



Instituto Politécnico
de Viana do Castelo

2021/CPU/001 – Upgrade dos equipamentos de segurança do Datacenter do IPVC

Caderno de Encargos

INSTITUTO POLITÉCNICO DE VIANA DO CASTELO

13 de janeiro de 2021

Criado por: IPVC

2021/CPU/001 – Upgrade dos equipamentos de segurança do Datacenter do IPVC

Caderno de Encargos

Índice

PARTE I - CLÁUSULAS JURÍDICAS	3
Entidade pública adjudicante	3
Objeto da adjudicação	3
Contrato.....	3
Financiamento do contrato	3
Prazo de execução do contrato.....	4
Gestor de contrato	4
Preço Base.....	4
Preço Contratual	4
Alterações ao Contrato	4
Condições de Pagamento.....	5
Sigilo	5
Penalizações	6
Subcontratação e Cessão da posição contratual.....	6
Casos fortuitos ou de força maior	7
Cessação do contrato	7
Rescisão do contrato.....	7
Legislação aplicável e foro competente.....	7
PARTE II – Responsabilidade social e ambiental dos fornecedores perante o IPVC	8
Objetivo.....	8
Âmbito.....	8
Responsabilidade	8
Regras a cumprir no interior das instalações do IPVC	8
PARTE III - CLÁUSULAS TÉCNICAS GERAIS	9
Locais de fornecimento do serviço	9
Atividades Desenvolvidas no IPVC	9
PARTE IV - CLÁUSULAS ESPECÍFICAS	10
Caracterização Genérica do Serviço	10
Arquitetura da solução a implementar.....	10
Quantidades	10
Especificações Técnicas	11
Dever de Colaboração.....	22

PARTE I - CLÁUSULAS JURÍDICAS

Artigo 1º

Entidade pública adjudicante

A entidade pública adjudicante é o **Instituto Politécnico de Viana do Castelo**, abreviadamente designado por IPVC, pessoa coletiva n.º 503 761 877, com sede na Rua Escola Industrial e Comercial de Nun'Álvares, n.º 34, 4900-347 Viana do Castelo

Artigo 2º

Objeto da adjudicação

O objeto do contrato consiste na aquisição de Upgrade dos equipamentos de segurança do Datacenter do Instituto Politécnico de Viana do Castelo, nas condições estabelecidas no presente caderno de encargos e de acordo com as subcategoria **48730000-4 - Pacote de software de segurança**, previstas no Regulamento (CE) n.º 213/2008 da Comissão, de 28 de Novembro (CPV).

Artigo 3º

Contrato

1. O contrato é composto pelo respetivo clausulado contratual e os seus anexos.
2. O contrato a celebrar integra ainda os seguintes elementos:
 - a. Os suprimentos dos erros e das omissões do Caderno de Encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
 - b. Os esclarecimentos e as retificações relativos ao Caderno de Encargos;
 - c. O presente Caderno de Encargos;
 - d. A proposta adjudicada;
 - e. Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
3. Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual aí são indicados.
4. Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato e seus anexos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do Código dos Contratos Públicos e aceites pelo adjudicatário nos termos do disposto no artigo 101.º desse mesmo diploma legal.

Artigo 4º

Financiamento do contrato

O encargo previsto no contrato será suportado pelo Orçamento do Instituto Politécnico de Viana do Castelo.

Artigo 5º

Prazo de execução do contrato

O contrato tem início à data da celebração e termo em 31 dezembro de 2023.

Artigo 6º

Gestor de contrato

Ao abrigo do art.º 96º do CCP o gestor de contrato nomeado para o presente procedimento é Duarte Nuno Castelo Lima da Silva, funcionário do IPVC e com a função de acompanhar permanentemente a execução do presente contrato, sendo que toda e qualquer anomalia, defeito ou desvio às cláusulas do mesmo devam ser reportadas por si e de imediato ao órgão competente, fazendo-se acompanhar por relatório com o elenco das medidas corretivas que julgue necessárias, nos termos e para os efeitos do artigo 290º - A do CCP.

Artigo 7º

Preço Base

1. Nos termos do n.º 1 do artigo 47º do Código dos Contratos Públicos (doravante designado CCP), o valor para efeito do preço base global do procedimento é de **82.500,00 euros** ao qual acresce o imposto sobre o valor acrescentado, preço fundamentado nos preços atualizados do mercado obtidos através da consulta preliminar prevista no artigo 35.º -A,
2. A informação pertinente resultante da consulta preliminar será, caso seja solicitada, disponibilizada aos futuros concorrentes do procedimento, após terminado o prazo de apresentação de propostas, através de um pedido em “outras comunicações” na plataforma Acingov.

