



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

CADERNO DE ENCARGOS

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

Parte I – Cláusulas jurídicas

Parte II – Cláusulas técnicas



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

ÍNDICE

CLÁUSULAS JURÍDICAS.....	3
Cláusula 1. ^a Objeto	3
Cláusula 2. ^a Local da entrega e instalação dos bens	3
Cláusula 3. ^a Preço base	3
Cláusula 4. ^a Duração do contrato	3
Cláusula 5. ^a Condições de pagamento	4
Cláusula 6. ^a Direitos de propriedade intelectual e industrial	4
Cláusula 7. ^a Sigilo	4
Cláusula 8. ^a Cessão da posição contratual e subcontratação.....	5
Cláusula 9. ^a Foro competente.....	5
Cláusula 10. ^a Legislação aplicável	5
CLÁUSULAS TÉCNICAS.....	6
Cláusula 11. ^a Especificações técnicas.....	6
Cláusula 12. ^a Conformidade e operacionalidade dos bens	27
Cláusula 13. ^a Prazos de entrega.....	28
Cláusula 14. ^a Condições de entrega.....	28
Cláusula 15. ^a Verificação e aceitação dos bens	29
Cláusula 16. ^a Garantia e suporte do equipamento.....	30
Cláusula 20. ^a Níveis de serviço	31
Cláusula 21. ^a Formação	31



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

CLÁUSULAS JURÍDICAS

Cláusula 1.ª

Objeto

- 1 - O contrato a celebrar tem como objeto a **Aquisição de Equipamento de Segurança para a Rede Alargada do Governo Regional dos Açores**, nos termos melhor definidos nas cláusulas técnicas do presente caderno de encargos.

Cláusula 2.ª

Local da entrega e instalação dos bens

- 1 - Os bens objeto do contrato serão entregues, instalados e configurados, em conformidade com as especificações técnicas constantes da PARTE II, no datacenter de Angra do Heroísmo, na morada a indicar pela Direção Regional das Comunicações.
- 2 - Todas as despesas relativas a transportes estão incluídas no preço constante da proposta.

Cláusula 3.ª

Preço base

- 1 - O preço base é de € 432.335,00 (Quatrocentos e trinta e dois mil, trezentos e trinta e cinco euros), acrescido de IVA à taxa legal em vigor.
- 2 - São excluídas as propostas cujo valor seja superior ao preço base.

Cláusula 4.ª

Duração do contrato

O contrato mantém-se em vigor até à entrega, instalação e configuração pelo fornecedor da totalidade dos bens objeto do contrato, em conformidade com as especificações técnicas constantes da PARTE II do presente caderno de encargos, e na proposta adjudicada, e o disposto na lei, sem prejuízo das obrigações acessórias que devam perdurar para além do cumprimento ou da cessação do contrato por qualquer motivo.



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Cláusula 5.ª

Condições de pagamento

- 1 - A faturação é efetuada após a aceitação definitiva do objeto do contrato.
- 2 - O pagamento será efetuado no prazo máximo de 60 dias a contar da data da receção das faturas correspondentes, as quais só podem ser emitidas após o vencimento da obrigação a que se referem.
- 3 - Nos termos da Lei n.º 8/2012, de 21 de fevereiro, a Entidade Adjudicante emite um número de compromisso válido e sequencial, que o cocontratante deverá indicar nas faturas.
- 4 - Desde que devidamente emitidas e observado o disposto na presente cláusula, as faturas são pagas através de transferência bancária, para o NIB a indicar pelo cocontratante.
- 5 - O cocontratante não pode efetuar a transmissão de créditos ao abrigo de contratos de factoring ou proceder à cessão de créditos, sem autorização prévia da Entidade Adjudicante.

Cláusula 6.ª

Direitos de propriedade intelectual e industrial

- 1 - São da responsabilidade do cocontratante quaisquer encargos decorrentes da utilização, na prestação de serviços, de marcas registadas, patentes registadas ou licenças.
- 2 - Se a Entidade Adjudicante vier a ser demandada por ter sido infringido, na execução do contrato, qualquer dos direitos mencionados no presente artigo, o cocontratante responderá nos termos do disposto no artigo 447.º, n.º 2, do Código dos Contratos Públicos.

Cláusula 7.ª

Sigilo

- 1 - O cocontratante obriga-se a observar sigilo quanto a informação e documentação, técnica e não técnica, comercial ou outra, relacionada com a atividade da Entidade Adjudicante ou qualquer outra entidade envolvida na execução do contrato.



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- 2 - A informação e 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 - O cocontratante obriga-se ainda a respeitar a confidencialidade sobre todos os dados ou informações de carácter funcional ou processual dos serviços da Administração Pública a que tenha acesso na execução do contrato.
- 4 - O cocontratante assume igualmente o compromisso de remover e destruir, no final do contrato, todo e qualquer registo, eletrónico ou em papel, relacionado com os dados e processos analisados e que a Entidade Adjudicante lhe indique para esse efeito.
- 5 - O cocontratante obriga-se, de um modo especial, a guardar sigilo quanto ao conteúdo e utilização dos sistemas de informação da responsabilidade da Entidade Adjudicante, nos termos legalmente previstos na Lei n.º 58/2019, de 8 de agosto.
- 6 - O cocontratante garante que terceiros que envolva na execução dos serviços respeitem as obrigações de sigilo e confidencialidade constantes nos números anteriores.

Cláusula 8.ª

Cessão da posição contratual e subcontratação

O cocontratante não pode ceder a sua posição no contrato ou subcontratar total ou parcialmente os serviços incluídos no mesmo sem autorização prévia da Entidade Adjudicante.

Cláusula 9.ª

Foro competente

Para a resolução de todos os litígios relativos, designadamente, à interpretação, execução, incumprimento, invalidade, resolução ou redução do contrato é competente o Tribunal Administrativo de Ponta Delgada.

Cláusula 10.ª

Legislação aplicável

Em tudo o omissso neste Caderno de Encargos, observar-se-á o previsto no Regime Jurídico dos Contratos Públicos da Região Autónoma dos Açores, no Código dos Contratos Públicos e demais legislação aplicável.



