



Caderno de Encargos

CONSULTA PRÉVIA

Aquisição de uma solução de segurança de última geração

04/05/2020

Motivo: Aprovo documento
Localização: Bragança, Portugal
Data da Assinatura: 14/05/2020 10:01:23

Hernani Dias

PARTE I – CLÁUSULAS JURÍDICAS

Capítulo I

Disposições gerais

Cláusula 1.ª

OBJETO

O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré – contratual que tem por objeto principal a “Aquisição de uma solução de segurança de última geração” para o Município de Bragança.

Cláusula 2.ª

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.

Cláusula 3.ª

PRAZO PARA FORNECIMENTO DOS BENS E PRESTAÇÃO DOS SERVIÇOS

1 - Após adjudicação, a solução deve ser implementada pelo adjudicatário no prazo máximo de 15 dias.

Cláusula 4.ª

VALOR BASE

1 – O valor base para o efeito do presente procedimento é de 6.200,00 €, ao qual acresce o valor do IVA à taxa aplicável.

Capítulo II
Obrigações contratuais
Secção I
Obrigações do prestador de serviços
Subsecção I
Disposições gerais

Cláusula 5.ª

OBRIGAÇÕES PRINCIPAIS DO FORNECEDOR

- 1 - Sem prejuízo de outras obrigações previstas na legislação aplicável, no Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorrem para o fornecedor a obrigação da entrega dos bens e prestação dos serviços identificados na sua proposta.
- 2 - O fornecedor fica obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados para a execução das tarefas a seu cargo.

Cláusula 6.ª

CONFORMIDADE E OPERACIONALIDADE DOS BENS

- 1 – O fornecedor obriga-se a entregar ao contraente público os bens objeto do contrato com as características, especificações e requisitos técnicos previstos na parte II (Cláusulas Técnicas) do presente Caderno de Encargos.
- 2 – 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.

Cláusula 7.ª

ENTREGA DOS BENS OBJETO DO CONTRATO

- 1 – O fornecedor obriga-se a disponibilizar, simultaneamente com a entrega dos bens/serviços objeto do contrato, todos os documentos (em língua portuguesa), que sejam necessários para a boa e integral utilização ou funcionamento daqueles.
- 2 – Todas as despesas e custos com o transporte dos bens/serviços objeto do contrato e respetivos documentos para o local de entrega são da responsabilidade do fornecedor.

Subsecção II
Dever de sigilo

Cláusula 8.ª

OBJETO DO 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 - O dever de sigilo perdura durante o período de execução do contrato e após a cessação, por qualquer forma ou motivo, do mesmo.

Secção II
Obrigações do Município de Bragança

Cláusula 9.ª

PREÇO CONTRATUAL

- 1 - Pelo fornecimento (bens e serviços) objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, o Município de Bragança deve pagar o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor.
- 2 - O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, incluindo as despesas de alojamento, alimentação e deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

Cláusula 10.ª

CONDIÇÕES DE PAGAMENTO

- 1 – As condições de pagamento do encargo do fornecimento são as seguintes:
 - a) A fatura deverá ser em conformidade com a solicitação apresentada pela Câmara Municipal.
 - b) O pagamento será efetuado contra a apresentação de fatura nas condições indicadas pelo concorrente não podendo a sua liquidação efetiva verificar-se depois de decorridos 60 dias úteis, contados da data de entrega da fatura.

Capítulo III
Penalidades contratuais e resolução

Cláusula 11.^a

PENALIDADES CONTRATUAIS

- 1 - Pelo incumprimento de obrigações emergentes do contrato, o Município pode exigir do fornecedor o pagamento de uma pena pecuniária, de montante a fixar em função da gravidade do incumprimento.
2. Em caso de resolução do contrato por incumprimento do prestador de serviços, o Município de Bragança pode exigir-lhe uma pena pecuniária de valor correspondente a metade do valor do contrato, se outra mais elevada não se apurar.
- 3 - Na determinação da gravidade do incumprimento, a entidade adjudicante tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do prestador de serviços e as consequências do incumprimento.
- 4 - A entidade adjudicante pode compensar os pagamentos devidos ao abrigo do contrato com as penas pecuniárias devidas nos termos da presente cláusula.
- 5 - As penas pecuniárias previstas na presente cláusula não obstam a que a entidade adjudicante exija uma indemnização pelo dano excedente.

