de contratação, adiante designada apenas por plataforma, disponível em <https://www.acingov.pt/acingovprod/2/> .
- 2 - O acesso ao procedimento e às peças do mesmo é gratuito e permite efetuar a consulta de todos os atos do procedimento que devam ser publicados, bem como a apresentação de propostas.
- 3 - O disposto no n.º 1 do presente artigo não é aplicável às entidades que já se encontrem registadas na plataforma.



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Artigo 5.º

Esclarecimentos, retificações, erros e omissões

- 1 - Os esclarecimentos necessários à boa compreensão e interpretação das peças do concurso devem ser apresentados pelos interessados até ao termo do 1/3 do prazo fixado para apresentação das propostas.
- 2 - Os esclarecimentos referidos no número anterior são prestados até termo do 2/3 do prazo fixado para apresentação das propostas.
- 3 - No prazo referido no n.º 1, os interessados podem apresentar ao órgão competente para a decisão de contratar uma lista na qual identifiquem, expressa e inequivocamente, os erros e omissões detetados nas peças do procedimento, nos termos do artigo 50.º do CCP.
- 4 - Até ao termo do 2/3 do prazo para apresentação das propostas o órgão competente para a decisão de contratar pronuncia-se sobre a lista de erros e omissões apresentada, podendo ainda, no mesmo prazo, proceder à retificação das peças do procedimento.
- 5 - Consideram-se rejeitados todos os erros e omissões apresentados que, até ao final do prazo indicado no número anterior, não tenham sido expressamente aceites pelo órgão competente para a decisão de contratar.
- 6 - Os esclarecimentos, as retificações e os erros e omissões aceites fazem parte integrante das peças do procedimento a que dizem respeito e prevalecem sobre estas em caso de divergência, devendo todos os interessados que as tenham obtido ser imediatamente notificados desse facto.
- 7 - Todos os atos mencionados no presente artigo são praticados através da plataforma eletrónica referida no artigo anterior.

Artigo 6.º

Prazo e modo de apresentação das propostas

- 1 - As propostas devem ser submetidas na plataforma indicada no artigo 4.º até às 23h59 do 30.ª dia a contar da data do envio do anúncio para publicação.
- 2 - A receção das propostas é registada com referência às respetivas data e hora, sendo entregue aos concorrentes um recibo eletrónico comprovativo do envio através da plataforma.
- 3 - Os concorrentes devem prever o tempo necessário para a inserção dos documentos, bem como para a sua assinatura eletrónica qualificada, em função do tipo de acesso à internet de que



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

dispõem, uma vez que só são admitidas a concurso as propostas que tenham sido assinadas e recebidas até à data referida no n.º 1 do presente artigo.

- 4 - Até ao termo do prazo fixado para a apresentação das propostas, os interessados que já as tenham apresentado devem retirá-las sempre que pretendam apresentar nova proposta dentro daquele prazo.
- 5 - Não são aceites propostas entregues por qualquer outro meio que não a plataforma.

Artigo 7.º

Documentos que constituem as propostas

1 - As propostas devem ser constituídas pelos seguintes documentos:

- a) Documento Europeu Único de Contratação Pública, conforme já pré-preenchido e disponível na plataforma;
- b) Proposta de preço elaborada em conformidade com o anexo I ao presente programa de concurso considerando o seguinte:
 - i. O preço, que não deve incluir o IVA, é também indicado em algarismos;
 - ii. Quando os preços constantes da proposta forem também indicados por extenso, em caso de divergência, estes prevalecem, para todos os efeitos, sobre os indicados em algarismos;
 - iii. Sempre que na proposta sejam indicados vários preços, em caso de qualquer divergência entre eles, prevalecem sempre, para todos os efeitos, os preços parciais, unitários ou não, mais decompostos.
- c) Matriz de análise de requisitos devidamente preenchida acordo com o ANEXO II ao presente programa do procedimento.
- d) Documento(s) do(s) fabricante(s) onde constem os requisitos, características técnicas e
- e) funcionalidades da solução a fornecer.
- f) Documento que indique o poder de representação e a assinatura do assinante, nos termos e situação prevista no n.º 2 do artigo 16.º;
- g) Certidão do registo comercial, com todas as inscrições em vigor, ou disponibilização do código de acesso para a sua consulta online.



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- 2 - Os documentos que constituem a proposta são obrigatoriamente redigidos em português, com exceção do documento previsto na alínea d) do número anterior que pode ser redigido em inglês.
- 3 - Quando a proposta seja apresentada por um agrupamento concorrente, a declaração e a proposta de preço referidas nas alíneas a) e b) do n.º 1 devem ser assinadas pelo representante comum dos membros que o integram, caso em que devem ser juntos à declaração os instrumentos de mandato emitidos por cada um dos seus membros ou, não existindo representante comum, devem ser assinados por todos os seus membros ou respetivos representantes.

Artigo 8.º

Apresentação de propostas variantes

Não é admissível a apresentação de propostas variantes.

Artigo 9.º

Prazo mínimo da obrigação de manutenção das propostas

O prazo mínimo de obrigação de manutenção das propostas é de 66 dias.

Artigo 10.º

Critério de adjudicação

- 1 - A adjudicação é feita segundo o critério da proposta economicamente mais vantajosa, com exclusiva avaliação do preço enquanto único aspeto da execução do contrato a celebrar submetido à concorrência.
- 2 - Em caso de empate no valor das propostas o desempate será realizado um sorteio em data e modo a fixar pelo Júri do concurso.