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

CLÁUSULAS TÉCNICAS

Cláusula 11.^a

Especificações técnicas

- 1 - Pretende-se adquirir equipamentos de segurança que garantam a fiabilidade e robustez adequadas e que permitam analisar, de forma eficiente e com a performance desejada, o tráfego entre as redes que compõem a Rede Alargada do Governo Regional dos Açores, os servidores existentes no Datacenter e a Internet. Simultaneamente, pretende-se garantir que estes equipamentos suportam o aumento de tráfego normal associado à evolução tecnológica das aplicações que suportam o Governo Regional dos Açores.
- 2 - As especificações técnicas mínimas a apresentar para a solução que se pretende adquirir são as seguintes:

- a. **HARDWARE:**

Cluster composto por dois equipamentos de firewall (appliances) configurados em HA (high availability).

Parâmetros a serem observados **por cada um dos equipamentos:**

- Número de portas 10Gbit/s RJ45 ≥ 4
- Número de portas Gigabit SFP+ 10Gbit/s ≥ 16 ;
- Número de portas Gigabit QSFP+ 40/100 Gbit/s ≥ 4 ;
- Discos rígido SSD em RAID para sistema $\geq 2 \times 240\text{GB}$;
- Discos rígido SSD em RAID para Log $\geq 2 \times 2\text{TB}$;
- Porta de gestão dedicada "Out of Band";
- Porta de consola RJ45;
- A appliance de FW deverá ter uma arquitetura com recursos de hardware dedicados e independentes entre os serviços de gestão e os serviços de inspeção;
- Deverá estar garantido que a appliance de FW quando gerida localmente e perante uma sobrecarga dos serviços de inspeção de tráfego não afete de forma alguma a performance dos serviços de gestão e vice-versa;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- Deverão ser incluídos 2 módulos SFP+ 10G para fibra ótica multimodo com conector dual LC/PC a instalar nas portas 10G SFP+;
 - Deverão ser incluídos 4 módulos QSFP28 100G SR4 para fibra ótica multimodo MTP/MPO a instalar nas portas 100G QSFP28;
 - Deverá estar incluído todo o material (cabos, módulos e etc.) necessário à composição do cluster, sendo que a distancia entre os equipamentos (appliances) obriga à utilização de cablagem com comprimento de 15m;
 - Fontes de alimentação redundantes.
- b. PERFORMANCE:
- Performance da appliance com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego) $\geq 37,0$ Gbps;
 - Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware, URL Filtering e Sandboxing $\geq 23,0$ Gbps;
 - Performance da appliance com a funcionalidade de VPN IPsec $\geq 19,0$ Gbps;
 - Número de novas sessões por segundo $\geq 380\,000$;
 - Número máximo de sessões $\geq 8\,000\,000$.
- c. GESTÃO LOCAL E CENTRALIZADA:
- Gestão e administração da própria appliance através de interface web, linha de comandos e API XML;
 - Possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio;
 - Na gestão centralizada deve ser possível criar perfis de administração que permita segmentar a gestão em diferentes tenants (Por Firewall, por número de firewalls) - Multi-tenancy;
 - Na gestão centralizada deve existir a possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio;
 - Na gestão centralizada deve existir a possibilidade de editar configurações pendentes que ainda não foram aplicadas;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- Possibilidade de visualizar e validar alterações à configuração antes de estas alterações serem aplicadas;
- Possibilidade de descartar alterações à configuração realizadas;
- Possibilidade de armazenar diferentes versões da configuração;
- Na gestão centralizada deve existir a capacidade de criar hierarquização da política de segurança para permitir ter políticas globais para toda infraestrutura instalada;
- Na gestão centralizada deve existir a capacidade de stacks de templates com configurações reutilizáveis para múltiplos equipamentos;
- Na gestão centralizada deve existir um ponto centralizado para efetuar upgrades e atualizações de versões e assinaturas;
- Capacidade de transformar políticas de layer4 em layer7 com machine learning e aprendizagem embebida na plataforma de gestão;
- Na gestão centralizada deve existir a capacidade de "zero touch provisioning" para simplificar o deployment de firewalls remotas;
- Gestão centralizada de SD-WAN para os escritórios remotos;
- Na gestão centralizada deve ser possível gerir até 1000 firewalls num único servidor de gestão;
- A gestão centralizada deve ter a capacidade de funcionar como gestão controladora de várias máquinas de gestão centralizadas debaixo dele para poder escalar para as dezenas de milhares de firewalls debaixo de uma única gestão;
- Deve existir a capacidade de correr a Gestão centralizada sobre hardware dedicado assim como numa Máquina Virtual em VMware ESXi™, KVM e Microsoft Hyper-V, ou então em clouds publicas incluindo Google Cloud Platform (GCP™), Amazon Web Services (AWS®), AWS GovCloud, Microsoft Azure e Azure GovCloud;
- Análise da utilização das regras para reduzir superfície de exposição e melhorar postura de segurança;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- Envio de logs via SYSLOG, FTP, SCP e TFTP para retenção e posterior tratamento;
- Possibilidade de envio seletivo de logs, de acordo com o nível de severidade ou outros atributos como por exemplo o tipo de ameaça;
- Suporte de SNMP, incluindo a possibilidade de obter estatísticas relacionadas com o processamento de logs e com as funcionalidades de alta disponibilidade.

d. REDE:

