ASSEMBLEIA DA REPÚBLICA

CADERNO DE ENCARGOS

Concurso Público

com Publicidade Internacional

DIT/2022/6

REFORMULAÇÃO DA INFRAESTRUTURA

DE SEGURANÇA INFORMÁTICA DA REDE DA ASSEMBLEIA DA REPÚBLICA

Índice

PARTE I
CLÁUSULAS JURÍDICAS

Cláusula 1.ª
Objeto

1. O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento acima identificado, que tem por objeto a *"reformulação da infraestrutura de segurança informática da rede da Assembleia da República"*, de acordo com as características técnicas definidas na Parte II – Requisitos Técnicos, do presente caderno de encargos.
2. Está incluído no objeto deste procedimento a remoção, recolha, transporte e tratamento, pelo adjudicatário, dos bens a substituir, como lixo tecnológico, de acordo com a legislação ambiental aplicável.

Cláusula 2.ª
Local da entrega e da instalação dos bens

1. O objeto deste procedimento será realizado nas instalações da Assembleia da República, sitas no Palácio de S. Bento, Largo das Cortes, 1249-068 em Lisboa.
2. Os bens deverão ser entregues no horário normal de expediente da entidade adjudicante.
3. Todas as despesas e custos com o transporte do bem objeto do contrato e respetivos documentos para o local de entrega são da responsabilidade do adjudicatário.

Cláusula 3.ª
Prazo de execução

1. O fornecimento dos bens e prestação dos serviços de instalação objeto do presente procedimento, deverão ser integralmente executados dentro do prazo indicado pelo adjudicatário na respetiva proposta, que não poderá ser superior a 12 (doze) semanas.
2. O prazo referido no número anterior deverá ser contado a partir da data da notificação ao adjudicatário da decisão de adjudicação, sob pena de aplicação das penalidades constantes na cláusula 16.ª.
3. Para efeitos do número anterior, cada período de 1 (uma) semana equivalerá a 7 (sete) dias contados de forma corrida, incluindo feriados e fins de semana.

Cláusula 4.ª
Requisitos técnicos

Os equipamentos a fornecer devem cumprir na íntegra, sob pena de exclusão das respetivas propostas, os Requisitos Técnicos definidos na Parte II do presente caderno de encargos, não sendo aceites propostas de configuração, ou com requisitos, diferenciados dos aí previstos.

Cláusula 5.ª
Condições de pagamento e preço base

1. A Assembleia da República pagará ao adjudicatário o preço total constante da respetiva proposta, o qual não poderá exceder os 280.000,00€ (duzentos e oitenta mil euros), acrescidos de IVA à taxa legal aplicável.
2. O pagamento do preço referido no número anterior será levado a cabo, de uma só vez, uma vez concluído e aceite pela Assembleia da República, o fornecimento e a instalação da totalidade dos equipamentos objeto do presente procedimento.
3. O pagamento será realizado pela Assembleia da República no prazo de 30 (trinta) dias após a apresentação pelo adjudicatário da fatura correspondente, desde que apresentada nos termos adequados à sua liquidação.
4. Em caso de discordância por parte da Assembleia da República quanto aos valores indicados na fatura, deve esta comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando o adjudicatário obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.

Cláusula 6.ª
Verificação dos bens

1. Os bens fornecidos e respetivos serviços de instalação, devem estar em conformidade com as respetivas características, especificadas em sede de proposta e de contrato, reservando-se a AR, a todo o tempo, ao direito de proceder às verificações que tiver por convenientes.
2. O adjudicatário obriga-se a substituir, sem qualquer encargo para a AR, os bens fornecidos que não cumpram os requisitos de qualidade oferecidos ou que apresentem qualidade insuficiente.
3. Todos os encargos com a substituição, a devolução ou a destruição dos bens rejeitados, são da exclusiva responsabilidade do adjudicatário.
4. As verificações efetuadas não excluem a obrigação de eventuais reparações, substituição de peças ou de outros elementos do circuito ao abrigo da garantia.

Cláusula 7.ª
Inspeção

1. Efetuado o fornecimento, montagem e instalação dos bens aqui em questão e de todas as suas componentes a AR, por si ou através de terceiro por ela designado, procede no prazo de 5 dias úteis à inspeção quantitativa e qualitativa dos mesmos, com vista a verificar se reúnem as características, especificações e requisitos técnicos e operacionais exigidos no presente caderno de encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei.
2. As inspeções a que se refere o número anterior serão efetuadas através da realização de testes.
3. Durante a fase de realização de testes, o adjudicatário deve prestar à AR, toda a cooperação e todos os esclarecimentos necessários, podendo fazer-se representar por colaboradores devidamente credenciadas para o efeito.

Cláusula 8.ª
Inoperacionalidade, defeitos ou discrepâncias

1. No caso de a inspeção quantitativa e qualitativa prevista na cláusula anterior não comprovarem a total operacionalidade do equipamento fornecido e de todas as suas componentes, bem como a sua conformidade com as exigências legais, ou no caso de existirem defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no presente caderno de encargos, a AR deve disso informar por escrito o adjudicatário.
2. No caso previsto no número anterior, o adjudicatário deve proceder à sua custa e no prazo de dois dias a contar da comunicação, às reparações ou substituições necessárias, sob pena de, findo esse prazo se considerarem rejeitados os bens e serviços em questão, não sendo conferido ao adjudicatário qualquer direito a indemnização ou compensação.
3. Após a realização das reparações ou substituições necessárias a AR procede à realização de nova inspeção e testes nos termos da cláusula anterior.

Cláusula 9.ª
Aceitação do fornecimento e dos serviços

Verificando-se a total operacionalidade do equipamento fornecido e todas as suas componentes, bem como a sua conformidade com as exigências legais, a AR emite auto de aceitação, conforme minuta que constitui o anexo I do presente caderno de encargos e que deste faz parte integrante, no prazo máximo de 5 dias a contar do final dos testes, que deve ser assinado por ambas as partes.

Cláusula 10.ª
Sigilo e Confidencialidade

1. O adjudicatário obriga-se a guardar sigilo e confidencialidade sobre todos os assuntos previstos no objeto do contrato, e a tratar como confidenciais todos os documentos e informações a que tenha acesso no âmbito da sua execução, abrangendo esta obrigação os seus agentes, funcionários, colaboradores ou terceiros que se encontrem envolvidos no fornecimento ou no procedimento ao qual o mesmo deu origem.
2. Para além das ações penais e processos disciplinares que ao caso couber, o adjudicatário pagará à Assembleia da República uma compensação pela divulgação, seja por que meio for, de factos e informações relativos a esta última, aos Deputados, funcionários ou outros agentes a ela vinculados, num montante calculado pela seguinte fórmula: **C = RMMG x 50**, em que **"C"** corresponde ao montante da compensação (em euros) e **"RMMG"** corresponde ao valor da remuneração mínima mensal garantida em vigor.
3. O disposto no número anterior não é aplicável em caso de imposição legal ou judicial de comunicação de factos sigilosos, desde que sejam cumpridos os estritos termos e objetivos inerentes à obrigação de comunicação.
4. A aplicação pela Assembleia da República da compensação prevista no n.º 2 da presente cláusula, obedece às regras previstas no presente caderno de encargos para a aplicação de penalidades.