Artigo 8º

Preço Contratual

1. Pelo fornecimento dos bens objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, o IPVC deve pagar ao fornecedor o preço constante das propostas adjudicadas, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.
2. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, nomeadamente os relativos ao transporte dos bens objeto do contrato para o respetivo local de entrega, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

Artigo 9º

Alterações ao Contrato

1. Qualquer alteração do contrato deverá constar de documento escrito assinado por ambos os outorgantes e produzira efeitos a partir da data da respetiva assinatura.

2. A parte interessada na alteração deve comunicar, por escrito, a outra parte essa intenção, com uma antecedência mínima de 60 (sessenta) dias em relação a data em que pretende ver introduzida a alteração;
3. O contrato pode ser alterado por:
 - a. Acordo entre as partes, que não pode revestir forma menos solene que o contrato;
 - b. Decisão judicial ou arbitral;
 - c. Razões de interesse público.
4. A alteração do contrato não pode conduzir a modificação de aspetos essenciais do mesmo, nem constituir uma forma de impedir, restringir ou falsear a concorrência.

Artigo 10º

Condições de Pagamento

1. As quantias devidas pelo Instituto Politécnico de Viana do Castelo, nos termos da cláusula anterior, **devem ser pagas no prazo de 60 dias**, nos termos previstos no art.º 299º do CCP, após a receção pelo Instituto das respetivas faturas, as quais só podem ser emitidas após a instalação e ativação do Hardware (após a obrigação respetiva do contrato).
2. Em caso de discordância por parte do contraente público, quanto aos valores indicados nas faturas, deve este comunicar ao cocontratante, por escrito, os respetivos fundamentos, ficando este obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida de acordo com as regras contabilísticas aplicadas.
3. Desde que devidamente emitidas e observado o disposto no n.º 1, as faturas são pagas através de transferência bancária.

Artigo 11º

Sigilo

O adjudicatário obriga-se ao sigilo de quaisquer informações que obtenha em virtude da execução do contrato, salvo se prévia e expressamente autorizado pela entidade contratante, nos termos e para os efeitos da Lei de Proteção de Dados Pessoais.

Artigo 12º

Proteção de dados pessoais

1. O segundo outorgante obriga-se ao estrito cumprimento do disposto no Regulamento Geral de Proteção de Dados (RGPD), aprovado pelo Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, na redação que lhe foi dada pela Retificação de 4 de maio de 2018, publicitada no Jornal Oficial da União Europeia de 23 de maio de 2018, nomeadamente no que diz respeito às obrigações relativas ao tratamento dos dados pessoais que lhe sejam transmitidos pelo primeiro outorgante para efeito de execução do presente contrato.

2. O segundo contratante compromete-se a adotar e apresentar garantias suficientes de execução das medidas técnicas e organizativas adequadas, de forma a se satisfaçam os requisitos do RGPD no tratamento dos dados pessoais e a defesa dos direitos dos titulares dos dados.

3. O segundo outorgante compromete-se ao cumprimento das demais obrigações e responsabilidades previstas na legislação vigente no que diz respeito ao tratamento dos dados pessoais.

Artigo 13º

Penalizações

1. No caso de mora no cumprimento ou cumprimento defeituoso das prestações do contrato por parte do adjudicatário e das garantias dadas, poderá o Instituto Politécnico de Viana do Castelo interpelar o adjudicatário para cumprir pontualmente as tarefas contratadas, quando tal ainda for possível e se mantenha o interesse do credor na prestação, devendo nesse caso o adjudicatário dar-lhe cumprimento imediato, bem como suportar os danos que o Instituto Politécnico de Viana do Castelo sofra na sequência de tais atos.

2. Ao ser interpelado para os efeitos previstos no número anterior, deverá o adjudicatário cumprir imediatamente e de forma integral e satisfatória a prestação em falta.

3. Em caso de atraso na conclusão da execução do serviço por facto imputável ao segundo outorgante, o primeiro outorgante pode aplicar, se assim o entender, uma sanção contratual pecuniária, por cada dia de atraso, de acordo com a lei (art.º 329º do CCP).

4. Para o efeito do disposto na cláusula anterior, não se considera que o segundo outorgante deu início à execução do serviço enquanto não tiver assinado o contrato.

Artigo 14º

Subcontratação e Cessão da posição contratual

1. O adjudicatário não poderá subcontratar ou ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato sem autorização da entidade adjudicante.

2. Para efeitos da autorização prevista no número anterior, deve:

- a. Ser apresentada pelo cessionário toda a documentação exigida ao adjudicatário no presente procedimento;
- b. A entidade adjudicante apreciar, designadamente, se o cessionário não se encontra em nenhuma das situações previstas no artigo 55º do Decreto-Lei n.º. 18/2008, de 29 de Janeiro e se tem capacidade técnica e financeira para assegurar o exato e pontual cumprimento do contrato.