- As interfaces de rede da appliance deverão suportar os seguintes modos de funcionamento: TAP, Layer 2, Layer 3;
- Suporte de IEEE 802.1Q;
- Suporte de IEEE 802.1AX, suportando até 8 grupos de agregação com 8 interfaces por cada grupo;
- Suporte de protocolos dinâmicos de routing: RIP, OSPF, BGP;
- Suporte de routing estático;
- Suporte de DHCP, NAT e PAT;
- Capacidade de deteção de falhas bidirecionais entre a appliance e router para aplicar a protocolos de routing dinâmico ou rotas estáticas;
- Capacidade de realizar policy based routing através do IP ou rede de origem;
- Capacidade de realizar policy based routing através do utilizador ou grupo;
- Capacidade de realizar policy based routing através do tipo de aplicação;
- Suporte para TLS 1.3 e capacidade de descriptar este tráfego;
- Possibilidade de criar Firewalls virtuais dentro de um chassis com tabela de rotas, interfaces e políticas segmentadas;
- Capacidade de associar múltiplos Virtual Routers (VRFs) a uma política única de firewall;
- Capacidade de correr routing dinâmico (BGP, OSPF) dentro de cada Virtual Router;
- Capacidade de criar Firewalls Virtuais de Layer2 e Layer 3 dentro do mesmo cluster;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- Capacidade de criar perfis de DDoS para proteger o chassis de ataques de larga escala;
 - Suporte de arquiteturas de alta disponibilidade do tipo ativo/passivo e ativo/ativo;
 - Suporte de arquiteturas de alta disponibilidade e escalar lateralmente até 16 membros dentro de um único cluster sem a necessidade de balanceadores externos;
 - Permitir a criação de cluster "multi-datacenter" sem a necessidade de passar layer2 de todas as VLANs entre eles;
 - Adicionar novos membros ao cluster sem perder sessões existentes do cluster existente;
 - Sincronismo de todas as sessões entre os membros do cluster em tempo real.
 - Suporte de Failover de "Datacenter para Datacenter" em diferentes localizações;
 - Suporte de tráfego assimétrico entre membros do cluster espalhados por múltiplos Datacenters;
 - Suporte de "All Active" ou "Active-Standby" entre Datacenters;
 - Suporte de sobrevivência de sessões entre Datacenters;
 - Permitir o mix dos pares de clusters em cada Datacenter que permite ter Ativo/Ativo no DC1 e Ativo/Passivo no DC2 e existir sincronismo entre eles;
 - Permitir ter pares de clusters num Datacenter e um Hot-standby noutro e funcionar como backup do outro DC.
- e. IDENTIFICAÇÃO DE UTILIZADORES:
- Possibilidade de aplicar políticas baseadas em utilizadores e grupos, em vez de por IP;
 - Integração com sistemas de diretórios para obtenção de utilizadores e grupos, incluindo Microsoft Active Directory, Novell eDirectory e Sun ONE Directory;
 - Possibilidade de integração de com sistemas multiutilizador como Citrix ou Microsoft Terminal Server para identificação de utilizadores;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- Capacidade de analisar mensagens de SYSLOG com informação de LOGIN/LOGOUT para identificação de utilizadores;
 - Possibilidade de gerir utilizadores através de API XML;
 - Possibilidade de identificação de utilizadores através de portal de autenticação próprio, fazendo uso dos seguintes protocolos: Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente e autenticação local;
 - Capacidade de obter a identidade dos utilizadores a partir dos seguintes métodos: LDAP, Captive Portal, VPN, NACs (XML e API), Syslog, Terminal Services, XFF Headers, Server Monitoring, e client probing.
- f. SOLUÇÃO DE ACESSOS REMOTOS E GESTÃO DE IDENTIDADES
- A solução deve dar a capacidade de estender as funcionalidades da Firewalls aos utilizadores remotos;
 - A solução deve ser capaz de garantir a segurança dos acessos aos recursos internos como também as aplicações de cloud;
 - Capacidade de garantir a segurança também do acesso à internet do utilizador que esteja fora da rede;
 - Proteger os utilizadores remotos contra-ataques de phishing e roubo de credenciais;
 - Capacidade de fazer quarentena a utilizadores remotos utilizando parâmetros e características imutáveis;
 - Suporte de VPNs por Aplicação e por utilizador;
 - Capacidade de fornecer acesso seguro e sem agente para parceiros e entidades externas as organizações;
 - Suporte de identificação automatizada de equipamentos que não são geridos pela entidade da firewall;
 - Capacidade de implementar Zero Trust efetuando uma identificação muito clara do utilizador;
 - Fornecer também a capacidade de efetuar a identificação de parâmetros do sistema operativo para poder criar regras de acesso do tipo NAC;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- O modulo de identificação tem que obrigatoriamente ser capaz de identificar os seguintes parâmetros do equipamento que esta aceder à rede:
 - Efetuar Patch Management;
 - Validar se a Firewall local está ativa;
 - Anti-Malware esta instalado;
 - Plataforma de Backups esta ativa;
 - Mecanismo de Encriptação de disco está ativo;
 - Modulo de DLP esta Ativo e parâmetros customizados do sistema operativo como processos, registries ou property lists.
- A solução deve disponibilizar um agente com suporte para os seguintes sistemas operativos: Windows 7 e posterior, macOS 10.11 e posterior, iOS 10 e posterior, Android 5 e posterior, CentOS e RHEL 7.0 até 7.7 e Ubuntu 14.04 até 19.04;
- O mesmo agente de acessos remotos deve também ser possível funcionar como agente de identidades dentro da infraestrutura para identificação do utilizador e mapeamento de políticas baseadas em identidades.

g. FUNCIONALIDADES GERAIS DE SEGURANÇA:

- Possibilidade de agrupar interfaces da appliance em conjuntos independentes, formando diferentes zonas de segurança;
- Possibilidade de definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança;
- Possibilidade de criar múltiplas regras de segurança entre zonas de origem e destino;
- Capacidade de identificação de aplicações em L7 com um mínimo de 2400 aplicações identificadas;
- Capacidade de identificação de subfunções dentro de uma aplicação;
- Capacidade de aplicar e/ou excecionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc) apenas ao tráfego de determinadas aplicações L7;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- Possibilidade de agrupar aplicações por categorias de forma que as políticas de segurança sejam aplicadas por categorias de aplicações;
- Possibilidade de identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP;
- Possibilidade de identificar aplicações proprietárias que usem os protocolos HTTP e TCP;
- Possibilidade de identificar aplicações que sejam transportadas em túneis encriptados SSL;
- Capacidade de decifrar tráfego SSH e detetar aplicações não legítimas que utilizem este protocolo para comunicar (SSH tunneling);
- Capacidade de criar regras de QoS segundo as aplicações utilizadas no tráfego
- Possibilidade de aplicar políticas de NAT de forma independente das restantes políticas de segurança;
- Capacidade de forçar o uso de MFA para acesso a aplicações internas;
- Deve existir uma versão da solução que possa ser instalada como um container dentro de um ambiente de docker/kubernetes.

h. IDS/IPS:

- Capacidade de aplicar políticas de prevenção ou de deteção contra a exploração de vulnerabilidades, tanto no tráfego que vai para a Internet como no tráfego que vem da Internet, sem incorrer numa latência superior a 1 ms para não penalizar a experiência do utilizador, efetuando a análise numa única passagem do tráfego para todas as ameaças;
- Possibilidade de aplicar diferentes perfis proteção contra exploração de vulnerabilidades de acordo com as aplicações identificadas;
- Possibilidade de escolher proteções contra a exploração de vulnerabilidades que se apliquem apenas a clientes ou servidores ou a ambos;
- As vulnerabilidades devem estar categorizadas por tipo e por nível de risco, de forma que a aplicação de perfis de proteção se possam realizar com base nestas categorias;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- Deve ser possível identificar as proteções pela identificação CVE das vulnerabilidades;
 - Capacidade de aplicar apenas as assinaturas necessárias para determinada aplicação identificada, através da seleção de perfis;
 - Deve ser possível converter assinaturas snort e suricata para dentro da plataforma.
- i. ANTIVÍRUS & ANTI-MALWARE:
- Detetar equipamentos possivelmente comprometidos que tentem estabelecer comunicações com servidores de C&C;
 - Capacidade de habilitar mecanismos de DNS sinkholing que permitam interceptar pedidos de resolução de nomes para domínios comprometidos com malware;
 - Capacidade de definir políticas de antivírus, de forma que a transferência de ficheiros realizada no sentido Internet para rede interna ou vice-versa, sejam inspecionados e bloqueados se o seu conteúdo for malicioso;
 - Capacidade de aplicar políticas que permitam aplicar o motor de antivírus sobre protocolos como ftp, http, imap, pop3, smb ou smtp, definindo para cada um destes protocolos a ação a realizar (permitir os ficheiros, descartar os ficheiros, desconectar a sessão ou registar mediante logs);
 - Possibilidade de enviar o ficheiro para serviços de inspeção adicionais na cloud que permitam analisar e emitir um veredicto para que appliance possa tomar uma ação no caso de um ficheiro malicioso;
 - Capacidade de aplicar políticas de antivírus de forma granular, permitindo aplicar essas políticas a utilizadores ou grupos, a determinados segmentos de rede com determinada direção e a determinadas aplicações;
 - Capacidade de identificar ficheiros não através das suas extensões, mas sim através do tipo MIME do ficheiro, permitindo no mínimo a identificação de 100 tipos de ficheiros;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- Deve-se poder aplicar políticas de bloqueio de ficheiros, de forma a poder bloquear a transferência de certo tipo de ficheiros ou que se permita após a confirmação por parte do utilizador e criando um log correspondente;
- Capacidade de aplicar políticas de bloqueio de ficheiros atendendo a critérios como origem e destino do tráfego, utilizador ou grupo, tipo de aplicação ou de tráfego que inicia a transferência do ficheiro;
- Possibilidade de bloquear a transferência de ficheiros quando utilizados URLs categorizados como perigosos do ponto de vista de ameaça de segurança;
- Capacidade pesquisa de padrões sensíveis no tráfego, evitando a exfiltração de dados;
- Deve existir a capacidade de analisar ficheiros executáveis e scripts powershell com um motor de machine learning local que permita bloquear ficheiros maliciosos localmente em tempo real sem necessidade de estabelecer ligações externas. Este motor deve permitir bloquear malwares nunca antes observados e para os quais não existem assinaturas sem necessidade de recorrer a sandboxing;
- Deve existir a capacidade de receber updates em tempo real de forma a não ter que aguardar minutos/horas/dias por determinado update. Assim que um novo malware é detetado por qualquer cliente do fabricante essa informação deve ser propagada em tempo real a todos os clientes de forma a diminuir o tempo de exposição a ameaças.

j. ACESSOS VPN

- Suporte de IKEv1 e IKEv2;
- Suporte de criptografia para 3DES e AES-256 para IKE Phase I e II IKEv2;
- Suporte de pelo menos os seguintes grupos de Diffie-Hellman: Group 1, Group 2, Group 5, Group 14, Group 19 and Group 20;
- IKE Phase2 - Encriptação de dados (DES, 3DES, AES-128, AES-192, AES-256) e suporte de integridade dos dados (MD5, SHA1, SHA256, SHA384, SHA512);
- VPNs Site to Site: Full Mesh (all to all) ou Star (Remote to center);



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- Suporte de IKE com PKI e pre-shared Secret;
- Aprovisionamento automático de VPNs site-to-site;
- Gestão automática de túneis IPSec de backup;
- Suporte de routing dinâmico em VPN IPSec;
- Clientes VPN para Windows, MacOS e iOS, Android;
- Suporte de OTP para VPN sem recurso a terceiros fabricantes ou servidores adicionais;
- Aplicação de políticas e restrições de acesso por utilizador ou por grupo de utilizadores;
- Single Sign On VPN;
- Portal HTML5 para maior compatibilidade com todo o tipo de dispositivos;
- Administração a partir da consola central.

k. URL FILTERING:

- Possibilidade de definir manualmente listas estáticas de URLs ou de IPs permitidos e não permitidos para a navegação, com a possibilidade de definir para os permitidos a ação a realizar (permitir, bloquear, permitir, mas advertir, etc.);
- Permitir a navegação baseando-se em categorias de URL, sendo estas categorias atualizadas periodicamente através de serviço em cloud;
- Possibilidade de incluir listas de URLs e IPs dinâmicas relacionadas com ameaças para que possam ser bloqueadas automaticamente (listas de reputação);
- Capacidade de detetar o envio de credenciais corporativas nas páginas de internet navegadas, de forma a poder advertir, bloquear ou permitir em função da categorização das páginas web;
- A filtragem de URLs deve poder ser aplicada mediante diferentes perfis e deverá ser aplicada ao tráfego que sai para a Internet ou que vem da Internet;
- A solução deve possuir um motor local de machine learning que seja aplicado às páginas web visitadas pelos utilizadores de forma a prevenir variantes



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

maliciosas de javascript e acesso a páginas de phishing. Este motor deverá funcionar em tempo real e bloquear acesso a páginas que não estejam previamente categorizadas como maliciosas.

