



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

SUMÁRIO

ANEXO I – TERMO DE REFERÊNCIA - PROJETO BÁSICO	4
1. OBJETO	4
2. JUSTIFICATIVA	5
3. CLASSIFICAÇÃO DO SERVIÇO	6
4. LEGISLAÇÕES PERTINENTES AO OBJETO	6
5. DA VISTORIA	6
6. GLOSSARIO	7
7. CERTIFICAÇÕES DO PRODUTO E QUALIFICAÇÃO TÉCNICA	13
8. PROPOSTA COMERCIAL	14
9. DA AVALIAÇÃO DO SISTEMA	15
10. DAS SOLICITAÇÕES, PRAZO DE ENTREGA E VIGÊNCIA.....	16
11. HORÁRIOS E LOCAL DA PRESTAÇÃO DOS SERVIÇOS.....	17
12. DO RECEBIMENTO.....	17
13. GARANTIAS DOS PRODUTOS	19
14. SERVIÇO DE IMPLANTAÇÃO DA SOLUÇÃO	20
14.1. CONDIÇÕES PARA IMPLEMENTAÇÃO DAS SOLUÇÕES:	20
14.2. INSTALAÇÃO E CONFIGURAÇÃO NO AMBIENTE DE REDE DO CRA-SP DE TODOS OS EQUIPAMENTOS, SOFTWARES E DEMAIS RECURSOS QUE COMPÕEM AS SOLUÇÕES:	20
14.3. DOCUMENTAÇÃO PÓS IMPLANTAÇÃO:.....	23
14.4. SERVIÇO DE TREINAMENTO DAS SOLUÇÕES CONTRATADAS:.....	24
14.5. ACOMPANHAMENTO PÓS IMPLANTAÇÃO (OPERAÇÃO ASSISTIDA):	25
15. DISPOSITIVO (<i>APPLIANCE</i>) DE CONTROLE DE ACESSO LÓGICO NO PADRÃO NEXT GENERATION FIREWALL – NGFW/UTM, COM LICENCIAMENTO DE TODOS OS SOFTWARES E RECURSOS ACERCA DA SOLUÇÃO:	26
16. SOLUÇÃO SOFTWARE DE <i>ENDPOINT</i> (ANTIVÍRUS) PARA, NO MÍNIMO, 150 USUÁRIOS/COMPUTADORES:	26
17. SERVIÇO DE MONITORAMENTO REMOTO, 24X7:	27
18. SERVIÇOS DE SUPORTE TÉCNICO, MANUTENÇÕES E CONSULTORIA ESPECIALIZADA:	29
18.1. SUPORTE TÉCNICO ESPECIALIZADO, COM SLA, SENDO: REMOTO E "ON <i>SITE</i> ":	29
19.1. GESTÃO DE INCIDENTES:	30
20.1. VISITA PERIÓDICA DE ESPECIALISTA E CONSULTORIA CONTÍNUA	30
20.2. CONSULTORIA PARA OS SERVIÇOS DE ANÁLISE DE VULNERABILIDADE E / OU TESTE DE PENETRAÇÃO (<i>PENTEST</i>).....	30
20.2.2. REQUISITOS GERAIS:	31



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

20.2.3.	ANÁLISE DE VULNERABILIDADE.....	31
20.2.4.	TESTE DE PENETRAÇÃO (PENTEST):.....	32
21.	OBRIGAÇÕES DO CONTRATANTE	33
22.	OBRIGAÇÕES DA CONTRATADA	34
23.	DA SUBCONTRATAÇÃO	35
24.	DA CONFIDENCIALIDADE	35
25.	DO ACOMPANHAMENTO E DA FISCALIZAÇÃO	36
26.	DAS SANÇÕES ADMINISTRATIVAS	36
ANEXO II - REQUISITOS TÉCNICOS DAS SOLUÇÕES CONTRATADAS		39
2. DISPOSITIVO (APPLIANCE) DE CONTROLE DE ACESSO LÓGICO NO PADRÃO NEXT GENERATION FIREWALL – NGFW/UTM, COM LICENCIAMENTO DE TODOS OS SOFTWARES E RECURSOS ACERCA DA SOLUÇÃO:.....		39
1.1.	REQUISITOS GERAIS:.....	39
1.2.	REQUISITOS DE CAPACIDADE.....	40
1.3.	REQUISITOS DE HARDWARE E PERFORMANCE	41
1.4.	ANTIVÍRUS / ANTI-SPYWARE / ANTI-MALWARE	43
1.5.	CONTROLE DE APLICAÇÕES	44
1.6.	CAPTURA DE PACOTES	46
1.7.	FUNCIONALIDADES DE REDE	47
1.8.	NAT (NETWORK ADDRESS TRANSLATION)	47
1.9.	VPN (VIRTUAL PRIVATE NETWORK)	48
1.10.	QOS (QUALITY OF SERVICE).....	49
1.11.	AUTENTICAÇÃO	50
1.12.	IPS (INTRUSION PREVENTION SYSTEM)	50
1.13.	CONTROLE DE APLICAÇÃO (APPLICATION CONTROL).....	52
1.14.	RECURSOS PARA FILTRO DE CONTEÚDO WEB (WWW)	53
1.15.	PROTEÇÃO CONTRA VIRUS E BOT-NETS	55
1.16.	ADMINISTRAÇÃO E RELATÓRIOS	56
1.17.	LOG E AUDITORIA.....	60
3. SOLUÇÃO SOFTWARE DE ENDPOINT (ANTIVÍRUS) PARA, NO MÍNIMO, 150 USUÁRIOS/COMPUTADORES.....		61
3.1.	REQUISITOS GERAIS:.....	61
3.2.	CONSOLE DE GERENCIAMENTO	62
3.3.	CARACTERÍSTICAS GERAIS.....	62
3.4.	PAINEL PARA MONITORAMENTO	62
3.5.	INVENTÁRIO DA REDE	63
3.6.	POLÍTICAS	63



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

3.7.	RELATÓRIOS	64
3.8.	QUARENTENA	Erro! Indicador não definido.
3.9.	USUÁRIOS.....	64
3.10.	LOGS.....	64
3.11.	CERTIFICADO DE SEGURANÇA.....	64
3.12.	PROTEÇÃO PARA ESTAÇÕES DE TRABALHO E SERVIDORES FÍSICOS	64
3.13.	GERENCIAMENTO E INSTALAÇÃO REMOTA.....	65
3.14.	PROTEÇÃO PARA ESTAÇÕES E SERVIDORES VIRTUAIS	66
3.15.	COMPONENTES E FUNCIONALIDADE DO ANTIVÍRUS GERAL.....	67
3.16.	QUARENTENA	68
3.17.	CONTROLE DE USUÁRIO.....	68
3.18.	CONTROLE DO DISPOSITIVO	69
3.19.	ATUALIZAÇÃO.....	69
3.20.	SEGURANÇA PARA SMARTPHONES	69
3.21.	CONFIGURAÇÕES DE SEGURANÇA	70
3.22.	CRIPTOGRAFIA	70
ANEXO III - AMBIENTE COMPUTACIONAL DO CONSELHO		71
ANEXO IV - COMPLEXO CRA-SP.....		73
ANEXO V – ROTEIRO DE HOMOLOGAÇÃO DOS SERVIÇOS		74
ANEXO VI - SERVIÇO DE SUPORTE TÉCNICO E ATUALIZAÇÃO DE VERSÕES		76
1.	REQUISITOS GERAIS:	76
2.	SOBRE A CENTRAL DE ATENDIMENTO:	78
3.	TROUBLESHOOTING	79
4.	ATUALIZAÇÃO DE VERSÕES:.....	80
5.	REPOSIÇÃO DE HARDWARE EM CASO DE FALHAS:.....	80
6.	EQUIPE TÉCNICA DA CONTRATADA	81
ANEXO VII – NÍVEIS MÍNIMOS DE SERVIÇO (SLA).....		83
ANEXO VIII - REQUISITOS DE SEGURANÇA DA INFORMAÇÃO		87
ANEXO IX – TERMO DE CONFIDENCIALIDADE.....		88
1.	COMPROMISSO DE SIGILO	88
2.	DO TRATAMENTO DE DADOS.....	88
ANEXO X - MODELO DE PROPOSTA COMERCIAL		91
ANEXO XI – MODELO DE COMPROVANTE DE QUALIFICAÇÃO TÉCNICA		94
ANEXO XII - DECLARAÇÕES		96



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ANEXO I – TERMO DE REFERÊNCIA (PROJETO BÁSICO)

1. OBJETO

1.1. A contratação de empresa especializada para o fornecimento de soluções integradas de segurança de dados, composto por *appliance* no padrão *Next Generation Firewall – NGFW/UTM*, software *Endpoint* (antivírus) para os dispositivos em rede, a ser instalada na sede do Conselho Regional de Administração de São Paulo, pelo período de 36 (trinta e seis) meses, em conformidade com as especificações e detalhamentos consignados no Termo de Referência;

1.2. O projeto se dará através dos itens abaixo:

	ITEM	DETALHAMENTO	SERVIÇO
GRUPO 1	1	Serviço de implantação das soluções contratadas, contemplando:	Implantação
		- Instalação e configuração no ambiente de rede do CRA-SP de todos os equipamentos, softwares e demais recursos que compõem as soluções;	
		- Serviço de treinamento das soluções contratadas.	
	2	Dispositivo (<i>Appliance</i>) para controle de acesso lógico no padrão <i>Next Generation Firewall – NGFW/UTM</i> , contemplando:	Mensal
		- Licenciamento dos softwares necessários para o funcionamento de todos os recursos e funcionalidade descritas neste certame;	
		- Implantação;	
		- Operação.	
		Solução software de <i>Endpoint</i> (antivírus) para, no mínimo, 150 usuários/computadores, contemplando:	Mensal
		- Licenciamento de software;	
		- Implantação;	
		- Operação.	
		Serviço de monitoramento remoto, 24 horas por dia e 7 dias por semana (24x7), contemplando:	7x24
		- Centro de Operação de Segurança (SOC - <i>Security Operation Center</i>), próprio e especializado;	
		- Plataforma/Software próprio para monitoramento dos principais hosts e serviços de rede do CRA-SP.	
		Serviços de suporte técnico, manutenções e consultoria especializada:	Horário Expediente CRA-SP
		- Suporte técnico especializado, com SLA, sendo: remoto e "on site";	
		- Consultoria para política de segurança;	
		- Gestão de incidentes;	
		- Visita periódica de especialista;	
		- Consultoria para os serviços de análise de vulnerabilidade e / ou teste de penetração (<i>pentest</i>).	



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

2. JUSTIFICATIVA

O CRA-SP passou por transformações institucionais nos últimos anos que ampliaram a sua abrangência e atuação no campo da Administração. Sendo que na mesma proporção, cresceu a sua infraestrutura tecnológica da empresa.

Esta expansão resultou no aumento do uso de recursos como e-mails, acesso a páginas e serviços na internet, compartilhamento de arquivos, vídeo conferências e etc., ou seja, maiores volumes de dados gerados e trafegados na rede da empresa.

Além disso, as ameaças virtuais estão cada vez mais sofisticadas e agressivas, e podem se manifestar das mais diversas formas, causando danos seríssimos ao órgão.

Neste contexto, este projeto visa a contratação de empresa especializada em soluções integradas de segurança da informação, de modo, a gerenciar os principais recursos da rede de dados do Conselho, além de prestar suporte e consultoria contínua todos os assuntos relacionados à segurança da informação, como: análise de vulnerabilidades, teste de penetração e gestão de incidentes relacionados à segurança da informação e outros.

Esta contratação visa também manter os serviços prestados pela atual solução, ampliando o nível de segurança digital em todo ambiente tecnológico do CRA-SP.

Atualmente a solução que está em uso é responsável por serviços importantes como:

- ✓ Publicação dos SERVIÇOS ONLINE: sistema responsável por funções no site do CRA-SP, como Pagamentos de Anuidades e outras Taxas, Emissões de Certidões, Pré-cadastro de Profissionais e Estudantes, Cadastro de Peritos e etc.;
- ✓ Publicação do Portal e demais sites do CRA-SP;
- ✓ Acesso aos principais sistemas em uso pelas áreas operacionais do órgão;
- ✓ Emissões das Carteiras de Identidade Profissional, sejam elas emitidas em formato físico ou digital;
- ✓ Integração entre sistemas do Conselho e meios de pagamentos online;
- ✓ Acesso à Internet através de dispositivos na rede do Conselho;
- ✓ Prevenção contra ameaças e vulnerabilidades à rede;
- ✓ Gerenciamentos de links de internet e Controle de banda;
- ✓ Monitoramento de ativos de rede, sistemas, usuários e etc.
- ✓ E outros.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

3. CLASSIFICAÇÃO DO SERVIÇO

- 3.1. O objeto a ser contratado é de natureza comum, cujos padrões de desempenho e qualidade estão objetivamente definidos pelo edital e seus anexos, por meio de especificações usuais no mercado, conforme termos do parágrafo único, do art. 1º, da Lei 10.520, de 2002;
- 3.2. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto nº 2.271, de 1997, constituindo-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal do órgão licitante, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos;
- 3.3. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

4. LEGISLAÇÕES PERTINENTES AO OBJETO

- 4.1. Este projeto está alinhado a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709/2018) e todas as suas exigências, além de demais legislações e normas relacionadas as Segurança da Informação como:
 - O Marco Civil da Internet (Lei nº 12.965/2014);
 - PEC 17/2019 (proteção de dados pessoais entre os direitos e garantias fundamentais);
 - Lei nº 12.527/2011 (Lei de acesso à informação);
 - Lei 12.737/2012 - que promoveu alterações no Código Penal Brasileiro tipificando os chamados delitos ou crimes informáticos;
 - Lei Estadual 12.228/2006, que dispõe de acesso à internet a redes sem fio, qualquer empresa que se propõe a fornecer internet em seu ambiente privado, é responsável legalmente (seja na esfera civil ou criminal);
 - Normas ISO/IEC 27000 – que convergem para o Sistema de Gestão de Segurança da Informação (SGSI);
 - E outras.

5. DA VISTORIA

- 5.1. Todas as vistorias serão realizadas das 10h00 às 12h00 e das 14h00 às 17h00, de 2ª a 6ª feira, **até o dia 27/03/2020** e deverão ser agendadas pelo e-mail: vistoria.tecnica@crasp.gov.br, por meio de mensagem contendo o assunto “Vistoria referente à Solução de Segurança da Informação”, constando da solicitação os seguintes dados: Razão



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

Social, CNPJ, Nome, RG e Cargo da pessoa que fará a vistoria, a fim de que seja agilizada a emissão do Atestado.

