Zimbra **daniloservilha@hortolandia.sp.gov.br**

Fwd: Esclarecimento PREGÃO ELETRÔNICO 06/2026-Ata de registro de preços para aquisição de solução de segurança de rede de dados da Prefeitura do Município de Hortolândia,

De : licitacao <licitacao@hortolandia.sp.gov.br> Qua, 04 de fev de 2026 09:22
Assunto : Fwd: Esclarecimento PREGÃO ELETRÔNICO 06/2026-Ata de registro de preços para aquisição de solução de segurança de rede de dados da Prefeitura do Município de Hortolândia, 2 anexos
Para : eduardo coelho <eduardo.coelho@telefonica.com>
Cc : DaniloServilha <daniloservilha@hortolandia.sp.gov.br>

Bom dia,

Segue em anexo resposta ao esclarecimento solicitado.

Atenciosamente,

PREFEITURA DE HORTOLÂNDIA
DEPARTAMENTO DE SUPRIMENTOS
FONE: (19) 3965-1400 - RAMAL: 6923

De: "LeonicioOliveira" <leonicioooliveira@hortolandia.sp.gov.br>
Para: "Licitacao" <licitacao@hortolandia.sp.gov.br>
Cc: "DaniloServilha" <daniloservilha@hortolandia.sp.gov.br>, "ClaudemirMarques" <claudemirmarques@hortolandia.sp.gov.br>
Enviadas: Quarta-feira, 4 de fevereiro de 2026 8:48:58
Assunto: Re: Esclarecimento PREGÃO ELETRÔNICO 06/2026-Ata de registro de preços para aquisição de solução de segurança de rede de dados da Prefeitura do Município de Hortolândia,

Segue em anexo resposta à solicitação de esclarecimento da Empresa Vivo 03/02.

À
Disposição

De: "Super Nosso" <licitacao@hortolandia.sp.gov.br>
Para: "LeonicioOliveira" <leonicioooliveira@hortolandia.sp.gov.br>
Cc: "DaniloServilha" <daniloservilha@hortolandia.sp.gov.br>, "ClaudemirMarques" <claudemirmarques@hortolandia.sp.gov.br>
Enviadas: Terça-feira, 3 de fevereiro de 2026 14:55:14
Assunto: Fwd: Esclarecimento PREGÃO ELETRÔNICO 06/2026-Ata de registro de preços para aquisição de solução de segurança de rede de dados da Prefeitura do Município de Hortolândia,

Boa tarde,

Segue o pedido de esclarecimento abaixo.

Atenciosamente,

PREFEITURA DE HORTOLÂNDIA
DEPARTAMENTO DE SUPRIMENTOS
FONE: (19) 3965-1400 - RAMAL: 6923

De: "eduardo coelho" <eduardo.coelho@telefonica.com>
Para: "Licitacao" <licitacao@hortolandia.sp.gov.br>
Enviadas: Terça-feira, 3 de fevereiro de 2026 14:46:33
Assunto: Esclarecimento PREGÃO ELETRÔNICO 06/2026-Ata de registro de preços para aquisição de solução de segurança de rede de dados da Prefeitura do Município de Hortolândia,

Boa tarde
Segue esclarecimento

À (ao)
Município de Hortolândia

Assunto: Esclarecimento

Ref.: PE 006/2026

TELEFONICA BRASIL S/A, Companhia Aberta, com sede na Avenida Engenheiro Luiz Carlos Berrini, nº. 1376, Bairro Cidade Monções, São Paulo/SP, CEP 04.571-000, inscrita no CNPJ sob o nº. 02.558.157/0001-62, NIRE nº. 35.3.001.5881-4, vem respeitosamente publicar o seguinte esclarecimento:

PEDIDO DE ESCLARECIMENTO

Ref.: Pregão Eletrônico Nº 06/2026 – Prefeitura de Hortolândia

Esclarecimento técnico

Esclarecimento

1.3.1.6 - Proteção contra ataques avançados:
1.3.2.5 - Proteção contra ataques avançados:
1.3.3.6 - Proteção contra ataques avançados:
A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças, com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