1. DNS SECURITY:

- A solução deve disponibilizar um serviço de proteção DNS baseado na cloud que seja capaz de bloquear acesso a domínios maliciosos conhecidos e desconhecidos;
- Este serviço deve utilizar mecanismos de machine learning para detetar Domain Generated Algorithms (DGAs) e bloquear o acesso a estes;
- A solução deve permitir bloquear tráfego de C&C através do canal de DNS assim como detetar e bloquear o uso indevido deste canal para efetuar exfiltração de dados (DNS tunneling);
- A funcionalidade de DNS Tunneling deve ser capaz de inspecionar o conteúdo dos pacotes de DNS;
- Este serviço deve permitir identificar quais as máquinas e utilizadores infetados, sem a necessidade de qualquer alteração na infraestrutura existente;
- A adição deste serviço não deve obrigar a qualquer alteração na infraestrutura de DNS do cliente;
- Para além da threat intelligence do fabricante, a solução deve utilizar informação proveniente de pelo menos 30 fontes distintas;
- Deve ser possível criar políticas simples que bloqueiem ou façam sinkholing aos pedidos de DNS maliciosos;
- Devem ser disponibilizadas as seguintes categorias para construção de políticas: Command and Control Domains, Malware Domains, Dynamic DNS Hosted Domains, Newly Registered Domains, Phishing Domains, Grayware Domains and Parked Domains;
- A solução não deve necessitar de updates para estar atualizada e proteger contra as mais recentes ameaças;
- A solução deve permitir a aplicações de tags a máquinas comprometidas, de forma a ser possível criar uma política de acesso diferenciada para estas.



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

m. SANDBOXING E PROTEÇÃO ZERO DAY:

- Possibilidade de disponibilizar um serviço na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma que se permita o envio desta informação para análise atendendo aos critérios: Tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload);
- Perante uma análise por parte do serviço de Sandboxing na cloud que categorize a informação enviada como maliciosa, deverão ser criadas assinaturas num prazo máximo de 5 minutos que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente);
- O serviço de sandboxing na cloud deverá permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios;
- A tecnologia de Sandboxing tem que ser capaz de inspecionar protocolos como HTTP, HTTPS, SMTP, FTP, POP3 e IMAP;
- A análise de malware deve ser inteligente o suficiente para analisar comportamentos do tipo "Call back" e IOC's durante a análise de malware e automaticamente criar assinaturas que permitam a prevenção de ameaças e que possam ser utilizadas pelas restantes funcionalidades da solução;
- Os sistemas de análise de malware devem ser capazes de detetar malware direcionado a sistemas operativos de MacOS, Windows, Android e Linux;
- O malware cada vez mais utiliza técnicas de Anti-VM para detetar que está a ser executado num ambiente virtual e prevenir que seja detonado, escondendo o seu comportamento malicioso. A análise "Bare Metal" é uma funcionalidade onde o malware é executado em hardware real, o que impede que o malware utilize qualquer técnica de Anti-VM. A solução deve ter esta funcionalidade embebida;
- Em termos de suporte de sistemas operativos Windows emulados deve suportar: Windows XP, Windows 7 e Windows 10;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- Deve ser garantido suporte para os seguintes ficheiros executáveis (EXE, DLL) e todos os tipos de ficheiros Microsoft Office, PDF, Flash, Java applets (JAR e CLASS);
- Android (ficheiros APK), macOS binaries (mach-O, DMG, PKG e application bundles) e Linux (ficheiros ELF);
- Incluir o suporte de ficheiros comprimidos (RAR, 7Zip) e conteúdo encriptado;
- Capacidade de descriptar malware (unpacker) para utilização na análise estática e machine learning.

n. IOT SECURITY:

- A plataforma deve disponibilizar um serviço cloud de segurança para dispositivos IOT;
- A firewall deve colecionar metadados do tráfego de rede dos dispositivos IoT, gerar logs com estas informações e enviá-los para um Data Lake na Cloud. O Serviço de IOT deve ter capacidade de analisar estes metadados através de um motor patenteado baseado em algoritmos de inteligência artificial e machine learning para detetar e identificar os dispositivos IoT e OT na rede;
- A identificação de dispositivos não se deve basear em fingerprinting, como por exemplo identificação de MAC addresses;
- O motor de identificação deve possuir 3 níveis: identificação da categoria do dispositivo (ex: camara de vigilância), identificação do seu perfil (ex: fabricante, modelo e versão) e identificação de cada instância do dispositivo;
- Após a identificação dos dispositivos, a solução deve criar um padrão de comportamento para cada um e detetar automaticamente comportamentos anormais que possam sugerir que o dispositivo está comprometido. Para este tipo de eventos, devem ser gerados alertas no dashboard da solução. Deve ser possível receber estes alertas via email e sms também;
- Quando é observado um comportamento anormal a solução deve sugerir automaticamente políticas de segurança a aplicar na firewall que permitam o correto funcionamento do dispositivo, mas bloqueie qualquer ligação anormal;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- A firewall deve permitir a criação de regras baseadas em tipos de dispositivos que devem ser identificados através da marca, modelo e versão. Não sendo assim necessário criar regras com base em IPs ou zonas;
 - Este serviço deve observar mais de 200 parâmetros nos metadados do tráfego de rede, incluindo parâmetros de DHCP (option 55), HTTP user agent IDs, protocolos, headers dos protocolos, etc.;
 - O serviço deve identificar vulnerabilidades presentes no software a correr nos respetivos dispositivos e diferenciar entre dispositivos vulneráveis e potencialmente vulneráveis. O serviço deve identificar vulnerabilidades de software assim como vulnerabilidades associadas ao uso/configuração incorreta dos mesmos. Exemplo: uso de credenciais default;
 - Deve existir a possibilidade do Data Lake ser utilizado para outro conjunto de use cases através de licenciamento adicional, nomeadamente: NTA (Network Traffic Analysis), UEBA (User Entity Behavior Analytics), shadow IT e integração com CASB(Cloud Access Security Broker).
- o. DATA LOSS PREVENTION
- A plataforma deve disponibilizar um módulo completo de Data Loss Prevention;
 - Esta funcionalidade deve ser disponibilizada como um serviço cloud que utilize supervised machine learning para identificar documentos sensíveis e atribuir-lhes uma categoria automaticamente como por exemplo: Financeiros, Legais, Saúde, informação pessoal, etc. A solução deverá também permitir controlar este tipo de documentos de forma evitar a sua exposição ou extravio;
 - Este serviço deverá permitir proteger estes documentos das seguintes formas:
 - Prevenir o upload de ficheiros com informação confidencial e/ou sensível para aplicações web não permitidas pela organização;
 - Monitorizar o upload de documentos para aplicações externas permitidas pela organização.
 - O serviço deve disponibilizar out-of-the-box pelo menos 380 “data patterns” e deve também disponibilizar perfis que agrupam determinados padrões de forma