- 5.2. Ressaltamos que toda despesa decorrente desse ato correrá por conta de cada licitante interessada.
- 5.3. Lembramos observar o prazo legal para a realização de consultas, para os questionamentos.
- 5.4. O agendamento será realizado respeitando-se a ordem de chegada das solicitações;
- 5.5. A vistoria será acompanhada por representante do CRA-SP, designado para esse fim, o qual emitirá a declaração comprobatória da vistoria efetuada.
- 5.6. No ato da vistoria a licitante receberá, entre outras, as seguintes informações sobre as instalações prediais do ambiente do CRA-SP:
 - 5.6.1. Local onde será instalado o equipamento;
 - 5.6.2. Condição lógicas para a configuração da rede;
 - 5.6.3. Política Corporativa de Segurança da Informação do contratante e normativos correlatos;
 - 5.6.4. Estrutura de cabeamento e ligações físicas entre os setores;
 - 5.6.5. Informações sobre a área de tecnologia da informação;
 - 5.6.6. Informações sobre o ambiente computacional.
- 5.7. Realizada a vistoria e obtida a declaração, deverá a licitante incluí-la entre os documentos obrigatórios para fins de habilitação;
- 5.8. A licitante avaliará, quando da vistoria, a infraestrutura de TI do contratante e os limites tecnológicos e demais elementos de hardware e software, aos quais estará submetida a Solução quando de sua entrega, inclusive quanto ao alcance dos níveis mínimos de serviço exigidos no Edital;
- 5.9. A licitante poderá levantar informações, caso considere pertinente, sobre os softwares do contratante a serem migrados para e integrados com a nova Solução.

6. GLOSSARIO

- 6.1. **ACCESS POINT:** ou ponto de acesso, são dispositivos que permitem interligar uma rede a vários dispositivos. O *access point* se conecta a uma rede cabeada, e fornece acesso sem fio a esta rede para dispositivos móveis no raio de alcance do sinal de rádio;
- 6.2. **AMEAÇAS DIGITAIS:**
 - 6.2.1. **CÓDIGO MALICIOSO (MALWARES):** são programas desenvolvidos para executar atividades maliciosas em um computador de forma a fazer parecer que o próprio usuário foi quem as realizou. Isso, além de comprometer os dados do próprio usuário, abre caminhos para que a máquina infectada se torne um vetor para envio de spams e para golpes virtuais efetuados por hackers;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 6.2.2. **EXPLOIT DE SOFTWARE:** Um subconjunto dos *malwares*, os *exploits* (do inglês, exploradores) são programas maliciosos desenvolvidos por hackers com códigos executáveis que vasculham vulnerabilidades de segurança dos softwares e se aproveitam delas para roubar dados e/ou criar bots para outros ataques mais complexos. Na maioria das vezes, os *exploits* são, de fato, a porta de entrada dos hackers para arquitetar e executar um ataque cibernético muito maior.
- 6.2.3. **PHISHING:** este tipo de ameaça consiste em um e-mail contendo o link de um website falso que, normalmente, é uma imitação muito realista de páginas de bancos, órgãos públicos ou sites de compras. No e-mail, o usuário é informado de que existe um problema com sua conta no website e quando acessa o link, ele é induzido a revelar dados sensíveis como CPF, números de cartão de crédito e senhas, que são coletadas pelos hackers para uso indevido, tal como o roubo de identidade.
- 6.2.4. **RANSOMWARE:** é um tipo de malware que restringe o acesso ao sistema, pastas arquivos, criptografando-os e exigindo um “resgate” em bitcoins para que a vítima recupere o acesso a seus dados;
- 6.2.5. **VIOLAÇÃO DE DADOS:** ocorre quando a empresa sofre algum incidente de segurança no qual pessoas ou entidades não autorizadas têm acesso a informações sensíveis que estejam em custódia da organização atacada. Essas informações podem ser e-mails, RG's, históricos médicos, números de telefone, informações bancárias, listas de clientes, processos internos, etc. Um caso muito famoso de violação de dados foi o da *Cambridge Analytica*, em que houve também o vazamento de dados de 87 milhões de usuários do Facebook;
- 6.2.6. **ROUBO DE CREDENCIAIS:** pode ocorrer por meio de *phishing*, engenharia social, *malwares* e brechas de segurança em sistemas. Em posse de uma credencial válida e legítima, um hacker pode ter acesso à contas e, consequentemente, dados sensíveis de pessoas e empresas, bem como serve de intermediário para que o atacante invada uma rede remotamente ou se utilize de recursos de nuvem para arquitetar ataques mais complexos e violações de dados.
- 6.3. **ANTISPAM:** Método para se prevenir o recebimento de lixo eletrônico por e-mail;
- 6.4. **CACHING:** Na área da computação, cache é um dispositivo de acesso rápido, interno a um sistema, que serve de intermediário entre um operador de um processo e o dispositivo de armazenamento ao qual esse operador acede. A vantagem principal na utilização de um cache consiste em evitar o acesso ao dispositivo de armazenamento - que pode ser demorado -, armazenando os dados em meios de acesso mais rápidos;
- 6.5. **CAPTIVE PORTAL:** é um programa de computador responsável por controlar e gerenciar o acesso à Internet em redes públicas, de forma "automatizada". Ao digitar o endereço de



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

qualquer site no navegador o usuário é interceptado pelo sistema do *captive portal* e redirecionado para uma interface que solicita a autenticação;

- 6.6. CLOUD COMPUTING:** ou computação em nuvem é a entrega da computação como um serviço ao invés de um produto, onde recursos compartilhados, software e informações são fornecidas, permitindo o acesso através de qualquer computador, tablet ou celular conectado à Internet;
- 6.7. CREDENCIAIS DE ACESSO:** A junção entre um nome de usuário e uma senha formam uma credencial que, no mundo online, é a exigência para conceder ao usuário o acesso a contas de e-mail, páginas e perfis em redes sociais, serviços de streaming, sites de compras, etc;
- 6.8. CRIPTOGRAFIA:** Criptografia é a prática de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de decriptografia específica. As técnicas de codificação constituem uma parte importante da segurança dos dados, pois protegem informações confidenciais de ameaças que incluem exploração por *malware* e acesso não autorizado por terceiros. A criptografia de dados é uma solução de segurança versátil: pode ser aplicada a um dado específico (como uma senha) ou, mais amplamente, a todos os dados de um arquivo, ou ainda a todos os dados contidos na mídia de armazenamento;
- 6.9. DATACENTER:** é um centro de processamento de dados (CPD) onde são concentrados os equipamentos de processamento e armazenamento de dados de uma empresa ou organização;
- 6.10. DENIAL OF SERVICE:** É um ataque de negação de serviço. Trata-se de uma tentativa em tornar os recursos de um sistema indisponíveis para seus utilizadores. Alvos típicos são servidores web, e o ataque tenta tornar as páginas hospedadas indisponíveis na *www*;
- 6.11. DIRECTORY HARVEST ATTACKS:** Ataque utilizado para tentar encontrar endereços de e-mails válidos para o domínio atacado e criar um banco de dados desses endereços que pode ser utilizado posteriormente ou vendido na Internet;
- 6.12. DNS (DOMAIN NAME SYSTEM - SISTEMA DE NOMES DE DOMÍNIOS):** é um sistema de gerenciamento de nomes hierárquico e distribuído operando segundo duas definições:
- 6.12.1. Examinar e atualizar seu banco de dados;
 - 6.12.2. Resolver nomes de domínios em endereços de rede.
- 6.13. FIREWALL:** É o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede. Sua função



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra;

- 6.14. GERENCIAMENTO UNIFICADO DE AMEAÇAS:** também chamada **UTM (*Unified Threat Management*)**, compreende ao termo de segurança de informações que se refere a uma única solução de segurança, e normalmente é um único dispositivo que oferece várias funções de segurança em um único ponto na rede. O dispositivo de UTM inclui funções como: antivírus, *antispyware*, firewall de rede, detecção e prevenção de intrusão, filtragem de conteúdo e prevenção de vazamento, serviços como roteamento remoto, conversão de endereço de rede (NAT) e suporte de rede privada virtual (VPN), entre outros recursos detalhados neste edital;
- 6.15. HOTSITE OU MICROSITE:** é um sítio momentâneo voltado a destacar uma ação de comunicação e marketing pontual. Usualmente, hotsites possuem tempo de vida útil predeterminado, isto é, são feitos para serem rápidos e são ligados a uma ação de marketing ou comunicação específica, com duração ligada a essa ação mercadológica, como lançamento de produtos, eventos, novas edições de produtos ou serviços, ações de CRM (*Customer Relationship Management*), entre outras;
- 6.16. IMAP (*INTERNET MESSAGE ACCESS PROTOCOL*):** é um protocolo de gerenciamento de correio eletrônico, que permite o armazenamento das mensagens no servidor, as quais o usuário pode acessá-las de qualquer computador;
- 6.17. INFRAESTRUTURA DE TI:** refere-se ao conjunto de hardwares a serem fornecidos pelo contratante para implantação da solução e dos softwares de apoio, levando-se em conta todo o ambiente de execução;
- 6.17.1. A infraestrutura de TI está especificada no **ANEXO I**
- 6.17.2. **II – AMBIENTE COMPUTACIONAL.**
- 6.18. IPS (*Intrusion Prevention System*):** Um Sistema de Prevenção de Intrusão (IPS) é uma tecnologia de segurança de rede / prevenção de ameaças que examina fluxos de tráfego de rede para detectar e prevenir vulnerabilidades;
- 6.19. LICENÇAS DE SOFTWARE:** são todos as licenças e componentes de software da solução de antivírus e do firewall UTM, os quais complementam as funcionalidades da solução ou dão suporte ao seu funcionamento, permitindo que todos os requisitos funcionais e não funcionais estabelecidos no edital sejam atendidos;
- 6.20. MÍDIA STREAMING:** é uma forma de distribuição de dados, geralmente de multimídia em uma rede através de pacotes. É frequentemente utilizada para distribuir conteúdo multimídia através da Internet. Em streaming, as informações não são armazenadas pelo usuário em seu próprio computador não ocupando espaço no Disco Rígido (HD), ele recebe o "*stream*", a transmissão dos dados (a não ser o arquivamento temporária no cache do sistema ou que o usuário ativamente faça a gravação dos dados) - a mídia é reproduzida à medida que chega ao



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

usuário, dependendo da largura de banda seja suficiente para reproduzir os conteúdos, se não for o suficiente ocorrerá interrupções na reprodução do arquivo;

- 6.21. **NEXT GERENERATION FIREWALL:** Diferentemente de um modelo tradicional de firewall que faz controle de IP de origem, IP de destino, porta de origem, porta de destino e flags somente, um *Next Generation Firewall* vai além, com análises mais profundas no pacote que é trafegado por ele;
- 6.22. **NORMA ANSI/TIA 942:** A norma TIA 942 da Associação das Indústrias de Telecomunicações (TIA) descreve os requisitos para a infraestrutura de centro de processamento de dados. O mais simples é um CPD padrão Tier 1, que é basicamente uma sala do servidor, seguindo as diretrizes básicas para a instalação de sistemas de computador. O nível mais complexo é um CPD no padrão Tier 4, que é projetado para hospedar sistemas computacionais de missão crítica, com os subsistemas totalmente redundante e zonas de segurança compartimentadas, controladas por métodos de acesso biométrico. Mais informações em: <http://www.tiaonline.org>;
- 6.23. **NORMA ISO 27000:** As normas da família ISO/IEC 27000 convergem para o Sistema de Gestão de Segurança da Informação (SGSI), tendo como as normas mais conhecidas as ISO 27001 e ISO 27002. São relacionadas à segurança de dados digitais ou sistemas de armazenamento eletrônico. O conceito de segurança da informação vai além do quesito informático e tecnológico, apesar de andarem bem próximos. O SGSI é uma forma de segurança para todos os tipos de dados e informações, e possui quatro atributos básicos: confidencialidade, integridade, disponibilidade e autenticidade. Mais informações em: <http://www.abnt.org.br>;
- 6.24. **PLUG-INS:** Na informática, um plug-in ou módulo de extensão (também conhecido por *plug-in*, *add-in*, *add-on*) é um programa de computador usado para adicionar funções a outros programas maiores, provendo alguma funcionalidade especial ou muito específica. Geralmente pequeno e leve, é usado somente sob demanda. Uma aplicação pode utilizar tal técnica por diversos motivos, como permitir que desenvolvedores de software externos estendam as funcionalidades do produto, suportem funcionalidades antes desconhecidas, reduzam o tamanho do programa ou, até mesmo, separem o código fonte de diferentes componentes devido a incompatibilidade de licenças de software;
- 6.25. **POP (Post Office Protocol):** Protocolo de entrada de e-mail que permite acesso a um webmail, transferência de mensagens para um gerenciador de e-mails e manipulação off-line;
- 6.26. **PORTAL:** Um portal é um site na internet projetado para aglomerar e distribuir conteúdo de várias fontes diferentes de maneira uniforme, sendo um ponto de acesso para uma série de outros sites ou subsites internamente ou externamente ao domínio ou subdomínio da empresa gestora do portal;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 6.27. POWER OVER ETHERNET (PoE):** é uma técnica que possibilita transmitir em um único cabo, energia e dados, eliminando a necessidade de infraestrutura elétrica para energizar dispositivos habilitados para IP;
- 6.28. SPAM:** Mensagem eletrônica não solicitada, enviada em massa;
- 6.29. SITE SURVEY:** nome comumente utilizado pelos fornecedores de soluções de redes Wi-fi, o *site survey* é a realização de uma inspeção técnica nos locais onde serão instalados os equipamentos de rádio frequência da rede sem fio. Este levantamento tem a finalidade de dimensionar a área e identificar o local mais apropriado para a instalação do(s) AP(s), a quantidade de células e de pontos de acesso necessários para que as estações clientes tenham qualidade de sinal aceitável de recepção, acesso à rede e utilizar aplicações e recursos de modo compartilhado. Estes levantamentos devem ser realizados tanto nos ambientes internos (indoor) como nos ambientes externos (outdoor).
- 6.30. SLA:** O termo proveniente do inglês *Service Level Agreement*, significa Acordo de Nível de Serviço e trata-se da parte de um contrato de serviços entre duas ou mais entidades no qual o nível da prestação de serviço é definido formalmente;
- 6.31. SMARTPHONES:** Um smartphone (palavra da língua inglesa que significa "telefone inteligente", ainda sem correspondente em português) é um tele móvel (celular, no Brasil) que combina recursos com computadores pessoais, com funcionalidades avançadas que podem ser estendidas por meio de programas executados por seu sistema operacional (OS), chamados de aplicativos ou apps (diminutivo de "*Applications*");
- 6.32. SOC - SECURITY OPERATION CENTER:** é um termo genérico que pode ser traduzido como Centro de Operação de Segurança e que descreve parte ou a totalidade de uma equipe ou plataforma, cujo objetivo é prestar serviços gestão de incidentes, monitoramento de ativos de TI, detecção e reação a incidentes de segurança. Podemos distinguir seis operações a serem executadas por um SOC:
- Identificação de eventos de segurança;
 - Coleta de dados;
 - Armazenamento;
 - Análise;
 - Reação.
 - Observação.