Cláusula 11.ª
Proteção de dados

1. O adjudicatário compromete-se a assegurar cumprimento das obrigações decorrentes da legislação de proteção de dados aplicável, em particular, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27/4 de 2016, (adiante, RGPD), bem como, a Lei de Execução Nacional aprovada pela Lei n.º 58/2019, de 8 de agosto, durante a vigência do contrato, nomeadamente as seguintes, conforme anexo II do presente caderno de encargos:
    a) Garantir a confidencialidade dos dados pessoais a que tenha ou venha a ter acesso por via do presente contrato, ou qualquer ato relacionado direta ou indiretamente a decorrer deste, nomeadamente, assegurando que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;

b) Tratar os dados pessoais a que tenha acesso por via do presente, apenas para as finalidades previstas no presente contrato e segundo as instruções da Assembleia da República;
c) Informar a Assembleia da República, caso considere que alguma das instruções por esta providenciada possa dar origem ao incumprimento da legislação aplicável em matéria de proteção de dados pessoais;
d) Implementar as medidas técnicas e organizativas de segurança, adequadas a assegurar a confidencialidade, a integridade e a disponibilidade dos dados pessoais, bem como a resiliência dos sistemas e serviços de tratamento, designadamente as previstas no artigo 32.º do RGPD, a fim de impedir a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, bem como, qualquer outra forma de tratamento ilícito dos dados pessoais;
e) Não subcontratar o tratamento de dados pessoais da entidade adjudicante, sem a sua prévia autorização escrita;
f) Em caso de autorização de subcontratação, impor ao subcontratado as obrigações em matéria de proteção de dados estabelecidas no presente contrato;
g) Notificar a Assembleia da República de quaisquer transferências de dados pessoais para país fora do Espaço Económico Europeu e que não apresente um nível adequado de proteção;
h) Informar a Assembleia da República, com a maior brevidade possível, em caso de efetivo ou potencial incidente de violação de dados pessoais;
i) Prestar assistência à Assembleia da República no sentido de permitir que esta cumpra a obrigação de dar resposta aos pedidos dos titulares dos dados, tendo em vista o exercício dos direitos previstos no RGPD, bem como as obrigações estabelecidas nos artigos 32.º a 36.º do RGPD;
j) Disponibilizar à Assembleia da República todas as informações necessárias para que sejam cumpridas todas as obrigações a que o Cocontratante esteja sujeito, contribuindo para auditorias, inspeções e demais fiscalizações conduzidas pelo Responsável pelo Tratamento, quando necessário e aplicável;
k) Sensibilizar o pessoal autorizado no âmbito do tratamento dos dados para as questões relacionadas com privacidade, proteção de dados e segurança da informação, garantindo ainda, a necessária formação ao correto manuseamento dos mesmos, e;
l) Finda a prestação de serviços, apagar ou devolver, segundo o critério da Assembleia da República, todos os dados pessoais tratados por sua conta, apagando as cópias existentes, sem prejuízo de conservação posterior que seja legalmente exigida.
m) Pelo contrato a celebrar, o adjudicatário declara possuir garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do RGPD e assegure a defesa dos direitos do titular dos dados.

n) O adjudicatário tratará dados pessoais por conta da Assembleia da República para as seguintes finalidades: "*reformulação da infraestrutura de segurança informática da rede da Assembleia da República.*

o) Para efeitos do presente caderno de encargos o adjudicatário tratará dados de identificação e contacto. pertencentes às seguintes categorias de titulares de dado: funcionários parlamentares.

Cláusula 12.ª
Casos fortuitos ou de força maior

1. Nenhuma das partes incorrerá em responsabilidade se, por caso fortuito ou de força maior, designadamente greves ou outros conflitos de trabalho, for impedido de cumprir as obrigações assumidas no contrato.
2. A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para restabelecer a situação.
3. Quando uma das partes não aceite por escrito que certa ocorrência invocada pela outra constitua força maior, cabe a esta fazer prova do mesmo.
4. A verificação de uma situação de 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.
5. Caso a impossibilidade de execução do contrato, em resultado de força maior, se prolongue por um período continuo superior a um mês, qualquer das partes pode proceder à respetiva resolução, mediante comunicação enviada à outra parte, com pelo menos 5 (cinco) dias de antecedência.

Cláusula 13.ª
Patentes, licenças e marcas registadas

1. São da responsabilidade da Entidade Adjudicatária quaisquer encargos decorrentes da utilização, no fornecimento, de marcas registadas, patentes registadas ou licenças.
2. Caso a Entidade Adjudicante venha a ser demandada por ter infringido a execução do contrato, qualquer dos direitos mencionados no número anterior, a Entidade Adjudicatária indemniza-a de todas as despesas.
3. Todos os equipamentos entregues têm que ser novos, adquiridos através dos canais oficiais e com suporte assegurado pelo menos em back-to-back com os respetivos fabricantes.

Cláusula 14.ª
Cessão da posição contratual

O adjudicatário não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do presente contrato sem autorização expressa da Assembleia da República, devendo para este efeito ser aplicado o regime previsto no Código dos Contratos Públicos.

Cláusula 15.ª
Resolução do contrato

1. A entidade adjudicante reserva-se ao direito de resolver o contrato em caso de incumprimento definitivo pelo(a) adjudicatário(a) das suas obrigações contratuais, nos termos do disposto na parte final do n.º 1 do artigo 325.º e ainda do disposto nos artigos 334.º, 335.º e 448.º do CCP.
2. Sem prejuízo de outros fundamentos de resolução previstos na lei, a AR pode resolver o contrato, a título sancionatório, no caso de o adjudicatário violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem.
3. Para os efeitos dos números anteriores, considera-se incumprimento definitivo do contrato pelo adjudicatário a ocorrência, entre outras, das seguintes situações:
   a) Atraso no fornecimento que exceda as 12 (doze) semanas fixadas como prazo máximo, no âmbito do presente caderno de encargos, para entrega da totalidade dos bens objeto do presente procedimento em condições de uso;
   b) Se os equipamentos fornecidos não corresponderem aos previstos na proposta do adjudicatário, ou se venha a apurar que não preenchem algum dos requisitos previstos na parte II do presente caderno e encargos e;
   c) O adjudicatário encontrar-se em estado de insolvência, liquidação, cessação de atividade ou qualquer outra situação análoga resultante de um processo de idêntica natureza, ou tenham o respetivo processo pendente.
4. A entidade adjudicante comunicará, por escrito, ao adjudicatário as deficiências do serviço, fixando um prazo para a sua regularização, findo o qual, se as anomalias não tiverem sido totalmente corrigidas, terá lugar a resolução do contrato que será comunicada ao adjudicatário, mediante carta registada com aviso de receção, na qual serão indicadas as razões que a entidade adjudicante considera justificativas da resolução.
5. Sem prejuízo da resolução do contrato nos termos previstos nos pontos anteriores, a entidade adjudicante mantém o direito ao pagamento das indemnizações e penalidades aplicáveis nos termos do presente caderno de encargos ou de qualquer disposição legal vigente.

Cláusula 16.ª
Penalidades

1. No caso de mora ou cumprimento defeituoso das obrigações objeto do contrato por parte do adjudicatário, poderá a Assembleia da República interpelar o adjudicatário para cumprir pontualmente com o fornecimento dos bens aqui em questão, quando tal ainda for possível e ainda se mantenha o interesse da Assembleia da República, devendo nesse caso o adjudicatário dar imediato cumprimento à referida interpelação, bem como suportar todos os danos que a Assembleia da República sofra na sequência de tais factos.
2. Sem prejuízo do disposto no número anterior, e da obrigação de indemnizar por parte do adjudicatário, no caso de incumprimento das obrigações fixadas no contrato e por causa imputável ao adjudicatário, poderá a Assembleia da República aplicar uma penalidade pecuniária a este último, calculada de acordo com a seguinte fórmula: P = V x A / 100.
3. Para os efeitos do número anterior: "P" corresponde ao montante da penalidade; "V" é igual ao preço contratual; e "A" é o número de dias em atraso no cumprimento da obrigação em causa.
4. As penalidades previstas no número anterior destinam-se a compelir o adjudicatário ao pontual cumprimento das prestações contratuais em falta e não põe em causa o ressarcimento de eventuais danos que se venham a apurar.
5. A aplicação de penalidades pela Assembleia da República nos termos previstos nos números anteriores, deverá ser precedida de comunicação endereçada ao adjudicatário, onde será feita menção à intenção de aplicação de penalidades, o seu valor, o respetivo fundamento e a indicação de que o mesmo dispõe de um prazo de 10 (dez) dias úteis para efeitos de exercício do seu direito de audiência prévia.
6. Decorrido o prazo de audiência prévia, deverá a entidade adjudicante comunicar ao adjudicatário se mantém, ou não, a aplicação das penalidades, e em caso afirmativo, conceder-lhe um prazo não inferior a 5 (cinco) dias úteis para levar a cabo o respetivo pagamento.

Cláusula 17.ª
Responsabilidade civil

O adjudicatário é responsável por todos e quaisquer danos causados à Assembleia da República ou a terceiros, resultantes de deficiências do sistema ou componentes dos equipamentos a fornecer objeto do presente procedimento.

