Aprovo o Caderno de Encargos

[Assinatura Qualificada] Bruno Henrique Figueiredo da Costa

Assinado de forma digital por [Assinatura Qualificada] Bruno Henrique Figueiredo da Costa
Dados: 2026.07.06 11:06:59 +01'00'

Vice-Presidente, Eng.º Bruno Henrique Figueiredo Costa
por despacho n.º 2025.11.07_05)

Assinatura digital de igual valor probatório dos congéneres em papel com assinatura manuscrita, ao abrigo do artigo 3.º do Decreto-Lei n.º 12/2021, de 09 de fevereiro, na sua redação atual. Cópias do documento são validadas com selo branco em uso na instituição.

Procedimento - BM 20/2026

CADERNO DE ENCARGOS

Aquisição de Bens

Consulta Prévia

Índice

Cláusula Primeira: Objeto

O caderno de encargos contém as cláusulas a incluir no(s) contrato(s) a celebrar na sequência do *procedimento para formação de contrato público* com o objeto **"Aquisição de Soluções Integradas de Cibersegurança (Firewall, EDR e Autenticação Forte) para Cumprimento da Diretiva NIS2, no âmbito do Aviso CENTRO2030-2024-75.**".

Cláusula Segunda: Obrigações principais do fornecedor

1. São obrigações principais do fornecedor:

   a. Cumprir com as especificações técnicas, requisitos mínimos e os níveis de serviço estabelecidos no Anexo I;

   b. (No momento do fornecimento dos bens) Disponibilização de todos os documentos necessários para o correto funcionamento e utilização dos bens, designadamente o manual e a ficha técnica, devendo todos os documentos ser disponíveis em idioma português (salvo solicitação do cocontratante devidamente fundamentada e aprovação do Município para a entrega de documentos em idioma diverso).

2. O fornecedor está obrigado ao fornecimento de bens em conformidade com o ordenamento jurídico nacional e europeu.

3. São da responsabilidade do fornecedor todos os meios necessários à correta execução do contrato, designadamente os meios humanos, materiais, técnicos e auxiliares, as deslocações, os contactos com outras entidades e quaisquer ações de recolha e tratamento de informações que visem a correta execução do contrato.

Cláusula Terceira: Condicionantes do fornecimento

1. O fornecedor está obrigado ao fornecimento de todos os bens com qualidade e aptidão e em conformidade com o caderno de encargos, considerando a natureza, o fim e a localização a que se destinam.

2. A falta de qualidade ou a inaptidão dos bens (considerando a natureza, o fim e a localização a que se destinam), são fundamento de rejeição do bem pelo Município, constituindo no fornecedor a obrigação de substituição por bem alternativo (ainda que o bem inicialmente apresentado coincida com o identificado na proposta).

3. O fornecimento deve ocorrer nas seguintes condições:

Quantidades de fornecimento	Consoante as solicitações do município
Horário de fornecimento	das 9h às13:30h e das 14h às 17:00h
Locais de fornecimento (custos associados ao fornecimento da responsabilidade do fornecedor)	Consoante as indicações do município aquando das solicitações de fornecimento
Prazo máximo de entrega total dos bens (incluindo transporte, descarga, montagem, instalação, configuração e preparação total dos bens, ficando aptos para a pronta utilização final e recolha e tratamento seletivo dos resíduos)	Máximo de 60 dias. É admissível, dentro do limite do prazo, a entrega faseada dos bens.
Prazo de garantia	Mínimo de 3 anos

4. Verificando-se a impossibilidade de fornecimento no prazo estipulado, o fornecedor fundamenta o respetivo atraso ao Município, propondo o prazo previsto para regularização (sujeito a aprovação do Município). A aprovação pelo Município não é impeditiva da aplicação do regime sancionatório contratual e legalmente previsto.

5. Todos os bens e respetivos componentes e acessórios são novos.

6. É aplicável o ordenamento jurídico relativo à venda de bens de consumo e respetivas garantias, designadamente quanto à conformidade dos bens com o contrato, à responsabilidade e obrigações do fornecedor e do produtor e aos direitos do consumidor (incluindo a garantia).

Cláusula Quarta: Aceitação das amostras e dos bens

1. A admissibilidade do fornecimento - e das amostras, se solicitadas - depende de análise e pronúncia (aprovação ou não aprovação) do gestor do contrato no prazo máximo de 30 dias.

2. O fornecimento - e as amostras, se solicitadas - são tacitamente aceites após o decurso do prazo constante no número anterior.

3. A análise e pronúncia incide sobre as quantidades, o estado, a qualidade e as especificações técnicas dos bens fornecidos (e sobre os elementos que os devam acompanhar), devendo o fornecedor prestar toda a cooperação, designadamente concedendo todos os esclarecimentos e elementos solicitados.

4. A não aprovação nos termos dos números anteriores, determina a obrigação do fornecedor à adoção da conduta e ao fornecimento conducente à aprovação. Sendo detetado, no momento do fornecimento (incluindo as amostras) ou nos 30 dias seguintes, qualquer defeito ou discrepância em relação ao contratualizado ou à sua operacionalidade (designadamente para o fim e a localização a que se destinam), a conduta do fornecedor inclui o pronto suprimento da falta de conformidade (reparação ou substituição). Findo o prazo para a adotação da conduta adequada, que é definido pelo Município, sem que esta tenha ocorrido, o Município pode proceder à aplicação de sanções contratuais e à resolução do contrato.

5. A conduta a que se refere o número anterior, deve ser assegurada num prazo razoável e sem grave inconveniente para o Município, sendo que quaisquer custos, encargos e despesas decorrentes da garantia técnica descrita na presente cláusula são da responsabilidade do fornecedor.

6. A nova apresentação nos termos dos números anteriores, está sujeita a análise e pronúncia (aprovação ou não aprovação) pelo gestor do contrato, aplicando-se o disposto na presente cláusula.

Cláusula Quinta: Prazo das obrigações principais do fornecedor

1. As obrigações principais que recaem sobre o fornecedor são cumpridas até **31 de outubro de 2026**, sem prejuízo das obrigações acessórias que, nos termos legais e do presente caderno de encargos, devam perdurar além desse prazo.

2. O contrato inicia vigência com a respetiva publicitação do contrato na plataforma digital BASE e a comunicação, pelo Município, da requisição externa.