Assim, um SOC é composto por cinco módulos distintos:

- Geradores de alertas;
- Coletores de eventos;
- Banco de dados de mensagens;
- Mecanismos de análise;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- Software de gerenciamento de reação.
- 6.33. SOFTWARES DE APOIO:** também conhecidas como *features*, são todos os softwares e componentes que complementam as funcionalidades da solução ou dão suporte ao seu funcionamento, permitindo que todos os requisitos funcionais e não funcionais estabelecidos no edital sejam atendidos;
- 6.34. TABLETS:** é um dispositivo pessoal em formato de prancheta que pode ser usado para acesso à Internet, organização pessoal, visualização de fotos, vídeos, leitura de livros, jornais e revistas e para entretenimento com jogos. Apresenta uma tela sensível ao toque (touchscreen) que é o dispositivo de entrada principal. A ponta dos dedos ou uma caneta aciona suas funcionalidades. É um novo conceito: não deve ser igualado a um computador completo ou um smartphone, embora possua funcionalidades de ambos;
- 6.35. TEMPLATE (OU MODELO DE DOCUMENTO):** é um documento de conteúdo, com apenas a apresentação visual (apenas cabeçalhos por exemplo) e instruções sobre onde e qual tipo de conteúdo deve entrar a cada parcela da apresentação — por exemplos conteúdos que podem aparecer no início e conteúdo que só podem aparecer no final. No contexto de portais, os *templates* podem ser modelos de temas, de páginas ou de posts;
- 6.36. VPN (VIRTUAL PRIVATE NETWORK):** trata-se de uma rede privada construída sobre a infraestrutura de uma rede pública. Essa é uma forma de conectar dois computadores através de uma rede pública, como a Internet. Ao invés de realizar esse procedimento por meio de links dedicados ou redes de pacotes, como Frame Relay e X.25, utiliza-se a infraestrutura da internet para conectar redes distantes e remotas.

7. CERTIFICAÇÕES DO PRODUTO E QUALIFICAÇÃO TÉCNICA

Atestados de Capacidade Técnica da CONTRATADA (Necessário para Habilitação):

- 7.1.** Apresentar, no mínimo, **01 (um) Atestado de Capacidade Técnica**, expedido(s) por pessoa jurídica de direito público ou privado, que comprove a anterior execução/fornecimento do **serviço pertinente e compatível** em características, quantidades e prazos com o objeto deste certame, com as seguintes características:
- 7.2.** A referida prova de qualificação técnica acima deverá ser fornecida de acordo com o **ANEXO X - COMPROVANTE DE QUALIFICAÇÃO TÉCNICA**.
- 7.2.1. OBSERVAÇÃO:** este documento deverá estar impresso em papel timbrado da atestante.
- 7.3.** Entende-se por pertinentes e compatíveis os serviços objetos desta licitação realizados com forma, características e regime de execução semelhante aos constantes do objeto e condições desta licitação, que comprove:



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 7.3.1. Fornecimento e instalação e gerenciamento de solução de *appliance* no padrão *Next Generation Firewall – NGFW/UTM*, para uma rede de, no mínimo, 150 usuários;
- 7.3.2. Fornecimento e instalação e gerenciamento de solução de *Endpoint* (antivírus) para até 150 usuários;
- 7.3.3. Prestação de serviços de consultoria em segurança da informação a redes computacionais, entregando serviços de forma contínua, como: análise de vulnerabilidade e gestão de incidentes.
- 7.4. O CRA poderá ainda, para efeito da verificação acima, solicitar qualquer documento pertinente, bem como proceder a diligências, inclusive perante terceiros;
- 7.5. O(s) atestado(s) será(ão) avaliado(s) com base nas seguintes informações:
- Data de início e término dos serviços;
 - Caracterização dos serviços realizados;
 - Nome, telefone, e-mail e identificação do signatário/data de emissão.
- 7.6. Contratada deverá comprovar que possui em seu quadro de funcionários no mínimo **01 (um) profissional com certificação oficial do fabricante** dos produtos ofertados (firewall UTM e antivírus);
- 7.7. A comprovação deverá ser feita através da apresentação da certificação (cópia autenticada) e documento demonstrando o vínculo deste **PROFISSIONAL** com a **PROPONENTE**;
- 7.8. **No momento da entrega dos equipamentos a proponente vencedora deverá fornecer declaração ou documento que comprove a parceria entre o vencedora e o(s) fabricante(s), sendo apto para fornecer os produtos ofertados e declarando que a proponente possui credenciamento do mesmo para a implantação e suporte técnico de seus produtos;**
- 7.9. O Fabricante deve comprovar participação no *MAPP* da *Microsoft*;
- 7.10. A tecnologia do *appliance* deverá ser certificada ou estar em fase de certificação pela *ICSA Labs*, comprovado através do site: (<https://www.icsalabs.com/products/>);
- 7.11. O fabricante do *appliance* deverá ser avaliado pela *NSS Labs (Network Security Services)* no desempenho do *Next Generation Firewall Comparative Analysis* mais recente, estando no “*Security Value Map*” acima de 90 % (noventa por cento) da avaliação de segurança efetiva;
- 7.12. O *appliance* deve ser, impreterivelmente, homologado pela ANATEL (Agência Nacional de Telecomunicações).

8. PROPOSTA COMERCIAL

- 8.1. Todos os custos de hardware, softwares, mão de obra ou quaisquer outros itens necessários para a implantação e operação de todas as funcionalidades e serviços da solução descritos



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

neste edital, sem nenhuma exceção, serão de responsabilidade da contratada e deverão estar disponíveis durante toda a vigência contratual;

- 8.2.** A LICITANTE deverá declarar de forma clara e detalhada as especificações dos itens ofertados, inclusive no que se refere ao:
- 8.2.1. Nome do fabricante do produto;
 - 8.2.2. Softwares de apoio;
 - 8.2.3. Política de licenciamento do produto;
 - 8.2.4. Nome do Produto / Serviço;
 - 8.2.5. Quantidade, preço unitário e preço total de cada item que compõe a solução.
- 8.3.** Observar, quando da formulação da proposta, as especificações e características obrigatórias, não sendo permitida a oferta de preços alternativos ou a inclusão de condições que impeçam o julgamento objetivo;
- 8.4.** Estar de acordo, e se necessário incluir na proposta comercial todos os custos e recursos, necessários para aceite integral de todos os prazos e exigências descritas no **ANEXO VII – NÍVEIS MÍNIMOS DE SERVIÇO (SLA)**, e demais itens deste edital;
- 8.5.** Declarar que a infraestrutura fornecida pelo CONSELHO, em relação aos itens de hardware, às soluções e aos softwares de apoio fornecidos pelo CONSELHO e de uso obrigatório pela CONTRATADA permitem a execução da Solução dentro dos níveis de serviço exigidos, conforme descrito no item “**DA VISTORIA**”, deste edital;
- 8.6.** Declarar que atenderá a todos os requisitos estabelecidos no Edital, nas condições, prazos e níveis de serviço informados;
- 8.7.** A LICITANTE que apresentar declaração falsa será desclassificado e sujeitar-se-á às sanções previstas no Edital.

9. DA AVALIAÇÃO DO SISTEMA

- 9.1.** A Licitante vencedora, a qual lhe foi adjudicado o objeto, deverá providenciar, com recursos próprios e **num prazo máximo de 05 (cinco) dias úteis**, a apresentação da plataforma de sistemas descritos neste certame, para a equipe técnica do CRA-SP, a fim de que sejam analisados os requisitos e funcionalidades estabelecidos neste edital. **NO CASO DE NÃO ATENDIMENTO DAS EXIGÊNCIAS DESTE ANEXO OU DOS DEMAIS REQUISITOS OBRIGATÓRIOS EXIGIDOS NO CERTAME, A LICITANTE SERÁ DESCLASSIFICADA;**
- 9.2.** Apresentação poderá ocorrer na sede do Conselho, em um ambiente próprio da empresa LICITANTE, ou mesmo em outra empresa em que a mesma solução esteja em funcionamento. Entretanto, todos os custos e logística para o deslocamento da equipe técnica do Conselho, será responsabilidade da LICITANTE;
- 9.3.** Na apresentação serão avaliados, todos os requisitos mínimos, exigidos no presente edital;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 9.4. É obrigatório que a Solução ofertada contenha nativamente, todos os recursos descritos no termo de referência;
- 9.5. **O prazo para a emissão do relatório final da avaliação da solução**, por parte da área técnica do CRA-SP, **será até 05 (cinco) dias corridos**, após a apresentação da solução;
- 9.6. Constatado o atendimento às exigências fixadas neste Edital, a LICITANTE será declarada vencedora;
- 9.7. Os detalhamentos do processo de avaliação da amostra do sistema estão descritos no **ANEXO V – ROTEIRO DE HOMOLOGAÇÃO DOS SERVIÇOS**.

10. DAS SOLICITAÇÕES, PRAZO DE ENTREGA E VIGÊNCIA

- 10.1. A CONTRATADA deverá providenciar a instalação de toda a solução descrita no objeto deste Termo de Referência, no prazo máximo **30 (TRINTA) DIAS CORRIDOS**, contados a partir da data de assinatura do contrato;
- 10.2. Todas as atividades envolvidas serão acompanhadas e validadas por analistas técnicos do Conselho;
- 10.3. Para a implantação, a contratada deverá alocar o (s) profissional (s) com certificações oficiais nas soluções, informados nos documentos de habilitação, conforme item “**CERTIFICAÇÕES DO PRODUTO E QUALIFICAÇÃO TÉCNICA**”, deste edital.
- 10.4. Esta documentação será avaliada também antes no início dos trabalhos;
- 10.5. A contratada deverá elaborar um projeto de implantação, em conjunto com as áreas técnicas do Conselho, onde deverão constar o desenho da solução (topologia, configurações, etc.), as atividades de preparação do ambiente, customização, testes e implantação;
- 10.6. A implantação da solução será realizada no ambiente de produção, portanto, se necessário, as atividades deverão ocorrer após o expediente (horários noturnos ou em finais de semana e feriados), a critério do Conselho;
- 10.7. A Contratada é responsável por efetuar as atividades de integração da solução com os ambientes operacionais do Conselho;
- 10.8. A Contratada deverá fornecer, em até **20 (vinte) dias corridos**, após o término da implantação da solução, documentação contendo: especificação de toda solução (características e funcionalidades implantadas), desenho lógico da implantação, comentários e configurações executadas. Essa documentação deverá ser entregue em meio magnético e impressa;
- 10.9. Quaisquer alterações nas condições acima deverão ser avaliadas e aprovadas pelo Conselho;
- 10.10. Todas as condições de nível de serviço (SLA) para a garantia da qualidade de todos os serviços prestados, estão descritos neste termo de referência e seus anexos.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

11. HORÁRIOS E LOCAL DA PRESTAÇÃO DOS SERVIÇOS

- 11.1.** A entrega do produto final e a prestação dos serviços deverão ser realizadas na sede do CRA-SP, na Rua Estados Unidos, 889 – Jd. América – São Paulo – SP;
- 11.2.** Expediente do CRA-SP é de segunda a sexta-feira, das **08h00** às **19h00**. Havendo necessidade, será autorizado à CONTRATADA o acesso às áreas para execução dos serviços fora desse horário;

12. DO RECEBIMENTO

- 12.1.** No ato da entrega serão conferidos os itens apresentados, e rejeitados, no todo ou em parte, aqueles que estiverem em desacordo com as especificações e com obrigações assumidas pelo fornecedor ou previstas neste Edital e/ou neste anexo.
- 12.2.** Caso seja necessário refazer o objeto rejeitado, o novo fornecimento deverá ocorrer no prazo máximo de 72 horas (corridas), sob pena de aplicação das sanções cabíveis.
- 12.3.** O CRA-SP se reserva no direito de receber os produtos na condição de posterior conferência caso não tenha condições de fazê-lo no ato da entrega.

13. DOS PAGAMENTOS A SEREM REALIZADOS

- 13.1.** A CONTRATADA enviará os relatórios necessários juntamente com a fatura para aprovação do Conselho. O pagamento será efetuado em 11 (onze) DFS (dias fora semana), após aprovação da respectiva nota fiscal/fatura. As notas fiscais/faturas poderão ser rejeitadas por erros ou incorreções em seu preenchimento, e serão formalmente devolvidas à empresa CONTRATADA para correção;
- 13.2.** A CONTRATADA deverá providenciar a instalação de toda solução bem como prestar os serviços descritos no objeto deste Projeto Básico, conforme condições e prazos estabelecidos neste edital e descritos nos itens:
- DAS SOLICITAÇÕES, PRAZO DE ENTREGA E VIGÊNCIA;
 - HORÁRIOS E LOCAL DA PRESTAÇÃO DOS SERVIÇOS;
 - SERVIÇO DE IMPLANTAÇÃO DAS SOLUÇÕES CONTRATADAS.
- 13.3.** Todas as atividades envolvidas serão acompanhadas e validadas por analistas técnicos do Conselho.
- 13.4.** Para a implantação, a CONTRATADA deverá alocar profissionais do seu quadro de funcionários, devidamente comprovado o vínculo empregatício, conforme lei trabalhista brasileira. É vedada qualquer tipo de terceirização de mão de obra, salvo apenas em casos de



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

mão de obra específica e devidamente comprovada pela empresa. Esta documentação será avaliada pelo Conselho, antes no início dos trabalhos.