Artigo 11.º

Documentos de habilitação

- 1 - O adjudicatário deve entregar através da plataforma, no prazo de 5 dias úteis a contar da notificação da decisão de adjudicação, os seguintes documentos de habilitação:
 - a) Declaração emitida conforme modelo constante do Anexo III do RJCPRAA;
 - b) Documentos comprovativos, ou disponibilização de acesso para a sua consulta online, de que se encontra nas seguintes situações:



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- i - Situação regularizada relativamente a contribuições para a segurança social em Portugal ou, se for o caso, no Estado de que sejam nacionais ou no qual se situe o seu estabelecimento principal, nos termos da alínea d) do artigo 55.º do CCP;
 - ii - Situação regularizada relativamente a impostos devidos em Portugal ou, se for o caso, no Estado de que sejam nacionais ou no qual se situe o seu estabelecimento principal, nos termos da alínea e) do artigo 55.º do CCP;
 - c) Certificado de registo criminal, para efeitos de celebração de contratos públicos, de todos os titulares dos órgãos sociais de administração, direção ou gerência que se encontrem em efetividade de funções, destinado a comprovar que não se encontram em nenhuma das situações previstas no artigo 55.º do CCP, bem como certificado do registo criminal da pessoa coletiva;
 - d) Certidão do registo comercial em vigor, ou disponibilização do código de acesso para a sua consulta online, para identificação dos titulares dos órgãos sociais de administração, direção ou gerência que se encontrem em efetividade de funções.
- 2 - Caso sejam detetadas irregularidades nos documentos de habilitação entregues pelo adjudicatário, será concedido um prazo adicional de 5 dias úteis destinado ao seu suprimento.

Artigo 12.º

Caução

- 1 - Caso a adjudicação recaia sobre proposta cujo preço contratual seja igual ou superior a 200.000,00€, o adjudicatário deverá prestar uma caução destinada a garantir a celebração do contrato, bem como o exato e pontual cumprimento de todas as obrigações legais e contratuais que assume com essa celebração.
- 2 - A caução, destinada a garantir a celebração do contrato, bem como o exato e pontual cumprimento de todas as obrigações legais e contratuais, deve ser prestada, no valor que se encontrar definido, em cumprimento do artigo 43.º do RJCPRAA:
- a) Por depósito em dinheiro ou em títulos emitidos ou garantidos pelo Estado Português à ordem da entidade adjudicante, nos termos do modelo constante do Anexo III;
 - b) Mediante garantia bancária ou seguro-caução, nos termos dos modelos constantes do Anexo III.



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- 3 - Sem prejuízo do disposto no número anterior, ao prazo e ao modo de prestação da caução, assim como à determinação da responsabilidade pelas respetivas despesas, é aplicável o previsto no artigo 90.º do CCP.

Artigo 13.º

Agrupamentos

Em caso de adjudicação, todos os membros do agrupamento adjudicatário, e apenas estes, devem associar-se, antes da celebração do contrato, na modalidade de consórcio externo em regime de responsabilidade solidária.

Artigo 14.º

Despesas inerentes à celebração do contrato

Correm por conta do adjudicatário as despesas inerentes à celebração do contrato.

Artigo 15.º

Comunicações e notificações

Todas as comunicações entre a entidade adjudicante ou o júri do procedimento e os interessados, concorrentes ou o adjudicatário, até à assinatura do contrato objeto do presente procedimento, são realizadas exclusivamente através da plataforma prevista no artigo 4.º.

Artigo 16.º

Assinatura eletrónica e selos temporais

- 1 - Todos os documentos carregados na plataforma, incluindo os documentos que constituem as propostas, devem ser assinados eletronicamente mediante a utilização de certificados de assinatura eletrónica qualificada, nos termos previstos no artigo 54.º da Lei 96/2015, de 17 de agosto.
- 2 - Nos casos em que o certificado digital não possa relacionar o assinante com a sua função e poder de assinatura, deve a entidade interessada submeter à plataforma um documento eletrónico oficial indicando o poder de representação e a assinatura do assinante (certidão permanente onde conste os poderes para representar ou procuração).
- 3 - A falta de assinatura eletrónica nos documentos que constituem as propostas é motivo de exclusão.



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- 4 - Todos os documentos submetidos na plataforma, bem como todos os atos que, nos termos do CCP, devem ser praticados dentro de um determinado prazo, são sujeitos à aposição de selos temporais emitidos por uma entidade certificadora credenciada para a prestação de serviços de validação cronológica, nos termos previstos no artigo 55.º da Lei 96/2015, de 17 de agosto.
- 5 - Os certificados de assinatura eletrónica qualificada e de selos temporais são emitidos por uma entidade certificadora credenciada pela Autoridade Nacional de Segurança (informação disponível em www.gns.gov.pt).

Artigo 17.º

Legislação aplicável

Ao presente procedimento é aplicável o disposto no Decreto Legislativo Regional n.º 27/2015/A, de 29 de dezembro, na sua redação atual, o Código dos Contratos Públicos na sua redação atual, e na restante legislação especialmente aplicável.



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Anexo I

Proposta de preço a que se refere a alínea b) do n.º 1 do artigo 7.º

... (nome, número de documento de identificação e morada), na qualidade de representante legal de ... (firma, número de identificação fiscal e sede ou, no caso de agrupamento concorrente, firmas, números de identificação fiscal e sedes), tendo tomado inteiro e perfeito conhecimento do caderno de encargos relativo à execução do contrato a celebrar na sequência do procedimento de **Aquisição de Equipamento de Segurança para a Rede Alargada do Governo Regional dos Açores**, declara, sob compromisso de honra, que a sua representada se obriga a executar o referido contrato em conformidade com o conteúdo do mencionado caderno de encargos pelo preço total de ..€ (indicar o valor por extenso)*.

