

SÍLVIA
CATARINA
ANDRÉ
SOUSA VALE
PEREIRA

Assinado de
forma digital
por SÍLVIA
CATARINA
ANDRÉ SOUSA
VALE PEREIRA

**Concurso Público
com publicidade internacional**

Proc.º 29/UMC/2022

**Aquisição da Atualização da infraestrutura de segurança e desenvolvimento da capacitação
técnica da
Secretaria-Geral do Ministério da Economia e do Mar em tecnologia Check Point**

Caderno de Encargos

PARTE I

CLÁUSULAS JURÍDICAS

CAPÍTULO I

DISPOSIÇÕES GERAIS

Cláusula 1.^a

Objeto

O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar, na sequência do procedimento pré-contratual que tem por objeto principal a aquisição da atualização da infraestrutura de segurança e desenvolvimento da capacitação técnica da Secretaria-Geral do Ministério da Economia e do Mar, em tecnologia Check Point, de acordo com enquadramento, requisitos e características técnicas constantes da Parte II do Caderno de Encargos.

Cláusula 2.^a

Preço base

1. O preço base do procedimento, que corresponde ao preço máximo que a entidade adjudicante se dispõe a pagar para a aquisição da atualização da infraestrutura de segurança e desenvolvimento da capacitação técnica da Secretaria-Geral do Ministério da Economia e do Mar em tecnologia Check Point, é de € 266.000,00 (duzentos e sessenta e seis mil euros), ao qual acresce o de IVA à taxa em vigor.
2. O preço base do procedimento corresponde ao somatório dos preços unitários máximos, de acordo com os encargos parciais do quadro infra, não podendo os preços base unitários máximos indicados ser ultrapassados, nem o preço base do procedimento.
3. Deste modo, o preço máximo que a entidade adjudicante se dispõe a pagar, no período contratual de 36 meses, envolve os seguintes encargos parciais:

Componentes e Serviços	Preço Base Unitário
Componente hardware	104 500,00 €
Componente Software(aquisição/Subscrição)	70 000,00 €
Componente de Formação	32 000,00 €
Serviços de instalação e configuração de equipamento	16 250,00 €
Suporte e manutenção técnica da nova infraestrutura	43 250,00 €
Preço Base Total	266 000,00 €

4. Pelo fornecimento dos bens e prestação dos serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, o contraente público deve pagar ao cocontratante o preço constante da proposta adjudicada, que tem de ser igual ou inferior ao preço máximo definido no presente caderno de encargos, acrescido de IVA à taxa legal em vigor.
5. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, englobando despesas de alojamento, alimentação e deslocação de meios humanos, transporte, armazenamento e manutenção de meios materiais, seguros, impostos ou taxas (excluindo IVA) bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licença.

Cláusula 3.^a

Condições de Pagamento

1. O pagamento será efetuado após a instalação e configuração do equipamento a fornecer e ativação do licenciamento, excetuando o pagamento do valor correspondente ao suporte e manutenção técnica da nova infraestrutura, cujo pagamento será repartido em três tranches, pelos 36 meses do contrato, realizando-se dois pagamentos, respetivamente, nos meses de fevereiro e novembro, relativamente à primeira e segunda tranches, no decorrer do ano 2023, e o pagamento da última tranche, no decorrer do ano 2024.
2. Em caso de discordância, por parte do contraente público, quanto aos valores indicados na(s) fatura(s), este comunicará ao cocontratante, por escrito, os respetivos fundamentos, ficando o cocontratante obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
3. A(s) fatura(s) são emitida(s) em nome do contraente público adquirente - Secretaria-Geral do Ministério da Economia e do Mar, onde deve(m) constar obrigatoriamente, sob pena de devolução das mesmas, os seguintes elementos:
 - a) Número de identificação fiscal do contraente público;
 - b) Número do Compromisso;
 - c) PEP.
4. As faturas devem ser remetidas para o Portal da Fatura Eletrónica da Administração Pública - FEAP, quando o cocontratante se encontre registado no mesmo, ou por meio eletrónico para faturacao.dsf@sgeconomia.gov.pt ou via postal para a morada do contraente público, devendo ser privilegiado um dos dois primeiros meios indicados.
5. Desde que devidamente emitidas e observado o disposto na presente cláusula, a(s) fatura(s) são pagas através de transferência bancária.
6. No caso de não cumprimento por parte do contraente público do estipulado no número anterior, incidirão sobre o montante em dívida e durante o tempo em que o atraso se mantiver, juros de mora à taxa legal em vigor, nos termos previstos na Lei n.º 3/2010, de 27 de abril e no Decreto-Lei nº 62/2013, de 10 de maio.
7. O contraente público procederá, única e exclusivamente, ao pagamento dos serviços que efetivamente venham a ser prestados e dos bens que efetivamente lhe sejam fornecidos.