- 13.5.** A CONTRATADA deverá dimensionar em sua proposta, todos os custos relativos a viagens, Descolamento e Diárias, hospedagem e etc., dos seus funcionários.
- 13.6.** Os pagamentos serão efetuados, conforme cronograma e condições descritas nos quadros abaixo;
- 13.7.** Para os custos referente ao projeto de implantação da sua solução, a LICITANTE deverá projetar todos os seus custos com o projeto de implantação da solução, como por exemplo:
- Mão de obra;
 - Licenciamento de todos os softwares e recursos acerca das soluções;
 - Descolamento;
 - Diárias;
 - e qualquer outro custo necessário para execução na integra de todos os itens e requisitos descritos neste edital.
- 13.8.** Os pagamentos se darão sempre ao termino de cada atividade e com o devido aceite da área técnica do Conselho, que avaliará se todos os itens projetados estão entregues ou não;
- 13.9.** Abaixo apresentamos cronograma físico/financeiro com a previsão dos pagamentos a serem realizados.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

13.10. CRONOGRAMA FÍSICO-FINANCEIRO:

DISCRIMINAÇÃO DOS CUSTOS - RESUMO					
ITEM	DETALHAMENTO		DIVISÃO DO ORÇAMENTO EM PORCENTUAIS (%) LIMITES SOBRE VALOR GLOBAL	CUSTOS	OBSERVAÇÕES
PROJETO DE IMPLANTAÇÃO (A)	Serviço de implantação da solução, contemplando: - instalação e configuração de todos os equipamentos, softwares e demais recursos que compõem a solução, no ambiente de rede do CRA-SP; - Serviço de treinamento das soluções contratadas.	Implantação	5%	R\$ -	Pagamento ao termino e aceite das atividades descritas nos itens do edital: - SERVIÇO DE IMPLANTAÇÃO DAS SOLUÇÕES CONTRATADAS; - ANEXO V – ROTEIRO DE HOMOLOGAÇÃO DOS SERVIÇOS; IMPORTANTE: Neste item a licitante deverá relacionar todos os seus custos com o projeto de implantação da solução, como por exemplo: Mão de obra, Licenciamento, Descolamento e Diárias e etc.
OPERAÇÃO EM PRODUÇÃO E SUPORTE TÉCNICO CONTINUO (B)	Dispositivo (Appliance) de controle de acesso lógico no padrão UTM (Gerenciamento Unificado de Ameaças), com Licenciamento de todos os softwares e recursos acerca da solução;	Mensal	95%	R\$ -	Percentual dividido conforme número de meses do tempo de contrato, para os serviços da solução em produção descritos nos itens do edital: - Fornecimento do Dispositivo (Appliance) para controle de acesso lógico no padrão Next Gereneration Firewall – NGFW/UTM; - Fornecimento da Solução software de Endpoint (antivírus); - Serviço de monitoramento remoto, 24 horas por dia e 7 dias por semana (24x7); - Serviços de suporte técnico, manutenções e consultoria especializada.
	Solução software de Endpoint para, no mínimo, 150 usuários/computadores, contemplando: - Licenciamento de software; - Implantação; - Operação.	Mensal			
	Serviço de monitoramento remoto, 24x7: - NOC (Network Operations Center), próprio e especializado; - Plataforma/Software próprio para monitoramento dos principais hosts e serviços de rede do CRA-SP.	7x24			
	Serviço de suporte técnico especializado "on site": - Gestão de incidentes e suporte técnico especializado com SLA; - Workshop de segurança para usuário final; - Consultoria para política de segurança; - Analise de vulnerabilidade; - Visita semestral de especialista; - Consultoria para serviço de análise de vulnerabilidade e teste de penetração (pentest).	Horário Expediente CRA-SP			
VALOR GLOBAL (A + B)			100%	R\$ -	

14. GARANTIAS DOS PRODUTOS

14.1. GARANTIA DOS FABRICANTES DOS PRODUTOS: A empresa CONTRATADA deverá garantir toda a cobertura de suporte e todas as garantias de produto por parte dos FABRICANTES, por igual período ao da vigência do contrato, e suas prorrogações, se houver, sendo o referido prazo contado a partir da entrega, instalação, configuração, teste, implantação e homologação dos produtos.

14.2. Declaração da CONTRATADA, apresentada na fase de habilitação, assumindo a responsabilidade pela complementação da garantia dos equipamentos, dispositivos e produtos,



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

em caso de não atendimento do Fabricante, contados da data do recebimento definitivo da solução.

15. SERVIÇO DE IMPLANTAÇÃO DAS SOLUÇÕES CONTRATADAS

15.1. CONDIÇÕES PARA IMPLEMENTAÇÃO DAS SOLUÇÕES:

- 15.1.1. A CONTRATADA deverá providenciar a instalação de toda a solução descrita no objeto deste Termo de Referência, no prazo máximo **30 (TRINTA) DIAS CORRIDOS**, contados a partir da data de assinatura do contrato;
- 15.1.2. Todo processo de implantação das soluções terá o acompanhamento da equipe técnica do Conselho que efetuará os testes de aceitação para que possa ser lavrado o Termo de Aceite definitivo;
- 15.1.3. Todo processo de implantação das soluções deverá ser realizado sem interrupção do funcionamento do ambiente atual de operação da rede e sem impactos significativos para o ambiente de trabalho do Conselho, admitindo-se apenas paradas programadas em períodos fora do horário de expediente, desde que previamente acordadas com o Conselho, por intermédio da Coordenação Tecnologia da Informação;
- 15.1.4. Os serviços para a implementação poderão ser executados em **regime 24X7 (vinte e quatro horas por dia, sete dias por semana, incluindo sábado, domingos e feriados)**, sendo que esta condição será acertada entre as partes no planejamento da implantação e será prevista nos cronogramas do projeto básico e aceita pelo Conselho;
- 15.1.5. As atividades consideradas incômodas ou que gerem qualquer tipo de impacto, perturbação ou desconforto nas atividades normais do Órgão, as quais serão programadas para o período noturno, após as 20h, ou para finais de semana;
- 15.1.6. Todos os dados atuais sobre Infraestrutura de rede e topologia do CONSELHO, que por ventura, não estiverem declarados neste edital, deverão ser levantados pela CONTRATADA, durante as fases: “DA VISTORIA”;

15.2. INSTALAÇÃO E CONFIGURAÇÃO NO AMBIENTE DE REDE DO CRA-SP DE TODOS OS EQUIPAMENTOS, SOFTWARES E DEMAIS RECURSOS QUE COMPÕEM AS SOLUÇÕES:

- 15.2.1. O projeto de implantação, trata-se do conjunto de atividades a serem executadas e necessárias para entregar as soluções descritas neste certame, adaptadas às necessidades do Conselho e plenamente operacional, em todo o ambiente de execução;
- 15.2.2. As atividades desta etapa serão divididas em fases de execução e estão descritas abaixo:



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ITEM	ATIVIDADE
1	Levantamento de requisitos, planejamento e elaboração do projeto para implantação;
2	Desenho da solução, incluindo, no mínimo, a topologia, as configurações de rede, e os endereçamentos IP's, deverá ser elaborado pela CONTRATADA;
3	Regras e políticas de segurança atualmente em uso no Conselho: - Migração de dados do atual dispositivo em uso no CRA-SP; - Definição das novas políticas e regras a serem aplicadas no <i>Firewall</i> e <i>Endpoint</i> .
4	Simulação dos procedimentos operacionais do conselho na solução ofertada;
5	Execução da implantação;
6	Treinamento;
	Acompanhamento pós implantação (operação assistida).

15.2.3. Todo o planejamento das fases de Instalação, Homologação e Implantação em produção deverão ser realizados pela CONTRATADA, sendo necessária a aprovação do CONSELHO;

15.2.4. Todo o processo de instalação, configuração e toda e qualquer atividade necessária para a implantação das soluções de hardware e software contratadas, incluindo mão de obra, acessórios ou quaisquer outras adequações necessárias, **serão de responsabilidade da CONTRATADA**, portanto, todos os **custos relativos a este item deverão ser contemplados à proposta comercial**;

15.2.5. A entrega, a instalação e a configuração dos equipamentos e softwares serão de inteira responsabilidade da Contratada;

15.2.6. Para perfeita implantação das soluções, todos os trabalhos deverão ser feitos, obrigatoriamente, nas dependências da sede do Conselho.

15.2.7. O PROJETO DE IMPLANTAÇÃO CONTEMPLA:

- A instalação física e lógica, além da configuração de todos os equipamentos, softwares e demais recursos que compõem a solução, no ambiente de rede do CRA-SP;
- O CRA-SP indicará o ambiente onde deverá ser instalado os equipamentos, assim como o ponto de rede cabeado. Diante disto, caberá à Contratada definir o posicionamento dos pontos de acesso de forma a obter as melhores condições de funcionamento da solução (desempenho e área de cobertura) e fazer a conexão dos pontos de acesso às tomadas lógicas existentes, fornecendo os materiais e a mão de obra necessários para tanto;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- Todo tipo de montagem e conexões necessárias para instalação e o uso do equipamento *appliance* em rack de rede, localizado no CPD do Conselho;
- Configurações dos Switches atualmente instalados rede do CRA-SP, de modo, que estes funcionem com as soluções deste certame. Além de validar todas as VLAN's e demais recursos em uso atualmente;
- Migração ou configuração do zero de todas as políticas, regras, configurações e funcionalidades existentes no atual Firewall do Conselho;
- Finalmente, será responsabilidade da Contratada instalar, configurar e customizar o software de Gerência, configurar as políticas de segurança (Filtro WWW, Aplicação, Antivírus / *Anti-spyware* e outros);
- Instalação e configuração completa da solução de *Endpoint*, tanto em seu servidor como nos computadores da rede do Conselho (Desktops, notebooks e outros);
- Realizar todo processo de instalação e distribuição dos agentes do *Endpoint* à todas as máquinas da rede do Conselho.
- DMZ (*Demilitarized Zone* - Zona Desmilitarizada): criação e configuração da DMZ abrigar todas as aplicações WEB e sites do Conselho e que estão publicados na internet.

15.2.8. Caso não esteja listada acima, mas ainda for uma atividade importante para a implantação e funcionamento completo da solução deste certame, a Contratada deverá informar a equipe técnica do Conselho;

15.2.9. O profissional indicado pela licitante que for contratada para gerenciar o projeto será responsável pela elaboração e condução do cronograma dos trabalhos junto às equipes internas do CONSELHO, observada a especificação das fases de Instalação, Customização, Homologação e implantação da Solução em produção;

15.2.10. A Contratada também deverá, se necessário, configurar os equipamentos switches do parque atual do CRA-SP, para que funcionem com a sua solução;

15.2.11. A descrição dos Switches, marca e modelo, estão descritas no **ANEXO III – AMBIENTE DE INSTALAÇÃO DA SOLUÇÃO**, deste edital;

15.2.12. Durante a etapa de instalação deverão ser efetuados, em conjunto com técnicos da CONTRATANTE, testes e ajustamento da qualidade, devendo ser entregues, ao final, toda a documentação da instalação, incluindo os detalhes de configuração dos produtos;

15.2.13. Ao finalizar a instalação dos materiais a CONTRATADA deverá entregar relatório informando as atividades realizadas e observações quanto ao uso do material objeto deste Termo de Referência:

- Configurações lógicas efetuadas em cada equipamento;
- Telefones de contato e procedimento para abertura de chamados em garantia.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 15.2.14. A Contratada deverá garantir a manutenção preventiva e corretiva do hardware ofertado, pelo prazo mínimo da vigência do contrato. A contratada deverá promover a atualização dos hardwares ofertados quando for detectado problema de desempenho que interfiram nos serviços prestados, sem ônus ao CONSELHO;
- 15.2.15. As versões dos softwares ofertados devem sempre estar com a versão mais atual disponível no mercado. A versão anterior não poderá permanecer instalada mais do que 03 (três) meses, após o lançamento da última versão homologada ou poderá permanecer instalada por tempo maior, desde que acordado com a equipe técnica do CONSELHO;
- 15.2.16. As novas versões disponibilizadas deverão ser instaladas pela Contratada, sem nenhum custo para CONSELHO;
- 15.2.17. Fornecimento contínuo de updates e upgrades da base de códigos maliciosos utilizada pelo IDS vinculado aos Firewalls, contemplando novos recursos e defesas contra falhas de segurança disponibilizadas, com atualização automática pelo período de vigência do contrato;
- 15.2.18. Toda e qualquer alteração na configuração da solução (atualização de versões, aplicações de “patches”, etc.) devem ocorrer mediante autorização formal do CONSELHO;
- 15.2.19. Durante o período de instalação da solução, os técnicos da CONTRATADA deverão ser mantidos à disposição do CONSELHO para o atendimento de dúvidas e correções.
- 15.2.20. As alterações das configurações deverão ocorrer em horários determinados pelo CONSELHO.

15.3. DOCUMENTAÇÃO PÓS IMPLANTAÇÃO:

- 15.3.1. A documentação a ser fornecida pela contratada deverá ser composta de projetos conceituais, documentação *AS BUILT* (conforme implementado) e documentos técnicos, tais como os relacionados abaixo, em meio digital, como condição necessária para o recebimento definitivo da solução:
- Cronogramas de planejamento e de execução;
 - Métodos de execução ou de implementação.
- 15.3.2. Juntamente com a documentação *AS BUILT*, a contratada deverá entregar os seguintes documentos:
- Documentação do sistema com descrição geral do sistema e funcional dos blocos componentes, tanto do *Firewall* quanto no *Endpoint*;
 - Deverão ser apresentados todos os catálogos, folders ou *datasheets* das soluções, originais dos fabricantes;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- Documentação de operação e manutenção, que contenha as especificações físicas, operacionais e de manutenção; descrição funcional de comandos e alarmes; procedimentos de carga, inicialização e localização de defeitos; manual de diagnósticos para interpretação de falhas, manual de operação dos sistemas de gerenciamento e etc.;

15.4. SERVIÇO DE TREINAMENTO DAS SOLUÇÕES CONTRATADAS:

15.4.1. Os treinamentos aplicam-se as soluções descritas neste certame e os seus principais recursos, como:

- Dispositivo (*Appliance*) para controle de acesso lógico no padrão *Next Generation Firewall* – NGFW/UTM;
- Solução software de *Endpoint* (antivírus);
- Plataforma/Software próprio para monitoramento dos principais hosts e serviços de rede do CRA-SP.

15.4.2. Os treinamentos serão aplicados aos membros da equipe técnica do Conselho e tem como objetivo garantir a transferência de conhecimento para as pessoas indicadas pelo Contratante;

15.4.3. A contratada será responsável por ministrar os treinamentos relativos à toda a solução, sendo que o conteúdo programático a ser aplicado será definido, detalhadamente, na fase de Planejamento do Projeto de Implantação, entre o Gestor de TI do Conselho e Gerente do Projeto por parte da contratada;

15.4.4. O conteúdo programático, dentre outras coisas, deve cobrir itens como: instalação, administração, operacionalização, manuseio, configuração e utilização da solução e seus componentes;

15.4.5. A carga horária, mínima, deverá ser de **16 (dezesseis) horas**;

15.4.6. O treinamento ocorrerá nas dependências do CRA-SP e a Contratada deverá seja responsável por todo e qualquer material, equipamento ou ferramenta de apoio para o treinamento.