Cláusula 12.^a

FORÇA MAIOR

- 1 - Não podem ser impostas penalidades ao prestador de serviços, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de quaisquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitam 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 fosse razoavelmente exigível contornar ou evitar.
- 2 - Podem constituir força maior, se se verificarem os requisitos do número anterior, 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.
- 3 - Não constituem força maior, designadamente:
 - a) Circunstâncias que não constituam força maior para os subcontratados do prestador de serviços, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades do prestador de serviços ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
 - c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo prestador de serviços de deveres ou ónus que sobre ele recaiam;

- d) Manifestações populares devidas ao incumprimento pelo prestador de serviços de normas legais;
- e) Incêndios ou inundações com origem nas instalações do prestador de serviços cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
- f) Avarias nos sistemas informáticos ou mecânicos do prestador de serviços não devidas a sabotagem;
- g) Eventos que estejam ou devam estar cobertos por seguros.

4 - A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.

5 - A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Cláusula 13.ª

RESOLUÇÃO POR PARTE DO CONTRAENTE

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, o Município de Bragança pode resolver o contrato, a título sancionatório, no caso de o fornecedor violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem.
2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao prestador de serviços.

Cláusula 14.ª

EXECUÇÃO DA CAUÇÃO

- 1 - Conforme o ponto n.º 2 do art.º 88.º do Decreto-Lei 18/2008, de 29 de Janeiro, não é exigível a prestação de caução dado o preço contratual ser inferior a 200.000 euros;

Capítulo IV

Resolução de litígios

Cláusula 15.ª

FORO COMPETENTE

- 1 - Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo e Fiscal de Mirandela, com expressa renúncia a qualquer outro.

Capítulo V
Disposições finais

Cláusula 16.ª

COMUNICAÇÕES E NOTIFICAÇÕES

1 - Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas, nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no contrato.

2 - Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 17.ª

LEGISLAÇÃO APLICÁVEL

1 - O contrato é regulado pela legislação portuguesa.

PARTE II – CLÁUSULAS TÉCNICAS

O Município de Bragança (MB) pretende adquirir uma solução de segurança com licenciamento pelo período de 36 meses para 260 clientes.

A atual solução instalada no MB é o Panda EndPoint Protection Plus, com data de expiração a 15/06/2020. A nova solução a implementar deve permitir proteger os ativos do MB contra as ameaças mais recentes. O produto deve repelir ameaças conhecidas e detetar comportamentos estranhos que nunca foram vistos antes.

Atualmente, um bom produto de segurança não é mais apenas uma proteção antivírus. Também se trata de proteção por firewall, proteção contra crimes cibernéticos ao navegar na Internet, proteção contra ransomware, proteção VPN contra monitoramento e censura de terceiros e assim por diante.

O antivírus tradicional (AV) não está mais à altura do desafio proposto por atacantes modernos. Antivírus baseado em assinatura e heurística é ineficaz contra os tipos de ataques que as organizações experienciam hoje. Os cibercriminosos estão continuamente a criar novos métodos para atacar os endpoints, utilizando-os como ponto de entrada para obter os dados das organizações.

O ransomware tem sido uma das principais causas de preocupação e é provável que continue no futuro próximo. Detetá-lo é uma prioridade. As soluções de proteção de endpoints devem oferecer uma maneira de reverter as alterações que software malicioso, como ransomware, executa no seu sistema.

REQUISITOS OBRIGATÓRIOS

Pretende-se um produto “Next Generation Endpoint Protection” para permitir detetar ameaças de dia zero usando o AI e o Deep Learning para analisar executáveis e ameaças sem arquivos antes da execução, durante a execução e a capacidade de reverter as ações de um ataque. A solução a adquirir deve proteger estações de trabalho e servidores Windows, estações de trabalho Mac OS, smartphones e tablets iOS e Android.