3. A cessão da posição contratual por incumprimento do cocontratante deve cumprir o estipulado no artigo 318º-A do CCP.

Artigo 15º

Casos fortuitos ou de força maior

1. Nenhuma das partes incorrerá em responsabilidade se por caso fortuito ou de força maior, 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, 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.

Artigo 16º

Cessaç o do contrato

O IPVC pode rescindir o contrato, logo que se verifique o n o cumprimento das condi  es definidas no presente Caderno de Encargos ou na Lei.

Artigo 17º

Rescis o do contrato

1. O incumprimento, por uma das partes, dos deveres resultantes do presente contrato confere, nos termos gerais de direito,   outra parte o direito de rescindir o contrato, sem preju zo das correspondentes indemniza  es legais.
2. Para efeitos do n mero anterior, considera-se incumprimento definitivo quando o adjudicat rio n o cumprir integralmente as condi  es e obriga  es deste contrato, no prazo previsto no artigo 6  do presente caderno de encargos.
3. A rescis o n o prejudica o pagamento ao adjudicat rio dos servi os j  prestados em conformidade com o contrato.
4. A rescis o n o poder  afetar os servi os num prazo inferior a 60 dias  teis a contar da data da notifica  o.

Artigo 18º

Legisla  o aplic vel e foro competente

1. Em tudo o que o presente Caderno de Encargos for omissa observar-se-  o disposto no C digo dos Contratos P blicos e demais legisla  o aplic vel e, em qualquer caso, sempre a Lei portuguesa.
2. Para dirimir todas as quest  es emergentes do contrato ser  competente o Tribunal de C rculo Administrativo Local, sem preju zo da faculdade legalmente prevista de as partes poderem, se assim o acordarem, celebrar compromisso arbitral, submetendo qualquer eventual quest  o a decis o por arbitragem.

PARTE II – Responsabilidade social e ambiental dos fornecedores perante o IPVC

Artigo 19º

Objetivo

O desempenho social, ambiental e económico do Instituto Politécnico de Viana do Castelo (IPVC) depende também do desempenho dos seus fornecedores. Desta forma, para que o IPVC possa concretizar os seus objetivos, é também necessário, que todas as entidades contratadas por este partilhem dos princípios e valores estabelecidos.

No âmbito do seu Sistema de Gestão e para garantir o cumprimento integral dos requisitos legais aplicáveis, das normas NP EN ISO 9001 e NP 4469-1, o IPVC disponibiliza na sua página (<http://www.ipvc.pt/politica-de-gestao>), todos os princípios de responsabilidade social e ambiental dos fornecedores perante o IPVC.

Artigo 20º

Âmbito

O disposto no número anterior é aplicável a todas as entidades adjudicatárias resultantes deste procedimento.

Artigo 21º

Responsabilidade

O fornecedor é responsável pelo cumprimento integral dos requisitos legais e pelos requisitos definidos no presente capítulo, devendo monitoriza-los e verificar o seu cumprimento, desde o momento o momento da adjudicação e aceitação da nota de encomenda.

O incumprimento dos requisitos e dos princípios de responsabilidade social e ambiental dos fornecedores perante o IPVC poderão originar a suspensão da execução do contrato ou a sua cessação.

Artigo 22º

Regras a cumprir no interior das instalações do IPVC

É da responsabilidade dos fornecedores dar a conhecer aos seus colaboradores e subcontratados as regras estabelecidas neste regulamento, de forma a assegurar o seu cumprimento.

O fornecedor e os seus trabalhadores, quando acederem às instalações do IPVC, devem cumprir os seguintes requisitos:

- Cumprir integralmente a legislação aplicável, nomeadamente os aspetos relativos à Segurança e Saúde, Ambiente e Relações de Trabalho.
- Respeitar as regras e sinalização de segurança existente;
- Assegurar a utilização de equipamentos de proteção individual (EPI's), de acordo com atividades desenvolvidas;

- Respeitar as regras de separação de resíduos;
- Caso ocorra algum acidente durante a prestação do serviço ou fornecimento de bens, comunicar de imediato, devendo ser elaborado e disponibilizado ao IPVC um relatório escrito, com a análise das causas e ações correção e corretivas aplicadas e/ou a aplicar
- Numa situação de emergência e em caso de evacuação, obedecer com rigor às instruções dadas pelos elementos das equipas de evacuação ou responsável interno.