- Poderão ser utilizados os equipamentos a serem fornecidos;

15.4.7. O treinamento deverá ocorrer ao termino da implantação (instalação e configuração) da solução;

15.4.8. Contratada deverá arcar com despesas de transporte, hospedagem, alimentação e qualquer outro custo associado aos seus colaboradores.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

15.5. ACOMPANHAMENTO PÓS IMPLANTAÇÃO (OPERAÇÃO ASSISTIDA):

- 15.5.1. Após a entrada em operação das soluções, iniciará o acompanhamento do uso, de forma presencial na sede do Conselho;
- 15.5.2. O período de operação assistida, terá duração mínima de **01 (uma) semana**, podendo ser estendida conforme forem apresentados os resultados positivos da implantação, ou seja, performance das soluções conforme esperado e ambiente estabilizado sem problemas e impactos aos usuários e serviços do Conselho;
- 15.5.3. O período de operação assistida, tem como objetivo minimizar todo e qualquer impacto que possa ocorrer no uso das novas aplicações, através do acompanhamento dos técnicos da CONTRATADA, de modo a responder de forma rápida e assertiva, questões como:
 - Correção de erros;
 - Solução de dúvidas dos usuários gestores e de TI;
 - Verificação do desempenho, Otimização e disponibilidade da Solução;
 - Atualização da documentação e scripts de atendimento de *help desk*;
 - Auxílio a equipe da CONTRATADA no atendimento de segundo e terceiro nível;
 - Entre outras atividades necessárias para estabilização do software.
- 15.5.4. A operação assistida abrange todo o ambiente de execução das soluções, tanto de Firewall quanto *Endpoint*;
- 15.5.5. Objetivando o menor impacto para as operações do órgão, inicialmente, a equipe técnica do Conselho, **estima** que será necessário, **pelo menos, 01 (um) profissional alocado na sede do Conselho** durante esta etapa;
- 15.5.6. O conjunto de atividades que envolvem esta etapa serão executados, **obrigatoriamente, in loco**, ou seja, na sede do Conselho, durante todo o período estipulado para esta fase. Entretanto, o período e a quantidade de profissionais da CONTRATADA alocados na sede do Conselho para esta atividade, poderá sofrer alterações conforme o andamento do projeto e anuência da equipe técnica do Conselho;
- 15.5.7. **O FORMATO DE EXECUÇÃO DESTA ATIVIDADE, SÓ PODERÁ SER ALTERADO DE PRESENCIAL PARA QUALQUER OUTRO FORMATO, COM A AUTORIZAÇÃO DO CONSELHO, POR INTERMÉDIO DE SEUS AGENTES RESPONSÁVEIS PELO PROJETO;**
- 15.5.8. **A RESPONSABILIDADE PELA GESTÃO DE SEUS FUNCIONÁRIOS, COMO TAMBÉM TODOS OS CUSTOS ENVOLVIDOS NESTE PROCESSO (EXEMPLO: DIÁRIAS, DESLOCAMENTOS, HOSPEDAGENS, ALIMENTAÇÃO E ETC.) E DEMAIS REQUISITOS NECESSÁRIOS PARA ESTA ATIVIDADE, SERÃO DE RESPONSABILIDADE DA CONTRATADA;**



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

15.5.9. Intervenções programadas que necessitem de paralisações da Solução deverão ser realizadas fora do horário de expediente, devendo ser agendadas pela CONTRATADA com o Conselho.

16. DISPOSITIVO (*APPLIANCE*) DE CONTROLE DE ACESSO LÓGICO NO PADRÃO NEXT GENERATION FIREWALL – NGFW/UTM, COM LICENCIAMENTO DE TODOS OS SOFTWARES E RECURSOS ACERCA DA SOLUÇÃO:

- 16.1. A CONTRATADA deverá fornecer, no período de vigência contratual, **01 (um) equipamento**, também denominado de *appliance*, dedicado e do padrão *Next Generation Firewall* – NGFW/UTM, configurado, em regime de comodato;
- 16.2. O equipamento deve ser novo, sem uso, de última geração e em linha atual de produção do seu fabricante, com todos os cabos, conectores e demais peças necessárias para seu perfeito funcionamento;
- 16.3. O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovada através de declaração ou documentos do fabricante do produto;
- 16.4. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em **listas que indicam a descontinuidade do produto**, como por exemplo: *end-of-life* e/ou *end-of-sale* ou situação semelhante;
- 16.5. Fornecer os manuais (impresso ou mídia eletrônica) originais do produto, constando todas as informações necessárias para a instalação, configuração e utilização;
- 16.6. **A solução deverá ser capaz de gerenciar todos os atuais links de internet em uso no CRA-SP, além de permitir o crescimento até pelo menos, 700 MB, considerando o tráfego full duplex;**
- 16.7. Demais detalhamentos sobre os links de internet atualmente em uso na rede do Conselho, poderão ser obtidos no **ANEXO III - AMBIENTE COMPUTACIONAL DO CONSELHO** ou no processo de vistoria, descrito no item **“DA VISTORIA”**;
- 16.8. Este equipamento será responsável por gerenciar todo o tráfego de dados, interno e externo, no ambiente do Conselho. Todas as suas especificações técnicas estão descritas no **ANEXO II - REQUISITOS TÉCNICOS DAS SOLUÇÕES CONTRATADAS**, deste edital.

17. SOLUÇÃO SOFTWARE DE *ENDPOINT* (ANTIVÍRUS) PARA, NO MÍNIMO, 150 USUÁRIOS/COMPUTADORES:

- 17.1. Será fornecida e instalada a solução software de *Endpoint* (antivírus) para, **até 150 usuários / computadores** da rede de dados do CRA-SP, sendo até 30% deles servidores, com console fornecida em uma das seguintes opções:



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- *Appliance* virtual (Microsoft Hyper-V), instalado no ambiente já existente disponibilizado pelo Conselho
- Ou ambiente em *Cloud Computing* do próprio fabricante da solução.

17.2. Todas as suas especificações técnicas deste item estão descritas no **ANEXO II - REQUISITOS TÉCNICOS DAS SOLUÇÕES CONTRATADAS**, deste edital.

18. SERVIÇO DE MONITORAMENTO REMOTO, 24X7:

18.1. CENTRO DE OPERAÇÃO DE SEGURANÇA (SOC - SECURITY OPERATION CENTER), PRÓPRIO E ESPECIALIZADO:

18.1.1. Para a realização dos serviços de Monitoramento Remoto da Solução, a contratada deverá possuir pessoal qualificado e ser especialista na solução ofertada, além de possuir infraestrutura de atendimento operacional baseada em Centro de Operação de Segurança (SOC - *Security Operation Center*), disponível em horário integral, ou seja, 24x7 (vinte e quatro horas por dia, sete dias por semana), com todos os custos operacionais já inclusos nos encargos de manutenção da solução;

18.1.2. Este serviço contempla, monitorar em tempo real:

- O status de funcionamento de todos os equipamentos da solução;
- Monitoramento de tráfego e utilização das redes do Conselho;
- Quantidade de usuários conectados.
- Registros de quedas e reestabelecimento.

18.1.3. Em casos de eventos registrados nesta atividade, a Contratada será responsável por comunicar a equipe técnica do Conselho e conduzir todas as atitudes necessárias para reestabelecimento do serviço;

18.1.4. Suporte técnico remoto com atendimento **24x7x365**, para avaliar constantemente a disponibilidade da monitoração e a aplicação remota de correções/atualizações necessárias para o perfeito funcionamento da solução.

18.1.5. A CONTRATADA terá responsabilidade por todos os equipamentos e softwares fornecidos por ela, não lhe caberá interagir com fornecedores terceiros, como por exemplo, a operadora do link de internet ou mesmo por alguma falha na infraestrutura do Conselho, como equipamento e conexões físicas de rede, ou mesmo alimentação elétrica. Para estes casos, a contratada terá como responsabilidade realizar o diagnóstico e orientar a equipe técnica do Conselho para a solução.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

18.2. PLATAFORMA/SOFTWARE PRÓPRIO PARA MONITORAMENTO DOS PRINCIPAIS HOSTS E SERVIÇOS DE REDE DO CRA-SP:

- 18.2.1. Com o objetivo de manter a operação com um nível satisfatório de disponibilidade e desempenho, a plataforma aqui descrita, consiste em aplicação Web, com acesso exclusivo através de login e senha, para obtenção de informações dos serviços e dispositivos de rede do CRA-SP monitorados;
- 18.2.2. O sistema deverá monitorar o ambiente relacionado ao edital, porém sua utilização poderá se estender para outros dispositivos da rede;
- 18.2.3. O sistema de monitoramento deverá ser capaz de monitorar os dispositivos através dos seguintes métodos:
- Agentes de monitoramento;
 - SNMP;
 - IPMI;
 - Dispositivos sem agente.
- 18.2.4. O sistema deverá ser capaz de apresentar os dados através dos seguintes mecanismos:
- Gráficos padrão;
 - Gráficos customizados;
 - Mapas customizáveis;
 - Dashboard geral.
- 18.2.5. O sistema deverá ser capaz de enviar notificações em casos de problemas para os seguintes tipos de mídia:
- E-mail;
 - SMS;
 - Script de comando;
 - O envio de mensagens deverá seguir o regime de escala;
- 18.2.6. A contratada deverá fornecer **01 (uma) tela com um tamanho mínimo de 32 (trinta e duas) polegadas**, nos qual será utilizado para a apresentação dos dashboards da gerados pela PLATAFORMA/SOFTWARE de monitoramento. Este equipamento será instalado nas dependências do CRA-SP e em local indicado pela equipe técnica;
- 18.2.7. A ferramenta atualmente utilizada no serviço contrato pelo CRA-SP, é a denominada “Zabbix” e nela estão configurados os seguintes hosts:

SERVIÇO	DESCRIÇÃO
---------	-----------



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

LINK DE INTERNET DEDICADO: - Principal; - Operadora: WCS.	LINK DE INTERNET DEDICADO – FIBRA ÓPTICA: - IP fixo (04 disponíveis): 187.62.218.234 - Velocidade mínima garantida: 100 Mbps; - Conexão dedicada à Internet full-duplex; - Meio físico: Fibra óptica - Dupla Abordagem em Anel. - 24x7 (horas/dias) ininterruptamente; - Porta do Firewall: X4.
LINK DE INTERNET DEDICADO: - Secundário; - Operadora: Valesat.	LINK DE INTERNET DEDICADO - SECUNDÁRIO: - IP fixo (04 disponíveis): 177.73.182.202; - Velocidade mínima garantida: 50 Mbps; - Conexão dedicada à Internet full-duplex; - Meio físico: Rádio Digital; - Utilizado para: Link Backup e Balanceamento de tráfego com outros links. - 24x7 (horas/dias) ininterruptamente; - Porta do Firewall: X2.
SITE CRA-SP	www.crasp.gov.br
Falha no monitoramento SNMP	
Problema no site cra-sp.implanta.net.br/ServicosOnline/	
Problema no site cra-sp.implanta.net.br/siscaf/	
Problema no site www.crasp.gov.br	
Sem resposta de ICMP	
Utilização de CPU acima de 80%	
Utilização de Memória RAM acima de 95%	

19. SERVIÇOS DE SUPORTE TÉCNICO, MANUTENÇÕES E CONSULTORIA ESPECIALIZADA:

19.1. SUPORTE TÉCNICO ESPECIALIZADO, COM SLA, SENDO: REMOTO E "ON SITE":

19.2. O serviço de suporte técnico e todas as condições descritas neste tópico, serão aplicadas a todos produtos e soluções contidos neste certame, são eles:

- Dispositivo (*appliance*) para controle de acesso lógico no padrão Next Generation Firewall – NGFW/UTM;
- Solução software de *Endpoint* (antivírus).

19.3. O serviço de suporte técnico terá vigência durante todo o período contratual;

19.4. O serviço de suporte técnico terá início ao termino da operação assistida em produção no projeto de implantação. Neste momento, iniciará a fase de operação, propriamente dita, ou seja, uso do sistema em produção por parte dos usuários de forma independente;

19.5. Todos detalhamentos destes serviços estão descritos nos seguintes anexos deste termo de referência:

19.5.1. **ANEXO VI - SERVIÇO DE SUPORTE TÉCNICO E ATUALIZAÇÃO DE VERSÕES;**

19.5.2. **ANEXO VII – NÍVEIS MÍNIMOS DE SERVIÇOS (SLA).**



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

19.6. GESTÃO DE INCIDENTES:

- 19.6.1. Após as avaliações de todo ambiente do Conselho, a contratada será responsável por identificar o nível de maturidade atual em segurança da informação e realizar todo apoio consultivo para melhoria desses processos com o objetivo de evolução contínua da proteção do ambiente;
- 19.6.2. Esse serviço é realizado de forma contínua através de contrato formal de serviço, onde também será realizada toda gestão de incidentes correlacionados a segurança da informação, através de equipe de atendimento técnico especializada.
- 19.6.3. Atendimento poderá ser acionado diretamente pelo Conselho ao identificar algum incidente de segurança, mas também será realizado o monitoramento constante das soluções de segurança fornecidas neste termo.

19.7. VISITA PERIÓDICA DE ESPECIALISTA E CONSULTORIA CONTÍNUA

- 19.7.1. Realização de Visita técnica programada com intervalos de **06 (seis) meses** no CONSELHO, realizada diretamente pela equipe da CONTRATADA, para a realização de manutenções e correções do ambiente CONSELHO.
- 19.7.2. Para estas visitas, a contratada deverá alocar profissionais especialistas nas soluções, onde, presencialmente analisará todo o ambiente tecnológico e se necessário, apresentará sugestões de melhorias;
- 19.7.3. Além das visitas programadas, sempre que necessário, a empresa CONTRATADA deverá apoiar o CRA-SP e a sua equipe técnica em atividades pontuais como:
 - a indicação de boas práticas para viabilidade de novos projetos;
 - consolidação dos processos de segurança;
 - parecer especializado para incidentes de segurança, como por exemplo um ataque virtual;
 - Especificações técnicas;
 - Criação de acessos via VPN para parceiros e filiais;
 - entre outros.