Cláusula 4.^a

Prazo e vigência do contrato

O contrato produz efeitos no dia seguinte ao da sua assinatura e é válido pelo período de 36 meses, em conformidade com os respetivos termos e condições e o disposto na lei, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato.

Cláusula 5.^a

Local de entrega dos bens e prestação de serviços

1. A entrega dos bens e a prestação dos serviços objeto do presente procedimento será realizada nas instalações da Secretaria-Geral do Ministério da Economia e do Mar, sita na Av. da República, n.º 79, 1069-218 Lisboa e nas instalações do DataCenter da IP Telecom (site de Disaster Recovery da Secretaria-

Geral), sitas na Rua Azevedo Pinto (antiga estação de Caminho de Ferro), em Viseu. Em alternativa, os serviços podem ser prestados, através de acesso remoto, sempre que a mesma se verifique viável.

2. O contraente público reserva-se o direito de alterar o local de execução mediante prévia comunicação ao cocontratante.

CAPÍTULO II
OBRIGAÇÕES CONTRATUAIS
SECÇÃO I
OBRIGAÇÕES DO COCONTRATANTE
Cláusula 6.^a

Obrigações do cocontratante

Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorrem para o cocontratante as seguintes obrigações:

- a) Entregar os bens e prestar os serviços em conformidade com as especificações constantes do Caderno de Encargos;
- b) Recorrer a todos os meios humanos e materiais que sejam necessários e adequados à execução da prestação de bens e serviços;
- c) Comunicar antecipadamente, logo que tenha conhecimento, ao contraente público, os factos que tornem total ou parcialmente impossível o cumprimento do presente Caderno de Encargos ou do Contrato a celebrar;
- d) Não alterar as condições da entrega dos bens e a prestação dos serviços fora dos casos previstos no presente Caderno de Encargos;
- e) Não subcontratar, no todo ou em parte, a execução do contrato sem a prévia autorização do contraente público;
- f) Comunicar qualquer facto que ocorra durante a execução do contrato e que altere, designadamente, a sua denominação e sede social, os seus representantes legais, a sua situação jurídica e a sua situação comercial, bem como as alterações aos contatos e moradas indicados para efeitos de celebração do contrato;
- g) Possuir todas as autorizações, consentimento, aprovações, registos e licenças necessárias para o pontual cumprimento das obrigações assumidas;
- h) Reserva-se ao contraente público o direito de executar as diligências que considerar necessárias para verificar a aplicação das condições fixadas na proposta adjudicada ao cocontratante.

Cláusula 7.^a

Requisitos e Especificações

Os requisitos e especificações da prestação de serviços e entrega dos bens, são os constantes da Parte II ao presente caderno de encargos, que dele faz parte integrante.

Cláusula 8.^a

Patentes, Licenças e Marcas Registadas

1. São da responsabilidade do cocontratante quaisquer encargos decorrentes da utilização, no fornecimento de marcas registadas, patentes registadas ou licenças, ou direitos de autor.

2. Caso o contraente público venha a ser demandado por ter infringido, na execução do Contrato, qualquer dos direitos mencionados no número anterior, o cocontratante indemniza-o de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar seja a que título for.