PARTE III - CLÁUSULAS TÉCNICAS GERAIS

Artigo 23º

Locais de fornecimento do serviço

O fornecimento dos serviços será prestado nos seguintes locais:

- a) Serviços Centrais sito na praça general Barbosa em Viana do Castelo;

Artigo 24º

Atividades Desenvolvidas no IPVC

O IPVC é uma instituição pública de ensino superior que tem como missão, difundir e transferir conhecimento e cultura, promover a formação integral dos cidadãos e a aprendizagem ao longo da vida, numa atitude de permanente inovação, qualidade e espírito empreendedor, centrado no desenvolvimento regional, do país e na internacionalização, em convergência com o espaço europeu do ensino superior.

PARTE IV - CLÁUSULAS ESPECÍFICAS

Artigo 25º

Caracterização Genérica do Serviço

O fornecimento dos bens e serviços, objeto deste procedimento, está relacionado com o upgrade dos atuais equipamentos de segurança do IPVC, com a finalidade de evolução tecnológica necessária para garantir a segurança dos serviços alojados e disponibilizados no Datacenter do IPVC.

Artigo 26º

Arquitetura da solução a implementar

A solução é composta por dois equipamentos em cluster que irão substituir os equipamentos existentes.

Solução requerida para implementação

- **Solução de firewall 2 x Sophos XG 550 ou equivalente**
 - 1 x XG 550 rev. 2 TotalProtect Plus, 3-year (EU power cord) ou equivalente
 - 1 x XG 550 rev. 2 Security Appliance - EU/UK power cord ou equivalente
 - 4 x 2 port 10GbE SFP+ Flexi Port module (for XG 750 and SG/XG 550/650 rev.2 only) ou equivalente
 - 4 x Dual Rate 10GBase-SR 10GbE Fiber Transceiver (GBIC), for UTM/SG/XG SFP+ ports ou equivalente
 - XG 550 Enhanced to Enhanced Plus Support Upgrade - 36 MOS ou equivalente
- **Solução de EDR para Servidores**
 - 200 x Central Intercept X Advanced for Server with EDR - 100-999 SERVERS - 36 MOS – EDU ou equivalente

Artigo 27º

Quantidades

A tabela seguinte discrimina as quantidades a comprar por cada item constante nas cláusulas técnicas, assim como, os respetivos valor base.

	Designação	Referência a marca	Quantidade	Preço TOTAL
Item 1	Equipamento de segurança – Firewall	Sophos XG 550 ou equivalente	2	69.735,55
Item 2	Serviços de implementação e suporte	N/A	1	12.764,45

Especificações Técnicas

Os serviços ou o fornecimento de bens a adquirir têm as seguintes especificações técnicas:

Item 1: Equipamentos de segurança – Firewall

1.1. Arquitetura

Características de Hardware (obrigatório dentro do mesmo equipamento)

- Formato 2U para rack de 19"
- Número de portas 1Gbit/s RJ45 ≥ 8
- Número de portas SFP+ 10Gbit/s ≥ 4
- Porta de consola RJ45;
- Baías de expansão ≥ 4
- Número de portas USB ≥ 3
- Discos rígidos SSD em RAID-1: $\geq 480\text{GB}$
- Memória RAM: $\geq 24\text{GB DDR4}$
- Temperatura (°C): ≥ 0 e ≤ 40
- Humidade (%): ≥ 5 e ≤ 90
- Consumo Energético (W/h): < 417
- Dissipação de Calor (BTU/h): < 1420
- Fonte de Alimentação Redundante: Sim

1.2. Performance

- Performance da appliance com a funcionalidade de firewall: $\geq 75\text{Gbps}$;
- Performance da appliance com a funcionalidade de firewall IMIX: $\geq 34\text{Gbps}$;
- Performance da appliance com a funcionalidade de VPN IPSec: $\geq 8.5\text{Gbps}$;
- Performance da appliance com a funcionalidade de IPS: $\geq 17\text{Gbps}$;
- Performance da appliance com a funcionalidade de NGFW (IPS e Application Control): $\geq 15.3\text{Gbps}$;
- Novas conexões TCP por segundo: ≥ 213.800 ;
- Conexões TCP concorrentes: ≥ 15.740 Milhões;
- Tuneis VPN SSL concorrentes: ≥ 3000 ;
- Suporte de IEEE 802.1Q até 4096 VLAN's;