1. PROTEÇÃO CONTRA A GAMA COMPLETA DE ATAQUES MODERNOS

- Vírus - programas com intenções maliciosas, caracterizados pelo fato de poderem se multiplicar e, assim, infectar outros computadores ou dispositivos.
- Trojans (Cavalos) - softwares maliciosos que podem se disfarçar de softwares comuns e, por isso, podem induzi-lo a fazer o download e executá-los no seu computador.
- Worms - programas maliciosos que tiram proveito das falhas de segurança e vulnerabilidades no sistema operativo ou outro software (como o navegador da web, por exemplo) e os utilizam para infectar o computador.

- Spyware - programas de software projetados para espionar e reunir informações sobre os utilizadores.
- Rootkits - um tipo específico de malware projetado para fornecer aos hackers acesso remoto e controle de um dispositivo, sem ser detectado pelas vítimas ou pelo software de segurança instalado nos dispositivos infectados.
- Ransomware - programas maliciosos que, uma vez infectados pelo computador, assumem o controle e criptografam os ficheiros, como fotos, documentos de trabalho e vídeos.
- Adware - programas de software que exibem anúncios no monitor, nos navegadores da web ou em outros locais do computador.
- Ataques à rede - quando os hackers tentam controlar seus dispositivos remotamente, eles podem fazer isso através de uma abordagem de "interrupção". É quando você precisa de um firewall para interromper ataques de rede. Um bom firewall deve ser capaz de desviar ataques externos, mas também informar sobre tráfego suspeito iniciado do seu computador para o mundo externo.
- Ameaças na Web – o seu navegador deve ser o primeiro da linha de defesa contra malware. É por isso que uma boa solução de segurança deve incluir um módulo de proteção da Web que pode impedir de visitar sites com conteúdo malicioso.

2. PROTEÇÃO CONFIÁVEL

Deve ser capaz de:

- Proteger sem causar conflitos com outros programas instalados no computador.
- Fornecer proteção atualizada permitindo atualização regular várias vezes ao dia.
- Automatizar verificações de segurança. Deve oferecer um meio de automatizar verificações antimalware. Deve permitir o agendamento de verificações antivírus.

3. IMPACTO NO DESEMPENHO

Deve:

- Ter um pequeno impacto nos tempos de inicialização do computador
- Ter um pequeno impacto no desempenho do computador
- Ser rápido na verificação de malware no computador

4. USABILIDADE

Deve ser fácil de usar tanto por utilizadores experientes quanto por utilizadores casuais, com pouco ou nenhum conhecimento sobre segurança. Isso significa:

- Ser fácil de navegar: Deve fornecer uma maneira intuitiva de navegar pelas várias janelas, guias, menus e configurações.

- Ser fácil de entender: As opções de configuração oferecidas devem ser fáceis de entender por todos os utilizadores.
- Fornecer documentação fácil de encontrar. Deve fornecer uma maneira fácil de aceder a documentação da Ajuda.
- A interface deve ser em língua portuguesa.

5. SOLUÇÃO BASEADA NA NUVEM

A gestão deve ser baseada a partir da Internet de forma a libertar o MB de hardware adicional ou outros recursos dedicados. A consola web deve permitir a gestão dos clientes através da Internet sem qualquer investimento adicional da infraestrutura inclusive para máquinas fora da rede.

A consola deve permitir a gestão centralizada de vários tipos de terminais: estações de trabalho, servidores e dispositivos móveis.

A consola de gestão deve ser organizada e intuitiva e com interface em língua portuguesa.

Os painéis devem fornecer uma avaliação completa do status de segurança de toda a empresa e, quando algo estiver errado, fornecer uma maneira rápida e fácil de aprofundar, avaliar o problema e resolvê-lo.

Os relatórios devem ser úteis e informativos, ativos ou passivos, ou ambos.

A solução deve gerar relatórios de segurança detalhados, que incluem resumos de ameaças, endpoints desprotegidos, resumos de navegação na web etc. etc.

As políticas devem ser pré-configuradas usando as práticas recomendadas, com a capacidade de fazer alterações rápida e facilmente, se o administrador desejar.