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

a simplificar a criação de políticas. Por exemplo, deverá existir um perfil associado com o GDPR de forma a facilitar a monitorização de documentos que possam contêm informação pessoal de utilizadores;

- Deverão existir os seguintes perfis out-of-the box: Bulk CCN, CCPA, Corporate Financial docs, Financial information, GDPR, GLBA, Healthcare, Intellectual Property, Legal, Malware, Personally-Identifiable Information, Profanity, Self Harm e Sensitive content;
- A solução deverá ser constantemente atualizada com novos padrões e perfis;
- De forma a melhorar o rácio de deteção e eliminar falsos positivos a solução deverá permitir especificar: proximity keywords, níveis de confiança e expressões regulares básicas ou “weighted”;
- Este serviço deve poder ser consumido por diferentes plataformas do fabricante, nomeadamente, firewalls, serviço SASE(Secure Access Service Edge), CASB(Cloud Access Security Broker) e CSPM(Cloud Security Posture Management). Isto permitirá aplicar políticas de DLP transversais à organização.

p. SD-WAN

- Deve ser possível através de licenciamento adicional adicionar um módulo de SD-WAN à plataforma;
- A plataforma deve permitir adicionar um overlay de SD-WAN que permita escolher de forma inteligente e dinâmica os links mais apropriados para envio de tráfego;
- Deve ser possível criar regras de SD-WAN por aplicação e definir os requisitos mínimos para cada link. No caso de os requisitos mínimos não serem cumpridos pelo link em uso, deve ser feito o failover do tráfego automaticamente;
- Para os links deve ser possível monitorizar e definir regras com base em: latência, jitter e perda de pacotes;
- A plataforma deve permitir fazer load-sharing através de múltiplos links de forma a melhorar o aproveitamento da largura de banda disponível;
- As firewalls devem suportar a funcionalidade de zero-touch provisioning;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- A plataforma deve disponibilizar informação sobre a performance das aplicações e links;
- Esta funcionalidade deve ser gerida centralmente através de uma única consola;
- Deve ser suportada a funcionalidade de Packet duplication, o que permite a um equipamento enviar o mesmo pacote em links diferentes. O equipamento que recebe ambos os pacotes deverá descartar o último a chegar;
- Deve ser suportada a funcionalidade de Forward Error Correction.

q. RELATÓRIOS E LOGS:

- A appliance deve ter a capacidade gerar relatórios tanto predefinidos ou personalizados, utilizando os logs criados pelo próprio equipamento sem necessidade de equipamentos externos adicionais;
- Deve ser possível gerar relatórios de atividade por utilizador, incluindo aplicações utilizadas e páginas web visitadas;
- Deve ser possível gerar relatórios de forma automática assim como agrupar vários relatórios num único documento em formato pdf;
- Entre os relatórios disponíveis devem constar relatórios com a largura de banda consumida pelas diferentes aplicações, relatórios sobre as origens e destinos geográficos das ameaças detetadas e relatórios sobre a análise do comportamento do tráfego observado que permita detetar equipamentos comprometidos que participem em botnets;
- Deve ser possível programar o momento em que se deseja a geração do relatório pretendido e o seu envio através de e-mail, assim como o intervalo temporal que se pretende;
- Possibilidade de armazenar os logs localmente tendo por única restrição a capacidade do disco do próprio equipamento;
- Possibilidade de enviar logs para uma plataforma externa de gestão e processamento especializado de logs com o objetivo de manter os logs a longo prazo;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- Capacidade de dispor de um painel de instrumentos personalizável por utilizador de administração da appliance com pelo menos a seguinte informação: Aplicações mais utilizadas, Aplicações de alto risco, Informação geral do sistema, Estado das interfaces, Logs relativos às ameaças mais observadas, Logs de URLs filtrados, Recursos do sistema;
- Capacidade de dispor de estatística gerada a partir de logs, personalizável por utilizador que permita fornecer informações como: utilizadores que mais geram tráfego, regras de segurança que mais utilizam, vulnerabilidades mais detetadas e bloqueadas, equipamentos que acederam a domínios maliciosos, vírus detetados, informação enviada ao serviço de sandboxing e equipamentos internos comprometidos;
- Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance de forma que a partir dos logs criados se possa obter informações de alto nível.

r. OUTRAS FUNCIONALIDADES EXIGIDAS:

- Possibilidade de definir aplicações e/ou vulnerabilidades customizadas mediante diferentes parâmetros como: Portos TCP/UDP que sejam usados na aplicação e combinação de padrões dentro dos "headers" dos pacotes ou mesmo no "payload" dos próprios pacotes que se devam cumprir para que se reconheça a aplicação e/ou vulnerabilidade;
- Suporte para TLS 1.3 e capacidade de descriptar este tráfego;
- Possibilidade de decifrar tráfego SSL e SSH de forma que se possa estabelecer políticas de descriptação baseadas em: zonas por onde passa o tráfego, IP de origem ou destino, utilizadores geram esse tráfego, portos utilizados;
- Capacidade de criar exceções à descriptação para determinado tipo de tráfego;
- Capacidade de decifrar tráfego com destino a sites web que utilizam certificados de curva elíptica (ECC);
- Possibilidade de enviar tráfego após descriptação para uma interface de port mirror para análise de terceiras partes;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- Capacidade de capturar tráfego em formato pcap, podendo ser estabelecido como critérios de captura do tráfego, uma determinada aplicação independentemente da origem ou destino desse tráfego;
- Capacidade de capturar tráfego em formato pcap exclusivamente quando se deteta um vírus ou um ataque em qualquer um dos motores de proteção.

