

Caderno de Especificações Técnicas



MUNICÍPIO DE
VISEU

Aquisição de Serviços de Proteção Endpoint e Plataforma de Correio Electrónico

20 de dezembro de 2021

DSTI – Divisão de Sistemas e Tecnologias e Inovação

Introdução

O Município de Viseu, no âmbito do processo de modernização técnica, fez uma aposta na qualidade onde as “TIC” estão sistematicamente ligadas à conjugação de imperativos de eficácia, eficiência, usabilidade, segurança e disponibilidade. Tem sido dado especial enfoque aos serviços a disponibilizar e à racionalização dos custos nas tecnologias e sistemas de informação.

O paradigma tecnológico mudou e o Município de Viseu adotou o “*cloud computing*” interno onde o recurso às tecnologias e sistemas de informação são disponibilizados na rede como um serviço de forma dinâmica, escalável e de alta disponibilidade sem com isso descurar os capítulos da segurança, integridade e confidencialidade dos diferentes sistemas interlocutores dos serviços disponibilizados.

1. Objeto

Com o objetivo de garantir a continuidade e a melhoria dos serviços prestados, o Município de Viseu pretende adquirir **serviços de proteção** ao nível do *endpoint*, bem como da plataforma de correio eletrónico, **por um período de 36 meses**.

2. Proteção *Endpoint* de equipamentos (Município)

2.1 Descrição das Subscrições, Suporte e Manutenção

Pretende-se um conjunto de funcionalidades que vão de encontro ao estipulado:

2.1.1. Gestão e suporte da solução a partir de uma consola Cloud. Pretende-se a gestão baseada a partir da Internet que liberte o Município de hardware adicional ou outros recursos dedicados. A interface deve permitir a gestão dos clientes através da Internet sem qualquer investimento adicional da infraestrutura inclusive para máquinas fora da rede;

2.1.2. Comunicação bidirecional entre os agentes instalados nas máquinas e a plataforma de gestão, permitindo que alterações operadas na consola se façam sentir nas máquinas no espaço de poucos segundos e sem intervenção local;

- 2.1.3. Proteção proactiva *anti-malware* para postos de trabalho Windows e Linux;
- 2.1.4. Proteção proactiva *anti-malware* para servidores Windows e Linux;
- 2.1.5. Proteção para Exchange Server (Antivírus, AntiSpam e Filtro de conteúdos);
- 2.1.6. Proteção *anti-malware* para Android;
- 2.1.7. Proteção antirroubo para Android com georreferenciação do equipamento;
- 2.1.8. Controlo de dispositivos;
- 2.1.9. Bloqueio de portas USB configuráveis por perfis;
- 2.1.10. *Malware Freezer* para bloqueio de falsos positivos;
- 2.1.11. *URL Filter* para controlo da utilização da Internet por categorias, *Whitelist* e *Blacklist* com possibilidade de políticas diferenciadas por máquina e por horário;
- 2.1.12. Instalação flexível;
- 2.1.13. Quarentena local com gestão centralizada;
- 2.1.14. Gestão da firewall pessoal;
- 2.1.15. Proteção da desinstalação por *password*;
- 2.1.16. Possibilidade desativar temporariamente funcionalidades da solução, quando necessário para efeitos de suporte, localmente, mas protegida com *password*;
- 2.1.17. Possibilidade de criação de contas com perfis de administração e monitorização diferenciáveis;
- 2.1.18. Atualizações e *upgrades* automatizados por P2P, direto à net ou através de máquina eleita para o efeito;
- 2.1.19. Relatórios detalhados e resumidos;
- 2.1.20. Inventário de *hardware* e *software* instalado nas máquinas;
- 2.1.21. Capacidade de usar filtros pré-definidos ou criação dos mesmos, podendo pesquisar por máquinas com determinadas características em termos de *hardware* ou *software*;