1. *Inspeção profunda de memória em tempo real;*
2. *Inspeção profunda de pacotes livre de remontagem;*
3. *Descriptografia e inspeção TLS versão 1.2 no mínimo;*
4. *Inteligência e controle de aplicativos;*

Considerando o requisito referente às tecnologias avançadas de proteção contra ameaças, com uso de sandboxing baseado em nuvem, entende-se que o objetivo deste requisito é assegurar que a solução de Firewall NGFW possua mecanismos robustos de detecção, identificação e mitigação

de ameaças em tempo real, abrangendo tráfego criptografado e controle por aplicações, mantendo desempenho compatível com ambiente corporativo.
Dessa forma, para fins de comprovação técnica e aceitação do atendimento, adota-se o entendimento de que o requisito contempla:
a) Análise avançada de malware em tempo real no tráfego de rede, incluindo inspeção de arquivos e conteúdo, com detecção e bloqueio automático de ameaças, inclusive desconhecidas, com suporte à submissão e análise em sandbox em nuvem;
b) Inspeção de pacotes em modo flow-based (packet-by-packet), assegurando inspeção sem necessidade de remontagem completa do tráfego para análise;
c) Descriptografia e inspeção SSL/TLS, com suporte mínimo à TLS 1.2, permitindo inspeção e aplicação de políticas de segurança também em tráfego criptografado;
d) Inteligência e controle de aplicações (Application Control), permitindo identificação, classificação e aplicação de políticas por aplicação/categoria.

Está correto entendimento?

Esclarecimento 2

1.3.1.6 - Proteção contra ataques avançados:
1.3.2.5 - Proteção contra ataques avançados:
1.3.3.6 - Proteção contra ataques avançados:
*As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se **alojam em memória,** atuando permanentemente e em tempo real;*

Entende-se que a intenção do Termo de Referência é assegurar que a solução de Firewall NGFW possua mecanismos avançados capazes de identificar e mitigar ameaças modernas, inclusive aquelas associadas a técnicas fileless e exploração que operam em múltiplas etapas, muitas vezes sem gravação evidente em disco.
Dessa forma, para fins de atendimento técnico e comprovação, considera-se que o requisito é contemplado por capacidades de proteção contínua em tempo real no plano de rede, tais como:

1. IPS (Intrusion Prevention System) com detecção de exploits e ataques em camadas de rede e aplicação;
2. Antimalware/ATP com inspeção contínua do tráfego e bloqueio automatizado;
3. Inspeção SSL/TLS (Deep Inspection) permitindo identificar ameaças mesmo em tráfego criptografado;
4. Sandboxing em nuvem para análise dinâmica e detecção de malware desconhecido;
5. Bloqueio por reputação e inteligência de ameaças, prevenindo conexões com infraestrutura maliciosa (C2/botnet), associada a ameaças avançadas.

Está correto entendimento?

Esclarecimento proposto 3 (para submissão ao órgão)

1.3.1.5 - Controle de ameaças:
1.3.2.4 - Controle de ameaças:
1.3.3.5 - Controle de Ameaças:
A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por vulnerabilidades do tipo meltdown;

Entende-se que a finalidade do Termo de Referência é garantir que a solução possua capacidade efetiva de prevenção, detecção e mitigação em tempo real contra explorações de vulnerabilidades e ataques avançados, inclusive aqueles associados a técnicas sofisticadas de comprometimento.
Dessa forma, para fins de atendimento e comprovação, adota-se o entendimento de que o requisito é plenamente contemplado por uma solução Firewall NGFW dotada de mecanismos de proteção em rede, tais como:

a) IPS (Intrusion Prevention System) com capacidade de detecção e bloqueio de exploits e tentativas de exploração de vulnerabilidades, com atualização contínua baseada em inteligência de ameaças;
b) Inspeção profunda de tráfego em camada de aplicação (L7), com análise do comportamento do tráfego e identificação de tentativas de exploração durante comunicações em rede;

c) Descriptografia e inspeção SSL/TLS (Deep Inspection), viabilizando a detecção e mitigação mesmo quando o tráfego estiver criptografado;
d) Sandboxing em nuvem para análise dinâmica multi-mecanismos de objetos suspeitos, complementando a prevenção de ataques avançados e malwares desconhecidos.