19.8. CONSULTORIA PARA OS SERVIÇOS DE ANÁLISE DE VULNERABILIDADE E / OU TESTE DE PENETRAÇÃO (PENTEST)

- 19.8.1. Contratação de serviço de consultoria para avaliação do nível de segurança do Conselho através de análise de vulnerabilidade e teste de penetração realizada anualmente durante o período contratado, nos seguintes ativos do Conselho:



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- Serão analisadas as vulnerabilidades dos servidores da rede interna;
- Serão analisadas as vulnerabilidades dos servidores web;
- Serão analisadas as vulnerabilidades dos IPs externos, oriundos dos links de internet em uso na rede do Conselho;
- Serão realizados testes de penetração do serviço de ERP, incluindo ambiente físico/virtual instalado, banco de dados e aplicação.

19.8.2. REQUISITOS GERAIS:

- O serviço de análise de vulnerabilidade consiste em buscar, no ambiente externo da empresa, sistemas que estejam vulneráveis e que possam comprometer a disponibilidade, integridade e segurança das informações;
- Através de ferramentas já conceituadas e homologadas nesse ramo de atuação será relacionado todas as vulnerabilidades desses sistemas, identificando suas falhas que são classificadas conforme sua criticidade;
- O serviço de teste de penetração tem o objetivo de verificar os controles e riscos existentes em suas nos serviços disponibilizados pela área de tecnologia, através da tentativa de ataque real ao ambiente de forma controlada, considerando os servidores, sistemas e aplicações alvo deste termo de referência.

19.8.3. ANÁLISE DE VULNERABILIDADE

- Serão avaliados os hosts e aplicações de mercado mais críticas do ambiente através de ferramentas especializadas, gerando um relatório com as vulnerabilidades encontradas, algumas formas de exploração e sugestões para a solução;
- O relatório de análise irá fornecer as seguintes informações:
 - ✓ Relação dos hosts analisados;
 - ✓ Vulnerabilidades agrupadas por host;
 - ✓ Identificação do sistema operacional vinculado a cada host;
 - ✓ Data e hora da análise;
 - ✓ Sumário quantificando as vulnerabilidades classificadas por níveis de severidade;
 - ✓ Lista de serviços (porta/protocolo) contendo as informações coletadas e vulnerabilidades encontradas;
- Para cada vulnerabilidade encontrada, é informado:
 - ✓ Sumário;
 - ✓ Descrição;
 - ✓ Solução;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- ✓ Fator de risco;
 - ✓ Base de consulta;
 - ✓ Evidência da análise.
- Relatório Conclusivo:
 - ✓ A fase final do teste de invasão é o relatório. Onde será informado todos falhas e vulnerabilidades encontradas e como foram exploradas. Será entregue uma matriz de risco e conforme o diagrama abaixo, a partir daí definimos as recomendações para que a probabilidade seja reduzida ao máximo.

19.8.4. TESTE DE PENETRAÇÃO (PENTEST):

- Reunião de *Kick Off*:
 - ✓ Nessa fase é será realizado uma reunião na sede da CONTRATANTE tirando todas dúvidas sobre a execução dos serviços, definindo quais tipos de ações o cliente permitirá que sejam realizados durante o teste, permissões para desativar potencialmente determinado serviço ou limitar a avaliação;
 - ✓ A equipe técnica da CONTRATANTE poderá solicitar que os testes sejam realizados somente em determinados dias e durante horários específicos.
- Coleta de Informações;
 - ✓ Nesta fase será analisada livremente as fontes de informações disponíveis, um processo conhecido como coleta de OSINT (*Open Source Intelligence*, ou dados de fontes abertas);
 - ✓ Essa pesquisa é realizada através de motores de busca, como o Google, Bing e Yahoo, redes sociais e demais fontes de informações públicas como registro de domínio.
- Mapeamento de Rede;
 - ✓ O DNS (*Domain Name System*, ou sistema de nomes de domínio) é um sistema de gerenciamento de nomes hierárquico e distribuído para computadores, serviços ou qualquer recurso conectado à Internet ou em uma rede privada. Através do DNS é possível descobrir a topologia da rede, endereços de IP e a quantidade de computadores na rede interna.
- Enumeração de Serviços e Varredura:
 - ✓ Utilizando ferramentas específicas, uma varredura de portas abertas é realizada nas máquinas descobertas e nos IPs informados com o fim de



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

descobrir quais sistemas estão presentes na Internet ou na rede interna, bem como quais softwares estão sendo executados.

- Identificação de Vulnerabilidades:
 - ✓ Tendo conhecimento das portas, softwares instalados e sistemas ativos, é iniciado o processo de análise de vulnerabilidades utilizando scanners e banco de vulnerabilidades conhecidas, com o objetivo de detectar falhas nos ativos do cliente que possam, através da execução de *exploits* (códigos específicos para exploração de falhas), permitir o acesso à rede e computadores.
- Exploração de Falhas:
 - ✓ Esta é a fase onde será executado os *exploits* nas vulnerabilidades detectadas nas fases anteriores, como por exemplo: acessar remotamente uma máquina sem a necessidade de autenticação através de login e senha, por meio de tentativas de autenticação com senhas padrão em determinados sistemas ou através da utilização das informações de acesso recolhidas na fase de engenharia social.
- Pós-Exploração de Falhas:
 - ✓ Nesta fase são reunidas informações sobre o sistema invadido, busca por arquivos relevantes ao teste de invasão, a criação de *backdoors* para posteriores acessos ao sistema, ampliar a exploração da rede ganhando assim acesso à demais máquinas / sistemas que não estavam visíveis na tentativa inicial de escaneamento da rede.
- Relatório Conclusivo
 - ✓ Serão fornecidos relatórios gerenciais e técnicos apontando as falhas de segurança encontradas e como foram exploradas, subsidiando por meio de um documento (laudo), para aferição do atual estado de segurança existente no ambiente. Também será entregue uma matriz de risco e será definida as recomendações de melhoria para que a probabilidade de incidentes seja reduzida ao máximo.

20. OBRIGAÇÕES DO CONTRATANTE

20.1. Caberá ao Conselho Regional de Administração de São Paulo (CRA-SP), como contratante:

20.1.1. Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos empregados da contratada ou por seu preposto;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 20.1.2. Efetuar o pagamento conforme entrega dos produtos, desde que cumpridas todas as formalidades e exigências do contrato;
- 20.1.3. Exercer a fiscalização dos fornecimentos prestados;
- 20.1.4. Comunicar oficialmente a contratada de quaisquer falhas verificadas no cumprimento do contrato;
- 20.1.5. Ficar a critério do órgão fiscalizador do CRA-SP impugnar qualquer fornecimento executado que não satisfaça as condições aqui prescritas.

21. OBRIGAÇÕES DA CONTRATADA

- 21.1. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade especificadas neste Termo de Referência e em sua proposta;
- 21.2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;
- 21.3. Responder por quaisquer danos causados diretamente a bens de propriedade do CRA-SP ou de terceiros, quando tenham sido causados por seus empregados durante a execução dos serviços;
- 21.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;
- 21.5. Administrar todo e qualquer assunto relativo aos seus empregados;
- 21.6. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;
- 21.7. Apresentar os empregados devidamente trajados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso;
- 21.8. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados durante a execução deste contrato, ainda que acontecido em dependência do CRA-SP;
- 21.9. Apresentar à Contratante, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 21.10.** Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Contratante;
- 21.11.** Recrutar e selecionar os empregados necessários à realização do objeto, de acordo com as especificações técnicas;
- 21.12.** Atender as solicitações da Contratante quanto à substituição dos empregados alocados, no prazo fixado pelo fiscal do contrato, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço, conforme descrito neste Termo de Referência;
- 21.13.** Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração;
- 21.14.** Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a Contratada relatar à Contratante toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;
- 21.15.** Relatar à Contratante toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;
- 21.16.** Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;
- 21.17.** Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
- 21.18.** Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;
- 21.19.** Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

22. DA SUBCONTRATAÇÃO

- 22.1.** Não será admitida a subcontratação do objeto licitatório.

23. DA CONFIDENCIALIDADE

- 23.1.** A Contratada não poderá, sob pena de aplicação das penalidades legais cabíveis, utilizar informações fornecidas pelo Conselho para qualquer outro tipo de uso que não os específicos para a execução do objeto deste certame;
- 23.2.** Demais detalhamentos e informações sobre confidencialidade, estão descritos no **ANEXO VII – REQUISITOS DE SEGURANÇA DA INFORMAÇÃO**;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

23.3. Demais detalhamentos sobre as pessoas e as obrigações da contratada e de seus funcionários, estão descritos nos:

- **ANEXO VI - SERVIÇO DE SUPORTE TÉCNICO E ATUALIZAÇÃO DE VERSÕES;**
- **ANEXO VII – NÍVEIS MÍNIMOS DE SERVIÇO (SLA).**

24. DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

24.1. A execução do objeto deste Contrato será acompanhada e fiscalizada pela **Coordenação do Departamento de TI**, em conformidade com o artigo 67 da Lei n.º 8.666, de 21 de junho de 1993 e com o artigo 6º do Decreto n.º 2.271, de 07 de julho de 1997;

24.2. O representante da referida Coordenação anotarà em registro próprio todas as ocorrências relacionadas com o fornecimento do objeto, determinando o que for necessário à regularização das faltas ou defeitos observados, quando aplicável;

24.3. A fiscalização de que trata esta Cláusula não exclui nem reduz a responsabilidade da CONTRATADA, até mesmo perante terceiro, por qualquer irregularidade, inclusive resultante de imperfeições técnicas, emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade do CONTRATANTE ou de seus agentes e prepostos (artigo 70 da Lei n.º 8.666, de 21 de junho de 1993);

24.4. Responsáveis pelo Termo de Referência:

WELTON MARQUES – COORDENADOR DEPTO. TECNOLOGIA DA INFORMAÇÃO.

25. DAS SANÇÕES ADMINISTRATIVAS

25.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:

25.1.1. Inexecução total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

- Ensejar o retardamento da execução do objeto;
- Fraudar na execução do contrato;
- Comportar-se de modo inidôneo;
- Cometer fraude fiscal;
- Não manter a proposta.

25.2. A Contratada que cometer qualquer das infrações discriminadas nos subitens acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

25.2.1. Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 25.2.2. Multa moratória de 0,1% (um décimo por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 20 (vinte) dias;
- 25.2.3. Multa compensatória de até 50% (cinquenta por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;
- Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;
- 25.2.4. Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;
- 25.2.5. Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;
- 25.2.6. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados.
- 25.3.** Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, a Contratada que:
- Tenha sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;
 - Tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;
 - Demonstre não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.
- 25.4.** A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 25.5.** A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Contratante, observado o princípio da proporcionalidade.
- 25.6.** As penalidades serão obrigatoriamente registradas no SICAF.

São Paulo, SP, de 16 de março de 2020.

WELTON MARQUES
Coordenador do Setor de Tecnologia da Informação

Pregão a ser operado por:

MARCOS BRANDÃO
Pregoeiro do CRA-SP

Conferido por:

Aprovo:

ANDREA MACEDO
Coordenadora de Compras, Contratos e
Licitações

ROBERTO CARVALHO CARDOSO
Presidente



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ANEXO II - REQUISITOS TÉCNICOS DAS SOLUÇÕES CONTRATADAS

1. DISPOSITIVO (*APPLIANCE*) DE CONTROLE DE ACESSO LÓGICO NO PADRÃO *NEXT GENERATION FIREWALL* – NGFW/UTM, COM LICENCIAMENTO DE TODOS OS SOFTWARES E RECURSOS ACERCA DA SOLUÇÃO

1.1. REQUISITOS GERAIS

- 1.1.1. A CONTRATADA deverá fornecer, no período de vigência contratual, **01 (um) equipamento**, também denominado de *appliance*, dedicado e do padrão *Next Generation Firewall* – NGFW/UTM, configurado, em regime de comodato;
- 1.1.2. O equipamento em questão, será responsável por gerenciar todo o tráfego de dados, interno e externo, do ambiente tecnológico do Conselho, conforme descrito neste termo de referência;
- 1.1.3. A solução deverá ser composta de Hardware e Software, que tenham o único objetivo de executar funções de transporte de dados e segurança da rede, com a característica de *appliance*;
- 1.1.4. Tanto o Hardware quanto o Software devem ser desenvolvidos pelo mesmo fabricante;
- 1.1.5. Todas as licenças devem ter validade igual ao período de vigência contratual.
- 1.1.6. Dispositivo de sistema de segurança de informação perimetral que inclui Firewall Corporativo de Alto Desempenho (Roteamento e Firewall de borda), administração de largura de banda de serviço de internet (QoS), suporte para conexões VPN IPSec e SSL, proteção contra ameaças de vírus e malware, bem como controle de transmissão de dados e acesso à internet;
- 1.1.7. Todas as funcionalidades descritas devem funcionar no mesmo *appliance* sem a necessidade de composição de um ou mais produtos;
- 1.1.8. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 (Camada de Aplicação);
- 1.1.9. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- 1.1.10. O equipamento deverá ser baseado em hardware desenvolvido com esta finalidade, ou seja, não sendo aceita soluções baseadas em plataforma PC (X86) ou equivalente;
- 1.1.11. Não serão permitidas soluções baseadas em sistemas operacionais abertos (*OpenSource*) como *Free BSD*, *Debian* ou mesmo *Linux*.
- 1.1.12. Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.1.13. Deve oferecer as funcionalidades de *backup* / *restore* tanto da configuração quanto do *firmware* / sistema operacional através da interface gráfica, assim como permitir ao administrador agendar procedimentos de backups da configuração em determinado dia e hora.
- 1.1.14. O *appliance* deve armazenar no mínimo 02 (duas) versões distintas do sistema operacional, sendo possível escolher qual versão será inicializada, de backups da configuração em determinado dia e hora;
- 1.1.15. A solução deve suportar configuração de *link-aggregation* de interfaces suportando o protocolo 802.3ad para aumento de *throughput*.
- 1.1.16. A solução deve suportar configuração de *port-redundancy* de interfaces para a alta disponibilidade de interfaces;
- 1.1.17. Deverá incluir um módulo de proteção contra ameaças avançadas, bloqueio de vírus, *spyware*, controle de transferência de arquivos, controle da navegação de internet e bloqueio de arquivos por tipo;
- 1.1.18. Os contextos virtuais devem suportar todas as funcionalidades base desde edital, como por exemplo, Firewall, VPN, Controle de Aplicações, IPS, Antivírus, Anti-Spyware, Sandbox, NAT, Filtro de URL, de-criptografia de SSL/SSH e Identificação de usuários.
- 1.1.19. Análise de tráfego criptografado TLS, SSL e SSH com inspeção total de camadas incluindo protocolos de criptografia, como HTTPS, SMTPS, NNTPS, LDAPS, FTPS, Telnets, IMAPS, IRCS e POPS;
- 1.1.20. A Solução deve utilizar sistema operacional próprio “hardened”, não sendo aceitos sistemas operacionais Linux ou baseados em distribuições abertas;
- 1.1.21. A plataforma deve realizar análise de conteúdo de aplicações em camada 7;
- 1.1.22. **IMPORTANTE:**
- Todos os valores para *throughputs* descritos neste documento devem ser comprovados por documento de domínio público do fabricante;
 - A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital;
 - Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitado. Todos os custos oriundos do teste de bancada serão por conta do fornecedor.