Cláusula 9^a

Responsabilidade do cocontratante pelos prejuízos

O cocontratante é responsável, a título criminal e civil, objetiva ou subjetivamente, ou outra, por todos os prejuízos e danos, patrimoniais e não patrimoniais, causados ao contraente público ou a terceiros que, por qualquer motivo, resultem da sua atividade, atuação dos seus trabalhadores ou deficiente execução dos serviços objeto do contrato.

Cláusula 10^a

Conformidade e garantia técnica

O cocontratante fica sujeito, com as devidas adaptações e no que se refere aos elementos entregues ao contraente público em execução do contrato, às exigências legais, obrigações do fornecedor e prazos respetivos aplicáveis aos contratos de aquisição de bens e serviços, nos termos da legislação em vigor.

Cláusula 11.^a

Dever de sigilo

1. O cocontratante deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa ao contraente público, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.
2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem ser objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
3. O dever de sigilo mantém-se em vigor até ao termo do prazo de 3 (três) anos a contar do cumprimento ou cessação, por qualquer causa, do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.
4. Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo cocontratante ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou de outras entidades administrativas competentes.

Cláusula 12.^a

Despesas e encargos

1. Todas as despesas ou encargos em que o cocontratante tenha de incorrer para o cumprimento de obrigações emergentes do contrato são da sua exclusiva responsabilidade e não podem ser reclamados ao contraente público, a menos que outro regime decorra da lei ou do contrato.
2. Constitui, nomeadamente, responsabilidade do contratante, o pagamento de quaisquer impostos, taxas, direitos de qualquer natureza ou outros encargos exigidos pelas autoridades competentes e relativos à execução do contrato.

Cláusula 13.^a

Cumprimento do Regulamento Geral de Proteção de Dados (RGPD)

1. O cocontratante obriga-se a cumprir e a fazer cumprir o disposto no Regulamento Geral sobre a Proteção de Dados (RGPD), Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, no que respeita às regras relativas à proteção das pessoas singulares, ao tratamento de dados pessoais e à livre circulação desses dados, que entrou em vigor em 25 de maio de 2018.
2. Sempre que sejam remetidos dados pessoais, os mesmos devem ser acompanhados de declaração (**Anexo II** ao programa de procedimento) de consentimento para o tratamento dos dados para esta finalidade, por parte dos seus titulares.

SECÇÃO II

OBRIGAÇÕES DO CONTRAENTE PÚBLICO

Cláusula 14.^a

Obrigações do contraente público

Constituem obrigações do contraente público:

- a) Pagar, no prazo acordado, as faturas emitidas pelo cocontratante;
- b) Nomear um gestor do contrato e comunicar quaisquer alterações dessa nomeação;
- c) Monitorizar a execução do contrato no que respeita às condições acordadas e aplicar as devidas sanções em caso de incumprimento.

Cláusula 15.^a

Gestor do Contrato

1. Nos termos do artigo 290.º-A do Código dos Contratos Públicos, o contraente público designará um gestor de contrato, com a função de acompanhar permanentemente a execução deste.
2. Caso o gestor detete desvios, defeitos ou outras anomalias na execução do contrato, deve comunicá-los de imediato ao órgão competente, propondo em relatório fundamentado as medidas corretivas que, em cada caso, se revelem adequadas.
3. Antes do início de funções o gestor do contrato irá subscrever a declaração de inexistência de conflitos de interesse, conforme modelo previsto no n.º 7 do artigo 290.º-A do Código dos Contratos Públicos.
4. Sempre que seja necessário proceder à alteração do gestor do contrato, a entidade adjudicante pode proceder à respetiva alteração, através de ato administrativo, que comunicará ao adjudicatário.

CAPÍTULO III

SANÇÕES CONTRATUAIS E RESOLUÇÃO

Cláusula 16.^a

Sanções contratuais

1. Pelo incumprimento das obrigações decorrentes do contrato, o contraente público pode exigir ao cocontratante o pagamento de uma sanção pecuniária, no valor 20% do preço contratual.
2. Os incumprimentos deverão ser denunciados por escrito no prazo máximo de 48 horas a contar do seu conhecimento, e dados a conhecer ao cocontratante por fax, e-mail ou através de correio em carta registada com aviso de receção.