Cláusula 18.ª
Garantia

1. O adjudicatário garantirá os bens fornecidos, sem qualquer encargo para a Assembleia da República, pelo prazo indicado na sua proposta, que não pode ser inferior a 2 (dois) anos, a contar da data efetiva de entrega dos bens, contra quaisquer defeitos ou discrepâncias com as exigências legais e com as características, especificações e requisitos técnicos definidos na **Parte II – Requisitos Técnicos** deste Caderno de Encargos.
2. São excluídos da garantia todos os defeitos que notoriamente resultarem de má utilização, de uma utilização abusiva ou de negligência da Assembleia da República, bem como todos os defeitos resultantes de fraude, ação de terceiros, de caso fortuito ou de força maior.
3. A garantia prevista no número 1 da presente cláusula, abrange:
   a) O fornecimento, a montagem ou a integração de quaisquer peças ou componentes em falta;
   b) A desmontagem de peças, componentes ou bens defeituosos ou discrepantes;
   c) A reparação ou a substituição das peças, componentes ou bens defeituosos ou discrepantes;
   d) O fornecimento, a montagem ou instalação das peças, componentes ou bens reparados ou substituídos;
   e) O transporte dos bens ou das peças ou componentes defeituosos ou discrepantes para o local da sua reparação ou substituição e a devolução daqueles bens ou a entrega das peças ou componentes em falta, reparados ou substituídos;
   f) A deslocação ao local da instalação ou de entrega e;
   g) A intervenção no dia útil seguinte à comunicação da ocorrência e nas instalações do cliente.

Cláusula 19.ª
Requisitos e certificações da entidade adjudicatária

1. Considerando a iteração e integração da solução a fornecer como um conjunto alargado de tecnologias existentes, a entidade adjudicatária deve possuir pelo menos 3 (três) das 4 (quatro) certificações/estatutos junto dos fabricantes abaixo indicados. A documentação comprovativa das certificações deverá ser válida à data da apresentação da proposta, com as seguintes classificações mínimas:
   - Check Point - 4 Star Partner;
   - Check Point - Certified Collaborative Support Partner (CCSP);
   - Cisco - Select Certified Partner;
   - Expert Partner ou equivalente, do fabricante da tecnologia proposta.
2. Paralelamente, a entidade adjudicatária deverá possuir pelo menos 1 (um) técnico certificado, em pelo menos 3 (três) das 4 (quatro) competências técnicas das principais áreas de integração da solução, a saber:

- Técnico certificado em tecnologia Check Point;
- Técnico certificado em tecnologia Cisco;
- Técnico certificado em tecnologia VMWare;
- Técnico certificado na tecnologia proposta.

3. A entidade adjudicatária deve possuir também, pelo menos, 1 (uma) acreditação de segurança conferida pela ANS e válida à data da apresentação da proposta, como forma de aferir a sua idoneidade e confiabilidade no acesso, manuseamento e guarda de informação sigilosa.
4. A entidade adjudicatária deverá ainda ser membro de uma rede de CSIRTs, de que é exemplo a Rede Nacional de CSIRT ou similar, que coordene a resposta a incidentes em entidades públicas, operadores de serviços essenciais e de infraestruturas críticas nacionais.

Cláusula 20.ª
Gestor do contrato

A Assembleia da República, dando cumprimentos ao previsto no artigo 290º-A do CCP, designará um gestor do contrato, com a função de acompanhar permanentemente a execução deste último.

Cláusula 21.ª
Prevalência

1. Fazem parte integrante do presente contrato o Caderno de Encargos e a proposta que for apresentada pelo adjudicatário, bem como os suprimentos dos erros e das omissões do Caderno de Encargos aceites pela Assembleia da República, os esclarecimentos e as retificações relativos ao Caderno de Encargos e os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
2. É aplicável aos documentos referidos no número anterior o disposto nos n.ºs 5 e 6 do artigo 96.º do Código dos Contratos Públicos.

PARTE II
REQUISITOS TÉCNICOS

1) Requisitos gerais

No âmbito do projeto, a proposta deverá considerar o fornecimento de uma solução de Firewall de CORE e Firewall de Internet, em ambiente híbrido, físico e virtual. A Firewall de CORE terá de ser de um fabricante distinto da Firewall de Internet que são equipamentos da marca Check Point. A sua instalação, configuração e integração na infraestrutura da Assembleia da República, garantindo o cumprimento dos objetivos definidos, bem como o suporte e manutenção nos termos definidos neste documento, pelo período de 36 (trinta e seis) meses, composta por:

- ITEM 1 - Solução Firewall CORE (Site Principal), nova solução;
- ITEM 2 - Solução Firewall CORE (Site de Disaster Recovery), nova solução;
- ITEM 3 - Consola Centralizada de Gestão das Firewalls de CORE (Site Principal e Site de Disaster Recovery), nova solução;
- ITEM 4 - Solução Firewall de perímetro Internet (Site Principal e Site Disaster Recovery) com funcionalidades de prevenção de ataques Zero-Day, upgrade e nova solução;
- ITEM 5 - Solução para automatização, verificação e gestão de políticas unificadas;
- ITEM 6 - Serviços de instalação, configuração, suporte e manutenção.

2) ITEM 1 - Firewall CORE (Site Principal)

A solução a fornecer deverá ser baseada em *appliances físicas (hardware)* numa arquitetura em *cluster*. Esta infraestrutura visa disponibilizar à Assembleia da República uma solução de firewall de CORE, proteção ao nível do datacenter, com as seguintes funcionalidades base:

- Cluster de firewall de 2 (duas) appliances físicas;
- Funcionalidades de *Unified Threat Protection*:
- Capacidade de segregação em ambientes virtuais, com um mínimo de 10 (dez);
- Gestão centralizada (através do ITEM 3);
- Suporte 24x7 e subscrições necessárias para as funcionalidades solicitadas com duração de 36 (trinta e seis) meses.

a) Requisitos, funcionalidades e capacidades da solução.

A solução efetuará a interligação com a infraestrutura da Assembleia da República, composta por 2 (dois) equipamentos do tipo All-in-one/Unified Threat Management (Firewall, Threat Protection [IPS, Web-filtering, Anti-Malware, SSL inspection]) em cluster e com fontes de alimentação

redundantes. O S.O. deve dispor de funcionalidades de Firewall, Routing e Intrusion Prevention/Detection System (IPS/IDS), com aceleração de tráfego por hardware dedicado na firewall.

i) Ao nível de Firewall deverão ser suportadas as seguintes funcionalidades:

- Modos de operação NAT/route e transparente/bridge;
- Agendamento de políticas, recorrentes ou apenas uma vez;
- Session helpers e ALGS: dcerpc, dns-tcp, dns-udp, ftp, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)
- Suporte para tráfego VoIP: SIP/H.323 /SCCP NAT traversal, RTP pin holing
- Suporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Visualização de políticas de forma global ou por secção
- Definição de objetos para utilização em políticas incluindo: predefinidos, customizados, agrupamento de objetos, tagging e definição de cor de objetos
- Definição de objetos de endereços de diferentes tipos: IP, Subnet, intervalo de endereços IP, Geografia e FQDN
- Configuração de NAT: por política e tabela central de NAT
- Suporte de NAT: NAT64, NAT46, NAT estático, NAT dinâmico, PAT, Full Cone NAT
- Traffic shaping e QOS: shaping de tráfego partilhado por política, shapping por IP, largura de banda máxima e garantida, número máximo de ligações por IP, priorização de tráfego, suporte de Type of Service (ToS) e Differentiated Services (DiffServ).

ii) Ao nível de IPS/IDS deverão ser suportadas as seguintes funcionalidades:

- Mínimo de 7.000 assinaturas, deteção de anomalias nos protocolos, assinaturas customizadas, update de assinaturas manual ou automático (push ou pull), integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados.
- Ações de IPS: por defeito na assinatura, monitorizar, bloquear, reset sessão ou quarentena (IP do atacante, IP de atacante e vítima, interface de entrada) com definição de duração
- Possibilidade de registo integral do pacote onde foi detetado o ataque
- Definição de diferentes perfis de IPS de forma manual ou baseada em filtro (severidade, alvo, sistema operativo, aplicação e/ou protocolo)
- Aplicação de perfis de IPS por política de firewall para maior flexibilidade
- Opção de excluir a aplicação de assinaturas de IPS especificas com base em IPs
- Proteção DOS sobre IPv4 e IPv6 com definições contra TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding (source/destination)
- Possibilidade de implementação de IDS em modo sniffer

iii) Ao nível de Threat Protection deverão ser suportadas as seguintes funcionalidades:

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, anti-vírus, filtragem WEB e DLP
- Deteção e bloqueio de BOTNETs com base em listas de reputação de IPs globais;

- Suporte de anti-vírus nos modos flow (pacote-a-pacote) e proxy (reconstrução de sessões)
- Suporte de inspeção de anti-vírus, em modo flow, nos protocolos: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, NNTP
- Integração com solução de Sandboxing (cloud ou premises)
- Suporte de anti-vírus em modo proxy, incluindo:
- Suporte dos seguintes protocolos: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, NNTP:
    - Suporte para análise de ficheiros em sistema baseado na cloud (OS Sandbox)
    - Listas de ficheiros autorizados/negados
    - Opção de análise heurística
- Deteção de sites WEB (web filtering):
    - Suporte de diferentes mecanismos de deteção de sites Web (proxy-based, flowbased and DNS)
    - Possibilidade de definição manual de filtragem sites com base em URL, conteúdo Web e cabeçalho MIME
    - Categorização dinâmica em tempo real, baseada na cloud com mais de 250 milhões de sites categorizados, em mais de 50 idiomas e 77 categorias
    - Opção para forçar a utilização de mecanismos de busca segura (safe search) disponibilizados pelos principais motores de busca, incluindo Google, Yahoo!, Bing & Yandex, e definição customizada de YouTube Education Filter
    - Deverá ser possível a opção para activar as seguintes funcionalidades:
        - Filtrar Java Applet, ActiveX e/ou cookies
        - Bloquear HTTP Post
        - Registar termos/palavras utilizados nas pesquisas em motores de busca
        - Identificar imagens pelo URL
        - Bloquear redirect de HTTP de acordo com a categoria
        - Excluir, de forma simples, a inspeção de tráfego encriptado (SSL) em categorias relevantes à manutenção da privacidade dos utilizadores
        - Definição de quotas de utilização WEB com base em categorias
    - Definição de categorias customizada e sobreposição de categorização
    - Mecanismos de exceção à utilização de perfis pré-definidos;
- Mecanismos de deteção e mitigação de utilização de proxy-avoidance: Categorias de sites com proxy, apontar URLs por domínio e endereço IP, bloquear redirects de cache para sites com cache e tradução de sites, bloqueio de ligação proxy por deteção de aplicação, bloqueio de tráfego com comportamento de proxy com base em assinaturas de IPS
- Suporte a prevenção e proteção de fugas de informação - DLP
    - Suporte de protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP:
        - Possibilidade de executar acções de: registar, bloquear, quarentena de utilizador

/ IP /Interface
- Filtros pré-difinidos, incluindo cartões de crédito e número de Seg. Social

- Suporte de protocolos na análise de ficheiros: HTTP-POST, HTTP=-GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP
  - Opções de filtragem disponíveis, tais como tamanho, tipo de ficheiro, watermark, conteúdo e deteção de encriptação
- Utilização de mecanismos de DLP watermarking, com disponibilização de ferramentas gratuitas de watermarking para Windows e Linux
- Fingerprinting de ficheiros
- Arquivamento de ficheiros detetado para inspeção forense, incluindo: todo o conteúdo de e-mail, FTP, IM, NNTP e tráfego WEB

iv) Ao nível de Alta Disponibilidade deverão ser suportadas as seguintes funcionalidades:

- Alta disponibilidade nos modos ativo-passivo, ativo-ativo
- Interfaces de heartbeat redundantes
- Interfaces reservadas para gestão
- Sem custos de licenciamento para suporte de funcionalidades de alta-disponibilidade
- Reposição automática de serviço (failover):
  - Monitorização de portas e links (locais e remotos)
  - Sem perda de sessões
  - Failover rápido “em menos de 10 segundo”
  - Notificações de eventos de failover
  - Diferentes opções de arquitetura
  - HA com agregação de links
  - Full mesh HÁ
  - Suporte para HA com equipamento geograficamente dispersos
- Opção de sincronização de sessões com equipamentos em modo Standalone

v) Ao nível de Administração, Monitorização e Diagnósticos deverão ser suportadas as seguintes funcionalidades:

- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser
- Acesso de gestão em modo de texto: SSH, Telnet ou consola
- Sem necessidade de utilização de software cliente específico para gestão gráfica
- Suporte a múltiplos idiomas de administração com acesso gráfico, incluindo Português e Inglês
- Suporte para gestão local e gestão centralizada em simultâneo
- Suporte para gestão centralizada com integração em plataforma específica para o efeito
- Integração com plataformas externas de gestão e monitorização, incluindo SNMP, sFlow e Syslog
- Implementação rápida da solução incluindo mecanismos de auto instalação por USB,

execução local e remota de scripts

- Visualização em tempo real do estado do equipamento através de interface gráfica (acesso HTTPS com recurso a web-browser) incluindo diversos conteúdos e funcionalidades.

vi) Registo de Eventos e Relatórios, com suporte para as seguintes funcionalidades:

- Suporte para registo de eventos (logs) em diferentes repositórios, tais como: memória e/ou discos rígidos locais, múltiplos servidores de syslog, múltiplos servidores específicos para registos de eventos e elaboração de relatórios, servidores do tipo WebTrends e plataformas disponíveis na cloud
- Opção de logging confiável com recurso a mecanismos TCP (RFC 3195)
- Encriptação de eventos para confidencialidade e integridade aquando da utilização de plataformas específicas;
- Possibilidade de exportar relatórios em formato PDF
- Calendarização de backups de logs para sistemas externos
- Registos detalhados de tráfego: tráfego enviado, bloqueado, sessões violadas, tráfego local, pacotes inválidos
- Organização de registos de acordo com a categoria: administração de sistema (para auditoria), routing e networking, VPN, autenticação de utilizadores
- Opção para registo encurtado ou completo de eventos
- Resolução de nomes de endereços IP e protocolos

vii) Simultaneamente, os equipamentos deverão ter as seguintes Certificações:

- Certificações ICSA de Firewall, IPsec, IPS, Antivirus, SSL-VPN
- Certificação USGv6/IPv6

b) Solução/Configuração

O Adjudicatário deve garantir as seguintes características e capacidades como requisitos obrigatórios:

Solução
Nº de equipamentos - 2 (dois)
Solução não pode ocupar mais que 4 Us em bastidor
Suporte 36 meses em regime de 24x7
Características de hardware, por equipamento
Mínimo de 16 portas a Gigabit em cobre (RJ45)
Mínimo de 8 portas (slots) em SFP a Gigabit
Mínimo de 12 portas (slots) GE / SFP, 10 GE / SFP+ e 25 GE / SFP28
Fornecimento de 2 x transceivers em fibra a 10GE / SFP+ short-range

Mínimo de 4 portas (slots) a 40 GE / QSFP+
1 x Porta USB 3.0 e 1 x Porta de consola (RJ45)
Fontes de alimentação hot-swap redundantes
Discos interno com mínimo de 1 TB NVMe/SSD x 2
Características/capacidade, por equipamento
Firewall throughput mínimo de 198 Gbps em IPV4 e IPV6 (1518 byte, UDP)
Mínimo de 12 milhões de sessões concorrentes
Mínimo de 750 mil novas sessões por segundo
Latência inferior a 3,3 µs (com pacotes de 64 byte, UDP)
IPS throughput mínimo de 17 Gbps
Threat Protection Throughput mínimo de 9 Gbps
SSL Inspection Throughput mínimo de 12 Gbps
Application Control Throughput mínimo de 34 Gbps
Licenciamento incluído para 10 sistemas (firewalls) virtualizados, com capacidade total para um mínimo de 20 com licenciamento adicional

3) ITEM 2 – Firewall CORE (Site de Disaster Recovery)

A solução a fornecer para esta componente deverá ser baseada em infraestrutura virtual (*VM*), ou seja, em software e numa arquitetura *stand-alone*. A infraestrutura visa disponibilizar à Assembleia da República uma solução de firewall de CORE, para o site de Disaster Recovery, com vista a concretizar as seguintes funcionalidades base:

- Firewall virtualizada, com utilização de 8 vCPU em plataforma VMWare existente, devendo ser obrigatoriamente do mesmo fabricante do ITEM 1;
- Funcionalidades de *Unified Threat Protection*:
- Gestão centralizada (e gerida pela solução do ITEM 3);
- Suporte 24x7 com duração de 36 meses.

a) Requisitos, funcionalidades e capacidades da solução.