1.3. Firewall

- **IDS/IPS:**
 - o Possibilidade de criação de regras personalizadas;
 - o Possibilidade de criação de assinaturas customizadas;
 - o Pelo menos 60 categorias;
 - o Assinaturas específicas para ambientes SCADA;
- Policy Routing e Forwarding para IPv4 e IPv6;
- LCAP – 802.3ad;
- NAT e PAT;
- Suporte para IPv4 e IPv6;
- Protocolos de Encaminhamento: RIP, OSPF, BGP e encaminhamento estático;
- Inspeção de Certificados e tráfego SSL;
- Proteção contra ataques DOS e DDOS;
- Duplo Motor de AntiMalware;
- Classificação do tráfego com DSCP Marking;
- Balanceamento de pelo menos 2 Links WAN, configurável por política;
- Políticas de SDWAN;
- Definição de políticas de Firewall por Zonas;
- Gestão de largura de banda por utilizador, grupos de utilizadores, VLAN, endereço IP, porto, horário, zonas (sejam estas internas ou externas) e aplicação;
- Deteção de Advanced Persistent Threats com recurso a sandboxing alojada na cloud;
- Identificação e bloqueio de aplicações desconhecidas com recurso a integração com uma solução de Endpoint Protection;
- Possibilidade de isolar máquinas comprometidas na rede com base no estado de saúde das mesmas sendo alcançado com a integração de uma solução de Endpoint Protection;
- Possibilidade de prevenção de movimento lateral no mesmo segmento de rede no caso de uma máquina ficar comprometida, mediante a comunicação com o Endpoint;

1.4. Autenticação

- Possibilidade de criação de utilizadores e grupos locais;
- Integração com Active Directory
- Integração com LDAP;
- Integração com TACACS+;

- Integração com RADIUS;
- Integração com eDirectory;
- Identificação de utilizadores conectados por Terminal Services;
- Certificados X.509v3;
- Identificação do Utilizador via integração com uma solução de Endpoint Protection;
- Autenticação Transparente (SSO) para criação de regras de utilizador em Firewall, Navegação Web, Controlo Aplicacional e Qualidade de Serviço;
- SSO para Windows e Mac OS X;
- Portal de Autenticação onde as conexões web devem ser redirecionadas para que se possa autenticar de forma manual;
- Autenticação por endereço IP;

1.5. Gestão

- Criação de perfis distintos de administração;
- Deve ser possível ser gerido desde uma consola cloud incluído no licenciamento;
- Gestão de backups, agendamento e armazenamento na Cloud;
- Licenciamento e atualização de assinaturas de forma offline;

1.6. VPN

- Suporte para IKEv1 e IKEv2: Sim
- Portal HTML5 para permitir acesso VPN sem recurso a cliente e que suporte os seguintes protocolos: RDP, TELNET, SSH, FTP, FTPS, SFTP, SMB e VNC;
- Compatibilidade com SDWAN;
- VPN Site-to-Site com recurso a IPSec e SSL;
- Configuração de túneis vpn ipsec com recurso a um wizard;
- Cliente VPN IPSec e SSL (baseado em OpenVPN) para Windows e MAC OS X incluído no licenciamento e sem limite de utilizadores;
- Acesso remoto via L2TP;
- Acesso remoto via PPTP;
- Compatibilidade com o Cisco VPN Client;

1.7. Controlo Aplicacional

- Reconhecimento de aplicações: >= 3000
- O controlo aplicacional deve ser capaz de identificar aplicações desconhecidas e que comuniquem por HTTPS sem a necessidade de quebrar o túnel SSL com recurso à comunicação com o endpoint. Deve também fornecer o caminho da aplicação para que esta possa ser classificada;

- Funcionalidade de CASB:
 - o Classificação de aplicações identificadas;
 - o QOS;

1.8. Filtragem Web

- Proteção contra páginas web maliciosas mediante filtragem por reputação;
- Proteção contra ameaças web com análise de malware;
- Filtragem de URL com mais de 100 categorias;
- Duplo motor de anti-malware;
- Capacidade para forçar “SafeSearch” para motor de busca Google, Yahoo e Bing;
- Funcionalidade de Cache para reduzir largura de banda;
- Detecção e bloqueio de proxies anónimos;
- Inspeção HTTPS com análise ao tráfego cifrado;
- Filtragem de tipos de ficheiros não autorizados;
- Filtragem web por palavras-chave dentro da própria página;
- Detecção do tipo real dos ficheiros (True File Type);
- Detecção de APT (com informação de equipamentos suspeitos);
- Suporte de acesso para convidados e equipamentos partilhados;
- Atualizações automáticas e LiveProtection;
- Autenticação flexível através de SSO (Single Sign-On) e Captive Portal;
- Políticas flexíveis por utilizador ou grupo de utilizadores com ou sem Active Directory ou eDirectory;
- Quotas de Navegação
 - o Quotas de Navegação cíclicas e não cíclicas;
 - o Quotas de Navegação por dia, semana, meses e anos;
- Bloqueio de Google QUIC;
- Bloqueio de downloads de aplicações potencialmente não desejadas;
- Possibilidade de fazer bypass a um URL bloqueado mediante de um voucher;