- 2.1.22. Logs de alteração de *software* e *hardware*;
- 2.1.23. Gestão e controlo de licenciamento;
- 2.1.24. Alertas personalizáveis;
- 2.1.25. Instalação e atualização remota de *software*;
- 2.1.26. Acesso remoto por RDP ou por VNC;
- 2.1.27. Acesso remoto não intrusivo, sem ser necessário interromper o dia a dia do utilizador;
- 2.1.28. Criação e execução remota de scripts;
- 2.1.29. Criação e gestão de *tickets* de suporte;
- 2.1.30. Gestão de dispositivos móveis (iOS e Android);
- 2.1.31. *Wake-on-Lan*;
- 2.1.32. Criação de políticas energéticas;
- 2.1.33. Monitorização de *routers*, *switches* e outros dispositivos via SNMP;
- 2.1.34. Suporte técnico em Português dado diretamente pelo fabricante;
- 2.1.35. Proteção EDR contra ameaças avançadas;
- 2.1.36. Proteção contra ataques direcionados;
- 2.1.37. Monitorização constante de todas as aplicações em execução;
- 2.1.38. Serviço automático de classificação de aplicações sem necessidade de validação e monitorização por parte da equipa de informática;
- 2.1.39. Autorização de execução somente de aplicações validadas como *goodware*;
- 2.1.40. Bloqueio de aplicações desconhecidas;
- 2.1.41. Garantia de confiabilidade sobre as aplicações executadas;
- 2.1.42. Informação sobre executáveis em análise;

20 de dezembro de 2021

- 2.1.43. Informação gráfica e detalhada sobre evolução do *malware* nas máquinas / rede;
- 2.1.44. Informação sobre ligações feitas ao exterior por processos maliciosos;
- 2.1.45. Informação sobre acesso a ficheiros efetuadas por processos maliciosos;
- 2.1.46. *Anti-Exploit* – Detecção de ciber ataques no seu estágio de *exploit*, através da contínua monitorização dos equipamentos;
- 2.1.47. Detecção automatizada dos chamados ataques *file-less*;
- 2.1.48. Identificação dos computadores usados para propagar ataques pela rede – Identificação da origem dos ataques;

Gestão de Patches

- 2.1.49 A solução proposta deve estar dotada da capacidade de efectuar o Patch Management de sistemas operativos Windows e das aplicações terceiras mais comuns no mercado (Java, Flash, Chrome, etc.);
- 2.1.50 Informação gráfica acessível a qualquer momento sobre o tipo de patch's que se encontram por instalar em todo o parque informático, mas também numa determinada máquina;
- 2.1.51 Informação por criticidade do patch – ligados à segurança, críticos, importantes, outros;
- 2.1.52 Capacidade de isolar uma máquina, bloqueando todas as comunicações para e a partir da mesma, mas mantendo a possibilidade de aplicar os patches necessários;
- 2.1.53 Informação sobre as aplicações/sistemas operativos em EOL (End Of Life).

2.2 Proteção de caixas de correio

Pretende-se o suporte e manutenção para proteção da plataforma de correio eletrónico, nos seguintes moldes:

- 2.2.1 Antivírus para o e-mail empresarial;
- 2.2.2 *Anti-phishing*;
- 2.2.3 *Anti-malware*;
- 2.2.4 Proteção contra ataques ao diretório;
- 2.2.5 Backup completo do e-mail *inbound*: 30 dias;
- 2.2.6 Filtros de ligação: listas de reputação de IP's;
 - 2.2.6.1 RBL: *blacklist* dos IP's geradores de spam;
 - 2.2.6.2 SPF: proteção contra a falsificação de endereços de e-mail;
 - 2.2.6.3 B/N: *black* e *white* lists globais (por domínio) e locais (por utilizador);
 - 2.2.6.4
- 2.2.7 Filtragem de remetentes:
 - 2.2.7.1 SenderDomVan (domínio);
 - 2.2.7.2 Recipient CallOut (remetente);
- 2.2.8 Filtragem de conteúdos, heurística e Baiesiana;
- 2.2.9 Sistema proactivo com atualizações dinâmicas dos filtros de spam em tempo real;
- 2.2.10 Motor configurável e com definição de regras;
- 2.2.11 Encriptação TLS;

2.3 Interface de Gestão

Especifica-se que a consola de gestão de utilizadores deve estar em concordância com os seguintes objetivos:

- 2.3.1 Interface de administração Web baseado em perfis;
- 2.3.2 Gestão em tempo real dos utilizadores;
- 2.3.3 Acesso SSL;
- 2.3.4 Relatórios do tráfego de e-mail;
- 2.3.5 Capacidade de configuração;