3. Na determinação da gravidade do incumprimento, o contraente público tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do cocontratante e as consequências do incumprimento.
4. As sanções contratuais previstas na presente cláusula não obstam a que o contraente público exiga uma indemnização pelo dano excedente.

Cláusula 17.^a

Cessão da posição contratual por incumprimento do cocontratante

1. Em caso de incumprimento, pelo cocontratante, das suas obrigações, que reúna os pressupostos para a resolução do contrato, o cocontratante deverá, caso o contraente público assim o entenda, ceder a sua posição contratual ao concorrente do procedimento pré-contratual na sequência do qual foi celebrado o contrato em execução, que venha a ser indicado pelo contraente público, pela ordem sequencial daquele procedimento, conforme no previsto no artigo 318.º-A do Código dos Contratos Públicos em vigor.
2. Para o efeito previsto na parte final do número anterior, o contraente público interpelará, gradual e sequencialmente, os concorrentes que participaram no procedimento pré-contratual original, de acordo com a respetiva classificação final, a fim de concluir um novo contrato para a adjudicação da conclusão dos trabalhos.
3. A execução do contrato ocorre nas mesmas condições já propostas pelo cedente no procedimento pré-contratual original.
4. A cessão da posição contratual opera por mero efeito de ato a proferir pelo contraente público, sendo eficaz a partir da data por este indicada.
5. Os direitos e obrigações do cocontratante, desde que constituídos em data anterior à da notificação do ato referido no número anterior, transmitem-se automaticamente para o cessionário na data de produção de efeitos daquele ato, sem que este a tal se possa opor.
6. As obrigações assumidas pelo cocontratante, depois da notificação referida no n.º 4, apenas vinculam a entidade cessionária quando este assim o declare, após a cessão.
7. A caução e as garantias prestadas pelo cocontratante inicial são objeto de redução na proporção do valor das prestações efetivamente executadas e são liberadas seis meses após a data da cessão, ou, no caso de existirem obrigações de garantia, após o final dos respetivos prazos, mediante comunicação dirigida pelo contraente público aos respetivos depositários ou emitentes.
8. A posição contratual do cocontratante nos subcontratos por si celebrados, transmite-se automaticamente para a entidade cessionária, salvo em caso de recusa por parte desta.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Cláusula 18.^a

Foro competente para a 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 19.^a

Legislação Aplicável

Em tudo o que não se encontre especialmente regulado no presente Caderno de Encargos, aplicar-se-á o regime previsto no Código dos Contratos Públicos, na sua redação atual, e demais legislação complementar, em razão do objeto do contrato.

PARTE II

ENQUADRAMENTO, REQUISITOS E CARACTERÍSTICAS TÉCNICAS

1. A atualização da infraestrutura de segurança (dados e comunicações) da Secretaria-Geral, baseada em tecnologia *Check Point*, envolve a aquisição de equipamento (hardware), licenciamento/subscrição de plataformas de gestão (software), aquisição de serviços de formação especializada e serviços de instalação e suporte técnico. Os bens e serviços a adquirir resumem-se nas seguintes vertentes essenciais, cujo enquadramento, requisitos e características técnicas se detalham:

Bem/Serviço	Qtd.	Descrição
Trade-in/refresh tecnológico de appliances 13500 para NGTX 16200 Plus (3 anos)		
CPAP-SG16200-PLUS-SNBT	2	16200 Plus Appliance with 5 Virtual Systems & SandBlast subscription pack for 1 year
CPCES-CO-STANDARD	6	CES Standard for 16200 Plus with 5 VS & SandBlast subscription package for 1 year
CPSB-SNBT-16200-PLUS-2Y	2	Next Generation Threat Prevention & Sandblast for 2 years for 16200 PLUS Appliance
Gateway para o site de Disaster Recovery - Appliance NGTX 6700 Plus (3 anos)		
CPAP-SG6700-PLUS-SNBT	1	6700 Plus appliance with SandBlast subscription package for 1 year
CPSB-MOB-U	1	Mobile Access Blade unlimited
CPCES-CO-STANDARD	3	CES Standard for 6700 Plus appliance with SandBlast subscription package for 1 year
CPCES-CO-STANDARD	3	CES Standard for Mobile Access Blade unlimited
CPSB-SNBT-6700-PLUS-2Y	1	Next Generation Threat Prevention & Sandblast for 2 years for 6700 PLUS Appliance
Expansão do cluster existente de SG 23500 NGTP para o site de Disaster Recovery		
CPAP-SG23500-NGTP	1	23500 Next Generation Threat Prevention Appliance
CPAC-RAM48GB-23500	1	Memory upgrade kit from 16GB to 64GB for 23500 appliance
CPSB-VS-10	2	10 Virtual Systems package
CPCES-CO-STANDARD	3	CES Standard for Memory upgrade kit from 16GB to 64GB for 23500 appliance
CPCES-CO-STANDARD	3	CES Standard for 23500 Next Generation Threat Prevention Appliance
CPCES-CO-STANDARD	6	CES Standard for 10 Virtual Systems package
CPSB-NGTP-23500-2Y	1	Next Generation Threat Prevention Package subscription for 2 years for 23500 Appliance
Formação presencial, exames de certificação (CCSA, CCSE, CCTA e CCTE) e workshops		
CCSA	1	Curso Check Point Security Administrator R80.40 (CCSA), 3 dias (3 x 7h), presencial
CCSA/SE	1	Curso Check Point CCSA & CCSE Bootcamp, 5 dias (5 x 7h), presencial
CCTA	2	Curso Check Point Troubleshooting Administrator (CCTA), 2 dias (2 x 7h), presencial
CCTE	1	Curso Check Point Troubleshooting Expert R80.40 (CCTE), 2 dias (2 x 7h), presencial
CPTS-TRN-CLC-2.5-1Y	2	Check Point CCSA exam voucher (2,5 CLC Credits)
CPTS-TRN-CLC-2.5-3Y	1	Check Point CCSE exam voucher (2,5 CLC Credits)
CPTS-TRN-CLC-2.5-1TY	2	Check Point CCTA exam voucher (2,5 CLC Credits)
CPTS-TRN-CLC-2.5-3TY	1	Check Point CCTE exam voucher (2,5 CLC Credits)
SEC-LRN-1-CCSA	2	Formação técnica, workshop CCSA do fabricante em Portugal
SEC-LRN-1-CCSE	2	Formação técnica, workshop CCSE do fabricante em Portugal
SEC-SEC-WKR-D	24	Formação técnica, workshops Check Point eSecurity, ministrada por CCSM/CCSE/CCTE

- 1.1. O equipamento objeto da presente aquisição irá funcionar em conjunto com o equipamento da mesma tecnologia, já instalado na infraestrutura existente na Secretaria-Geral do Ministério da Economia e do Mar.

1. Enquadramento e requisitos gerais

A Secretaria-Geral do Ministério da Economia e do Mar pretende renovar e reforçar a sua infraestrutura de cibersegurança de redes de dados e comunicações, quer ao nível do desempenho, quer alargando-a de forma estruturada e integrada ao site de *disaster recovery* em Viseu.

Atualmente, a referida infraestrutura está desenvolvida com produtos e serviços *Check Point*, pretendendo-se manter todos aqueles cujo suporte esteja assegurado pelo fabricante até ao final de 2025. Simultaneamente, pretende-se que, quer as componentes a manter, quer aquelas que serão fornecidas, continuem a ser geridas de forma nativa e integrada pelas atuais plataformas de gestão, reporte e logging de eventos, existentes e em produção em contexto de multidomínio (Provider-1), a saber: *Check Point Next Generation Security Management Multi-domain* para 50 gateways e 5 domínios, *Check Point Next Generation Security Management Multi-Log Manager* para 50 gateways e 10 domínios e *Check Point Next Generation Security Management SmartEvent dedicated Server* para 50 gateways, todas em software com licenciamento perpétuo.

Todas as soluções fornecidas deverão incluir uma garantia de 3 (três) anos cobrindo a resolução de problemas de mau funcionamento de hardware (incluindo substituição do equipamento) e software, o acesso a minor releases, updates, patches, hotfixes e similares, bem como a novas versões incluindo major releases.