3. Independentemente do prazo estabelecido, o contrato cessará quando atingido o valor máximo estabelecido.

Cláusula Sexta: Responsabilidade do fornecedor

Na situação do Município ser responsabilizado por qualquer infração (seja mediante decisão administrativa ou decisão jurisdicional) decorrente da desconformidade dos bens fornecidos ao ordenamento jurídico em vigor (designadamente direitos de propriedade industrial), o fornecedor é solidariamente responsável, constituindo-se na sua esfera jurídica a obrigação de indemnização do Município por quaisquer valores que esta, no âmbito daquela responsabilização, tenha de pagar.

Cláusula Sétima: Dever de sigilo

1. O fornecedor deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa ao Município 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 objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.

3. Exclui-se do dever de sigilo previsto, a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo fornecedor ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

4. A utilização de qualquer elemento identificativo do Município (designadamente o logótipo) depende de prévia autorização.

5. O dever de sigilo é uma obrigação acessória, perdurando após o cumprimento, pelo fornecedor, das obrigações principais.

Cláusula Oitava: Sustentabilidade ambiental

O fornecedor deve adotar práticas que respeitem o ordenamento jurídico (nacional e da União Europeia) e promovam a *legis artis* em sustentabilidade ambiental.

Cláusula Nona: Proteção de dados pessoais

1. O fornecedor apenas pode tratar dados pessoais na medida do estritamente necessário para a integral e adequada execução do contrato, mediante consentimento do Município e nos termos do ordenamento jurídico, das normas internas do Município e da *legis artis*.

2. No tratamento de dados pessoais, o fornecedor:

   a. Não pode reproduzir, gravar, copiar ou divulgar os dados pessoais para outros fins que não constem do contrato;

   b. Comunica ao *Delegado de Proteção de Dados* (DPO) quaisquer situações relativas à incorreta recolha, tratamento ou eliminação de dados pessoais;

   c. Compromete-se, no final do contrato, a eliminar a totalidade de dados pessoais que tenha recolhido e tratado.

3. A proteção de dados pessoais é uma obrigação acessória, perdurando após o cumprimento, pelo fornecedor, das obrigações principais.

Cláusula Décima: Preço-base e preço contratual

1. Pela execução do contrato, o Município pagará ao fornecedor o valor adjudicado, sendo o preço-base **53.140,00** (cinquenta e três mil, cento e quarenta euros), acrescido de IVA.

2. O preço contratual é pago após o cumprimento integral das prestações contratuais nos termos do caderno de encargos e da legislação aplicável, devendo a fatura ser apresentada com uma antecedência mínima de 30 dias em relação à data de vencimento.

3. A obrigação considera-se vencida aquando da declaração da aprovação pelo gestor do contrato, quando esta deva existir.

4. O preço referido no número 1 inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao Município, designadamente despesas de alojamento, de alimentação e de deslocação de meios humanos, despesas de aquisição, transporte, descarga, montagem, instalação, configuração e preparação total dos bens, ficando aptos para a pronta utilização final, de recolha e tratamento seletivo dos resíduos e quaisquer encargos decorrentes da utilização de marcas registadas, de patentes ou de licenças e quaisquer dos encargos mencionados nos artigos 445.º e 447.º do CCP.

Cláusula Décima-Primeira: Faturação

1. A fatura a apresentar pelo fornecedor ao Município de Fornos de Algodres, emitida em observância com o disposto no artigo 299.º-B do CCP, deve conter os elementos necessários a uma completa, clara e adequada compreensão dos valores faturados, os quais devem ser apresentados de forma desagregada.

2. A faturação deve obedecer às seguintes condições:

a. Ser emitida após o serviço, podendo ser mensal, caso seja enquadrável, objeto do contrato e aceitação pelo Município de Fornos de Algodres;

b. Conter o número de compromisso e/ou requisição emitida pelo Município de Fornos de Algodres;

c. Indicar o preço global;

d. Indicar o IVA à taxa legal aplicável.

3. O fornecedor deve proceder à **emissão das faturas em formato eletrónico (EDI)**, se tal lhe for aplicável, decorrente da aplicação e cumprimento da legislação em vigor para a implementação da faturação eletrónica nos contratos públicos (Decreto-Lei n.º 111-B/2017, de 31 de agosto, alterado pelo Decreto-Lei, n.º 123/2018, de 28 de dezembro, atualizado com o estabelecido pelo Decreto-Lei n.º 14-A/2020 de 7 de abril. pelo Decreto-Lei n.º 104/2021, de 27 de novembro, e pelo Decreto-Lei n.º 42-A/2022, de 30 de junho ou outra que venha a estar em vigor no decorrer do contrato.

4. O Município de Fornos de Algodres aderiu aos portais e-BILLING Suite da PI Informática e FE-AP da eSPap para a receção de documentos em formato eletrónico (EDI).

5. Para informação sobre a adesão aos referidos portais deverá o fornecedor consultar a informação disponível em Contratação Pública - Município de Fornos de Algodres.

6. A emissão de segundas vias das faturas solicitadas pelo Município de Fornos de Algodres não serão objeto de qualquer cobrança adicional.

Cláusula Décima-Segunda: Condições de modificação do contrato

Não estão contratualmente previstas quaisquer modificações contratuais, sendo aplicável o previsto no CCP.

Cláusula Décima-Terceira: Força maior

1. Nenhuma das partes incorrerá em responsabilidade contratual se, por caso de força maior, for impedido de cumprir as obrigações contratualmente assumidas.

2. O número anterior não prejudica a possibilidade, nos termos legais, de resolução por razões de interesse público.

3. Para efeitos do número 1, constituem casos de força maior as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fossem razoavelmente exigível contornar ou evitar, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.

4. Para efeitos do número 1, não constituem casos de força maior, designadamente:

a. Greves ou conflitos laborais relativos ao fornecedor, a grupos de sociedades em que se integre ou a sociedades ou grupos de sociedades dos seus subcontratados;

b. Determinações governamentais, administrativas, ou judiciais, de natureza sancionatória ou outra, resultantes do incumprimento pelo fornecedor de deveres ou ónus que sobre ele recaiam;

c. Manifestações populares devidas ao incumprimento pelo fornecedor de normas legais;

d. Incêndios ou inundações com origem nas instalações do fornecedor cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;

e. Avarias nos sistemas informáticos ou mecânicos do fornecedor não devidas a sabotagem;

f. Eventos que estejam ou devam estar cobertos por seguros.

5. A parte que invocar situação de força maior deverá comunicar e justificar tais situações à outra parte e informar o prazo previsível para reestabelecer o cumprimento das obrigações principais.

Cláusula Décima-Quarta: Resolução por parte do Município

1. O Município pode resolver o contrato, a título sancionatório, em qualquer das situações estabelecidas no CCP (designadamente no seu artigo 448.º) ou em situações de grave violação, pelo fornecedor, de qualquer das obrigações contratuais.