Está correto o entendimento?

Atenciosamente,

Eduardo Lavras Queiroz Teles Coelho
Gerente de Negócios
Rua Carolina Prado Penteado, nº 477
CEP 13092-470 | Campinas – SP
+Cel + 55 19 99709-8675
www.vivo.com.br

--

Atenciosamente;

Leonicio Ornelas de Oliveira
Departamento de Tecnologia da Informação
Fone: 3965-1400 ramal 9028

Respostas à solicitação de esclarecimentos VIVO 03_02.pdf
507 KB

Campinas, 03 de fevereiro de 2026

À (ao)
Município de Hortolândia

Assunto: Esclarecimento

Ref.: PE 006/2026

TELEFONICA BRASIL S/A, Companhia Aberta, com sede na Avenida Engenheiro Luiz Carlos Berrini, nº. 1376, Bairro Cidade Monções, São Paulo/SP, CEP 04.571-000, inscrita no CNPJ sob o nº. 02.558.157/0001-62, NIRE nº. 35.3.001.5881-4, vem respeitosamente publicar o seguinte esclarecimento:

PEDIDO DE ESCLARECIMENTO

Ref.: Pregão Eletrônico Nº 06/2026 – Prefeitura de Hortolândia

Assunto: dúvida técnica

Esclarecimento

1.3.1.6 - Proteção contra ataques avançados:
1.3.2.5 - Proteção contra ataques avançados:

1.3.3.6 - Proteção contra ataques avançados:

A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças, com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

1. *Inspeção profunda de memória em tempo real;*
2. *Inspeção profunda de pacotes livre de remontagem;*
3. *Descriptografia e inspeção TLS versão 1.2 no mínimo;*
4. *Inteligência e controle de aplicativos;*

Considerando o requisito referente às tecnologias avançadas de proteção contra ameaças, com uso de sandboxing baseado em nuvem, entende-se que o objetivo deste requisito é assegurar que a solução de Firewall NGFW possua mecanismos robustos de detecção, identificação e mitigação de ameaças em tempo real, abrangendo tráfego criptografado e controle por aplicações, mantendo desempenho compatível com ambiente corporativo.

Dessa forma, para fins de comprovação técnica e aceitação do atendimento, adota-se o entendimento de que o requisito contempla:

a) Análise avançada de malware em tempo real no tráfego de rede, incluindo inspeção de arquivos e conteúdo, com detecção e bloqueio automático de ameaças, inclusive desconhecidas, com suporte à submissão e análise em sandbox em nuvem;

b) Inspeção de pacotes em modo flow-based (packet-by-packet), assegurando inspeção sem necessidade de remontagem completa do tráfego para análise;

c) Descriptografia e inspeção SSL/TLS, com suporte mínimo à TLS 1.2, permitindo inspeção e aplicação de políticas de segurança também em tráfego criptografado;

d) Inteligência e controle de aplicações (Application Control), permitindo identificação, classificação e aplicação de políticas por aplicação/categoria.

Está correto entendimento?

Esclarecimento 2

1.3.1.6 - Proteção contra ataques avançados:

1.3.2.5 - Proteção contra ataques avançados:

1.3.3.6 - Proteção contra ataques avançados:

As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se ***alojam em memória,*** *atuando permanentemente e em tempo real;*

Entende-se que a intenção do Termo de Referência é assegurar que a solução de Firewall NGFW possua mecanismos avançados capazes de identificar e mitigar ameaças modernas, inclusive aquelas associadas a técnicas fileless e exploração que operam em múltiplas etapas, muitas vezes sem gravação evidente em disco.

Dessa forma, para fins de atendimento técnico e comprovação, considera-se que o requisito é contemplado por capacidades de proteção contínua em tempo real no plano de rede, tais como:

1. IPS (Intrusion Prevention System) com detecção de exploits e ataques em camadas de rede e aplicação;
2. Antimalware/ATP com inspeção contínua do tráfego e bloqueio automatizado;
3. Inspeção SSL/TLS (Deep Inspection) permitindo identificar ameaças mesmo em tráfego criptografado;
4. Sandboxing em nuvem para análise dinâmica e detecção de malware desconhecido;
5. Bloqueio por reputação e inteligência de ameaças, prevenindo conexões com infraestrutura maliciosa (C2/botnet), associada a ameaças avançadas.