Caso as funcionalidades propostas para cumprimento dos requisitos estejam sujeitas a licenciamento, perpétuo ou por subscrição, deverão estar incluídos todos os recursos e custos necessários para que as soluções funcionem incondicionalmente durante o referido período de 3 (três) anos.

2. Trade-in / refresh tecnológico

Considerando o final do ciclo de suporte das atuais firewalls de perímetro, *Check Point NGTP 13500* (duas), pretende-se efetuar o *trade-in* com *refresh* tecnológico para equipamentos atuais e cujo desempenho seja compatível com o exatável crescimento de necessidades de conectividade de uma forma generalizada, devendo por isso assegurar as seguintes características mínimas:

- Cluster de 2 nós de firewall de nova geração em alta disponibilidade com funcionalidades mínimas de:
 - Intrusion Prevention/Detection System (IPS/IDS);
 - Application Control e Web Security;
 - Antivírus e Antibots;
 - Proteção contra ameaças do tipo *zero-day* através de sanitização de ficheiros e sandboxing, com deteção ao nível do CPU e sistema operativo;
- Alta disponibilidade com nós em activo/activo (layer2), activo/passivo (layer 2 e layer 3);
- Failover de sessões por alteração de rotas ou falha de dispositivo ou link;
- Possibilidade de segregação com um mínimo de 20 virtual systems (possível licenciamento adicional);
- Suporte IPv4 e IPv6 (incluindo NAT66, NAT64 e NAT46);
- Hardware appliances rack mountable com um máximo de 4 U (total do cluster);
- Throughput de 12 Gbps com todas a funcionalidades de proteção ativas;

- Throughput de 20 Gbps em modo de Next Generation Firewall (IPS+App Control);
- Throughput de 50 Gbps em modo Firewall (rules only);
- Oito portas Ethernet / RJ45 (cobre) a 1 Gbps;
- Oito portas Ethernet SFP+ (fibra) a 10 Gbps (incluindo os transceivers em *short-range*);
- Porta de gestão out-of-band ou lights-out-management (LOM);
- Possibilidade de expansão com portas a 25/100 Gbps e/ou 40 Gbps (mínimo de duas);
- Fontes de alimentação hot-swappable redundantes;
- Discos internos redundantes SSD com mínimo de 480 GB;
- Integração direta de diretórios de utilizadores/recursos: Microsoft Active Directory e RADIUS;
- Políticas sobre utilizadores remotos e on-premise com Windows, macOS, Linux, Android e Apple iOS;
- Integração com appliance *Check Point Sandblast Networking TE-1000X* para reencaminhamento de ficheiros para sandboxing local (on-premise).

3. Gateway para o site de *disaster recovery*

O novo cluster de equipamentos a fornecer no *trade-in* (ponto 2.) deverá ser funcionalmente complementado por 1 (um) firewall adicional a instalar no site de *disaster recovery*, em Viseu, que permita replicar de forma simplificada e adaptada todas as políticas, regras, objetos, funcionalidades e acesso a recursos em cenários de desastre, sem quebra assinalável do desempenho da gateway de Internet, devendo por isso assegurar as seguintes características mínimas:

- Firewall de nova geração em alta disponibilidade com funcionalidades mínimas de:
 - Intrusion Prevention/Detection System (IPS/IDS);
 - Application Control e Web Security;
 - Antivírus e Antibots;
 - Proteção contra ameaças do tipo *zero-day* através de sanitização de ficheiros e sandboxing, com deteção ao nível do CPU e sistema operativo;
- Possibilidade de segregação com um mínimo de 20 virtual systems (possível licenciamento adicional);
- Suporte IPv4 e IPv6 (incluindo NAT66, NAT64 e NAT46);
- Hardware appliance rack mountable com um máximo de 1 U;
- Throughput de 5 Gbps com todas a funcionalidades de proteção ativas;
- Throughput de 12,5 Gbps em modo de Next Generation Firewall (IPS+App Control);
- Throughput de 25 Gbps em modo Firewall (rules only);
- Oito portas Ethernet / RJ45 (cobre) a 1 Gbps;
- Quatro portas Ethernet SFP+ (fibra) a 10 Gbps (incluindo os transceivers em *short-range*);
- Porta de gestão out-of-band / lights-out-management (LOM);
- Possibilidade de expansão com portas a 40 Gbps (mínimo de duas);
- Fontes de alimentação hot-swappable redundantes;
- Disco interno SSD com mínimo de 480 GB;
- Integração direta de diretórios de utilizadores/recursos: Microsoft Active Directory e RADIUS;
- Políticas sobre utilizadores remotos e on-premise com Windows, macOS, Linux, Android e Apple iOS;