2. Para efeitos do número anterior, constitui, nomeadamente, grave violação, o incumprimento (incluindo o cumprimento defeituoso) reiterado das obrigações contratuais (designadamente o incumprimento, por três vezes, de qualquer das suas obrigações, ainda que distintas).

3. O Município pode, nos termos da lei, resolver o contrato por motivos de interesse público.

Cláusula Décima-Quinta: Sanções contratuais

1. Existindo incumprimento (incluindo cumprimento defeituoso) culposo, pelo fornecedor, de qualquer das obrigações contratuais, pode ser aplicada sanção calculada em $1^{0}/_{00}$ do valor contratual por cada dia de incumprimento até à respetiva regularização.

2. Para efeitos do número anterior, presume-se a imputabilidade da culpa ao fornecedor.

3. Não existindo caução ou tendo esgotado o respetivo montante, o contraente público pode compensar os pagamentos devidos ao abrigo do contrato com as sanções contratuais devidas nos termos da presente cláusula.

4. As eventuais sanções nos termos do presente artigo não impedem, nem de algum modo afetam:

- A resolução do contrato nos termos acordados ou legais; ou,
- Qualquer indeminização a que o contraente público tiver direito nos termos legais.

Cláusula Décima-Sexta: Caução

1. A caução em execução de contrato é determinada nos seguintes termos:

CAUÇÃO MEDIANTE DEDUÇÃO AOS PAGAMENTOS	Não aplicável

2. Existindo, a caução inicial e/ou mediante dedução aos pagamentos é liberada nos termos legais.

Cláusula Décima-Sétima: Subcontratação e cessão da posição contratual

1. A subcontratação pelo fornecedor e a cessão da posição contratual por qualquer das partes dependem, nos termos do CCP, da autorização da parte contrária, sem prejuízo do disposto no número seguinte.

2. Perante incumprimento do fornecedor que reúna os pressupostos para a resolução do contrato, o Município pode, nos termos do artigo 318.º-A do CCP, ceder a posição contratual do fornecedor ao concorrente classificado em posição subsequente no *procedimento para a formação de contrato público*.

Cláusula Décima-Oitava: Comunicações e notificações

1. Quaisquer comunicações e notificações entre as partes relativas à execução contratual ocorrem via correio eletrónico para os endereços a identificar em contrato.

2. As partes estão obrigadas à atualização dos endereços eletrónicos identificados no número anterior, não sendo as comunicações ou notificações prejudicadas pela desatualização dos endereços.

Cláusula Décima-Nona: Remissão e legislação aplicável

1. Todos os documentos para os quais o caderno de encargos remeta (designadamente as especificações técnicas), são sua parte integrante.

2. A execução do contrato a celebrar é regida pelo CCP.

Cláusula Vigésima: Competência territorial da jurisdição administrativa

Para as pretensões relativas à execução do contrato é convencionada a competência do Tribunal Administrativo e Fiscal de Viseu.

Anexo I: Especificações técnicas

1. Condições de Admissão

No âmbito do presente procedimento, constitui condição obrigatória de admissão a apresentação de declaração ou certificado emitido pelo fabricante das soluções propostas, datado e devidamente assinado por representante habilitado para o efeito. A não apresentação deste documento, ou a sua apresentação em termos que não cumpram o disposto na presente cláusula, constitui fundamento de exclusão da proposta. A declaração ou certificado deverá fazer referência expressa ao presente procedimento concursal e confirmar, no mínimo, os seguintes pontos:

- O proponente encontra-se devidamente autorizado a apresentar e comercializar as soluções propostas no âmbito do presente procedimento, no país de execução do contrato;
- As soluções propostas serão fornecidas através dos canais oficiais ou autorizados do fabricante, assegurando a sua elegibilidade para registo, ativação, garantia e suporte junto do fabricante;
- Todos os equipamentos a fornecer deverão ser novos, originais e não reacondicionados, nos termos das condições oficiais do fabricante aplicáveis aos produtos adquiridos através de canal autorizado;
- O fabricante assegura o suporte técnico, o acesso a atualizações de software e firmware, atualizações de assinaturas de segurança e correções de vulnerabilidades durante todo o período contratual, desde que os respetivos serviços de suporte e subscrições sejam devidamente adquiridos, registados e ativados.

2. Plataforma de segurança de rede (NGFW)

A plataforma de segurança de rede deverá ser um equipamento físico dedicado (Next-Generation Firewall) e cumprir, **no mínimo**, os seguintes requisitos de hardware, desempenho e funcionalidade:

- A solução deverá ser fornecida obrigatoriamente em formato equipamento físico dedicado, incluindo hardware, sistema operativo embebido, interface de administração e mecanismos de atualização.
- O equipamento deverá apresentar, no mínimo, as seguintes características de desempenho e capacidade:

Características	Valor mínimo
Throughput de Firewall (IPv4)	≥ 39 Gbps
Throughput de Proteção contra Ameaças (Threat Protection)	≥ 2.8 Gbps
Throughput de IPS/IDS	≥ 5.3 Gbps
Throughput de Inspeção SSL/TLS	≥ 3 Gbps
Throughput de VPN IPSec	≥ 35 Gbps
Sessões concorrentes	≥ 3 000 000
Novas sessões por segundo	≥ 140 000
Políticas de firewall	≥ 10 000
Domínios virtuais (VDOMs)	10
Pontos de acesso wireless geridos	≥ 128
Switches geridos	≥ 48
Tokens de autenticação multifator	≥ 5000

- O equipamento deverá incluir, no mínimo, as seguintes interfaces de rede físicas:

Tipo de interface	Quantidade mínima
SFP+ 10GbE	**4**
RJ45 1GbE	**18**
SFP 1GbE	**8**

- equipamento deverá incluir armazenamento interno composto por 1 disco de 480 GB em formato SSD, para armazenamento local de logs e configurações.
- equipamento deverá incluir fontes de alimentação redundantes (mínimo 2 PSU), garantindo continuidade de operação em caso de falha de uma das fontes.
- equipamento deverá dispor de aceleração por hardware dedicada ao processamento de funções de rede e de segurança, através de processadores especializados (não devendo o desempenho depender exclusivamente de CPU de uso geral), de modo a garantir os débitos exigidos com inspeção ativa.
- A aceleração por hardware deverá abranger, no mínimo, funções críticas de processamento de tráfego de rede, incluindo encaminhamento, NAT, IPv4/IPv6 e cifragem/decifragem IPSec, bem como apoiar, sempre que suportado pela arquitetura do modelo proposto, funções de segurança computacionalmente intensivas. A solução deverá, em qualquer caso, comprovar o cumprimento dos débitos mínimos exigidos com as funcionalidades de inspeção ativa habilitadas.
- A arquitetura de hardware deverá privilegiar a eficiência energética, apresentando um rácio de desempenho por watt otimizado para as funções de segurança exigidas.
- A solução deverá suportar criação e gestão de zonas de segurança, com aplicação de políticas de controlo de acesso entre zonas.
- A solução deverá suportar NAT de origem e destino, incluindo NAT 1:1 e NAT de pool.
- A solução deverá disponibilizar portal Web de administração centralizado, com controlo de acesso baseado em perfis administrativos diferenciados.