1.2. REQUISITOS DE CAPACIDADE

- 1.2.1. Capacidade para gerenciar links de internet, nos quais somando as suas velocidades atinjam, no mínimo, **700 MB, considerando o tráfego full duplex**, com todos os recursos descritos neste certame habilitados. Atualmente, o CRA-SP possui 02 (dois) links de internet e as suas



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

características estão descritas no **ANEXO III - AMBIENTE COMPUTACIONAL DO CONSELHO**;

- 1.2.2. Capacidade mínima de conexões suportadas em modo DPI (análise profunda de pacotes com os serviços IPS, *Anti-Malware* (Antivírus e *Anti-Spyware*) deverá ser de **750.000**;
- 1.2.3. Capacidade para, no mínimo, **500 (quinhentos) usuários conectados** simultaneamente, autenticados por LDAP ou Active Directory, com todos os serviços ativos e identificados passando por este dispositivo de segurança;
- 1.2.4. A solução deverá utilizar a tecnologia de firewall SPI (*Stateful Packet Inspection*) com *Deep Packet Inspection*, ou seja, suportar a inspeção da área de dados do pacote para filtragem de tráfego IP;
- 1.2.5. Possuir mecanismo de SPI (*Stateful Packet Inspection*), onde o firewall reconhece o estado da conexão com desempenho igual ou superior a **3.7 Gbps**;
- 1.2.6. Performance de **IPS de 1.8 Gbps ou superior**;
- 1.2.7. Desempenho de inspeção de aplicativos de **2 Gbps**;
- 1.2.8. Suporte a no mínimo **2.000.000 de conexões do tipo SPI simultâneas**;
- 1.2.9. Capacidade para, no mínimo, suportar **14.000 (quatorze mil) novas conexões por segundo**;
- 1.2.10. Inspeção de Anti-Malware integrado ao mesmo *appliance*: **800 Mbps ou superior**;
- 1.2.11. Suportar no mínimo **250 interfaces de VLAN** (802.1q) suportando a definição de seus endereços IP através da interface gráfica;
- 1.2.12. Suportar, no mínimo, **500 conexões** clientes do tipo *IPSec VPN clients* sem custo e 3.000 licenças/conexões futuras baseadas em licenciamento adicional;
- 1.2.13. Suportar no mínimo 2 conexões clientes do tipo SSL sem custo e **500 licenças/conexões futuras baseadas em licenciamento adicional**;
- 1.2.14. Todos os itens habilitados (IPS, Antivírus, *Antispyware* e Controle de Aplicações), com uma performance, no mínimo, de 700 Mb de UTM *Throughput* DPI SSL considerando tráfego HTTPS.
- 1.2.15. **Performance de Inspeção de tráfego criptografado (SSL)** de, no mínimo, **300 Mbps**.

1.3. REQUISITOS DE HARDWARE E PERFORMANCE

- 1.3.1. Mínimo de **2GB de memória RAM** para maior confiabilidade do sistema;
- 1.3.2. No máximo **2U de altura**, com kit de montagem em **rack de 19"**;
- 1.3.3. Disco interno SSD para armazenamento de no mínimo 16 Gb;
- 1.3.4. Deve suportar fonte de alimentação interna redundante com chaveamento automático de 100-240 VAC;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.3.5. Possuir redundância do sistema de refrigeração do produto (Fan);
- 1.3.6. Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, documentação técnica e manuais;
- 1.3.7. Não possuir limitação lógica na capacidade nós;
- 1.3.8. Possuir LEDs indicativos do estado de operação, da atividade dos rádios;
- 1.3.9. Possuir estrutura que permita fixação do equipamento em rack e fornecer acessórios para que possa ser feita a fixação;
- 1.3.10. Deverá possuir pelo menos 04 (quatro) interfaces de 2.5 GbE SFP;
- 1.3.11. Deverá possuir pelo menos 04 (quatro) interfaces de 2.5 GbE;
- 1.3.12. Suportar, no mínimo, 12 (doze) interfaces 10/100/1000Base-TX, todas operando em modo *auto-sense*, e em modo *half duplex / full duplex*;
- 1.3.13. A seleção da velocidade e duplex deve ser realizada obrigatoriamente através da interface gráfica de gerenciamento. As interfaces devem suportar as seguintes atribuições:
 - Segmento WAN, ou externo;
 - Segmento WAN secundário, com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN *Failover* por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema;
 - Segmento LAN ou rede interna;
 - Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada);
 - Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade;
 - Segmento ou Zona dedicada para controle de dispositivos Wireless dedicado com controle e configuração destes dispositivos:
 - ✓ 01 (uma) interface do tipo console ou similar;
 - ✓ 01 (uma) interface de rede dedicada para gerenciamento.
- 1.3.14. Balanceamento e *Failover* (Redundância) de links entre 2 ou mais links WAN;
- 1.3.15. Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Ativo e Ativo/*Standby*, com as implementações de *Fail Over* e *Load Balance*, sendo que na implementação de *Load Balance* o estado das conexões e sessões TCP e UDP deve ser replicados sem restrições de serviços como, por exemplo, tráfego *multicast*.
- 1.3.16. Possuir uma interface de rede dedicada para o gerenciamento do produto, operando em 1Gbps, no mínimo. Seu processamento deverá ser de forma isolada ao processamento dos demais tráfegos que passam pelo produto;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.3.17. Possuir porta console (serial) para possíveis manutenções no produto. Configurações básicas via interface CLI como suporte a comandos para debug deverão ser suportadas por esta interface;

1.4. ANTIVÍRUS / ANTI-SPYWARE / ANTI-MALWARE

- 1.4.1. Para proteção do ambiente contra *Malware* conhecido, deve ser incluído módulo de Antivírus e *Anti-Spyware* de gateway integrado na própria ferramenta de Firewall ou entregue com composição com outro equipamento ou fabricante;
- 1.4.2. A atualização de assinaturas deverá ser automática (sem necessidade de intervenção humana) e manual;
- 1.4.3. As atualizações de ameaças, Antivírus e *Anti-spyware* não devem depender de reboot do equipamento para efetivação;
- 1.4.4. A solução deve contemplar mecanismos de proteção de dia-zero (*zero-day protection*), através da atualização adequada de assinaturas para tais ameaças;
- 1.4.5. Devem ser fornecidas todas as atualizações de Anti-Malware de Gateway da base de assinaturas, por todo o período contratual, sem custo adicional ao Conselho;
- 1.4.6. Deverá ser possível a inspeção de Antivírus, no mínimo, dos seguintes tipos de tráfegos: HTTP, SMTP, POP3, IMAP, FTP e SMB, CIFS, NETBIOS;
- 1.4.7. Para este item, também não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao *appliance* para análise de arquivos ou pacotes de dados, a solução obrigatoriamente, deverá ser instalada nas dependências do Conselho;
- 1.4.8. Devem ser fornecidas todas as atualizações para a base de assinaturas do IPS, sem custo adicional, por todo o período contratual, sem custo adicional ao Conselho;
- 1.4.9. O equipamento deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL onde o mesmo deverá ser descriptografado de forma transparente à aplicação, verificado possíveis ameaças e então re-criptografado enviado juntamente ao seu destino caso este não contenha ameaças ou vulnerabilidades. O recurso poderá ser fornecido através de uma licença adicional/opcional ao equipamento.
- 1.4.10. Prover mecanismos de proteção contra ataques baseados em "DNS Rebinding" protegendo contra códigos embutidos em páginas Web com base em JavaScript, Flash e base Java com "malwares". O recurso deverá prevenir ataques e análises aos seguintes endereços: Host que pertence há alguma das sub-nets conectadas a: LAN, DMZ ou WLAN;
- 1.4.11. O *appliance* deve permitir a utilização de políticas de Antivírus, Anti-Spyware. E IPS/IDP e filtro de Conteúdo em todos os segmentos (todos os serviços devem ser suportados no mesmo segmento) ou por zonas de acesso ou VLANs;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.4.12. Possuir flexibilidade para liberar aplicações da inspeção profunda de pacotes, ou seja, excluir a aplicação da checagem de IPS, Gateway Antivírus / AntiSpyware;
- 1.4.13. Possuir verificação de vírus para aplicativos de mensagens instantâneas (AIM, MSN, Yahoo Messenger, ICQ)
- 1.4.14. Possuir proteção contra conexões a servidores Botnet;
- 1.4.15. Deverá permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);
- 1.4.16. Deverá suportar bloqueio de arquivos por tipo (pelo menos 40 tipos);
- 1.4.17. Suportar notificações e alertas via e-mail, SNMP traps e log de pacotes;
- 1.4.18. Deve ser possível a configuração de diferentes políticas de controle de malwares baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc., ou seja, cada política de firewall poderá ter uma configuração diferentes de Antivírus e Antispyware sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

1.5. CONTROLE DE APLICAÇÕES

- 1.5.1. Deverá contar com ferramentas de visibilidade e controle que permitam administrar o tráfego de aplicações, permitindo o tráfego de aplicações autorizadas e bloqueio de aplicações não autorizadas;
- 1.5.2. Deve ser possível a liberação e bloqueio somente das aplicações sem a necessidade de liberação de portas e protocolos;
- 1.5.3. O controle de aplicações deve identificar as aplicações independente das portas e protocolos assim como técnicas de evasão utilizadas;
- 1.5.4. Deverá suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos assinaturas e decoders de protocolos;
- 1.5.5. Deverá incluir a capacidade de atualização para identificar novas aplicações;
- 1.5.6. Deverá atualizar a base de assinaturas de aplicações automaticamente;
- 1.5.7. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas do fabricante;
- 1.5.8. Deverá ser possível adicionar controle de aplicações em todas as regras de segurança do equipamento, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 1.5.9. Deverá ser possível bloquear o uso dos serviços de aplicativos de mensagens instantâneas (Instant Messengers), como:
 - SKYPE;
 - MSN Messenger;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- Yahoo Messenger
- Google Talk;
- ICQ;
- Facebook Chat;
- e outros.

1.5.10. Capacidade para realizar filtragens e inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como:

- Kazaa;
- Morpheus;
- BitTorrent
- Ou outros aplicativos baseados em redes P2P.

1.5.11. O controle sobre os aplicativos citados no item acima, deve ocorrer de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item;

1.5.12. Deverá alertar o usuário quando uma aplicação foi bloqueada;

1.5.13. Possibilitar o controle do tráfego para os protocolos e serviços de rede, baseados nos endereços de origem e destino, como: TCP, UDP, ICMP, FTP, DNS, P2P, entre outros;

1.5.14. Possibilitar o controle do tráfego para os protocolos, baseados nos endereços origem e destino da comunicação, como: GRE, H323 Full v1-5, suporte à tecnologia a gatekeeper, SIP e IGMP;

1.5.15. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, Real Áudio, Real Vídeo, SIP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro;

1.5.16. Possibilitar o controle sobre aplicações de forma granular com criação de políticas sobre o fluxo de dados de entrada, saída ou ambos, como também recursos de:

- Suporte à aplicação de políticas por usuário e / ou grupo;
- Políticas de horários e dias da semana;
- Associação a endereçamento IP baseados em sub-redes;
- Permitir a restrição de arquivos por sua extensão, e bloqueio de anexos através de protocolos SMTP e POP3 baseado em seus nomes ou tipos mime;
- Permitir a filtragem de e-mails pelo seu conteúdo, através da definição de palavras-chave e a sua forma de pesquisa;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.5.17. Deverá possibilitar a diferenciação de aplicações Proxies (*ultrasurf, ghostsurf, freegate, etc.*) possuindo granularidade de controle / políticas para os mesmos;
- 1.5.18. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local;
- 1.5.19. Deverá possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle / políticas baseadas em Usuários e Grupos de usuários;
- 1.5.20. Deverá possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle / políticas baseadas em Usuários e Grupos de usuários;
- 1.5.21. Deverá possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 1.5.22. Deverá incluir a capacidade de criação de políticas baseadas no controle por aplicação, categoria de aplicação, tecnologia e fator de risco;
- 1.5.23. Deverá incluir a capacidade de criação de políticas baseadas no controle por usuário, grupos de usuários ou endereço IP;
- 1.5.24. Deverá incluir a capacidade de criação de políticas baseadas em “*traffic shaping*” por aplicação, usuário, origem, destino, túnel VPN-IPSEC-SSL.
- 1.5.25. Deverá permitir o controle, **sem instalação de cliente de software**, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
Deverá possuir suporte a identificação de usuários em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 1.5.26. Prover matriz de horários que possibilite o bloqueio de serviços com granularidade baseada em hora, minutos, dia, dias da semana, mês e ano que a ação deverá ser tomada;
- 1.5.27. Controle e gerenciamento de banda para a tecnologia VoIP sobre diferentes segmentos de rede/segurança, com inspeção profunda de segurança sobre este serviço.

1.6. CAPTURA DE PACOTES

- 1.6.1. Deverá ser possível a captura de pacotes por:

- Endereço de Origem;
- Endereço de destino;
- Aplicações;
- Aplicações desconhecidas;
- Portas;
- IPS;
- Filtro de dados;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- Qualquer combinação acima.