- Possibilidade de integração com appliance *Check Point Sandblast Networking TE-1000X*, appliance virtual de Sandblast Networking ou serviço na Cloud para reencaminhamento de ficheiros para sandboxing (on-premise ou Cloud).

4. Expansão do cluster existente 23500 NGTP para o site de *disaster recovery*

Para complemento funcional do site de disaster recovery, em Viseu, pretende-se adicionar 1 (um) novo nó de firewall ao cluster existente, que assegura a proteção ao nível da rede interna e composto por hardware appliances NGTP 23500 da *Check Point*, permitindo estender esse cluster geograficamente ao site de Viseu e aplicar simplificadaamente todas as políticas, regras, objetos, funcionalidades e acesso a recursos em cenários de desastre, sem quebra do nível de desempenho, devendo por isso assegurar as seguintes características mínimas:

- Firewall de nova geração em alta disponibilidade com funcionalidades mínimas de:
 - Intrusion Prevention/Detection System (IPS/IDS);
 - Application Control e Web Security;
 - Antivírus e Antibots;
- Possuir 20 virtual systems (contextos/domínios) incluídos.
- Suporte IPv4 e IPv6 (incluindo NAT66, NAT64 e NAT46);
- Hardware appliance rack mountable com um máximo de 2 U;
- Throughput de 10 Gbps com todas as funcionalidades de proteção ativas;
- Throughput de 12,5 Gbps em modo de Next Generation Firewall (IPS+App Control);
- Throughput de 50 Gbps em modo Firewall (rules only);
- Oito portas Ethernet / RJ45 (cobre) a 1 Gbps;
- Duas portas Ethernet SFP+ (fibra) a 10 Gbps (incluindo os transceivers em *short-range*);
- Porta de gestão out-of-band / lights-out-management (LOM);
- Possibilidade de expansão com portas a 25/100 Gbps e/ou 40 Gbps (mínimo de duas);
- Fontes de alimentação hot-swappable redundantes;
- Dois discos internos de 1 TB cada em Raid-1;
- Integração direta de diretórios de utilizadores/recursos: Microsoft Active Directory e RADIUS;
- Políticas sobre utilizadores remotos e on-premise com Windows, macOS, Linux, Android e Apple iOS;
- Possibilidade de integração com appliance *Check Point Sandblast Networking TE-1000X*, appliance virtual de Sandblast Networking ou serviço na Cloud para reencaminhamento de ficheiros para sandboxing (on-premise ou Cloud).

5. Capacitação técnica das equipas internas do Ministério da Economia e do Mar e dos organismos associados

Com o objetivo de capacitar as equipas internas de IT com um nível de conhecimento que permita uma maior autonomia em relação a fornecedores externos, reduzindo por consequência os prazos de resposta na resolução de incidentes e a dependência na execução de pedidos de alterações, pretende a Secretaria-Geral do Ministério da Economia e do Mar que seja ministrada formação aos seus

colaboradores e a colaboradores das equipas de IT de outros organismos da área governativa da Economia e do Mar, a si associados, nos seguintes termos:

- a) Formação em centro de formação autorizada do fabricante das tecnologias propostas, ministrada presencialmente nas instalações do centro, para:
- 1 [um(a)] formando(a) com o nível de “administração das soluções”, incluindo o respetivo exame de certificação;
 - 1 [um(a)] formando(a) com os níveis de “administração das soluções” e “expert/especialista das soluções”, incluindo os respetivos exames de certificação;
 - 2 [dois(duas)] formandos(as) com o nível de “administração de troubleshooting das soluções”, incluindo os respetivos exames de certificação;
 - 1 [um(a)] formando(a) com o nível de “especialista de troubleshooting as soluções”, incluindo o respetivo exame de certificação;

Caso o(s) centro(s) de formação autorizados não estejam localizados na cidade ou na zona da Grande Lisboa, deverá o concorrente suportar os custos de deslocação e estadia dos formandos.