- A solução deverá suportar gestão via CLI (SSH) e API REST para integração e automatização.
- A solução deverá disponibilizar registos detalhados de auditoria e eventos de segurança, com capacidade de exportação para plataformas SIEM em formatos standard (syslog conforme RFC 3164/5424, CEF - Common Event Format - e CSV).
- A solução deverá suportar mecanismos de backup, restore e exportação de configuração.

3. Funcionalidades de Rede e Plataforma

A solução deverá disponibilizar nativamente um conjunto abrangente de funcionalidades de rede e de plataforma, nomeadamente:

- A solução deverá suportar os modos de operação NAT/Route e Transparente (bridge), permitindo a sua integração em diferentes topologias de rede.
- A solução deverá suportar a operação simultânea de múltiplos domínios virtuais (VDOMs), com modos de operação NAT/Route ou Transparente independentes por domínio.
- A solução deverá suportar segmentação de rede através de VLANs (IEEE 802.1Q), interfaces virtuais e sub-interfaces.
- A solução deverá suportar a criação de switch por software, permitindo a agregação lógica de múltiplas interfaces num único segmento e a aplicação de políticas de tráfego entre portas do mesmo switch. Deverá ainda suportar, quando aplicável, controlo de acesso por 802.1X, MAB e atribuição dinâmica de VLAN.
- A solução deverá suportar encaminhamento estático e por políticas (policy routing).
- A solução deverá suportar protocolos de encaminhamento dinâmico para IPv4 e IPv6, incluindo RIP/RIPng, OSPFv2/OSPFv3, IS-IS e BGP/BGP4+, conforme aplicável ao protocolo IP utilizado.
- A solução deverá suportar encaminhamento multicast (PIM em modos sparse e dense) em modo NAT/Route.
- A solução deverá suportar Virtual Routing and Forwarding (VRF), permitindo a coexistência de múltiplas instâncias da tabela de encaminhamento, com route leaking entre VRFs.

- A solução deverá disponibilizar, de forma integrada, servidores e serviços de rede essenciais, nomeadamente servidor DHCP, servidor e proxy DNS, e servidor NTP.
- A solução deverá suportar DNS dinâmico (DDNS) para IPv4 e IPv6.
- A solução deverá incluir proteção contra ataques de negação de serviço (DoS e determinados padrões de tráfego DDoS), com deteção por anomalias e baseada em taxas (rate-based), proteção contra inundações (flood) de TCP, UDP, SCTP e ICMP, e contra port scan e ICMP sweep, para IPv4 e IPv6.
- A solução deverá suportar a identificação e classificação automática de dispositivos na rede (device identification/fingerprinting), com gestão de inventário para efeitos de visibilidade e de definição de políticas.
- A solução deverá disponibilizar, na consola de gestão, métricas de utilização por política (nomeadamente volume de tráfego em bytes e pacotes, número de correspondências/hit count e data/hora da última utilização - last used), bem como capacidades de pesquisa e filtragem sobre estas métricas, de modo a identificar as políticas de maior impacto ou mais utilizadas, facilitando a gestão e o diagnóstico (troubleshooting).

4. Alta Disponibilidade (HA)

A solução deverá ser implementada em alta disponibilidade, garantindo a continuidade do serviço em caso de falha. Para o efeito, deverá cumprir os seguintes requisitos:

- A solução deverá ser fornecida em configuração de alta disponibilidade, composta por dois equipamentos idênticos em cluster, operando em modo Ativo/Passivo.
- No modo Ativo/Passivo, um dos nós processa o tráfego enquanto o segundo permanece em espera (standby), assumindo automaticamente o serviço em caso de falha do nó ativo.
- cluster de HA deverá garantir failover automático, minimizando a interrupção do serviço, em caso de falha de hardware, de software ou de ligação de um dos nós.
- A solução deverá assegurar proteção contra falha de equipamento (device failover), falha de ligação local (link failover) e falha de ligação remota (remote link failover).

- A solução deverá suportar sincronização contínua e em tempo real da configuração entre os nós do cluster, garantindo que ambos mantêm uma configuração idêntica.
- A solução deverá suportar a sincronização (session pickup) das sessões ativas entre os nós, incluindo sessões TCP e, mediante ativação específica, sessões UDP, ICMP, NAT e túneis VPN IPSec, tanto IPv4 como IPv6, de modo a minimizar a interrupção das sessões em curso durante um evento de failover. Poderão verificar-se limitações na sincronização de sessões processadas por perfis proxy-based.
- A solução deverá suportar a sincronização das tabelas de encaminhamento e da informação de estado relevante entre os nós do cluster, podendo existir parâmetros ou exceções de sincronização específicos de implementação.
- A solução deverá suportar monitorização do estado das interfaces (interface/link monitoring), despoletando o failover quando uma interface monitorizada fica indisponível.
- A solução deverá suportar deteção de falha de caminho de rede a montante (verificação de disponibilidade de gateway/destino remoto), despoletando o failover quando o caminho deixa de estar acessível.
- A solução deverá permitir a definição de prioridades e de critérios de eleição do nó primário (ex: estado das interfaces monitorizadas, prioridade configurada, tempo de atividade).
- A solução deverá suportar a comunicação de sincronização e de estado (heartbeat) entre os nós através de uma ou mais ligações, com a possibilidade de utilizar múltiplas ligações para redundância da comunicação do cluster.
- A solução deverá suportar mecanismos de atualização coordenada de firmware dos nós do cluster (ex: uninterrupted upgrade), de modo a minimizar a indisponibilidade do serviço durante o processo de atualização.
- A solução deverá suportar a segmentação lógica do cluster, permitindo que diferentes domínios virtuais sejam distribuídos entre os nós (clustering virtual), quando aplicável.
- A solução deverá permitir a substituição de um nó com falha sem necessidade de reconfiguração manual da configuração de serviço, após a aplicação dos parâmetros mínimos de HA no nó substituto, com posterior sincronização automática da configuração a partir do nó em operação.