Data

Assinatura do Concorrente/ Representante Legal

* O preço total a propor não poderá, em caso algum, exceder o preço base fixado no caderno de encargos.



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Anexo II

[a que se refere a alínea c) do n.º 1 do artigo 9.º do presente programa do procedimento]

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se cumpre		Nome do Documento do fabricante	Nº da Página
	SIM	NÃO		
Número de portas 10Gbit/s RJ45 >= 4				
Número de portas Gigabit SFP+ 10Gbit/s >= 16				
Número de portas Gigabit QSFP+ 40/100 Gbit/s >= 4				
Discos rígido SSD em RAID para sistema >= 2 x 240GB				
Discos rígido SSD em RAID para Log >= 2 x 2TB				
Porta de gestão dedicada "Out of Band"				
Porta de consola RJ45				
A appliance de FW deverá ter uma arquitetura com recursos de hardware dedicados e independentes entre os serviços de gestão e os serviços de inspeção.				
Deverá estar garantido que a appliance de FW quando gerida localmente e perante uma sobrecarga dos serviços de inspeção de tráfego não afete de forma alguma a performance dos serviços de gestão e vice-versa.				
Deverão ser incluídos 2 módulos SFP+ 10G para fibra ótica multimodo com conector dual LC/PC a instalar nas portas 10G SFP+				
Deverão ser incluídos 4 módulos QSFP28 100G SR4 para fibra ótica multimodo MTP/MPO a instalar nas portas 100G QSFP28				
Deverá estar incluído todo o material (cabos, módulos e etc.) necessário à composição do cluster, sendo que a distancia entre os equipamentos (appliances) obriga à utilização de cablagem com comprimento de 15m				
Fontes de alimentação redundantes.				
Performance				
Performance da appliance com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego) >= 37,0 Gbps				
Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware, URL Filtering e Sandboxing >= 23,0 Gbps				
Performance da appliance com a funcionalidade de VPN IPSec >= 19,0 Gbps				
Número de novas sessões por segundo >= 380 000				
Número máximo de sessões >= 8 000 000				
Gestão local e Centralizada				
Gestão e administração da própria appliance através de interface web, linha de comandos e API XML				
Possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio				



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se cumpre		Nome do Documento do fabricante	Nº da Página
	SIM	NÃO		
Na gestão centralizada deve ser possível criar perfis de administração que permita segmentar a gestão em diferentes tenants (Por Firewall, por número de firewalls) - Multi-tenancy				
Na gestão centralizada deve existir a possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio				
Na gestão centralizada deve existir a possibilidade de editar configurações pendentes que ainda não foram aplicadas				
Possibilidade de visualizar e validar alterações à configuração antes de estas alterações serem aplicadas				
Possibilidade de descartar alterações à configuração realizadas				
Possibilidade de armazenar diferentes versões da configuração				
Na gestão centralizada deve existir a capacidade de criar hierarquização da política de segurança para permitir ter políticas globais para toda infraestrutura instalada				
Na gestão centralizada deve existir a capacidade de stacks de templates com configurações reutilizáveis para múltiplos equipamentos.				
Na gestão centralizada deve existir um ponto centralizado para efetuar upgrades e atualizações de versões e assinaturas				
Capacidade de transformar políticas de layer4 em layer7 com machine learning e aprendizagem embebida na plataforma de gestão				
Na gestão centralizada deve existir a capacidade de "zero touch provisioning" para simplificar o deployment de firewalls remotas				
Gestão centralizada de SD-WAN para os escritórios remotos				
Na gestão centralizada deve ser possível gerir até 1000 firewalls num único servidor de gestão.				
A gestão centralizada deve ter a capacidade de funcionar como gestão controladora de várias máquinas de gestão centralizadas debaixo dele para poder escalar para as dezenas de milhares de firewalls debaixo de uma única gestão.				
Deve existir a capacidade de correr a Gestão centralizada sobre hardware dedicado assim como numa Máquina Virtual em VMware ESXi™, KVM e Microsoft Hyper-V, ou então em clouds publicas incluindo Google Cloud Platform (GCP™), Amazon Web Services (AWS®), AWS GovCloud, Microsoft Azure e Azure GovCloud.				
Análise da utilização das regras para reduzir superfície de exposição e melhorar postura de segurança.				
Envio de logs via SYSLOG, FTP, SCP e TFTP para retenção e posterior tratamento				
Possibilidade de envio seletivo de logs, de acordo com o nível de severidade ou outros atributos como por exemplo o tipo de ameaça				
Suporte de SNMP, incluindo a possibilidade de obter estatísticas relacionadas com o processamento de logs e com as funcionalidades de alta disponibilidade				
Networking				
As interfaces de rede da appliance deverão suportar os seguintes modos de funcionamento: TAP, Layer 2, Layer 3				