O Adjudicatário deve fornecer uma solução e efetuar a sua integração na topologia da Assembleia da República composta por uma VM do tipo All-in-one/Unified Threat Management [Firewall, Threat Protection (IPS, Web-filtering, Anti-Malware, SSL inspection)] em stand-alone. O S.O. deve permitir funcionalidades de BFD, BGP e VRRP, bem como Firewall, Routing, Intrusion Prevention System/Intrusion Detection System.

i) Ao nível de Firewall deverão ser suportadas as seguintes funcionalidades:

- Modos de operação NAT/route e transparente/bridge;
- Agendamento de políticas, recorrentes ou apenas uma vez;
- Session helpers e ALGS: dcerpc, dns-tcp, dns-udp, ftp, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)
- Suporte para tráfego VoIP: SIP/H.323 /SCCP NAT traversal, RTP pin holing
- Suporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Visualização de políticas de forma global ou por secção
- Definição de objetos para utilização em políticas incluindo: predefinidos, customizados, agrupamento de objetos, tagging e definição de cor de objetos
- Definição de objetos de endereços de diferentes tipos: IP, Subnet, intervalo de endereços IP, Geografia e FQDN
- Configuração de NAT: por política e tabela central de NAT
- Suporte de NAT: NAT64, NAT46, NAT estático, NAT dinâmico, PAT, Full Cone NAT
- Traffic shaping e QOS: shaping de tráfego partilhado por política, shapping por IP, largura de banda máxima e garantida, número máximo de ligações por IP, priorização de tráfego, suporte de Type of Service (ToS) e Differentiated Services (DiffServ).

ii) Ao nível de IPS deverão ser suportadas as seguintes funcionalidades:

- Mínimo de 7.000 assinaturas, deteção de anomalias nos protocolos, assinaturas customizadas, update de assinaturas manual ou automático (push ou pull), integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados.
- Ações de IPS: por defeito na assinatura, monitorizar, bloquear, reset sessão ou quarentena (IP do atacante, IP de atacante e vítima, interface de entrada) com definição de duração
- Possibilidade de registo integral do pacote onde foi detetado o ataque
- Definição de diferentes perfis de IPS de forma manual ou baseada em filtro (severidade, alvo, sistema operativo, aplicação e/ou protocolo)
- Aplicação de perfis de IPS por política de firewall para maior flexibilidade
- Opção de excluir a aplicação de assinaturas de IPS especificas com base em IPs
- Proteção DOS sobre IPv4 e IPv6 com definições contra TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding (source/destination)
- Possibilidade de implementação de IDS em modo sniffer

iii) Ao nível de Threat Protection deverão ser suportadas as seguintes funcionalidades:

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, anti-vírus, filtragem WEB e DLP
- Deteção e bloqueio de BOTNETs com base em listas de reputação de IPs globais;
- Suporte de anti-vírus nos modos flow (pacote-a-pacote) e proxy (reconstrução de sessões)
- Suporte de inspeção de anti-vírus, em modo flow, nos protocolos: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, NNTP

- Integração com solução de Sandboxing (cloud ou premises)
- Suporte de anti-vírus em modo proxy, incluindo:
- Suporte dos seguintes protocolos: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, NNTP:
    - Suporte para análise de ficheiros em sistema baseado na cloud (OS Sandbox)
    - Listas de ficheiros autorizados/negados
    - Opção de análise heurística
- Deteção de sites WEB (web filtering):
    - Suporte de diferentes mecanismos de deteção de sites Web (proxy-based, flowbased and DNS)
    - Possibilidade de definição manual de filtragem sites com base em URL, conteúdo Web e cabeçalho MIME
    - Categorização dinâmica em tempo real, baseada na cloud com mais de 250 milhões de sites categorizados, em mais de 50 idiomas e 77 categorias
    - Opção para forçar a utilização de mecanismos de busca segura (safe search) disponibilizados pelos principais motores de busca, incluindo Google, Yahoo!, Bing & Yandex, e definição customizada de YouTube Education Filter
    - Deverá ser possível a opção para activar as seguintes funcionalidades:
        - Filtrar Java Applet, ActiveX e/ou cookies
        - Bloquear HTTP Post
        - Registar termos/palavras utilizados nas pesquisas em motores de busca
        - Identificar imagens pelo URL
        - Bloquear redirect de HTTP de acordo com a categoria
        - Excluir, de forma simples, a inspeção de tráfego encriptado (SSL) em categorias relevantes à manutenção da privacidade dos utilizadores
        - Definição de quotas de utilização WEB com base em categorias
    - Definição de categorias customizada e sobreposição de categorização
    - Mecanismos de exceção à utilização de perfis pré-definidos;
- Mecanismos de deteção e mitigação de utilização de proxy-avoidance: Categorias de sites com proxy, apontar URLs por domínio e endereço IP, bloquear redirects de cache para sites com cache e tradução de sites, bloqueio de ligação proxy por deteção de aplicação, bloqueio de tráfego com comportamento de proxy com base em assinaturas de IPS
- Suporte a prevenção e proteção de fugas de informação - DLP
    - Suporte de protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP:
        - Possibilidade de executar acções de: registar, bloquear, quarentena de utilizador / IP /Interface
        - Filtros pré-difinidos, incluindo cartões de crédito e número de Seg. Social
    - Suporte de protocolos na análise de ficheiros: HTTP-POST, HTTP=-GET, SMTP, POP3,

IMAP, MAPI, FTP, NNTP
    - Opções de filtragem disponíveis, tais como tamanho, tipo de ficheiro, watermark, conteúdo e deteção de encriptação
  - Utilização de mecanismos de DLP watermarking, com disponibilização de ferramentas gratuitas de watermarking para Windows e Linux
  - Fingerprinting de ficheiros
  - Arquivamento de ficheiros detetado para inspeção forense, incluindo: todo o conteúdo de e-mail, FTP, IM, NNTP e tráfego WEB

iv) Ao nível de Administração, Monitorização e Diagnósticos deverão ser suportadas as seguintes funcionalidades:

- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser
- Acesso de gestão em modo de texto: SSH, Telnet ou consola
- Sem necessidade de utilização de software cliente específico para gestão gráfica
- Suporte a múltiplos idiomas de administração com acesso gráfico, incluindo Português e Inglês
- Suporte para gestão local e gestão centralizada em simultâneo
- Suporte para gestão centralizada com integração em plataforma específica para o efeito
- Integração com plataformas externas de gestão e monitorização, incluindo SNMP, sFlow e Syslog
- Implementação rápida da solução incluindo mecanismos de auto instalação por USB, execução local e remota de scripts
- Visualização em tempo real do estado do equipamento através de interface gráfica (acesso HTTPS com recurso a web-browser) incluindo diversos conteúdos e funcionalidades.

v) Registo de Eventos e Relatórios, com suporte para as seguintes funcionalidades:

- Suporte para registo de eventos (logs) em diferentes repositórios, tais como: memória e/ou discos rígidos locais, múltiplos servidores de syslog, múltiplos servidores específicos para registos de eventos e elaboração de relatórios, servidores do tipo WebTrends e plataformas disponíveis na cloud
- Opção de logging confiável com recurso a mecanismos TCP (RFC 3195)
- Encriptação de eventos para confidencialidade e integridade aquando da utilização de plataformas específicas;
- Possibilidade de exportar relatórios em formato PDF
- Calendarização de backups de logs para sistemas externos
- Registos detalhados de tráfego: tráfego enviado, bloqueado, sessões violadas, tráfego local, pacotes inválidos
- Organização de registos de acordo com a categoria: administração de sistema (para auditoria), routing e networking, VPN, autenticação de utilizadores
- Opção para registo encurtado ou completo de eventos

- Resolução de nomes de endereços IP e protocolos

vi) Simultaneamente, os equipamentos deverão ter as seguintes Certificações:

- Certificações ICSA de Firewall, IPsec, IPS, Antivirus, SSL-VPN
- Certificação USGv6/IPv6

b) Solução/Configuração

O Adjudicatário deve garantir as seguintes características e capacidades como requisitos obrigatórios:

Solução
N.º de equipamentos: 1 (uma) Virtual Appliance
Solução certificada para VMWare
Suporte 36 meses em regime de 24x7
Características da VM
Permitir que sejam alocados no mínimo 8 vCPU
Permitir que sejam alocados no mínimo 500 GB de disco
Não ter limitação de RAM, ao nível do licenciamento
Características/capacidade
Permitir um mínimo de 10.000 políticas
Não ter limite de número de utilizadores

4) ITEM 3 - Consola Centralizada de Gestão das Firewalls de CORE

A proposta deverá incluir uma consola centralizada de gestão das firewalls de core (site principal e site de disaster recovery) baseada numa solução virtualizada em software (VM) certificada para ambiente VMWare vSphere que proporcione uma gestão centralizada das políticas, configurações e visibilidade dos vários equipamentos de firewall (ITEM 1 e ITEM 2), adiante designada simplificadamente por Consola de Gestão.

a) Requisitos, funcionalidades e capacidades da solução

Através da Consola de Gestão deverá ser possível gerir equipamentos e políticas, bem como automatizar tarefas e configurações. A consola deverá ter a capacidade de otimizar a panorâmica das violações e das tentativas de violação, como o incremento ou decremento de ameaças cibernéticas.

i) Para a componente de Gestão, deverão ser suportadas as seguintes funcionalidades:

- Possibilidade de definir domínios administrativos

- Possibilidade de definir políticas globais
- Permitir que um administrador principal crie grupos de firewalls que outros administradores (secundários) poderão gerir e monitorizar
- Permitir a administração a partir de firewalls no site central ou de sites remotos
- Múltiplos contextos virtuais de firewall podem ser geridos por múltiplos contextos virtuais de administração
- Atribuição de permissões de gestão a utilizadores por diferentes contextos virtuais de administração e apenas acessos de gestão aos contextos virtuais de firewalls assignados
- Criar modelos de configuração (templates) para novos firewalls

ii) Gestão dos conteúdos de segurança aplicacional

- Gestão dos conteúdos de segurança aplicacional permite ao administrador ter um maior controlo sobre as atualizações de segurança, incluindo suporte para:
    - Atualizações de definições de antivírus
    - Atualizações de prevenção de intrusões
    - Atualizações de gestão de vulnerabilidades
    - Web Filtering
    - Antispam

iii) Controlo e gestão

- Gestão de firewalls individualmente ou por grupos lógicos
- Possibilidade de gestão da atualização do firmware das firewalls
- Descoberta de novas firewalls de forma automática
- Criação, implementação e monitorização de VPNs e politicas de segurança
- Delegação do controlo a utilizadores com diferentes permissões de administração
- Auditoria sobre as alterações de configuração efetuadas

b) Solução/Configuração

O Adjudicatário deve garantir as seguintes características e capacidades como requisitos obrigatórios:

Solução
N.º de equipamentos: 1 (uma) Virtual Appliance
Solução certificada para VMWare
Suporte 36 meses em regime de 24x7
Características da VM
Gestão de um mínimo de 10 (dez) firewalls fisicas ou virtuais
Permitir que sejam alocados no mínimo 100 GB de disco

Características/capacidade
Permitir um mínimo de 1 GB /dia de logs
Possibilidade de integração com plataformas de SIEM [mínimo 3, devendo ser pelo menos 2 (duas) diferentes do fabricante da solução de firewalls e consola]

5) ITEM 4 - Solução de Firewall de perímetro Internet (Site Principal e Site de Disaster Recovery) com funcionalidades de prevenção de ataques Zero-Day

A solução a fornecer para dar resposta ao requisito de "*Firewall de perímetro Internet (Site Principal e Site de Disaster Recovery) com funcionalidades de prevenção de ataques Zero-Day*" terá que integrar nativamente com as gateways físicas Check Point SG 15400 e com as consolas de gestão e de reporting da Check Point, todas já existentes no Site Principal, proporcionando a inspeção e sanitização local (on-premise) de ficheiros, através de técnicas de sandboxing e emulação, por forma a mitigar os principais riscos conhecidos e desconhecidos (*zero day*), integrada Simultaneamente, deverá ser implementada uma nova solução similar, ainda que totalmente virtualizada para instalar na infraestrutura de virtualização VMware vSphere, existente na Assembleia da República para utilização no Site de Disaster Recovery.

Estas funcionalidades NGTX deverão ser atividadas nas firewalls de perímetro Internet (Site Principal e Site de Disaster Recovery), transferindo os ficheiros a inspecionar para equipamentos locais (on-premise) independentes, por forma a não impactar no desempenho dessas firewalls, que por sua vez retornarão os resultados do comportamento desses mesmos ficheiros.

a) Requisitos, funcionalidades e capacidades da solução

- Proteção contra ataques do tipo "Zero Day", com base comportamental, antes de serem criadas as assinaturas estáticas contra o malware
- Análise e deteção de ataques "Zero Day" em diversos tipos de ficheiros, nomeadamente Adobe PDF, Microsoft Office, EXE, arquivos ZIP, Flash, Java e PIF
- Sanitização em tempo-real (entrega segura aos utilizadores, livre de scripts e similares) de ficheiros habituais de trabalho como Microsoft Office e Adobe PDF
- Emulação de ataques contra vários ambientes do sistema operativo Microsoft Windows, nas versões Windows XP ou superior.
- Emulação de ataques contra vários ambientes do sistema operativo Mac: MacOS na versão 10.14.6 (Mojave) ou superior;
- Emulação/sandboxing com capacidade de inspecionar e bloquear ataques por HTTPS sem recurso a dispositivos adicionais
- Possibilidade de implementação de sandboxing em modo 'in-line' na cloud, em equipamento out-of-band ou como MTA (Mail Transfer Agent).
- Análise ao nível do CPU para mitigação do risco de evasão

- Suporte de emulação para os protocolos HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel e FTP;
- Suporte de extração para os protocolos HTTP, HTTPS e ICAP (Web downloads) e SMTP, IMAP, POP3, SMTPS - MTA (anexos de emails);
- Inspeção de conteúdos SSL.

b) Solução/Configuração

O Adjudicatário deve garantir as seguintes características e capacidades como requisitos obrigatórios:

Solução
Nº de equipamentos - 1 (uma) hardware appliance
Solução não pode ocupar mais que 2 Us em bastidor
Suporte 36 meses em regime de 24x7 (para a hardware appliance)
Características de hardware, por equipamento
Mínimo de 4 portas a Gigabit em cobre (RJ45)
Mínimo de 2 portas (slots) 10 GE / SFP+
Fontes de alimentação hot-swap redundantes
Discos internos redundantes com mínimo de 1 TB
Características/capacidade, por equipamento
Tratamento de um mínimo de 2.500 ficheiros únicos por hora
Mínimo de 25 máquinas virtuais (VM) de emulação
Não ter limite de número de utilizadores

Solução
N.º de equipamentos: 1 (uma) Virtual Appliance
Solução certificada para VMWare
Suporte 36 meses em regime de 24x7
Características da VM
Permitir que sejam alocados no mínimo 4 vCPU
Não ter limitação de disco, nem de RAM ao nível do licenciamento
Características/capacidade

Licenciamento/subscrição de NGTX
Gestão através das consolas de gestão e reporting Check Point existentes
Não ter limite de número de utilizadores

Solução
N.º de equipamentos: 1 (uma) Virtual Appliance
Solução certificada para VMWare
Suporte 36 meses em regime de 24x7
Características da VM
Permitir que sejam alocados no mínimo 4 vCPU
Não ter limitação de disco, nem de RAM ao nível do licenciamento
Não ter limite de número de utilizadores

6) ITEM 5 - Solução para automatização, verificação e gestão de políticas unificadas

A solução proposta deverá permitir a automatização e gestão de políticas complexas de segurança implementadas em ambientes híbridos, nomeadamente aplicadas em firewalls, proxies, routers e outros dispositivos similares, físicos ou virtuais.

Simultaneamente, a solução deverá proporcionar visibilidade e controlo sobre ambientes heterogéneos, de diversos fabricantes, assegurando a monitorização e gestão de alterações nas regras implementadas, a otimização das regras, identificando riscos e não conformidades.