- A solução deverá ser compatível com mecanismos de redundância de gateway baseados em normas abertas (ex: VRRP), para interoperabilidade com equipamentos de terceiros, quando aplicável.
- A solução deverá disponibilizar mecanismos de monitorização do estado do cluster (estado de cada nó, sincronização e papel ativo/passivo), com geração de alertas e registo de eventos em caso de alteração de estado ou failover.

5. Inspeção aplicacional e controlo de conteúdo (NGFW)

A solução deverá disponibilizar capacidades de inspeção aplicacional e controlo de conteúdo sobre o tráfego de rede, de acordo com os requisitos técnicos descritos nos pontos seguintes. As funcionalidades identificadas constituem requisitos exigíveis à plataforma, podendo a sua ativação depender de licenciamento ou subscrição específica. As subscrições obrigatórias no âmbito do presente procedimento encontram-se identificadas na secção "Subscrições de segurança".

- A solução deverá suportar inspeção e controlo de tráfego ao nível da aplicação (Layer 7), com identificação de aplicações independentemente da porta ou protocolo utilizado.
- A solução deverá disponibilizar base de dados de assinaturas de aplicações (Application Control) e Inline CASB, com atualização automática pelo fabricante.
- A solução deverá suportar a inspeção de tráfego cifrado SSL/TLS, nos termos detalhados na secção relativa à gestão de certificados e inspeção profunda.
- A solução deverá ter capacidade de prevenção de intrusões (IPS/IDS), com deteção baseada em assinaturas e análise de protocolo, atualização automática da base de assinaturas e bloqueio de URLs maliciosas.
- A solução deverá ter capacidade de proteção avançada contra malware (AMP), incluindo antivírus, proteção contra mobile malware, Virus Outbreak Protection, Content Disarm & Reconstruct (CDR), deteção heurística por inteligência artificial e análise em ambiente isolado (sandbox cloud).
- A solução deverá ter capacidade de prevenção inline de malware com base em inteligência artificial (AI-based Inline Malware Prevention), assegurando proteção em tempo real contra ameaças desconhecidas e zero-day, com veredicto sub-segundo.

- A solução deverá ter capacidade de filtragem de URL por categorias, filtragem DNS e filtragem de vídeo (YouTube e outras plataformas), com base de dados de reputação Web atualizada pelo fabricante.
- A solução deverá ter capacidade de proteção Anti-Botnet e contra comando e controlo (C2), com bloqueio dinâmico em tempo real de comunicações com servidores maliciosos.
- A solução deverá ter capacidade de bloqueio de certificados maliciosos (blacklist dinâmica baseada em fingerprint), de modo a bloquear comunicações de botnet sobre SSL e tentativas de contornar as proteções de malware e IPS.
- A solução deverá ter capacidade anti-spam, com identificação de IPs e remetentes de spam, URLs de phishing e checksums de mensagens de spam, por consulta a serviços do fabricante.
- A solução deverá ter capacidade de Prevenção de Perda de Dados (DLP), com base de dados de padrões predefinidos para deteção de dados sensíveis em trânsito (ex: dados pessoais, dados de cartões de pagamento).
- A solução deverá ter capacidade de Inline CASB com visibilidade e controlo granular sobre o acesso e utilização de aplicações SaaS.
- A solução deverá ter capacidade de avaliação da superfície de ataque (Attack Surface Security ou equivalente), com monitorização contínua da infraestrutura, classificação (scoring) da postura de segurança, deteção de dispositivos IoT e correlação de vulnerabilidades.
- A solução deverá ter capacidade de segurança para ambientes de tecnologia operacional (OT), com deteção de dispositivos OT, correlação de vulnerabilidades, virtual patching e assinaturas específicas para aplicações e protocolos industriais.
- A solução deverá ter capacidade de orquestração e monitorização SD-WAN (orquestração de overlay, monitorização de underlay e de aplicações), complementando a funcionalidade SD-WAN base que é nativa do equipamento.

6. SD-WAN

A solução deverá disponibilizar capacidades de SD-WAN nativas, para otimização e resiliência das ligações de rede alargada, cumprindo os seguintes requisitos:

- A solução deverá incluir capacidades base de SD-WAN nativas, integradas no sistema operativo do equipamento, sem necessidade de hardware ou software adicional para a sua utilização.
- A solução deverá suportar a agregação de múltiplas ligações WAN simultâneas, de diferentes tecnologias, incluindo fibra, xDSL, 4G/5G e MPLS, desde que apresentadas ao equipamento através de interfaces físicas ou lógicas suportadas, ficando a escalabilidade limitada pela capacidade e interfaces suportadas pelo modelo proposto.
- A solução deverá suportar seleção dinâmica de caminho com base em métricas de qualidade de ligação, incluindo latência, jitter e perda de pacotes.
- A solução deverá suportar políticas de encaminhamento de tráfego por aplicação, utilizador, origem, destino, serviço, base de dados de serviços de Internet, marcação DSCP ou qualidade de serviço.
- A solução deverá suportar load balancing e failover automático entre ligações WAN, encaminhando o tráfego por ligações alternativas em caso de degradação ou indisponibilidade, com minimização do impacto nas sessões em curso.
- A solução deverá permitir a definição de SLAs por aplicação, serviço ou destino, com monitorização contínua da qualidade das ligações WAN.
- A solução deverá suportar QoS, com priorização de tráfego crítico, controlo de largura de banda e aplicação de políticas de traffic shaping.
- A solução deverá disponibilizar monitorização e visibilidade em tempo real do desempenho das ligações WAN e do tráfego SD-WAN.