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se cumpre		Nome do Documento do fabricante	Nº da Página
	SIM	NÃO		
Suporte de IEEE 802.1Q				
Suporte de IEEE 802.1AX, suportando até 8 grupos de agregação com 8 interfaces por cada grupo				
Suporte de protocolos dinâmicos de routing: RIP, OSPF, BGP				
Suporte de routing estático				
Suporte de DHCP, NAT e PAT				
Capacidade de deteção de falhas bidirecionais entre a appliance e router para aplicar a protocolos de routing dinâmico ou rotas estáticas				
Capacidade de realizar policy based routing através do IP ou rede de origem				
Capacidade de realizar policy based routing através do utilizador ou grupo				
Capacidade de realizar policy based routing através do tipo de aplicação				
Suporte para TLS 1.3 e capacidade de descriptar este tráfego				
Possibilidade de criar Firewalls virtuais dentro de um chassis com tabela de rotas, interfaces e políticas segmentadas.				
Capacidade de associar múltiplos Virtual Routers (VRFs) a uma política única de firewall				
Capacidade de correr routing dinâmico (BGP, OSPF) dentro de cada Virtual Router.				
Capacidade de criar Firewalls Virtuais de Layer2 e Layer 3 dentro do mesmo cluster				
Capacidade de criar perfis de DDoS para proteger o chassis de ataques de larga escala.				
Suporte de arquiteturas de alta disponibilidade do tipo ativo/passivo e ativo/ativo				
Suporte de arquiteturas de alta disponibilidade e escalar lateralmente até 16 membros dentro de um único cluster sem a necessidade de balanceadores externos.				
Permitir a criação de cluster "multi-datacenter" sem a necessidade de passar layer2 de todas as VLANs entre eles.				
Adicionar novos membros ao cluster sem perder sessões existentes do cluster existente				
Sincronismo de todas as sessões entre os membros do cluster em tempo real.				
Suporte de Failover de "Datacenter para Datacenter" em diferentes localizações.				
Suporte de tráfego assimétrico entre membros do cluster espalhados por múltiplos Datacenters				
Suporte de "All Active" ou "Active-Standby" entre Datacenters				
Suporte de sobrevivência de sessões entre Datacenters.				
Permitir o mix dos pares de clusters em cada Datacenter que permite ter Ativo/Ativo no DC1 e Ativo/Passivo no DC2 e existir sincronismo entre eles.				
Permitir ter pares de clusters num Datacenter e um Hot-standby noutra e funcionar como backup do outro DC.				



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se cumpre		Nome do Documento do fabricante	Nº da Página
	SIM	NÃO		
Identificação de Utilizadores				
Possibilidade de aplicar políticas baseadas em utilizadores e grupos, em vez de por IP				
Integração com sistemas de diretórios para obtenção de utilizadores e grupos, incluindo Microsoft Active Directory, Novell eDirectory e Sun ONE Directory				
Possibilidade de integração de com sistemas multiutilizador como Citrix ou Microsoft Terminal Server para identificação de utilizadores				
Capacidade de analisar mensagens de SYSLOG com informação de LOGIN/LOGOUT para identificação de utilizadores				
Possibilidade de gerir utilizadores através de API XML				
Possibilidade de identificação de utilizadores através de portal de autenticação próprio, fazendo uso dos seguintes protocolos: Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente e autenticação local				
Capacidade de obter a identidade dos utilizadores a partir dos seguintes métodos: LDAP, Captive Portal, VPN, NACs (XML e API), Syslog, Terminal Services, XFF Headers, Server Monitoring, e client probing				
Solução de Acessos Remotos e Gestão de Identidades				
A solução deve dar a capacidade de estender as funcionalidades da Firewalls aos utilizadores remotos				
A solução deve ser capaz de garantir a segurança dos acessos aos recursos internos como também as aplicações de cloud				
Capacidade de garantir a segurança também do acesso à internet do utilizador que esteja fora da rede.				
Proteger os utilizadores remotos contra-ataques de phishing e roubo de credenciais				
Capacidade de fazer quarentena a utilizadores remotos utilizando parâmetros e características imutáveis.				
Suporte de VPNs por Aplicação e por utilizador				
Capacidade de fornecer acesso seguro e sem agente para parceiros e entidades externas as organizações.				
Suporte de identificação automatizada de equipamentos que não são geridos pela entidade da firewall.				
Capacidade de implementar Zero Trust efetuando uma identificação muito clara do utilizador.				
Fornecer também a capacidade de efetuar a identificação de parâmetros do sistema operativo para poder criar regras de acesso do tipo NAC.				
O modulo de identificação tem que obrigatoriamente ser capaz de identificar os seguintes parâmetros do equipamento que esta aceder á rede: Efetuar Patch Management, validar se a Firewall local está ativa, Anti-Malware esta instalado, Plataforma de Backups esta ativa, Mecanismo de Encriptação de disco esta Ativo, Modulo de DLP esta Ativo e parâmetros customizados do sistema operativo como processos, registries ou property lists.				



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se cumpre		Nome do Documento do fabricante	Nº da Página
	SIM	NÃO		
A solução deve disponibilizar um agente com suporte para os seguintes sistemas operativos: Windows 7 e posterior, macOS 10.11 e posterior, iOS 10 e posterior, Android 5 e posterior, CentOS e RHEL 7.0 até 7.7 e Ubuntu 14.04 até 19.04.				
O mesmo agente de acessos remotos deve também ser possível funcionar como agente de identidades dentro da infraestrutura para identificação do utilizador e mapeamento de políticas baseadas em identidades.				
Funcionalidades Gerais de Segurança				
Possibilidade de agrupar interfaces da appliance em conjuntos independentes, formando diferentes zonas de segurança				
Possibilidade de definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança				
Possibilidade de criar múltiplas regras de segurança entre zonas de origem e destino				
Capacidade de identificação de aplicações em L7 com um mínimo de 2400 aplicações identificadas				
Capacidade de identificação de subfunções dentro de uma aplicação				
Capacidade de aplicar e/ou excecionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc.) apenas ao tráfego de determinadas aplicações L7				
Possibilidade de agrupar aplicações por categorias de forma que as políticas de segurança sejam aplicadas por categorias de aplicações				
Possibilidade de identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP				
Possibilidade de identificar aplicações proprietárias que usem os protocolos HTTP e TCP				
Possibilidade de identificar aplicações que sejam transportadas em túneis encriptados SSL				
Capacidade de decifrar tráfego SSH e detetar aplicações não legítimas que utilizem este protocolo para comunicar (SSH tunneling)				
Capacidade de criar regras de QoS segundo as aplicações utilizadas no tráfego				
Possibilidade de aplicar políticas de NAT de forma independente das restantes políticas de segurança				
Capacidade de forçar o uso de MFA para acesso a aplicações internas				
Deve existir uma versão da solução que possa ser instalada como um container dentro de um ambiente de docker/kubernetes				
IDS/IPS				
Capacidade de aplicar políticas de prevenção ou de deteção contra a exploração de vulnerabilidades, tanto no tráfego que vai para a Internet como no tráfego que vem da Internet, sem incorrer numa latência				