Devem estar incluídos os seguintes recursos:

- **Recursos de Segurança**
 - Proteção contra ameaças a arquivos, Web e email - Proteger as estações de trabalho do Windows contra ameaças de malware conhecidas, desconhecidas e avançadas.
 - Prevenção contra Exploits e ransomware - Reverter as ações executadas por malware no sistema operacional, oferecendo proteção contra cryptolockers.
 - Firewall - Proteger os computadores contra ameaças à rede ao navegar na Internet ou usar uma rede local.
 - Bloqueador de ataque de rede - Evitar ataques à rede, como a intrusão de um dispositivo remoto no sistema operacional.

- Verificação de vulnerabilidade - Identificar os patches disponíveis para atualizar os aplicativos para as versões mais recentes.
- Proteção móvel - Proteger dispositivos Android e iOS (Duas licenças móveis por utilizador)
- Descoberta na nuvem - Ver o uso de serviços em nuvem, bem como o tempo usado nas redes sociais e messengers.
- **Recursos de Gestão**
 - Bloqueio de nuvem - Bloquear o acesso do utilizador a recursos de nuvem, redes sociais ou messengers inadequados ou não autorizados.
 - Segurança para Microsoft Office 365 - Proteção completa contra ameaças para os serviços de comunicação e colaboração do Microsoft Office 365
 - Controle da Web - Controlar o acesso do utilizador aos recursos da Internet, dependendo do conteúdo ou do local de um site.
 - Controle de dispositivos - Gerir o acesso do utilizador a dispositivos externos e removíveis ligados ao computador.
 - Gestão de criptografia - Criptografar os dispositivos dos funcionários via BitLocker ou FileVault para manter os dados corporativos protegidos se um dispositivo for perdido ou roubado.
 - Gestão de patches - Automatizar a aplicação de patches para ter sempre as versões mais recentes das aplicações

6. SUPORTE

Deverão ser incluídos os seguintes serviços:

- Remoção da totalidade dos clientes de antivírus atualmente instalados (Panda);
- Instalação do novo agente de Antivírus em 20 endpoints, com acompanhamento por parte do MB o qual instalará os restantes. Devem existir políticas predefinidas, recomendadas por especialistas, entrando em vigor imediatamente após a instalação e sincronização da solução com a consola de gestão;
- No final o fornecedor deve entregar um relatório detalhado da instalação.

O fornecedor deverá dispor de Help-Desk para suporte ao cliente. Se houver problemas com o produto, deverá existir capacidade de resposta através dos seguintes meios: email, chat, telefone e apoio técnico remoto. Nenhuma das opções de suporte deve ter custos adicionais, além do que foi pago aquando da compra do produto.

As atualizações do produto devem ser asseguradas sem custos adicionais durante a vigência do contrato.

A proposta deve ser esclarecedora no que concerne ao cumprimento dos requisitos obrigatórios acima elencados. Deve ainda apresentar resposta às seguintes questões:

1. O produto depende de técnicas fundamentais, técnicas modernas ou uma combinação de ambos?
2. Como o produto deteta ameaças desconhecidas? Utiliza aprendizagem de máquina?
3. Que tecnologia existe para impedir ataques baseados “exploit-based” e “file-less”?
4. O produto possui tecnologia projetada especificamente para interromper o ransomware?
5. O produto possui um nível aceitável de falsos positivos? Se um falso positivo for detetado, qual a facilidade de reduzir o seu impacto?
6. O produto responde automaticamente a uma ameaça? Pode limpar automaticamente uma ameaça e responder a um incidente?
7. Qual nível de esforço é requerido para a implementação e uso da solução?
8. Que relatórios de testes recentes existem relativamente à pontuação do produto? Ex: AV-Test, AV-comparative, SE-Labs. Apresentar documentos ou links.
9. Em que quadrante Gartner está posicionado?
10. Qual o posicionamento em termos de testes de desempenho comparativamente a outros produtos?
11. Que certificações tem?
12. Está em conformidade com o RGPD (Regulamento Geral de Proteção de Dados)?