- b) Duas ações de formação para o nível de “administração das soluções” em formato de workshop, a realizar pelo próprio fabricante das soluções ou por formadores por si indicados, ministrada presencialmente nas instalações da Secretaria-Geral ou em local por si indicado, com a duração mínima de 3 (três) dias cada, para elementos das equipas de IT da Secretaria-Geral e elementos das equipas de IT dos organismos;
- c) Duas ações de formação para o nível de “expert/especialista das soluções” em formato de workshop, a realizar pelo próprio fabricante das soluções ou por formadores por si indicados, ministrada presencialmente nas instalações da Secretaria-Geral ou em local por si indicado, com a duração mínima de 3 (três) dias cada, para elementos das equipas de IT da Secretaria-Geral e elementos das equipas de IT dos organismos;
- d) Diversas ações de formação técnica de *eSecurity* em formato de workshop de pelo menos 1/2 (meio-dia) para esclarecimento de dúvidas e treino especializado dos elementos das equipas de IT da Secretaria-Geral e dos organismos, ministrada presencialmente nas instalações da Secretaria-Geral ou em local por si indicado, com um total de 24 (vinte e quatro) dias de duração acumulada.

Estas ações de formação deverão ser ministradas por técnicos com a certificação mínima de “expert/especialista das soluções” ou superior, com uma experiência mínima de três anos.

Apesar do concorrente ser convidado a sugerir a planificação das ações de formação ao longo do tempo, será da exclusiva competência da Secretaria-Geral a definição da sequência efetiva dessas mesmas ações de formação, independentemente do seu formato e audiência, podendo a Secretaria-Geral utilizar os meios de formação que ficarão ao seu dispor durante o prazo de garantia das soluções, ou seja três anos.

6. Serviços do projeto

O concorrente deverá considerar todos os serviços necessários à instalação e configuração das novas componentes da arquitetura de segurança da Secretaria-Geral, bem como todos os ajustes necessários

na infraestrutura existente e em produção, que garanta a integração, compatibilização e funcionamento das novas componentes.

No âmbito dos referidos serviços, deverão ser consideradas, ainda que não exclusivamente, as seguintes tarefas:

- Levantamento dos pré-requisitos para a implementação;
- Identificação de possíveis riscos na implementação e desenho de medidas de mitigação;
- Definição do cronograma de implementação da solução;
- Preparação e instalação dos novos equipamentos no site principal;
- Integração das gateways do site principal nas consolas existentes de gestão, reporting e logging;
- Transferência de configurações para novos equipamentos e descomissionamento dos substituídos;
- Instalação e configuração de todas as componentes e funcionalidades necessárias ao cumprimento dos requisitos definidos nas especificações técnicas;
- Revisão de políticas que permitam a implementação do disaster recovery;
- Preparação e instalação dos novos equipamentos no site de disaster recovery;
- Integração das gateways do site de disaster recovery nas consolas existentes;
- Ajuste das políticas existentes no site principal para correto funcionamento da arquitetura global;
- Implementação das novas políticas que materializem os cenários de disaster recovery;
- Testes e ajustes de configurações;
- Definição e configuração de relatórios;
- Documentação da solução.

Os serviços de instalação e configuração deverão ser realizados em horários adequados ao tipo de tarefas a executar, nomeadamente tendo em consideração eventuais interrupções ou riscos de interrupção de serviços.

Os serviços técnicos de instalação, configuração, migração, formação ou outros só poderão ser executados por técnicos devidamente habilitados e certificados pelos fabricantes das soluções propostas.