Com esta solução, que tem por objetivo garantir a permanente e adequada configuração dos equipamentos e das políticas de segurança, pretende-se reduzir o risco de ataques baseados em movimentos laterais, aumentando os níveis de proteção dos ativos de informação e analisando proativamente os riscos que eventuais alterações da política possam provocar.

a) Requisitos, funcionalidades e capacidades da solução

i) A plataforma a fornecer deverá disponibilizar as seguintes funcionalidades:

- Abordagem centralizada das políticas de segurança de rede de forma transversal em ambientes híbridos (On-premise e Cloud) de vários fabricantes;
- Disponibilização de mapa interativo e dinâmico da topologia da rede, com:
  - Mapeamento dos fluxos de tráfego com as aplicações associadas;
  - Avaliação do impacto das políticas no tráfego da rede;
  - Indicadores para troubleshooting de questões de conetividade;
  - Indicadores de apoio à mudança e query do tipo “what-if”;

- Disponibilização de um conjunto alargado de recomendações automatizadas que proporcionem a limpeza e otimização periódica de políticas (regras), nomeadamente:
  - Descoberta e remoção de regras duplicadas, não utilizadas ou em conflito;
  - Consolidação ou reorganização de regras com vista a um melhor desempenho;
  - Identificação e mitigação de regras de risco elevado;
  - Validação do alinhamento das regras com a política de segmentação de rede;
  - Validação da operacionalidade de serviços face a alterações das regras;
  - Redução da amplitude de regras desnecessariamente demasiado permissivas;
  - Revalidação de regras expiradas com base em segurança e impacto na operação;
  - Sanitização e redesenho das políticas de segurança nos momentos mudança;
  - Remoção de acessos de aplicações descomissionadas;
  - Disponibilização de mecanismos de informação de apoio a troubleshooting;
  - Geração de relatórios automatizados de conformidade relativamente a normativas standards, com modelos pré-populados e prontos a usar para as principais normas de mercado como por exemplo PCI-DSS e ISSO 27001;
  - Capacidade de criação de relatórios automatizados para normas de conformidade com base em controlos e pressupostos de avaliação definidos pelas equipas de IT;
  - Capacidade de análise proactiva do alinhamento com as normas definidas a cada alteração das configurações das políticas;
  - Emissão de relatórios de risco baseados no alinhamento com boas práticas;
- Disponibilização de informação que permita implementar novas políticas efetivas de segmentação na rede;
- Criação e manutenção de registo de mudanças e aprovações dessas mudanças nas regras, objetos e políticas de segurança;
- Capacidade de análise, sugestão e interação com micro segmentação SDN em plataformas como Cisco ACI e VMware NSX.

ii) A solução a propor deverá suportar e integrar com as seguintes tecnologias:

- Check Point Firewalls R77.x, R80.x e superiores, incluíndo suporte às capacidades de Application Control e Identity Awareness, Check Point Firewalls VSX, R77.x, R80.x e superiores e Check Point Security Gateway, R77.x, R80.x e superiores,
- Fortinet FortiGate (Firewalls), FortiOS 6.0, 6.2, 6.4, 7.0 e superior.
- KEMP LoadMaster
- Cisco IOS Routers, Cisco Nexus Routers, Cisco ASA, Cisco Firepower e Cisco ACI
- Outras através de API

Ainda que recorrendo a licenciamento adicional, a solução deverá ter capacidade de integração com soluções standard de mercado de:

- Ticketing, nomeadamente Servicenow, BNC e CA
- Scan de vulnerabilidades, nomeadamente Rapid7, Qualys e Tenable (Nessus)

iii) A solução a fornecer deverá ser entregue em software e possuir as seguintes características:

- Instalação em ambientes de virtualização e ser compatível pelo menos com VMware vSphere e Microsoft Hyper-V
- Possibilidade de instalação em alta-disponibilidade e/ou ambiente de Disaster Recovery

b) Solução/Configuração

O Adjudicatário deve garantir as seguintes características e capacidades como requisitos obrigatórios:

Solução
Software Virtual Appliance
Solução certificada para VMWare
Subascrição por 36 meses, incluíndo suporte e manutenção
Gestão do mínimo de 10 (dez) dispositivos fisicos ou virtuais (fw, proxy, ADC)

7) ITEM 6 – Serviços de instalação, configuração, suporte e manutenção

Na proposta, deverá o Adjudicatário considerar os serviços de instalação e configuração das novas soluções bem como a atualização/configuração das novas funcionalidades das soluções existentes.

a) Requisitos dos serviços de instalação, configuração e integração

No âmbito dos serviços de instalação, configuração e integração na infraestrutura da Assembleia da República, deverão ser consideradas, pelo menos, as seguintes tarefas:

- Levantamento dos pré-requisitos para a implementação;
- Identificação de possíveis riscos na implementação e de medidas de mitigação;
- Definição do cronograma de implementação da solução;
- Instalação dos vários equipamentos e VM;
- Instalação e configuração de todas as componentes e funcionalidades necessárias ao cumprimento dos requisitos definidos nas especificações técnicas;
- Configuração nos equipamentos já existentes da infraestrutura da Assembleia da República de todos os parâmetros que permitam a correta integração e funcionamento da solução proposta, incluindo, ainda que não exclusivamente, eventuais alterações de switching e routing;
- Implementação de políticas base nas firewall de CORE (DC e DR);
- Implementação de nova política de firewall de perímetro Internet, no site de DR;
- Implementação de novas funcionalidades nas firewalls Check Point existentes;

- Ajuste das políticas existentes na firewall de perímetro Internet, existente no DC, para correto funcionamento da arquitetura global;
- Implementação e integração de todas as gateways novas da Check Point nas consolas de gestão e reporting existentes;
- Instalação e configuração da solução de automatização, verificação e gestão de políticas unificadas (ITEM 5), integrando-a com todas as componentes finais da arquitetura de segurança;
- Workshop de transferência de conhecimentos e operação corrente da solução de automatização, verificação e gestão de políticas unificadas, nas instalações da Assembleia da República**,** com uma duração mínima de 2 (dois) dias;
- Definição e configuração de alarmística disponível nas diversas componentes da arquitetura de segurança final;
- Definição e configuração de relatórios;
- Documentação da solução.

Ainda que seja o Adjudicatário a assumir a totalidade dos serviços necessários ao correto funcionamento das soluções propostas, a Assembleia da República**,** fixa os serviços de instalação, configuração e integração com uma duração máxima de 12 (doze) semanas.

b) Requisitos dos serviços de suporte e manutenção.

Os serviços de suporte e manutenção, bem como eventuais subscrições associadas, deverão ser fornecidos obrigatoriamente com *back-to-back* com o fabricante, pelo período contratado de 36 (trinta e seis) meses, pretendendo ainda que sejam prestados os seguintes serviços:

- Suporte do fabricante da solução implementada no regime de 24x7;
- Subscrição de fontes de informação (atualização de assinaturas) e similares;
- Pacote de 150 (cento e cinquenta) horas de serviços de suporte técnico local, a utilizar em tarefas de fine tuning, troubleshooting e apoio na exploração das soluções aos longo dos 36 meses.

c) Notas adicionais

- Excecionalmente, o upgrade das subscrições NGTX das firewalls SG 15400 (previsto no ITEM 4) deverão terminar na data final de 30 de junho de 2022.
- Ainda que o suporte seja prestado em primeira linha pelo Adjudicatário, pretende a Assembleia da República ter acesso a knowledgebases, novas versões e outras funcionalidades de suporte de forma autónoma e direta, bem como todo o licenciamento deverá ser registado em nome da Assembleia da República.

ANEXO I

Minuta de auto de aceitação

Nos termos e para os efeitos da cláusula ..ª do contrato n.º ……, que tem por objeto a "……..", vêm as partes, neste ato representadas por:----------

A Assembleia da República, pelo ……., na qualidade de ……, e;----------

A ……, pelo ……, na qualidade de ……..----------

Declarar que os seguintes bens:----------

- ……
- ……

Objeto do presente contrato, já se encontram integralmente fornecidos, instalados e configurados, encontrando-se já em pleno funcionamento e em conformidade com as exigências legais e contratuais.----------

Feito em duplicado, ficando um exemplar para cada outorgante, no dia .. de ……. de …….-------

P'la Assembleia da República,

Anexo II
ACORDO DE TRATAMENTO DE DADOS PESSOAIS EM SUBCONTRATAÇÃO

Nos termos e para os efeitos do disposto no artigo 28.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (Regulamento Geral sobre Proteção de Dados, adiante designado RGPD), e considerada, ainda, a Lei 58/2019, de 8 de agosto, que o executa na ordem jurídica portuguesa, o presente acordo rege-se pelas cláusulas seguintes:

Definições:

Dados Pessoais: informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Tratamento: uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

Responsável pelo Tratamento: pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro.