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se cumpre		Nome do Documento do fabricante	Nº da Página
	SIM	NÃO		
superior a 1 ms para não penalizar a experiência do utilizador, efetuando a análise numa única passagem do tráfego para todas as ameaças				
Possibilidade de aplicar diferentes perfis proteção contra exploração de vulnerabilidades de acordo com as aplicações identificadas				
Possibilidade de escolher proteções contra a exploração de vulnerabilidades que se apliquem apenas a clientes ou servidores ou a ambos				
As vulnerabilidades devem estar categorizadas por tipo e por nível de risco, de forma que a aplicação de perfis de proteção se possam realizar com base nestas categorias				
Deve ser possível identificar as proteções pela identificação CVE das vulnerabilidades				
Capacidade de aplicar apenas as assinaturas necessárias para determinada aplicação identificada, através da seleção de perfis				
Deve ser possível converter assinaturas snort e suricata para dentro da plataforma				
Antivírus & Anti-Malware				
Detetar equipamentos possivelmente comprometidos que tentem estabelecer comunicações com servidores de C&C				
Capacidade de habilitar mecanismos de DNS sinkholing que permitam intercepar pedidos de resolução de nomes para domínios comprometidos com malware				
Capacidade de definir políticas de antivírus, de forma que a transferência de ficheiros realizada no sentido Internet para rede interna ou vice-versa, sejam inspecionados e bloqueados se o seu conteúdo for malicioso				
Capacidade de aplicar políticas que permitam aplicar o motor de antivírus sobre protocolos como ftp, http, imap, pop3, smb ou smtp, definindo para cada um destes protocolos a ação a realizar (permitir os ficheiros, descartar os ficheiros, desconectar a sessão ou registar mediante logs)				
Possibilidade de enviar o ficheiro para serviços de inspeção adicionais na cloud que permitam analisar e emitir um veredicto para que appliance possam tomar uma ação no caso de um ficheiro malicioso				
Capacidade de aplicar políticas de antivírus de forma granular, permitindo aplicar essas políticas utilizadores ou grupos, a determinados segmentos de rede com com determinada direção e a determinadas aplicações				
Capacidade de identificar ficheiros não através das suas extensões, mas sim a través do tipo MIME do ficheiro, permitindo no mínimo a identificação de 100 tipos de ficheiros				
Deve-se poder aplicar políticas de bloqueio de ficheiros, de forma a poder bloquear a transferência de certo tipo de ficheiros ou que se permita após a confirmação por parte do utilizador e criando um log correspondente				
Capacidade de aplicar políticas de bloqueio de ficheiros atendendo a critérios como origem e destino do tráfego, utilizador ou grupo, tipo de aplicação ou de tráfego que inicia a transferência do ficheiro				



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se cumpre		Nome do Documento do fabricante	Nº da Página
	SIM	NÃO		
Possibilidade de bloquear a transferência de ficheiros quando utilizados URLs categorizados como perigosos do ponto de vista de ameaça de segurança				
Capacidade pesquisa de padrões sensíveis no tráfego, evitando a exfiltração de dados.				
Deve existir a capacidade de analisar ficheiros executáveis e scripts powershell com um motor de machine learning local que permita bloquear ficheiros maliciosos localmente em tempo real sem necessidade de estabelecer ligações externas. Este motor deve permitir bloquear malwares nunca antes observados e para os quais não existem assinaturas sem necessidade de recorrer a sandboxing.				
Deve existir a capacidade de receber updates em tempo real de forma a não ter que aguardar minutos/horas/dias por determinado update. Assim que um novo malware é detetado por qualquer cliente do fabricante essa informação deve ser propagada em tempo real a todos os clientes de forma a diminuir o tempo de exposição a ameaças.				
Acessos VPN				
Suporte de IKEv1 e IKEv2;				
Suporte de criptografia para 3DES e AES-256 para IKE Phase I e II IKEv2;				
Suporte de pelo menos os seguintes grupos de Diffie-Hellman: Group 1, Group 2, Group 5, Group 14, Group 19 and Group 20				
IKE Phase2 - Encriptação de dados (DES, 3DES, AES-128, AES-192, AES-256) e suporte de integridade dos dados (MD5, SHA1, SHA256, SHA384, SHA512);				
VPNs Site to Site: Full Mesh (all to all) ou Star (Remote to center);				
Suporte de IKE com PKI e pre-shared Secret;				
Aprovisionamento automático de VPNs site-to-site;				
Gestão automática de túneis IPsec de backup;				
Suporte de routing dinâmico em VPN IPsec;				
Cientes VPN para Windows, MacOS e iOS, Android;				
Suporte de OTP para VPN sem recurso a terceiros fabricantes ou servidores adicionais;				
Aplicação de políticas e restrições de acesso por utilizador ou por grupo de utilizadores				
Single Sign On VPN;				
Portal HTML5 para maior compatibilidade com todo tipo de dispositivos				
Administração a partir da consola central				
URL Filtering				
Possibilidade de definir manualmente listas estáticas de URLs ou de IPs permitidos e não permitidos para a navegação, com a possibilidade de definir para os permitidos a ação a realizar (permitir, bloquear, permitir, mas advertir, etc.)				