7. VPN e Acesso Remoto Seguro

A solução deverá disponibilizar mecanismos de VPN e de acesso remoto seguro, para interligação de localizações e acesso de utilizadores, cumprindo os seguintes requisitos:

- A solução deverá suportar VPN IPSec site-to-site para interligação segura entre localizações, com suporte a IKEv1 e IKEv2.
- A solução deverá suportar acesso remoto seguro através de VPN IPSec dial-up, em modo client-to-gateway, preferencialmente com IKEv2, com cliente compatível para Windows, macOS, Linux, iOS e Android, considerando as funcionalidades suportadas por cada sistema operativo.
- A solução deverá suportar ZTNA (Zero Trust Network Access) para acesso aplicacional seguro, com verificação contínua de identidade e postura do dispositivo, dispensando o modelo tradicional de VPN de acesso remoto baseado em túnel.
- O acesso ZTNA deverá ser baseado em políticas por aplicação, garantindo o princípio de menor privilégio e validação do contexto de acesso (identidade, dispositivo, localização).
- A solução deverá suportar a publicação segura de aplicações e serviços internos através de um modelo de proxy de acesso (access proxy), efetuando reverse-proxy das ligações dos utilizadores para os servidores protegidos sem os expor diretamente à rede externa.
- A solução deverá ter capacidade para integrar com pontos de acesso ou proxies ZTNA externos, quando suportado pela versão de sistema operativo proposta, podendo atuar como conector de serviço e estabelecer uma ligação de controlo persistente para o encaminhamento seguro de pedidos de acesso aos recursos protegidos, quando essa arquitetura for pretendida.
- A solução deverá suportar autenticação multifator para acesso remoto, integrando com soluções de MFA externas via RADIUS.
- A solução deverá suportar split tunneling, permitindo controlo granular do tráfego encaminhado pelo túnel.
- A solução deverá suportar um mínimo de 2000 túneis IPSec simultâneos e 500 sessões de acesso remoto simultâneas.
- A solução deverá suportar algoritmos de cifragem modernos, incluindo AES-256, SHA-256 e superiores.

8. Integração com arquitetura de segurança integrada

A solução deverá ser fornecida como parte de uma arquitetura integrada do mesmo fabricante, incluindo a firewall e os restantes componentes propostos, assegurando interoperabilidade nativa, gestão coordenada, partilha automática de informação de segurança e visibilidade centralizada. Esta arquitetura deverá simplificar a operação, facilitar o diagnóstico, permitir políticas consistentes e acelerar a resposta a incidentes.

- A solução deverá integrar nativamente com a arquitetura de segurança integrada do fabricante (security fabric ou equivalente), permitindo a partilha de informação de ameaças e a coordenação de respostas entre os diferentes componentes de segurança.
- A solução deverá suportar conectores de integração (fabric connectors ou equivalente) para integração com produtos do mesmo fabricante e com plataformas de terceiros (cloud pública, SDN, soluções de identidade).
- A solução deverá disponibilizar uma topologia visual da arquitetura de segurança, com visibilidade dos dispositivos, endpoints e respetivo estado de segurança.
- A solução deverá incluir capacidades de avaliação de postura de segurança, Security Rating ou equivalente, com verificação da conformidade com boas práticas e apresentação de recomendações. As verificações avançadas, incluindo correlação de vulnerabilidades, deteção de IoT e alertas de surtos, deverão estar incluídas quando exigidas na secção de subscrições de segurança.

9. Gestão de Certificados e Inspeção Profunda

A solução deverá disponibilizar capacidades nativas de gestão de certificados digitais e de inspeção profunda de tráfego cifrado, cumprindo os seguintes requisitos:

- A solução deverá suportar inspeção profunda de tráfego cifrado SSL/TLS (deep inspection), com desencriptação e reencriptação para análise de conteúdo, aplicando as restantes funcionalidades de segurança (IPS, antivírus, filtragem) ao tráfego cifrado.
- A solução deverá suportar TLS 1.3 em cenários de inspeção SSL/TLS, permitindo a inspeção de tráfego cifrado com protocolos atuais, de acordo com as capacidades da versão de sistema operativo proposta.

- A solução deverá disponibilizar certificados/autoridade certificadora interna para utilização em inspeção SSL/TLS, bem como suportar a importação de certificados emitidos por CA corporativa existente.
- A solução deverá permitir a definição de exceções de inspeção por categoria, domínio, endereço ou aplicação, de modo a respeitar requisitos de privacidade e conformidade (ex: tráfego bancário, saúde).
- A solução deverá suportar inspeção SSL/TLS em cenários outbound e inbound, incluindo a proteção de utilizadores e de servidores internos publicados através de políticas de firewall, de acordo com as capacidades do modelo e da versão do sistema operativo propostos.
- A solução deverá suportar inspeção de certificados (certificate inspection) como modo alternativo, validando o certificado do servidor sem desencriptação completa do tráfego.
- A solução deverá validar certificados de servidor, permitindo detetar e bloquear certificados expirados, revogados, não fidedignos ou inválidos, bem como certificados maliciosos quando suportado pela subscrição de segurança aplicável.
- A solução deverá suportar gestão centralizada de certificados digitais, incluindo importação, exportação, geração de pedidos de assinatura e renovação, com suporte a formatos normalizados, incluindo PEM e PKCS#12.

10. Subscrições de segurança

A presente secção identifica as subscrições de segurança obrigatórias no âmbito do presente procedimento, correspondentes às funcionalidades que deverão ser efetivamente licenciadas, fornecidas e mantidas ativas com a solução durante todo o período contratual.

- A proposta deverá incluir uma subscrição em formato de pacote integrado de segurança de nível Avançado, válida pelo período mínimo de 36 meses, fornecida de forma contínua durante todo o período contratual e sem lacunas de cobertura. O pacote deverá incluir, no mínimo, as funcionalidades descritas nos pontos seguintes:
- Sistema de prevenção de intrusões (IPS/IDS): a subscrição deverá fornecer deteção e bloqueio de tráfego malicioso baseado em assinaturas e análise de protocolo, com atualização automática

e contínua da base de assinaturas pelo fabricante, incluindo proteção contra a exploração de vulnerabilidades conhecidas (virtual patching).

- Proteção avançada contra malware (antivírus): a subscrição deverá fornecer inspeção de ficheiros em trânsito com deteção de malware conhecido e desconhecido, proteção contra malware móvel, deteção heurística baseada em inteligência artificial, sanitização de conteúdo (CDR) e análise em ambiente isolado (sandbox cloud).
- Filtragem Web, DNS e de conteúdos: a subscrição deverá fornecer filtragem de URL por categorias, filtragem de pedidos DNS e filtragem de conteúdos de vídeo, com base de dados de classificação e reputação Web atualizada continuamente pelo fabricante.
- Filtragem de conteúdos de vídeo: a subscrição deverá fornecer filtragem granular de conteúdos de vídeo em plataformas como YouTube e outras, com classificação e controlo por categoria de conteúdo.
- Proteção anti-botnet e contra comando e controlo (C2): a subscrição deverá fornecer o bloqueio dinâmico, em tempo real, de comunicações com servidores de comando e controlo e domínios maliciosos, com base em feeds de informação de ameaças atualizados pelo fabricante.
- Bloqueio de certificados maliciosos: a subscrição deverá fornecer uma blacklist dinâmica de certificados (baseada em fingerprint), permitindo bloquear comunicações de botnet que utilizam SSL e tentativas de contornar as proteções de malware e IPS.
- Anti-spam: a subscrição deverá fornecer a identificação, por consulta a serviços do fabricante, de endereços IP e remetentes de spam, URLs de phishing e de spam conhecidas e checksums de mensagens de spam.
- Serviços base de atualização (incluídos no suporte): a solução deverá incluir, sem custo adicional, os serviços de atualização base, nomeadamente: controlo de aplicações, Inline CASB, deteção de dispositivos/SO, GeoIP, certificados de CA fidedignos, base de serviços de Internet e IPs de botnet, DDNS, proteção local (virtual patching das interfaces de gestão), verificação PSIRT, anti-phishing e atualização de fuso horário.
- Suporte e manutenção do fabricante: a subscrição deverá incluir o suporte técnico do fabricante e o acesso a atualizações de software, firmware e correções de segurança durante todo o período contratual.