1.9. Quality of Service

- Catalogação de aplicações, serviços e aplicação de parâmetros de QoS limitando a largura de banda máxima, garantindo a largura de banda mínima e prioridades;
- QoS por utilizador, aplicação, URL e regras;
- Possibilidade de garantir uma determinada largura de banda;

- A limitação poderá ser por utilizador individual ou compartilhado por vários;
- Possibilidade de seleccionar a prioridade;
- Possibilidade de seleccionar a largura de banda de upload e download;
- Possibilidade de configurar uma programação de quando o QOS será aplicado;

1.10. Portal de Utilizador

- Através do portal de utilizador é possível a gestão de:
 - o Tickets para aceder ao WIFI;
 - o Acessos VPN HTML5;
 - o Quarentena de email do utilizador;
 - o Criação de vouchers de bypass do filtro web;

1.11. Web Application Firewall

- Form hardening;
- Scan do Dual antivirus, tanto para Upload como Downloads;
- Cookie signing;
- Static URL hardening;
- Bloqueio de clientes com má reputação;
- Protocol Violations;
- Protocol Anomalies;
- Request Limits;
- HTTP Policy;
- Bad Robots;
- Generic Attacks;
- SQL Injection Attacks;
- XSS Attacks;
- Tight Security;
- Trojans;
- Outbound;
- Criação de formulários de autenticação personalizados:
- Limite da sessão do utilizador
 - o Timeout
 - o Lifetime

1.12. Relatórios e Logs

- Os relatórios devem ser gerados e consultados sem recurso a um servidor externo;
- Possibilidade de integração com SIEM;
- Relatórios de utilizadores UTQ, coeficiente de ameaças de utilizador, que atribui uma pontuação aos utilizadores e que unifica no mesmo relatório alertas da firewall e do endpoint se estes existirem;
- Application Risk meter;
- Visualizador de logs em raw que permite ver vários módulos de logs ao mesmo tempo e com possibilidade de aplicar filtros de visualização;
- Policy tester, que permite testar tanto regras de firewall como filtros web antes de serem aplicados;
- Possibilidade de integração com sistema centralizado de reporting do mesmo fabricante;
- Possibilidade de criar capturas de tráfego pelo GUI;
- Automatização de configurações pela API;

1.13. Proteção de Email

- Filtro de email transparente;
- Filtro de email em modo MTA;
- Detecção, limpeza e quarentena de malware, spyware, trojans e worms;
- Taxa de deteção superior a 99% com baixo índice de falsos positivos;
- Proteção de perímetro avançada;
- Atualizações automáticas de AntiMalware e AntiSpam;
- WhiteLists/BlackLists e individual;
- Filtro de conteúdos para bloquear emails e ficheiros não autorizados;
- Detecção do real tipo de ficheiros (True File Type);
- DLP;
- Verificação SPF;
- Recipient validation;
- Adição de “disclaimer” aos emails enviados;
- Encriptação de email SPX/PDF para proteger dados sensíveis. Irá ser criado um PDF encriptado com todo o conteúdo do email, tanto o corpo do email como os anexos. Pode-se responder de forma encriptada também;
- Suporte de encriptação TLS;

- Políticas flexíveis por utilizadores ou grupos provenientes ou não de LDAP/Active Directory;
- Quarentena para utilizadores via web opcional;
- Resumo do email em quarentena opcional;
- Análise do email em SMTP, SMTPS, POP3, POP3S, IMAP e IMAPS;

1.14. WIFI

- A firewall pode atuar como o controlador dos dispositivos WIFI do mesmo fabricante;
- Os APs são plug&play, se conectados à rede da firewall irão aparecer na firewall para serem configurados;
- Modos de configuração:
 - o Bridge to AP LAN;
 - o Bridge VLAN;
 - o Redes separadas;
- Possibilidade de criar redes mesh;
- Hotspot:
 - o Password do dia
 - o limites de uso
 - o Autenticação backend com base em serviços de diretório, como LDAP, AD, Radius, etc.
 - o Criação de tickets por utilizadores através do portal de utilizador, com possibilidade de gerar tickets em bulk que podem ser descarregados em PDF ou Excel para impressão com os logos corporativos, podem ainda ser configurados para que expirem com o primeiro login podendo assim serem guardados durante um longo período. Estes tickets podem dar acesso por:
 - o Tempo, por exemplo, válido por dois dias.
 - o Tempo de sessão, por exemplo, tempo de navegação de duas horas.
 - o Volume de dados, limitar a 2GB durante a duração do ticket
 - o Opções anteriores em conjunto.
- Até 8 SSID por radio;
- Radius SSO authentication;
- VLAN tagging;
- Grupos de AP;
- Rogue AP detection;