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se cumpre		Nome do Documento do fabricante	Nº da Página
	SIM	NÃO		
Permitir a navegação baseando-se em categorias de URL, sendo estas categorias atualizadas periodicamente através de serviço em cloud				
Possibilidade de incluir listas de URLs e IPs dinâmicas relacionadas com ameaças para que possam ser bloqueadas automaticamente (listas de reputação)				
Capacidade de detetar o envio de credenciais corporativas nas páginas de internet navegadas, de forma a poder advertir, bloquear ou permitir em função da categorização das páginas web				
A filtragem de URLs deve poder ser aplicada mediante diferentes perfis e deverá ser aplicada ao tráfego que sai para a Internet ou que vem da Internet				
A solução deve possuir um motor local de machine learning que seja aplicado às páginas web visitadas pelos utilizadores de forma a prevenir variantes maliciosas de javascript e acesso a páginas de phishing. Este motor deverá funcionar em tempo real e bloquear acesso a páginas que não estejam previamente categorizadas como maliciosas.				
DNS Security				
A solução deve disponibilizar um serviço de proteção DNS baseado na cloud que seja capaz de bloquear acesso a domínios maliciosos conhecidos e desconhecidos.				
Este serviço deve utilizar mecanismos de machine learning para detetar Domain Generated Algorithms (DGAs) e bloquear o acesso a estes.				
A solução deve permitir bloquear tráfego de C&C através do canal de DNS assim como detetar e bloquear o uso indevido deste canal para efetuar exfiltração de dados (DNS tunneling).				
A funcionalidade de DNS Tunneling deve ser capaz de inspecionar o conteúdo dos pacotes de DNS.				
Este serviço deve permitir identificar quais as máquinas e utilizadores infetados, sem a necessidade de qualquer alteração na infraestrutura existente.				
A adição deste serviço não deve obrigar a qualquer alteração na infraestrutura de DNS do cliente				
Para além da threat intelligence do fabricante, a solução deve utilizar informação proveniente de pelo menos 30 fontes distintas.				
Deve ser possível criar políticas simples que bloqueiem ou façam sinkholing aos pedidos de DNS maliciosos				
Devem ser disponibilizadas as seguintes categorias para construção de políticas: Command and Control Domains, Malware Domains, Dynamic DNS Hosted Domains, Newly Registered Domains, Phishing Domains, Grayware Domains and Parked Domains				
A solução não deve necessitar de updates para estar atualizada e proteger contra as mais recentes ameaças.				
A solução deve permitir a aplicações de tags a máquinas comprometidas, de forma a ser possível criar uma política de acesso diferenciada para estas.				
Sandboxing e proteção Zero day				



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se cumpre		Nome do Documento do fabricante	Nº da Página
	SIM	NÃO		
Possibilidade de disponibilizar um serviço na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma que se permita o envio desta informação para análise atendendo aos critérios: Tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload)				
Perante uma análise por parte do serviço de Sandboxing na cloud que categorize a informação enviada como maliciosa, deverão ser criadas assinaturas num prazo máximo de 5 minutos que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente)				
O serviço de sandboxing na cloud deverá permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios				
A tecnologia de Sandboxing tem que ser capaz de inspecionar protocolos como HTTP, HTTPS, SMTP, FTP, POP3 e IMAP				
A análise de malware deve ser inteligente o suficiente para analisar comportamentos do tipo "Call back" e IOC's durante a análise de malware e automaticamente criar assinaturas que permitam a prevenção de ameaças e que possam ser utilizadas pelas restantes funcionalidades da solução.				
Os sistemas de análise de malware devem ser capazes de detetar malware direcionado a sistemas operativos de MacOS, Windows, Android e Linux				
O malware cada vez mais utiliza técnicas de Anti-VM para detetar que está a ser executado num ambiente virtual e prevenir que seja detonado, escondendo o seu comportamento malicioso. A análise "Bare Metal" é uma funcionalidade onde o malware é executado em hardware real, o que impede que o malware utilize qualquer técnica de Anti-VM. A solução deve ter esta funcionalidade embebida.				
Em termos de suporte de sistemas operativos windows emulados deve suportar: Windows XP, Windows 7 e Windows 10				
Deve ser garantido suporte para os seguintes ficheiros executáveis (EXE, DLL) e todos os tipos de ficheiros Microsoft Office, PDF, Flash, Java applets (JAR e CLASS),				
Android (ficheiros APK), macOS binaries (mach-O, DMG, PKG e application bundles) e Linux (ficheiros ELF)				
Capacidade de descriptar malware (unpacker) para utilização na análise estática e machine learning.				
IoT Security				
A plataforma deve disponibilizar um serviço cloud de segurança para dispositivos IOT.				
A firewall deve colecionar metadados do tráfego de rede dos dispositivos IoT, gerar logs com estas informações e enviá-los para um Data Lake na Cloud. O Serviço de IOT deve ter capacidade de analisar estes metadados através de um motor patenteado baseado em algoritmos de inteligência artificial e machine learning para detetar e identificar os dispositivos IoT e OT na rede.				