s. GESTÃO LOCAL E CENTRALIZADA

- Gestão e administração da própria appliance através de interface web, linha de comandos e API XML;
- Possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio;
- Na gestão centralizada deve ser possível criar perfis de administração que permita segmentar a gestão em diferentes tenants (Por Firewall, por número de firewalls) - Multi-tenancy;
- Na gestão centralizada deve existir a possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio;
- Na gestão centralizada deve existir a possibilidade de editar configurações pendentes que ainda não foram aplicadas;
- Possibilidade de visualizar e validar alterações à configuração antes de estas alterações serem aplicadas;
- Possibilidade de descartar alterações à configuração realizadas;
- Possibilidade de armazenar diferentes versões da configuração;
- Na gestão centralizada deve existir a capacidade de criar hierarquização da política de segurança para permitir ter políticas globais para toda infraestrutura instalada;
- Na gestão centralizada deve existir a capacidade de stacks de templates com configurações reutilizáveis para múltiplos equipamentos;
- Na gestão centralizada deve existir um ponto centralizado para efetuar upgrades e atualizações de versões e assinaturas;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- Capacidade de transformar políticas de layer4 em layer7 com machine learning e aprendizagem embebida na plataforma de gestão;
 - Na gestão centralizada deve existir a capacidade de "zero touch provisioning" para simplificar o deployment de firewalls remotas;
 - Gestão centralizada de SD-WAN para os escritórios remotos;
 - Na gestão centralizada deve ser possível gerir até 1000 firewalls num único servidor de gestão;
 - A gestão centralizada deve ter a capacidade de funcionar como controladora de várias máquinas de gestão centralizadas debaixo dele para poder escalar para as dezenas de milhares de firewalls debaixo de uma única gestão;
 - Deve existir a capacidade de correr a Gestão centralizada sobre hardware dedicado assim como numa Máquina Virtual em VMware ESXi™, KVM e Microsoft Hyper-V, ou então em clouds públicas incluindo Google Cloud Platform (GCP™), Amazon Web Services (AWS®), AWS GovCloud, Microsoft Azure e Azure GovCloud;
 - Análise da utilização das regras para reduzir superfície de exposição e melhorar postura de segurança;
 - Envio de logs via SYSLOG, FTP, SCP e TFTP para retenção e posterior tratamento;
 - Possibilidade de envio seletivo de logs, de acordo com o nível de severidade ou outros atributos como por exemplo o tipo de ameaça;
 - Suporte de SNMP, incluindo a possibilidade de obter estatísticas relacionadas com o processamento de logs e com as funcionalidades de alta disponibilidade.
- t. SOLUÇÃO REDUNDANTE PARA ARMAZENAMENTO E CONSULTA DE EVENTOS DE FIREWALL (LOGGING)
- Deve ser possível através do sistema de gestão centralizado consultar registos e fazer filtros nas pesquisas;
 - Deve existir a capacidade de correr sistema de logging sobre hardware dedicado assim como numa Máquina Virtual em VMware ESXi™, KVM e Microsoft Hyper-V, ou então em clouds públicas incluindo Google Cloud



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

Platform (GCP™), Amazon Web Services (AWS®), AWS GovCloud, Microsoft Azure e Azure GovCloud;

- Deve ter capacidade para suportar ≥ 40000 registos por segundo;
- Deve ser possível implementar redundância por forma a não perder registos no caso de falha de um sistema de logging.

u. **INSTALAÇÃO:**

- Os equipamentos que compõem o cluster serão entregues e instalados nas instalações a indicar pela entidade adjudicante;
- Instalação e configuração da solução em modo HA, de acordo com as características da infraestrutura existente da Rede Alargada do Governo Regional dos Açores;
- Configuração das regras e políticas, adequadas ao normal funcionamento de um organismo público;
- Configuração da appliance para gestão/monitorização do tráfego (routing) interno.

v. **LICENCIAMENTOS:**

- Licenciamento perpétuo para 25 firewalls virtuais (virtual systems) independentes;
- Licenciamento, em HA, com subscrição por 36 meses:
- Threat Prevention;
- IDS/IPS;
- Antivírus & Anti-Malware;
- Sandboxing;
- Controlo Aplicacional;
- URL Filtering;
- Controlo de utilizadores;
- DLP.

w. **NÍVEIS DOS SERVIÇOS:**



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

As atividades de manutenção e assistência técnica devem ser garantidas pelo período de 36 meses com tempos de resolução até um dia útil seguinte para os casos de avarias ou erros do software ou de desconfiguração do sistema.

x. FORMAÇÃO:

Formação da equipa técnica de segurança do contraente público pelo prazo, mínimo, de 16 horas.

3 - Mapa de quantidades:

Descrição	Quantidade
Firewall (appliance) com 75 contextos virtuais.	2 (1 HA cluster) com suporte a 3 anos
Solução de gestão com capacidade para gerir até 100 firewalls.	2 licenças com suporte a 3 anos
Licenciamento: ● Firewall Aplicacional (Layer7) ● Controlo de utilizadores ● DLP – Controlo de conteúdos dos ficheiros ● Threat Prevention; ● IDS/IPS ● Antivírus & Anti-Malware ● URL Filtering ● Analise de eventos ● Reporting	2 licenças com suporte a 3 anos
Solução para armazenamento e consulta de eventos de firewall (LOGGING) com capacidade para gerir até 25 firewalls	4 licenças com suporte a 3 anos
Dns Security	4 licenças com suporte a 3 anos
SOLUÇÃO DE ACESSOS REMOTOS E GESTÃO DE IDENTIDADES	4 licenças com suporte a 3 anos
50 contextos virtuais adicionais	2 licenças

Cláusula 12.^a

Conformidade e operacionalidade dos bens



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- 4 - O cocontratante obriga-se a entregar à Entidade Adjudicante os bens objeto do contrato nas quantidades requeridas e com os requisitos técnicos e funcionais previstos no presente caderno de encargos.
- 5 - Os bens objeto do contrato devem ser entregues em perfeitas condições de serem utilizados para os fins a que se destinam e dotados de todo o material de apoio necessário à sua entrada em funcionamento.
- 6 - O cocontratante é responsável perante a Entidade Adjudicante por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que os bens lhe são entregues.

Cláusula 13.^a

Prazos de entrega

- 1 - O cocontratante obriga-se a entregar, instalar e configurar os bens cuja aquisição é objeto do presente caderno de encargos, nos locais indicados pela Entidade Adjudicante, no prazo máximo de 60, contados da data da assinatura do contrato.
- 2 - Sempre que ocorra um caso de força maior, devidamente comprovado e que implique a suspensão da entrega, deve o cocontratante, logo que dele tenha conhecimento, requerer à Entidade Adjudicante que lhes seja concedida uma prorrogação do respetivo prazo, fundamentando adequadamente o pedido.