1.15. Sandboxing

- Solução pode estar integrada na consola de gestão da Firewall;
- A plataforma de Sandboxing deverá estar alojada na Cloud, dispensando a instalação de qualquer servidor on-premise dedicado;
- Deve analisar:
 - o Executáveis Windows (incluindo EXE, COM e DLL);
 - o Documentos Word (incluindo .doc, .docx, docm e .rtf);
 - o Documentos PDF;
 - o Arquivos com os seguintes tipos de ficheiro (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet);
 - o Análise comportamental de malware através de deep learning, corre o ficheiro num ambiente real;
 - o Relatório de ficheiro malicioso e possibilidade de remoção do ficheiro, tempo médio de análise de menos de 120 segundos, políticas flexíveis de utilizador e de grupo para tipo de ficheiros, exclusões, e ações durante a análise. Suporte para one-time download links;
- Utilização de tecnologia Deep Learning;

1.16. Certificações

- CC EAL4+
- IPv6 Ready
- ICSA Labs Corporate Firewall

1.17. EDR para Servidor

- Consola de Gestão Centralizada única e alojada na Cloud que faça a gestão da componente de Endpoint e de EDR – Endpoint Detection and Response;
- Um único agente para a proteção de endpoint e EDR;
- Capacidade para promover Windows Servers com o agente de endpoint instalado a Cache Servers com vista a reduzir o consumo de largura de banda com updates dos endpoints Workstations sempre que estes estejam na rede local;
- Capacidade para promover Windows Servers a Message Brokers, com vista a permitir que endpoint Workstations sem comunicação direta com a Internet possam através destes comunicar com a consola de gestão centralizada;
- Capacidade de Workload Discovery para ambientes Amazon AWS e Microsoft Azure;
- Exclusões Automáticas para Softwares instalados no Endpoint como Microsoft Exchange, SQL Server, etc;
- Agente Endpoint específico para ambientes virtuais, com uma plataforma centralizada de varrimento de ameaças;

- Filtragem de URL's com a capacidade de bloqueio por Categorias Pré-Definidas;
- Capacidade de criação de uma Whitelist de Softwares autorizados a correr no endpoint, sendo que os restantes serão bloqueados;
- Controlo Aplicacional com base em Categorias Pré-Definidas;
- Controlo de Periféricos Externos com a capacidade de Monitorizar apenas ou Bloquear, sendo possível criar uma Whitelist de hardware id's de dispositivos autorizados;
- Motor DLP com a capacidade de criar regras com palavras ou expressões customizadas;
- Motor Anti-Malware com recurso a Machine Learning;
- Prevenção contra pelo menos os seguintes Exploits:
 - o Enforce Data Execution Prevention
 - o Mandatory Address Space Layout Randomization
 - o Bottom-up ASLR
 - o Null Page (Null Deference Protection)
 - o Heap Spray Allocation
 - o Dynamic Heap Spray
 - o Stack Pivot
 - o Stack Exec (MemProt)
 - o Stack-based ROP Mitigations (Caller)
 - o Branch-based ROP Mitigations
 - o Structured Exception Handler Overwrite (SEHOP)
 - o Import Address Table Filtering (IAF)
 - o Load Library
 - o Reflective DLL Injection
 - o Shellcode
 - o VBScript God Mode
 - o Wow64
 - o Syscall
 - o Hollow Process
 - o DLL Hijacking
 - o Squiblydoo Applocker Bypass
 - o APC Protection (Double Pulsar / AtomBombing)