Está correto entendimento?

Esclarecimento proposto 3 (para submissão ao órgão)

1.3.1.5 - Controle de ameaças:
1.3.2.4 - Controle de ameaças:
1.3.3.5 - Controle de Ameaças:

A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por vulnerabilidades do tipo meltdown;

Entende-se que a finalidade do Termo de Referência é garantir que a solução possua capacidade efetiva de prevenção, detecção e mitigação em tempo real contra explorações de vulnerabilidades e ataques avançados, inclusive aqueles associados a técnicas sofisticadas de comprometimento.

Dessa forma, para fins de atendimento e comprovação, adota-se o entendimento de que o requisito é plenamente contemplado por uma solução Firewall NGFW dotada de mecanismos de proteção em rede, tais como:

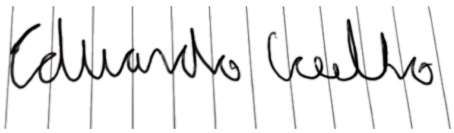
a) IPS (Intrusion Prevention System) com capacidade de detecção e bloqueio de exploits e tentativas de exploração de vulnerabilidades, com atualização contínua baseada em inteligência de ameaças;

b) Inspeção profunda de tráfego em camada de aplicação (L7), com análise do comportamento do tráfego e identificação de tentativas de exploração durante comunicações em rede;

c) Descriptografia e inspeção SSL/TLS (Deep Inspection), viabilizando a detecção e mitigação mesmo quando o tráfego estiver criptografado;

d) Sandboxing em nuvem para análise dinâmica multi-mecanismos de objetos suspeitos, complementando a prevenção de ataques avançados e malwares desconhecidos.

Está correto o entendimento?



Atenciosamente,

TELEFONICA BRASIL S/A
Eduardo Coelho

RG: 32.954.452-4 / CPF: 310.854.098-05
Gerente de Negócios | PWCCC
Divisão Comercial Governo SP | Telefônica Brasil
Procurador
Rua Carolina Prado Penteado, nº 477
CEP 13092-470 | Campinas – SP
+Cel + 55 19 99709-8675
eduardo.coelho@telefonica.com

Campinas, 03 de fevereiro de 2026

À (ao)

Município de Hortolândia

Assunto: Esclarecimento

Ref.: PE 006/2026

TELEFONICA BRASIL S/A, Companhia Aberta, com sede na Avenida Engenheiro Luiz Carlos Berrini, nº. 1376, Bairro Cidade Monções, São Paulo/SP, CEP 04.571-000, inscrita no CNPJ sob o nº. 02.558.157/0001-62, NIRE nº. 35.3.001.5881-4, vem respeitosamente publicar o seguinte esclarecimento:

PEDIDO DE ESCLARECIMENTO

Ref.: Pregão Eletrônico Nº 06/2026 – Prefeitura de Hortolândia

Assunto: dúvida técnica

Esclarecimento

1.3.1.6 - Proteção contra ataques avançados:

1.3.2.5 - Proteção contra ataques avançados:

1.3.3.6 - Proteção contra ataques avançados:

A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças, com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

1. Inspeção profunda de memória em tempo real;

2. Inspeção profunda de pacotes livre de remontagem;

3. Descriptografia e inspeção TLS versão 1.2 no mínimo;

4. Inteligência e controle de aplicativos;

Considerando o requisito referente às tecnologias avançadas de proteção contra ameaças, com uso de sandboxing baseado em nuvem, entende-se que o objetivo deste requisito é assegurar que a solução de Firewall NGFW possua mecanismos robustos de detecção, identificação e mitigação de ameaças em tempo real, abrangendo tráfego criptografado e controle por aplicações, mantendo desempenho compatível com ambiente corporativo.