Cláusula 14.^a

Condições de entrega

- 1 - O cocontratante deverá comunicar previamente a data de entrega e as condições necessárias à instalação física dos equipamentos, em condições normais de uso, com vista a garantir o perfeito funcionamento do equipamento.
- 2 - Todas as despesas e custos com o transporte dos bens objeto do contrato e respetivos documentos para o local de entrega bem como a respetiva montagem, instalação, configuração e testes são da responsabilidade do cocontratante.
- 3 - Os riscos na fase de transporte, de acondicionamento, da embalagem, da carga e da descarga, da entrega, são da exclusiva responsabilidade do cocontratante, sem quaisquer encargos adicionais para a Entidade Adjudicante.



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- 4 - Os bens deverão incorporar todas as peças e ser acompanhadas do certificado de garantia, dos manuais, das instruções técnicas e outros elementos necessários a garantir o seu funcionamento em condições normais de uso e que estão incluídas no respetivo preço.
- 5 - As embalagens dos bens devem ser conservadas fechadas e seladas pelo cocontratante até à instalação dos mesmos em condições normais de uso.
- 6 - Após a instalação, as embalagens ficarão na posse da Entidade Adjudicante e devem conter etiquetagem com as referências do cocontratante, do fabricante, da marca, do modelo, do lote de fabrico/ano, do número de série, e de todas as indicações necessárias à sua segurança.

Cláusula 15.^a

Verificação e aceitação dos bens

- 1 - Efetuada a montagem, instalação, configuração e testes dos bens nos termos previstos, a Entidade Adjudicante, por si ou através de terceiro designado para o efeito, procede à aceitação provisória dos mesmos através de uma inspeção quantitativa e qualitativa, com vista a verificar, respetivamente, se os mesmos correspondem às quantidades estabelecidas na requisição e se reúnem os requisitos técnicos e funcionais definidos nas cláusulas técnicas do presente caderno de encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei.
- 2 - Durante a fase de inspeção dos bens objeto do contrato, o cocontratante deve prestar toda a cooperação e todos os esclarecimentos necessários.
- 3 - Em caso de silêncio da Entidade Adjudicante, findo o prazo de 2 semanas após a aceitação provisória, os bens consideram-se aceites definitivamente, ocorrendo a transferência da posse e da propriedade dos mesmos, sem prejuízo das obrigações de garantia e suporte que impendem sobre o cocontratante.
- 4 - No caso de a inspeção referida no n.º 1 não comprovar a conformidade dos bens, a Entidade Adjudicante informa, por escrito, o cocontratante.
- 5 - No caso previsto no número anterior, o cocontratante deve proceder, à sua custa e no prazo referido nos números seguintes, às reparações ou substituições necessárias para garantir



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

a operacionalidade dos bens e o cumprimento das exigências legais e dos requisitos técnicos e funcionais exigíveis.

- 6 - O cocontratante dispõe de um prazo máximo de cinco dias úteis a contar da comunicação referida no n.º 4, para proceder à substituição dos bens em caso de rejeição dos mesmos ou para suprir as deficiências e irregularidades detetadas durante a entrega e que não impliquem a rejeição dos bens.
- 7 - Após a realização das reparações ou substituições necessárias pelo cocontratante, no prazo respetivo, a Entidade Adjudicante procede à realização de nova inspeção, nos termos dos números anteriores.

Cláusula 16.ª

Garantia e suporte do equipamento

- 1 - A aquisição de bens objeto do presente caderno de encargos contempla uma garantia com os níveis de serviço de suporte referidos nas cláusulas técnicas do presente caderno de encargos, e nos números seguintes.
- 2 - Todos os equipamentos estão sujeitos a garantia, com a duração de 2 anos a contar da aceitação definitiva de cada bem fornecido.
- 3 - Considera-se incluído na garantia dos bens:
 - a) As operações de natureza preventiva, designadamente, revisões, afinações, limpezas e testes necessários à redução dos riscos de avaria dos bens, de forma a garantir, em tempo, a manutenção das respetivas características a um nível semelhante às iniciais;
 - b) As operações de natureza corretiva, que têm como objetivo repor os produtos em condições normais de funcionamento sempre que ocorram falhas ou avarias;
 - c) O fornecimento e substituição de peças ou outros materiais por peças ou elementos de origem, necessárias ao funcionamento dos equipamentos em condições normais de uso;
 - d) A reinstalação em condições normais de uso, no caso de transporte, dos bens avariados;
 - e) A substituição dos bens no caso de avaria não reparável;
 - f) Os custos de mão-de-obra e restantes encargos com pessoal, incluindo o transporte, para efeito das prestações previstas nas alíneas anteriores;



SECRETARIA REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

DIREÇÃO REGIONAL DAS COMUNICAÇÕES

- g) Todos os encargos com o transporte do material necessário à execução das prestações previstas nas alíneas anteriores.
- 4 - As reparações terão lugar no local de funcionamento do bem em causa.
- 5 - A permanência do cocontratante nas instalações referidas no número anterior que implique paragem dos bens instalados deverá ocorrer fora das horas normais de serviço do local de funcionamento do bem em causa, salvo nas situações previamente autorizadas pela Entidade Adjudicante.
- 6 - Em casos em que manifestamente se verifique ser impossível a resolução do problema reportado no local dentro do prazo, deverá o cocontratante proceder à substituição temporária do equipamento enquanto decorrer a reparação em instalações próprias deste, mediante autorização escrita da Entidade Adjudicante.

Cláusula 20.ª

Níveis de serviço

As atividades de manutenção e assistência técnica têm a necessidade de ser garantidas (24 horas por dia, 7 dias por semana – 24x7) através de um tempo máximo de intervenção para os casos de avarias ou erros do software ou de desconfiguração do sistema com tempos de resolução até ao dia útil seguinte (Next Business Day).

Cláusula 21.ª

Formação

- 1 - O fornecedor deve proporcionar a formação necessária aos técnicos indicados pelo contraente público pelo período mínimo de 16 horas, devendo, para o efeito, disponibilizar aos mesmos a documentação de suporte.
- 2 - A formação deverá ser ministrada nos próprios locais de instalação dos bens e, de preferência, durante o processo de instalação e configuração.
- 3 - O cocontratante não poderá exigir qualquer quantia adicional relacionada com a formação.