11. Serviços de Gestão, Operação e Migração

Os serviços de gestão, operação e migração identificados na presente secção deverão ser prestados exclusivamente pelo fabricante da solução firewall, assegurando a integração nativa com a plataforma proposta, a qualidade técnica do serviço e a uniformidade de responsabilidades. Não serão admitidos serviços prestados por terceiros, ainda que parceiros do fabricante.

A solução deverá incluir um serviço de Security Operations Center as a Service, prestado pelo fabricante da solução firewall, em regime 24x7x365, para monitorização contínua de logs e alertas de segurança, triagem de eventos e identificação de potenciais incidentes.

- O serviço deverá recorrer a equipas especializadas de operações de segurança, suportadas por capacidades avançadas de análise, inteligência artificial e machine learning, para deteção de ameaças, análise de alertas e apoio à resposta a incidentes.
- Após a investigação de um incidente, o serviço deverá assegurar a notificação à entidade adjudicante com informação sobre a natureza do incidente e recomendações de remediação.
- O serviço deverá disponibilizar portal cloud para visibilidade dos eventos de segurança, comunicação operacional com especialistas, reporting e acompanhamento da melhoria contínua da postura de segurança.
- O serviço deverá permitir integração com serviços geridos complementares do mesmo fabricante, incluindo gestão remota da firewall e serviços de investigação forense, quando contratados, de modo a reforçar a resposta coordenada a incidentes.

Todos os serviços de gestão, operação e migração incluídos deverão estar cobertos pelo licenciamento proposto, sem custos adicionais para cumprimento destes requisitos.

12. Plataforma de Proteção e Deteção de Endpoint

A solução deverá incluir uma plataforma unificada de proteção, deteção e resposta em endpoint, fornecida em modelo de serviço cloud, com gestão centralizada dos dispositivos geridos e cumprindo os seguintes requisitos:

- A plataforma deverá ser fornecida em modelo de serviço cloud, com consola de gestão centralizada que permita a administração de um mínimo de 100 endpoints, incluindo dispositivos Windows, macOS e Linux.
- A plataforma deverá disponibilizar um dashboard em tempo real com o estado de segurança dos endpoints, inventário de software, gestão de vulnerabilidades, controlo de quarentena e atribuição dinâmica de grupos e políticas.
- A plataforma deverá suportar integração com Active Directory e Azure Active Directory para gestão de identidades e atribuição automática de grupos.
- A plataforma deverá disponibilizar controlo de acesso baseado em funções (RBAC), permitindo a separação de responsabilidades entre equipas de IT e de operações de segurança.
- A plataforma deverá incluir um agente unificado com capacidades de Zero Trust Network Access (ZTNA) e VPN, permitindo o acesso seguro a aplicações privadas, recursos internos e serviços corporativos, independentemente da localização do utilizador.
- A solução deverá permitir a aplicação de políticas de acesso baseadas na identidade do utilizador, grupo e postura de segurança do endpoint, com validação dinâmica do estado de conformidade do dispositivo.
- A solução deverá suportar acesso granular por aplicação, evitando a exposição ampla da rede interna e permitindo que os utilizadores apenas acedam às aplicações e recursos explicitamente autorizados.
- A solução deverá suportar validação contínua, ou quase em tempo real, da postura do endpoint antes e durante o acesso, incluindo verificação de conformidade, estado de segurança do dispositivo e políticas de acesso dinâmicas.
- A solução deverá permitir a substituição ou complementaridade com modelos tradicionais de VPN, suportando túneis encriptados ZTNA e VPN, bem como mecanismos de acesso remoto seguro geridos centralmente.
- A solução deverá permitir integração com gateway de aplicação, firewall ou componente equivalente do fabricante para aplicação das políticas ZTNA, incluindo verificação de identidade do utilizador, identidade do dispositivo e postura do endpoint.

- A solução deverá disponibilizar visibilidade centralizada sobre utilizadores, dispositivos, aplicações acedidas, estado de conformidade e eventos de acesso, permitindo auditoria e resposta a incidentes.
- A plataforma deverá incluir filtragem Web e de vídeo no endpoint, com proteção contra phishing e botnets, e controlo granular de aplicações Web, YouTube e aplicações SaaS.
- A plataforma deverá incluir capacidades CASB inline e baseado em API para visibilidade, controlo, proteção de dados e aplicação de políticas de segurança sobre aplicações SaaS, quando aplicável à arquitetura proposta.
- A plataforma deverá incluir capacidades de análise, priorização e remediação de vulnerabilidades nos endpoints, permitindo identificar aplicações instaladas, versões, vulnerabilidades conhecidas e CVEs aplicáveis.
- A plataforma deverá permitir a criação de políticas granulares de virtual patching baseadas em utilizadores e grupos de dispositivos, permitindo mitigar riscos antes da aplicação de patches tradicionais.
- A plataforma deverá permitir a aplicação de políticas de mitigação através de integração com políticas de firewall, políticas ZTNA ou quarentena de endpoints comprometidos.
- A plataforma deverá suportar gestão de patching dos endpoints, incluindo dispositivos remotos ou fora da rede corporativa, reduzindo a necessidade de intervenção manual.
- A plataforma deverá incluir capacidades de Endpoint Protection Platform (EPP), com proteção avançada contra malware, ransomware, exploits, ameaças fileless e ficheiros desconhecidos, em tempo real e de forma integrada com o agente instalado no endpoint.
- A plataforma deverá utilizar mecanismos de análise comportamental, inteligência artificial, sandboxing cloud e inteligência de ameaças do fabricante, permitindo a prevenção e classificação de ameaças conhecidas e desconhecidas.
- A plataforma deverá incluir prevenção de exploits e proteção contra técnicas de ataque avançadas, reduzindo a superfície de exposição do endpoint e bloqueando comportamentos maliciosos associados a abuso de aplicações, scripts, memória ou execução de código.