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se cumpre		Nome do Documento do fabricante	Nº da Página
	SIM	NÃO		
A identificação de dispositivos não se deve basear em fingerprinting, como por exemplo identificação de MAC addresses.				
O motor de identificação deve possuir 3 níveis: identificação da categoria do dispositivo (ex: camara de vigilância), identificação do seu perfil (ex: fabricante, modelo e versão) e identificação de cada instância do dispositivo.				
Após a identificação dos dispositivos, a solução deve criar um padrão de comportamento para cada um e detetar automaticamente comportamentos anormais que possam sugerir que o dispositivo está comprometido. Para este tipo de eventos, devem ser gerados alertas no dashboard da solução. Deve ser possível receber estes alertas via email e sms também.				
Quando é observado um comportamento anormal a solução deve sugerir automaticamente políticas de segurança a aplicar na firewall que permitam o correto funcionamento do dispositivo, mas bloqueie qualquer ligação anormal.				
A firewall deve permitir a criação de regras baseadas em tipos de dispositivos que devem ser identificados através da marca, modelo e versão. Não sendo assim necessário criar regras com base em IPs ou zonas.				
Este serviço deve observar mais de 200 parâmetros nos metadados do tráfego de rede, incluindo parâmetros de DHCP (option 55), HTTP user agent IDs, protocolos, headers dos protocolos, etc.				
O serviço deve identificar vulnerabilidades presentes no software a correr nos respetivos dispositivos e diferenciar entre dispositivos vulneráveis e potencialmente vulneráveis. O serviço deve identificar vulnerabilidades de software assim como vulnerabilidades associadas ao uso/configuração incorreta dos mesmos. Exemplo: uso de credenciais default.				
Deve existir a possibilidade do Data Lake ser utilizado para outro conjunto de use cases através de licenciamento adicional, nomeadamente: NTA (Network Traffic Analysis), UEBA (User Entity Behavior Analytics), shadow IT e integração com CASB (Cloud Access Security Broker).				
Data Loss Prevention				
A plataforma deve disponibilizar um módulo completo de Data Loss Prevention				
Esta funcionalidade deve ser disponibilizada como um serviço cloud que utilize supervised machine learning para identificar documentos sensíveis e atribuir-lhes uma categoria automaticamente como por exemplo: Financeiros, Legais, Saúde, informação pessoal, etc. A solução deverá também permitir controlar este tipo de documentos de forma evitar a sua exposição ou extravio.				
Este serviço deverá permitir proteger estes documentos das seguintes formas: Prevenir o upload de ficheiros com informação confidencial e/ou sensível para aplicações web não permitidas pela organização; Monitorizar o upload de documentos para aplicações externas permitidas pela organização.				



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se cumpre		Nome do Documento do fabricante	Nº da Página
	SIM	NÃO		
O serviço deve disponibilizar out-of-the-box pelo menos 380 “data patterns” e deve também disponibilizar perfis que agrupam determinados padrões de forma a simplificar a criação de políticas. Por exemplo, deverá existir um perfil associado com o GDPR de forma a facilitar a monitorização de documentos que possam conter informação pessoal de utilizadores.				
Deverão existir os seguintes perfis out-of-the box: Bulk CCN, CCPA, Corporate Financial docs, Financial information, GDPR, GLBA, Healthcare, Intellectual Property, Legal, Malware, Personally-Identifiable Information, Profanity, Self Harm e Sensitive content				
A solução deverá ser constantemente atualizada com novos padrões e perfis.				
De forma a melhorar o rácio de deteção e eliminar falsos positivos a solução deverá permitir especificar: proximity keywords, níveis de confiança e expressões regulares básicas ou “weighted”.				
Este serviço deve poder ser consumido por diferentes plataformas do fabricante, nomeadamente, firewalls, serviço SASE(Secure Access Service Edge), CASB(Cloud Access Security Broker) e CSPM(Cloud Security Posture Management). Isto permitirá aplicar políticas de DLP transversais à organização.				
SD-WAN				
Deve ser possível através de licenciamento adicional adicionar um módulo de SD-WAN à plataforma.				
A plataforma deve permitir adicionar um overlay de SD-WAN que permita escolher de forma inteligente e dinâmica os links mais apropriados para envio de tráfego.				
Deve ser possível criar regras de SD-WAN por aplicação e definir os requisitos mínimos para cada link. No caso de os requisitos mínimos não serem cumpridos pelo link em uso, deve ser feito o failover do tráfego automaticamente.				
Para os links deve ser possível monitorizar e definir regras com base em: latência, jitter e perda de pacotes.				
A plataforma deve permitir fazer load-sharing através de múltiplos links de forma a melhorar o aproveitamento da largura de banda disponível.				
As firewalls devem suportar a funcionalidade de zero-touch provisioning.				
A plataforma deve disponibilizar informação sobre a performance das aplicações e links.				
Esta funcionalidade deve ser gerida centralmente através de uma única consola				
Deve ser suportada a funcionalidade de Packet duplication, o que permite a um equipamento enviar o mesmo pacote em links diferentes. O equipamento que recebe ambos os pacotes deverá descartar o último a chegar.				
Deve ser suportada a funcionalidade de Forward Error Correction.				
Relatórios & Logs				
A appliance deve ter a capacidade gerar relatórios tanto predefinidos ou personalizados, utilizando os logs criados pelo próprio equipamento sem necessidade de equipamentos externos adicionais				