- o Process Privilege Escalation
- Prevenção contra ameaças do tipo “active adversary” tais como:
 - o Prevent Credential Theft;
 - o Prevent APC violation;
 - o Prevent privilege escalation;
 - o Prevent code cave utilization;
 - o Prevent application verifier exploits;
- Proteção contra ataques Ransomware com a capacidade de reverter os ficheiros que foram manipulados para o seu estado inicial antes da deteção;
- Proteção contra ataques Ransomware executados de forma remota, com a capacidade de cortar a comunicação com o dispositivo que originou o ataque;
- Proteção contra ataques específicos ao MBR – Master Boot Record;
- Capacidade de isolar um endpoint de forma manual, cortando a comunicação com a internet e com outros dispositivos na mesma rede;
- Monitorização de alterações em ficheiros críticos, pastas, chaves de registo e respetivos valores, sendo possível customizar as suas localizações;
- Capacidade de integração com Firewall de Perímetro\Network Firewall com vista a criação de regras de Firewall com base no estado de saúde do endpoint;
- O Licenciamento do EDR para Servidor deve disponibilizar um EDR para ambientes de Cloud Pública como Amazon AWS, Google CGP e Microsoft Azure, onde é possível obter um inventário de assets, por ex., IAM roles, security groups, shared storage, databases, serverless, containers;
- Na componente de EDR para ambientes de Cloud Pública, deverá ser possível:
 - o verificar tentativas de login anormais e suspeitas de tráfego anormal;
 - o configuration guardrails;
 - o Validações contra políticas de melhores práticas do CIS – Center for Internet Security;
- Capacidade de geração automática de Indicadores de Ameaça com base na data de primeira interação com determinado ficheiro, o nome deste, o seu hash SHA-256, o seu nível de suspeita, os dispositivos onde este ficheiro foi encontrado, se o ficheiro foi executado em algum dos dispositivos. Permite criar também um Caso de Investigação para análise;
- Capacidade de geração automática de Casos, onde é verificado a cadeia de eventos de uma determinada ameaça, onde podemos verificar que processos, ficheiros, conexões de rede ou chave de registo foram manipuladas. Esta informação deve ser possível de ser exportada em formato csv. O Caso também deve indicar sugestões de próximos passos para facilitar ações de Threat Hunting;

- Capacidade para exportar forensic snapshots com base em informações dos processos, ficheiros, conexões de rede e outra atividade de sistema que ocorreu quando uma ameaça foi detetada, com vista a realizar investigação forense. Estes snapshots devem ser possíveis de ser convertidos em bases de dados SQLite ou em ficheiros do tipo JSON;
- Deverá ser possível de solicitar uma análise junto de um serviço de inteligência disponibilizado pelo fabricante, para que este devolva uma análise assertiva sobre o processo, indicando a reputação do mesmo com base numa análise de Machine Learning, indicando outras semelhanças a nível de ficheiros\caminhos e semelhanças no código com outros processos considerados benignos ou maliciosos. Deverá também fornecer propriedades e atributos tais como por ex., o compilador utilizado, se o processo\ficheiro está assinado com um certificado digital e qual, que ficheiros .dll foram importados, etc.
- Capacidade para consultar através de queries SQL informações dos endpoint Windows Server e Linux, em grupo ou de forma individualizada, sendo que a Consola deve disponibilizar queries pré-definidas;
- Capacidade para realizar uma reverse-shell desde a Consola contra um endpoint Windows Server e Linux, de forma a poder gerir este de forma remota;

1.18. Gestão Centralizada

- Consola de Gestão Centralizada alojada na Cloud que permita a gestão unificada das Firewalls e Endpoints;
- A consola deve estar localizada dentro da União Europeia;
- A consola deve ser auditada em SOC Type 1;
- Suporte para MFA – Multi Factor Authentication;
- Suporte para autenticação com Azure AD Federation;
- Suporte para automatização de tarefas via API, sendo estas RESTful, utilizando JSON para pedidos e respostas, sendo a comunicação via HTTPS;
- Capacidade de criar diferentes utilizadores de administração com diferentes perfis de permissões;
- Capacidade de abrir tickets de suporte diretamente da consola de Gestão Centralizada;
- Capacidade de retenção de logs enviados pelas Firewalls;
- Pesquisa de informações dentro dos logs arquivados;
- Relatório sobre o estado de saúde das Firewalls;
- Relatório sobre o panorama geral dos Endpoints e o seu estado de saúde;
- Capacidade de criação de relatórios customizáveis para a parte de Endpoint e Firewall;

Item 2: Serviços de implementação e suporte

Serviços de apoio devem incluir:

1.19. Tarefas a incluir no serviço de implementação das firewalls e solução aplicaional de segurança

- 1.19.1. Kick-Off e Planeamento
- 1.19.2. Instalação e Configuração
- 1.19.3. Validação
- 1.19.4. Documentação + Formação
- 1.19.5. Produção
- 1.19.6. Encerramento

1.20. Exigências mínimas de Certificação para execução do serviço

- Nível de parceria Silver com o fabricante da solução
- Dois técnicos do quadro do concorrente com a certificação comprovada de Certified Engineer do fabricante
- Um dos técnicos do quadro do concorrente deverá ter igualmente a certificação comprovada de Certified Architect do Fabricante

1.21. Bolsa de horas adicional de apoio à solução

- Bolsa de 108 horas mínimo
- Serviço de apoio remoto 8 x 5 sob pedido expresso a utilizar durante o periodo do contrato

Artigo 29º

Dever de Colaboração

O IPVC obriga-se a colaborar com o adjudicatário na adoção de soluções e na obtenção dos meios necessários ao correto desempenho dos serviços ou fornecimento do bens.