- A plataforma deverá incluir análise de ficheiros desconhecidos em sandbox cloud, com classificação automática de objetos suspeitos e partilha de indicadores com os serviços de inteligência de ameaças do fabricante.
- A plataforma deverá incluir proteção contra ransomware baseada em comportamento, com capacidade de bloqueio da atividade maliciosa e reversão da encriptação provocada por ransomware, permitindo repor o endpoint para um estado anterior à infeção em dispositivos Windows, macOS e Linux.
- A plataforma deverá permitir o isolamento ou quarentena centralizada de endpoints comprometidos, prevenindo a propagação de ameaças na rede.
- A plataforma deverá permitir ações remotas de contenção e remediação a partir da consola de gestão.
- A plataforma deverá permitir a configuração centralizada de políticas de proteção, políticas de segurança, grupos, alertas e ações automáticas, garantindo uma postura homogénea de proteção em ambientes Windows, macOS e Linux.

13. Plataforma de Gestão de Identidade e Autenticação

A solução deverá incluir uma plataforma de gestão de identidade e autenticação multifator (MFA), fornecida em formato de máquina virtual (ou equivalente), integrada com os restantes componentes da solução e cumprindo os seguintes requisitos:

- A plataforma deverá ser fornecida em formato de máquina virtual, compatível com infraestruturas de virtualização standard (VMware ESXi, Microsoft Hyper-V, KVM ou equivalente), com capacidade de suportar um mínimo de 200 utilizadores geridos, e de escalar através de licenciamento adicional.
- A plataforma deverá suportar alta disponibilidade em modo ativo/passivo, com sincronização automática de configuração e base de dados de utilizadores entre nós.
- A plataforma deverá suportar gestão local de utilizadores e grupos, com importação e sincronização automática a partir de diretórios LDAP/Active Directory, permitindo a gestão centralizada de identidades.

- A plataforma deverá suportar múltiplos domínios e fontes de autenticação simultâneos, permitindo a segregação de utilizadores por contexto organizacional.
- A plataforma deverá suportar autenticação via RADIUS, permitindo a integração com equipamentos de rede e de segurança para autenticação de acessos VPN, wireless e outros serviços de rede.
- A plataforma deverá suportar SAML 2.0 como Identity Provider (IdP), permitindo a autenticação federada em aplicações e serviços cloud e on-premises compatíveis.
- A plataforma deverá suportar OAuth 2.0 e OpenID Connect (OIDC), permitindo a integração com aplicações modernas, serviços cloud e cenários de single sign-on compatíveis com estes protocolos.
- A plataforma deverá suportar autenticação multifator (MFA), incluindo tokens de software (OTP por aplicação móvel), tokens de hardware OTP, validação por SMS/email e métodos baseados em FIDO2/WebAuthn, podendo combinar múltiplos fatores por política.
- A plataforma deverá permitir a definição de políticas de MFA por utilizador, grupo, localização ou contexto de acesso, incluindo a possibilidade de dispensar o segundo fator em cenários de risco reduzido.
- A plataforma deverá integrar-se nativamente com a plataforma de firewall proposta, permitindo a aplicação de políticas de acesso baseadas em identidade de utilizador autenticado.
- A plataforma deverá disponibilizar um portal de self-service para utilizadores, permitindo a gestão autónoma de tokens, alteração de credenciais e registo de dispositivos MFA, reduzindo a dependência do serviço de helpdesk.
- A plataforma deverá disponibilizar um portal de gestão de convidados (guest portal), com fluxos de aprovação configuráveis, expiração automática de contas temporárias e personalização da experiência do utilizador.
- A plataforma deverá suportar captive portal para autenticação de utilizadores em redes de acesso, com integração com os equipamentos de rede geridos.

- A plataforma deverá disponibilizar uma API REST para integração com sistemas de gestão de identidade (IAM) e automação de processos de provisionamento e desprovisionamento de utilizadores.
- A plataforma deverá integrar-se com a arquitetura de segurança integrada do fabricante, partilhando informação de identidade e contexto de autenticação com os restantes componentes.
- A plataforma deverá disponibilizar registos de auditoria detalhados dos eventos de autenticação, incluindo sucesso, falha, método utilizado, origem e contexto de acesso, com capacidade de exportação para plataformas SIEM através de syslog, API ou outros formatos standard suportados pela solução.

A proposta deverá incluir os seguintes tokens de autenticação multifator, para utilização com a plataforma de gestão de identidade proposta:

- Token Mobile (100 licenças): a proposta deverá incluir 100 licenças de token de autenticação por aplicação móvel, compatíveis com dispositivos iOS e Android, permitindo a geração de códigos OTP baseados nos standards TOTP (RFC 6238) e HOTP (RFC 4226). As licenças deverão ser geridas, atribuídas e ativadas através da plataforma de gestão de identidade proposta.
- Token OTP em formato porta-chaves (10 unidades): a proposta deverá incluir 10 tokens de autenticação por hardware em formato porta-chaves, com geração autónoma de códigos OTP baseados nos standards TOTP (RFC 6238) e/ou HOTP (RFC 4226), sem necessidade de conectividade de rede para geração do código. Os tokens deverão ser compatíveis com a plataforma de gestão de identidade proposta e geridos através da mesma.

14. Suporte técnico e manutenção

A solução deverá incluir suporte técnico e manutenção do fabricante durante todo o período contratual, cumprindo os seguintes requisitos:

- A proposta deverá incluir suporte técnico do fabricante pelo período mínimo de 36 meses, com acesso a atualizações de software, firmware e correções de segurança.
- O suporte deverá garantir tempo de resposta máximo de 4 horas para incidentes críticos (severidade 1).

- A proposta deverá incluir substituição avançada de hardware (NBD - Next Business Day) em caso de falha de equipamento durante o período de suporte.
- A proposta deverá incluir todos os componentes, licenças, bundles e subscrições necessários ao funcionamento integral da solução, não sendo admissíveis custos adicionais para cumprimento dos requisitos constantes do presente Caderno de Encargos.

Anexo II: Mapa de quantidades

Designação	Quantidade
Appliance firewall (Next-Generation Firewall), em alta disponibilidade	**2**
Suporte técnico do fabricante - 36 meses	**2**
Serviço SOCaaS do fabricante - 36 meses	**1**
Plataforma de proteção e deteção de endpoint — tier EPP (100 endpoints) - 36 meses	**1**
Plataforma de gestão de identidade e autenticação MFA (VM) — 200 utilizadores	**1**
Token de autenticação móvel	**100**
Token OTP hardware	**50**