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se cumpre		Nome do Documento do fabricante	Nº da Página
	SIM	NÃO		
Deve ser possível gerar relatórios de atividade por utilizador, incluindo aplicações utilizadas e páginas web visitadas				
Deve ser possível gerar relatórios de forma automática assim como agrupar vários relatórios num único documento em formato pdf				
Entre os relatórios disponíveis devem constar relatórios com a largura de banda consumida pelas diferentes aplicações, relatórios sobre as origens e destinos geográficos das ameaças detetadas e relatórios sobre a análise do comportamento do tráfego observado que permita detetar equipamentos comprometidos que participem em botnets				
Deve ser possível programar o momento em que se deseja a geração do relatório pretendido e o seu envio através de e-mail, assim como o intervalo temporal que se pretende				
Possibilidade de armazenar os logs localmente tendo por única restrição a capacidade do disco do próprio equipamento				
Possibilidade de enviar logs para uma plataforma externa de gestão e processamento especializado de logs com o objetivo de manter os logs a longo prazo				
Capacidade de dispor de um painel de instrumentos personalizável por utilizador de administração da appliance com pelo menos a seguinte informação: Aplicações mais utilizadas, Aplicações de alto risco, Informação geral do sistema, Estado das interfaces, Logs relativos às ameaças mais observadas, Logs de URLs filtrados, Recursos do sistema				
Capacidade de dispor de estatística gerada a partir de logs, personalizável por utilizador que permita fornecer informações como: utilizadores que mais geram tráfego, regras de segurança que mais utilizam, vulnerabilidades mais detetadas e bloqueadas, equipamentos que acederam a domínios maliciosos, vírus detetados, informação enviado ao serviço de sandboxing e equipamentos internos comprometidos				
Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance de forma que a partir dos logs criados se possa obter informações de alto nível.				
Outras Funcionalidades				
Possibilidade de definir aplicações e/ou vulnerabilidades customizadas mediante diferentes parâmetros como: Portos TCP/UDP que sejam usados na aplicação e combinação de padrões dentro dos "headers" dos pacotes ou mesmo no "payload" dos próprios pacotes que se devam cumprir para que se reconheça a aplicação e/ou vulnerabilidade				
Suporte para TLS 1.3 e capacidade de descriptar este tráfego				
Possibilidade de decifrar tráfego SSL e SSH de forma que se possa estabelecer políticas de descriptação baseadas em: zonas por onde passa o tráfego, IP de origem ou destino, utilizadores geram esse tráfego, portos utilizados.				
Capacidade de criar exceções à descriptação para determinado tipo de tráfego.				
Capacidade de decifrar tráfego com destino a sites web que utilizam certificados de curva elíptica (ECC).				



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se cumpre		Nome do Documento do fabricante	Nº da Página
	SIM	NÃO		
Possibilidade de enviar tráfego após descriptação para uma interface de port mirror para análise de terceiras partes.				
Capacidade de capturar tráfego em formato pcap, podendo ser estabelecido como critérios de captura do tráfego, uma determinada aplicação independentemente da origem ou destino desse tráfego.				
Capacidade de capturar tráfego em formato pcap exclusivamente quando se deteta um vírus ou um ataque em qualquer um dos motores de proteção.				



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Anexo III

Modelos relativos à caução prevista no artigo 12.º

Modelo de guia de depósito bancário

Euros _____ €

Vai _____ (nome do adjudicatário), com sede em _____ (morada), depositar na _____ (sede, filial, agência ou delegação) do Banco _____ a quantia de _____ (por algarismos e por extenso) em dinheiro/em títulos _____ (eliminar o que não interessar), como caução exigida para _____ (identificação do procedimento), nos termos do artigo 90.º do Código dos Contratos Públicos. Este depósito, sem reservas, fica à ordem de _____ (entidade adjudicante), a quem deve ser remetido o respetivo conhecimento.

[Data e assinatura do(s) representante(s) legal(ais)]

Modelo de garantia bancária/seguro de caução

Garantia bancária/seguro de caução n.º _____

Em nome e a pedido de _____ (adjudicatário), vem o(a) _____ (instituição garante), pelo presente documento, prestar, a favor de _____ (entidade adjudicante beneficiária), uma garantia bancária/seguro-caução (eliminar o que não interessar), até ao montante de _____ (por algarismos e por extenso), destinada(o) a caucionar o integral cumprimento das obrigações assumidas pelo(s) garantido(s) no âmbito do _____ (identificação do procedimento), nos termos dos n.ºs 6 e 8/7 e 8 (eliminar o que não interessar) do artigo 90.º do Código dos Contratos Públicos.



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

A presente garantia corresponde a (...) % do preço contratual e funciona como se estivesse constituída em moeda corrente, responsabilizando-se o garante, sem quaisquer reservas, por fazer a entrega de toda e qualquer importância, até ao limite da garantia, logo que interpelado por simples notificação escrita por parte da entidade beneficiária.

Fica bem assente que o banco/companhia de seguros (eliminar o que não interessar) garante, no caso de vir a ser chamado(a) a honrar a presente garantia, não poderá tomar em consideração quaisquer objeções do(s) garantido(s), sendo-lhe igualmente vedado opor à entidade beneficiária quaisquer reservas ou meios de defesa de que o garantido se possa valer face ao garante.

A presente garantia permanece válida até que seja expressamente autorizada a sua libertação pela entidade beneficiária, não podendo ser anulada ou alterada sem esse mesmo consentimento e independentemente da liquidação de quaisquer prémios que sejam devidos.

[Data e assinatura do(s) representante(s) legal(ais)]