Dessa forma, para fins de comprovação técnica e aceitação do atendimento, adota-se o entendimento de que o requisito contempla:

a) Análise avançada de malware em tempo real no tráfego de rede, incluindo inspeção de arquivos e conteúdo, com detecção e bloqueio automático de ameaças, inclusive desconhecidas,com suporte à submissão e análise em sandbox em nuvem;

b) Inspeção de pacotes em modo flow-based (packet-by-packet), assegurando inspeção sem necessidade de remontagem completa do tráfego para análise;

c) Descriptografia e inspeção SSL/TLS, com suporte mínimo à TLS 1.2, permitindo inspeção e aplicação de políticas de segurança também em tráfego criptografado;

d) Inteligência e controle de aplicações (Application Control), permitindo identificação, classificação e aplicação de políticas por aplicação/categoria.

Está correto entendimento?

Resposta:

Sim está correto o entendimento.

Todas as características acima citadas deverão fazer parte do firewall ofertado.

Esclarecimento 2

1.3.1.6 - Proteção contra ataques avançados:

1.3.2.5 - Proteção contra ataques avançados:

1.3.3.6 - Proteção contra ataques avançados:

As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real;

Entende-se que a intenção do Termo de Referência é assegurar que a solução de Firewall NGFW possua mecanismos avançados capazes de identificar e mitigar ameaças modernas, inclusive aquelas associadas a técnicas fileless e exploração que operam em múltiplas etapas, muitas vezes sem gravação evidente em disco.

Dessa forma, para fins de atendimento técnico e comprovação, considera-se que o requisito é contemplado por capacidades de proteção contínua em tempo real no plano de rede, tais como:

1. IPS (Intrusion Prevention System) com detecção de exploits e ataques em camadas de rede e aplicação;

2. Antimalware/ATP com inspeção contínua do tráfego e bloqueio automatizado;

3. Inspeção SSL/TLS (Deep Inspection) permitindo identificar ameaças mesmo em tráfego criptografado;

4. Sandboxing em nuvem para análise dinâmica e detecção de malware desconhecido;

5. Bloqueio por reputação e inteligência de ameaças, prevenindo conexões com infraestrutura maliciosa (C2/botnet), associada a

ameaças avançadas.

Está correto entendimento?

Resposta:

Sim, está correto o entendimento.
Todas as funções citadas acima deverão acompanhar a solução de firewall.

Esclarecimento proposto 3 (para submissão ao órgão)

1.3.1.5 - Controle de ameaças:

1.3.2.4 - Controle de ameaças:

1.3.3.5 - Controle de Ameaças:

A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por

vulnerabilidades do tipo meltdown;

Entende-se que a finalidade do Termo de Referência é garantir que a solução possua capacidade efetiva de prevenção, detecção e mitigação em tempo real contra explorações de vulnerabilidades e ataques avançados, inclusive aqueles associados a técnicas sofisticadas de comprometimento.

Dessa forma, para fins de atendimento e comprovação, adota-se o entendimento de que o requisito é plenamente contemplado por uma solução Firewall NGFW dotada de mecanismos de proteção em rede, tais como:

a) IPS (Intrusion Prevention System) com capacidade de detecção e bloqueio de exploits e tentativas de exploração de vulnerabilidades, com atualização contínua baseada em inteligência de ameaças;

b) Inspeção profunda de tráfego em camada de aplicação (L7), com análise do comportamento do tráfego e identificação de tentativas de exploração durante comunicações em rede;

c) Descriptografia e inspeção SSL/TLS (Deep Inspection), viabilizando a detecção e mitigação mesmo quando o tráfego estiver criptografado;

d) Sandboxing em nuvem para análise dinâmica multi-mecanismos de objetos suspeitos, complementando a prevenção de ataques avançados e malwares desconhecidos.

Está correto o entendimento?

Resposta:

Sim está correto o entendimento.
Todas as funcionalidades deverão acompanhar a solução de firewall.

Atenciosamente,

TELEFONICA BRASIL S/A

Eduardo Coelho

RG: 32.954.452-4 / CPF: 310.854.098-05

Gerente de Negócios | PWCCC

Divisão Comercial Governo SP | Telefônica Brasil

Procurador

Rua Carolina Prado Penteado, nº 477

CEP 13092-470 | Campinas – SP

+Cel + 55 19 99709-8675

eduardo.coelho@telefonica.com