- 2.3.6 Proteção de multi-domínios;
- 2.3.7 Personalização simples;
- 2.3.8 Configuração por empresa, domínio e utilizador;
- 2.3.9 Configuração de relatórios para utilizador e administradores;
- 2.3.10 Integração com LDAP para registo de utilizadores (OpenLDAP, Active Directory e Domino);
- 2.3.11 Serviço de monitorização 24x7x365 com garantia de continuidade do serviço mesmo em caso de falhas;
- 2.3.12 Não deve necessitar de hardware dedicado, sendo escalável sem esforço;



MUNICÍPIO DE
VISEU

2.4 Proteção *Endpoint* de equipamentos (Licenças Escolares)

Pretende-se um conjunto de funcionalidades que vão de encontro ao estipulado para dar resposta às necessidades emergentes de equipamentos fora da rede do Município:

2.4.1. Gestão e suporte da solução a partir de uma consola *Cloud*. Pretende-se gestão baseada a partir da Internet que liberte o Município 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;

2.4.2. Comunicação bidirecional entre os agentes instalados nas máquinas e a plataforma de gestão, permitindo que alterações operadas na consola se façam sentir nas máquinas no espaço de poucos segundos e sem intervenção local;

2.4.3. Proteção proactiva *anti-malware* para postos de trabalho Windows e Linux;

2.4.4. Proteção proactiva *anti-malware* para servidores Windows e Linux;

2.4.5. Proteção *anti-malware* para Android;

2.4.6. Proteção antirroubo para Android com georreferenciação do equipamento;

2.4.7. Controlo de dispositivos;

2.4.8. Bloqueio de portas USB configuráveis por perfis;

2.4.9. *Malware Freezer* para bloqueio de falsos positivos;

2.4.10. URL Filter para controlo da utilização da Internet por categorias, *Whitelist* e *Blacklist* com possibilidade de políticas diferenciadas por máquina e por horário;

2.4.11. Instalação flexível;

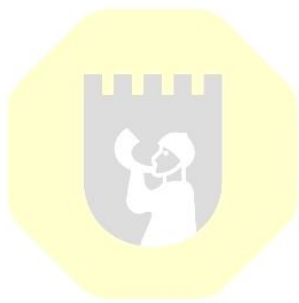
2.4.12. Quarentena local com gestão centralizada;

2.4.13. Gestão da firewall pessoal;

2.4.14. Proteção da desinstalação por password;

- 2.4.15. Possibilidade desativar temporariamente funcionalidades da solução, quando necessário para efeitos de suporte, localmente mas protegida com password;
- 2.4.16. Possibilidade de criação de contas com perfis de administração e monitorização diferenciáveis;
- 2.4.17. Atualizações e *upgrades* automatizados por P2P, direto à net ou através de máquina eleita para o efeito;
- 2.4.18. Relatórios detalhados e resumidos;
- 2.4.19. Inventário de *hardware* e *software* instalado nas máquinas;
- 2.4.20. Capacidade de usar filtros pré-definidos ou criação dos mesmos, podendo pesquisar por máquinas com determinadas características em termos de *hardware* ou *software*;
- 2.4.21. Relatórios detalhados e resumidos;
- 2.4.22. Suporte técnico dado em Português, diretamente pelo fabricante;
- 2.4.23. Inventariação de *Software*;
- 2.4.24. Inventariação de *Hardware*;
- 2.4.25. Logs de alteração de *software* e *hardware*;
- 2.4.26. Gestão e controlo de licenciamento;
- 2.4.27. Monitorização de máquinas com monitores já criados e com possibilidade de criação de monitores;
- 2.4.28. Alertas personalizáveis;
- 2.4.29. Gestão de *patch*;
- 2.4.30. Instalação remota de *software*;
- 2.4.31. Atualização remota de *software*;
- 2.4.32. Acesso remoto por RDP ou por VNC;
- 2.4.33. Acesso remoto não intrusivo, sem ser necessário interromper o dia a dia do utilizador;

- 2.4.34. Criação e execução remota de scripts;
- 2.4.35. Criação e gestão de *tickets* de suporte;
- 2.4.36. Gestão de dispositivos móveis compatível com Android e iOS;
- 2.4.37. *Wake on Lan*;
- 2.4.38. Criação de políticas energéticas;
- 2.4.39. Monitorização de impressoras por monitores;
- 2.4.40. Monitorização de *routers*, *switches* e/ou outros dispositivos por SNMP;



MUNICÍPIO DE
VISEU