Cocontratante: Pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes, definida no RGPD como *Subcontratante*.

Subcontratado: Pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo, designada no RGPD como *Outro Subcontratante*, que trate os dados pessoais por conta do Responsável do Tratamento, subcontratado pelo Cocontratante.

Cláusula 1.ª
Objeto e âmbito de aplicação

1. O presente acordo vincula o Cocontratante à Assembleia da República e regula o tratamento de dados a realizar pelo Cocontratante, por conta da Responsável pelo Tratamento, nos termos do artigo 28.º do RGPD.
2. O presente acordo complementa e faz parte integrante do contrato de prestação de serviços celebrado entre as partes e que tem por objeto a reformulação da infraestrutura de segurança informática da rede da Assembleia da República.
3. Para efeitos do presente, o Cocontratante tratará: dados de identificação, dados de contacto pertencentes às seguintes categorias de titulares de dados: funcionários da AR.

Cláusula 2.ª
Duração do presente acordo

1. O presente acordo de tratamento de dados pessoais em regime de subcontratação vigorará enquanto se mantiver em vigor o contrato de prestação de serviços entre a Assembleia da República e o Cocontratante ou até tais dados serem apagados ou devolvidos, por instrução daquela.
2. O acordo de tratamento de dados em apreço terminará com efeitos imediatos caso cesse o contrato de prestação de serviços celebrado entre as partes, por qualquer forma de cessação dos contratos, seja por resolução, caducidade, revogação ou denúncia, exceto se existirem

instruções em contrário da Assembleia da República.

Cláusula 3.ª
Da relação entre a Assembleia da República e Cocontratante

1. Compete à Assembleia da República determinar o âmbito, finalidades e forma pela qual o Cocontratante poderá aceder ou proceder ao tratamento dos dados pessoais.
2. O Cocontratante tratará os dados pessoais somente em conformidade com as instruções documentadas que lhe forem fornecidas pela Assembleia da República.
3. O Cocontratante notificará por escrito a Assembleia da República, e fundamentará, caso entenda que uma instrução que receba infringe o RGPD ou outra legislação nacional ou da União relativa à proteção de dados.

Cláusula 4.ª
Da contratação de outro subcontratado

1. O Cocontratante apenas contrata outro subcontratado quando a Assembleia da República tenha dado, previamente e por escrito, autorização específica para esse efeito.
2. Em caso de autorização por escrito, o Cocontratante informa a Assembleia da República de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratados, dando assim à Assembleia da República a oportunidade de se opor a tais alterações.
3. Caso o Cocontratante contrate outro subcontratado para a realização de operações específicas de tratamento de dados por conta da Assembleia da República, são impostas a esse outro subcontratado, por contrato ou outro ato normativo ao abrigo do direito da União ou da legislação nacional, as mesmas obrigações em matéria de proteção de dados que as estabelecidas neste acordo.
4. Caso esse outro subcontratado não cumpra as suas obrigações em matéria de proteção de dados, o Cocontratante que é parte neste contrato continua a ser plenamente responsável, perante a Assembleia da República, pelo cumprimento das obrigações desse outro subcontratado.

5. Em caso de autorização para subcontratação pela Assembleia da República o Cocontratante deverá preencher o ANEXO III.

Cláusula 5.ª
Das garantias de segurança do tratamento

1. As partes assumiram o presente vínculo jurídico reconhecendo a Assembleia da República as competências técnicas e de segurança do Cocontratante e este a possibilidade de delas dispor e poder implementar, a fim de ser levado a cabo o tratamento de dados pessoais para as finalidades definidas pela Assembleia da República.
2. Nos termos do artigo 32.º do RGPD, as partes devem aplicar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, sem excluir outras que o tratamento exija ou venha a exigir, nomeadamente, a capacidade de garantir a confidencialidade, integridade e disponibilidade da informação e a resiliência dos sistemas de tratamento.
3. A Assembleia da República e o Cocontratante implementaram medidas que garantem que qualquer pessoa singular que tenha acesso a dados pessoais e agindo sob a autoridade da Assembleia da República ou do Cocontratante, só procede ao seu tratamento mediante instruções daquela, exceto se tal lhe for exigido pelo direito da União ou pela legislação nacional.

Cláusula 6.ª
Da confidencialidade

1. O Cocontratante deve assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade.
2. O fim do presente acordo de tratamento de dados pessoais em subcontratação não exonera o Cocontratante ou outros subcontratados do seu dever de confidencialidade, o qual se mantém sem limite temporal.

Cláusula 7.ª
Transferências de dados

1. O Cocontratante deverá imediatamente notificar a Assembleia da República de quaisquer transferências temporárias ou permanentes de dados pessoais para país fora do E.E.E.- Espaço Económico Europeu - que não apresente um nível adequado de proteção.
2. Essa transferência deverá ser apenas efetuada após a obtenção de autorização da Assembleia da República, que poderá recusá-la na medida do seu critério que entender adotar.

Cláusula 8.ª
Da assistência à Assembleia da República

1. O Cocontratante, na medida do possível e tomando em conta a natureza do tratamento, presta assistência à Assembleia da República através de medidas técnicas e organizativas adequadas, permitindo que esta cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos previstos RGPD, bem como as obrigações estabelecidas nos artigos 32.º a 36.º do RGPD.
2. O Cocontratante deve facilitar e contribuir para as auditorias, inclusive as inspeções, conduzidas pela Assembleia da República ou por outro auditor por este mandatado para o efeito.

Cláusula 9.ª
Do destino dos dados finda a prestação de serviços

1. De harmonia com o critério ou escolha da Assembleia da República, o Cocontratante apaga ou devolve-lhe todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros.

Cláusula 10.ª
Gestão de incidentes

No caso de o Cocontratante tomar conhecimento de incidente que afete o tratamento de dados pessoais deverá prontamente notificar a Assembleia da República desse facto, com ela cooperar e seguir as suas instruções relativas a tais incidentes, de modo a permitir-lhe executar uma investigação aprofundada do incidente e responder-lhe corretivamente tomando as medidas adequadas.

Cláusula 11.ª
Da responsabilidade do Cocontratante

O Cocontratante deverá indemnizar a Assembleia da República e assumir a responsabilidade em relação a qualquer queixas, procedimentos, queixas de terceiros, perdas, danos e encargos em que a Assembleia da República incorra e que decorram, direta ou indiretamente de violações do presente contrato e/ou legislação de proteção de dados aplicável imputáveis ao Cocontratado.

Cláusula 12.ª
Entrada em vigor

O presente acordo de tratamento de dados pessoais em subcontratação entre a Assembleia da República e o Cocontratante vigorará a partir da data da outorga do contrato subjacente a este procedimento pré-contratual.

Cláusula 13.ª
Lei do contrato e Conflitos

1. O presente acordo rege-se pela lei portuguesa e pelas normas europeias diretamente aplicáveis.
2. Na eventualidade de existir um conflito entre o contrato de prestação de serviços e este acordo de tratamento de dados pessoais em subcontratação entre a Assembleia da República e o Cocontratante, este deverá prevalecer sobre o primeiro.

A Assembleia da República nomeou um Encarregado da Proteção de Dados que poderá ser contactado através de encarregado.protecao.dados@ar.parlamento.pt

ANEXO III – Lista de Subcontratados

Foi autorizada pela Assembleia da República a subcontratação pelo Cocontratante, das seguintes entidades:

(Nome da empresa)	
Morada:	
Nome da pessoa responsável:	
Contacto da pessoa responsável:	
Descrição do tratamento:	

Qualquer alteração à lista dos subcontratados deverá ser autorizada pela Assembleia da República nos termos do disposto no n.º 2 art.º 28.º do Regulamento Geral de Proteção de Dados utilizando-se as vias de comunicação acordadas e utilizadas entre as partes**.**