1.7. FUNCIONALIDADES DE REDE

- 1.7.1. Suporte a definição de VLAN no firewall, conforme padrão IEEE 802.1q e ser possível criar sub-interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (*Stateful Firewall*) entre elas;
- 1.7.2. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos:
- 1.7.3. Suportar funcionamento em interface modo *sniffer*;
 - Modo *sniffer* (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
 - Suportar funcionamento em modo transparente (*Bridge* ou similar);
 - Suportar funcionamento em *Layer 3*;
 - Suportar a implementação simultânea em todos os modos descritos acima (Interface em modo *sniffer*, Transparente e *Layer3*) no mesmo equipamento.
 - Deve suportar VLAN TAGGING (802.1Q) em todas os cenários de implementação acima (Transparente e *Layer3*);
 - Deve suportar controle de aplicações em IPV6 em todas os cenários de implementação acima (Tap, Transparente e *Layer3*);
- 1.7.4. Prover servidor DHCP Interno suportando múltiplos escopos de endereçamento para a mesma interface e a funcionalidade de DHCP Relay;
- 1.7.5. Prover a capacidade de encaminhamento de pacotes UDP (*multicast / broadcast*) entre diferentes interfaces e zonas de segurança como *IP Helper*;
- 1.7.6. Implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;
- 1.7.7. Suportar a criação de túneis IP sobre IP (IPSEC Túnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

1.8. NAT (NETWORK ADDRESS TRANSLATION)

- 1.8.1. Prover mecanismo de conversão de endereços (NAT), de forma a possibilitar que uma rede com endereços reservados acesse a Internet a partir de um único endereço IP e possibilitar também um mapeamento 1-1 de forma a permitir com que servidores internos com endereços reservados sejam acessados externamente através de endereços válidos;
- 1.8.2. Deverá suportar:
 - Porta/IP Nat dinâmico (*Many-to-1* e *Many-to-Many*);
 - IP Nat dinâmico (*Many-to-Many*);



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- IP Nat estático (*1-to-1, Many-to-Many, IPS*);
- Nat estático bidirecional 1-to-1.

- 1.8.3. IP Virtual (VIP); NAT de Origem e de Destino; Suportar NAT de Origem e NAT de Destino simultaneamente;
- 1.8.4. Permitir, sobre o recurso de NAT, o balanceamento interno de servidores e suas aplicações sem a necessidade de inserção de um equipamento como switches de que atuam entre as camadas 4 (quatro) e 7 (sete) do modelo ISO/OSI.
- 1.8.5. Possuir mecanismo que permita que a conversão de endereços (NAT) seja feita de forma dependente do destino de uma comunicação, possibilitando que uma máquina, ou grupo de máquinas, tenham seus endereços convertidos para endereços diferentes de acordo com o endereço destino;
- 1.8.6. Possuir mecanismo que permita conversão de portas (PAT).

1.9. VPN (VIRTUAL PRIVATE NETWORK)

- 1.9.1. A VPN *Client-to-Site IPsec* deve ser licenciada para, no mínimo, 50 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 1000 usuários simultâneos, com aquisição de licença futura;
- 1.9.2. A VPN SSL deve ser licenciada para, no mínimo, 02 (dois) usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 350 usuários simultâneos;
- 1.9.3. Acesso remoto através de VPN, nos padrões: IPSEC; Client; SSL;
- 1.9.4. Suportar, no mínimo, 1000 túneis de VPN IPSEC simultâneos;
- 1.9.5. Suportar, no mínimo, 1,45 Gbps de *throughput* de VPN IPSEC;
- 1.9.6. IPsec VPN deve suportar:
- 3DES, AES;
 - Autenticação MD5 e SHA;
 - *Diffie-Hellman Group 1*, Group 2 e Group 5;
 - Algoritmo *Internet Key Exchange (IKE)*;
 - AES 128, 192 & 256 (*Advanced Encryption Standard*).
- 1.9.7. Suportar SSL VPN;
- 1.9.8. Suportar atribuição de IPs nos clientes remotos de VPN;
- 1.9.9. Suportar atribuição de DNS nos clientes remotos de VPN;
- 1.9.10. Suportar, no mínimo, **1.000 túneis VPN IPSEC do tipo site-to-site já licenciadas**;
- 1.9.11. Deve possuir interoperabilidade com os seguintes outros fabricantes:
- 1.9.12. Deverá permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.9.13. Deverá contar com um software cliente de VPN-SSL para os sistemas operacionais Windows XP, Windows 7 (32 e 64 bits) e Windows 8 (32 e 64 bits);
- 1.9.14. Deverá permitir criar políticas para tráfego VPN-SSL;
- 1.9.15. Suporte para autenticação de VPNs SSL, LDAP e base de dados própria;
- 1.9.16. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;
- 1.9.17. Permitir a criação de políticas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego;
- 1.9.18. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário;
- 1.9.19. Possibilitar VPN com equipamentos e softwares de fabricantes diferentes da solução entregue, através de comunicação IPSec.

1.10. **QOS (QUALITY OF SERVICE)**

- 1.10.1. Possuir gerenciamento de tráfego de entrada, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida;
- 1.10.2. Deverá permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário;
- 1.10.3. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como *youtube, ustream, etc.*) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deva ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de *vídeo streaming*;
- 1.10.4. Suportar a criação de políticas de QoS por:
 - Endereço de origem;
 - Endereço de destino;
 - Por usuário ou Grupo do AD;
 - Por aplicações (como por exemplo *Skype, Bittorrent, YouTube* e outras);
 - Por grupos de aplicações (como por exemplo: Instant Messaging ou grupo de aplicações P2P).
- 1.10.5. O QoS deve possibilitar a definição de classes por:
 - Banda Garantida;
 - Banda Máxima;
 - Fila de Prioridade;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- Suportar marcação de pacotes *Diffserv*;

1.11. AUTENTICAÇÃO

- 1.11.1. Permitir a utilização de LDAP, AD e RADIUS;
- 1.11.2. Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerencia remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo;
- 1.11.3. Para autenticação de VPN SSL deve ser suportado: LDAP; *Radius*;
- 1.11.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;
- 1.11.5. Suporte a rede com múltiplos domínios, possibilitando a integração em um ambiente onde existas domínios diferentes e totalmente segregados;
- 1.11.6. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou *Active Directory*. O perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (*Deep Packet Inspection*) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como FTP, HTTP, HTTPS devem consultar uma base de dados de usuários e grupos de servidores da plataforma Windows, versões 2003, 2008 ou 2012, com *Active Directory*;
- 1.11.7. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP, HTTPS e Gopher, utilizando as bases de dados de usuários e grupos de servidores NT e Unix, de forma simultânea;
- 1.11.8. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por *Pré-Shared Key*, Certificados digitais e *XAUTH client authentication*;
- 1.11.9. Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerencia remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo;
- 1.11.10. Permitir o controle de acesso por usuário, para plataformas MS Windows a partir da versão XP, de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;
- 1.11.11. Possuir perfis de acesso hierárquicos;
- 1.11.12. Permitir a restrição de atribuição de perfil de acesso a um usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando.

1.12. IPS (*INTRUSION PREVENTION SYSTEM*)



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.12.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio *appliance* de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos *appliances* de segurança, com **suporte a pelo menos 3.000 assinaturas**;
- 1.12.2. A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas e trabalhar em conjunto com o controle de aplicações;
- 1.12.3. A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho;
- 1.12.4. A solução de IPS deve fazer a inspeção de todo o tráfego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitada neste edital;
- 1.12.5. Possuir capacidade de remontagem de pacotes para identificação de ataques;
- 1.12.6. O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o *appliance*;
- 1.12.7. Para cada proteção de segurança, deve ser possível consultar informações no site do fabricante;
- 1.12.8. A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada;
- 1.12.9. As regras de exceção devem possuir: origem, destino e serviço;
- 1.12.10. A solução deve ser capaz de inspecionar tráfego HTTPS.
- 1.12.11. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como *Denial of Service (DoS)* do tipo *Flood*, *Scan*, *Session* e *Sweep*;
- 1.12.12. Detecção de anomalias;
- 1.12.13. A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção);
- 1.12.14. O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de SMTP, Web e DNS;
- 1.12.15. O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o *appliance*;
- 1.12.16. Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino;
- 1.12.17. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, *SQL Injection*, ataques a sistemas operacionais e VOIP;
- 1.12.18. Deve incluir proteção contra *worms*;
- 1.12.19. Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao longo do tempo dispondo o sumário quantitativo das ameaças analisadas.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.12.20. A solução deve possuir um esquema de atualização de assinaturas através de um click;
- 1.12.21. Atualização de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;
- 1.12.22. A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP (HTTPS);
- 1.12.23. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;
- 1.12.24. A solução deverá possuir proteções para sistemas SCADA;
- 1.12.25. Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear.

1.13. **CONTROLE DE APLICAÇÃO (APPLICATION CONTROL)**

- 1.13.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades abaixo:
 - Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
 - Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent, Serviços de Mensageria e outros;
 - Controlar o uso dos serviços de *Instant Messengers* como MSN, YAHOO, Google Talk, ICQ e outros, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item;
 - Deverá controlar software *FreeProxy* tais como ToR, Ultrasurf, Freegate e outros semelhantes;
 - Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
 - Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;
 - Atualizar a base de assinaturas de aplicações automaticamente;
 - Limitar a banda (download/upload) usada por aplicações (*traffic shaping*), baseado no IP de origem, usuários e grupos do LDAP/AD;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- A solução de controle de aplicação WEB deve criar regras granulares possibilitando adicionar tipos de aplicação WEB e categorias por regra, sendo assim criando controle granular de qualquer tipo de acesso não permitido pela empresa;
- Deve implementar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e protocolos;
- Caso a solução não tenha assinaturas pré-definida na solução a mesma deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, FTP, E-mail e extensão de arquivos;
- O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos;
- Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
- Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, uTorrent, etc.) possuindo granularidade de controle/políticas para os mesmos;
- Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo: permitir o Facebook e bloquear chat;
- Deverá possibilitar a diferenciação de aplicações Proxies possuindo granularidade de controle/políticas para os mesmos;
- Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:
 - ✓ Nível de risco da aplicação.
 - ✓ Categoria de aplicações.

1.14. RECURSOS PARA FILTRO DE CONTEÚDO WEB (WWW)

- 1.14.1. Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no firewall;
- 1.14.2. Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática;
- 1.14.3. Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes;
- 1.14.4. Suportar políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo. Esta comprovação poderá ser exigida em testes sob o ambiente de produção com o fornecimento do produto para comprovação deste e demais itens;
- 1.14.5. Deverão ser fornecidas licenças de Filtro de Conteúdo para cada toda a solução, na quantidade de usuários suficientes, com licenciamento a contar da data de sua ativação, com validade igual ao tempo de contrato, sem custos adicionais ao Conselho;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.14.6. Controle de conteúdo filtrado por categorias de filtragem com base de dados continuamente atualizada e extensível;
- 1.14.7. A plataforma de proteção deve possuir as seguintes funcionalidades de filtro de URL:
- Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra) ;
 - Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).
- 1.14.8. Filtro de URL avançado para políticas de controle da Navegação dos Usuários, baseadas em:
- Categorias de acesso;
 - Protocolos.
- 1.14.9. Deve possibilitar à criação de políticas por usuários, grupos de usuários, IPs, redes e grupos de redes;
- 1.14.10. O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização (*hit count*);
- 1.14.11. Deverá permitir criar política de confirmação de acesso;
- 1.14.12. Deve possibilitar a inspeção de tráfego HTTPS (*Inbound/Outbound*), sendo que para a opção de Outbound não será necessário efetuar o "*man-in-the-middle*", ou seja, a solução deverá prover mecanismo que irá analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso, de acordo com a política configurada;
- 1.14.13. Capacidade de submissão instantânea de novos sites e palavras chaves;
- 1.14.14. O administrador poderá adicionar filtros por palavra-chave de modo específico;
- 1.14.15. Deverá permitir o bloqueio Web através de senha pré configura pelo administrador;
- 1.14.16. Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que, antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (*Captive Portal*);
- 1.14.17. Permitir a classificação dinâmica de sites Web, URLs e domínios;
- 1.14.18. Possuir módulo integrado ao mesmo *Firewall DPI (Deep Packet Inspection)* para classificação de páginas web com no mínimo 50 categorias distintas, com mecanismo de atualização automática;
- 1.14.19. A solução deve fornecer um mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;
- 1.14.20. Possuir pelo menos 50 categorias de URLs;
- 1.14.21. Suporte à filtragem para, no mínimo, as seguintes categorias:
- violência, nudismo, roupas íntimas / banho, pornografia, armas, ódio / racismo, cultos / ocultismo, drogas ilegais, crimes / comportamento ilegal, educação sexual, jogos, álcool / tabagismo, conteúdo adulto, conteúdo questionável, artes e entretenimento, bancos / e-trading, chat, negócios e economia, tecnologia de



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

computadores e Internet, e-mail pessoal, jogos de azar , *hacking*, humor, busca de empregos, newsgroups, encontros pessoais, restaurantes / jantar, portais de busca, shopping e portais de compras, MP3, download de software, viagens e WEB *hosting* e outras.

- 1.14.22. Suporta a criação de categorias de URLs customizadas;
- 1.14.23. Suporta a exclusão de URLs do bloqueio, por categoria;
- 1.14.24. Deverá possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente;
- 1.14.25. A solução deverá permitir um mecanismo que permita sobrescrever as categorias de URL;
- 1.14.26. Permite a customização de página de bloqueio;
- 1.14.27. O administrador de política de segurança poderá definir grupos de usuários e diferentes políticas de filtragem de sites WEB, personalizando quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet;
- 1.14.28. Suporte à adição de filtros por palavra-chave de modo específico e individual em cada um dos firewalls da rede, de forma centralizada;
- 1.14.29. A política de Filtros de conteúdo deverá ser baseada em horário do dia e dia da semana;
- 1.14.30. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação;
- 1.14.31. Possibilitar a filtragem da linguagem Javascript e de applets Java e Active-X em páginas WWW, para o protocolo HTTP;
- 1.14.32. Deverão ser fornecidas todas as atualizações de software, assim como a atualização da base de conhecimento (URLs categorizadas), sem custo adicional, por um período de XX meses/anos.

1.15. PROTEÇÃO CONTRA VIRUS E BOT-NETS

- 1.15.1. Deve possuir módulo de antivírus e *anti-bot* integrado no próprio *appliance* de segurança;
- 1.15.2. A solução de antivírus integrada deve ter capacidade de analisar arquivos maiores que 1Gbps;
- 1.15.3. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos *appliances* através de assinaturas;
- 1.15.4. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;
- 1.15.5. Implementar funcionalidade de detecção e bloqueio de *callbacks*;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.15.6. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;
- 1.15.7. A solução *Anti-bot* deve possuir mecanismo de detecção que inclui, reputação de endereço IP;
- 1.15.8. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.
- 1.15.9. Implementar interface CLI segura através do protocolo SSH;
- 1.15.10. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream;
- 1.15.11. A solução deve permitir criar regras de exceção de acordo com a proteção;
- 1.15.12. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;
- 1.15.13. Permitir o bloqueio de malwares (vírus, worms, spyware e etc);
- 1.15.14. A solução deve ser capaz de proteger contra ataques para DNS;
- 1.15.15. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares;
- 1.15.16. A solução deve ser capaz de prevenir acesso a websites maliciosos;
- 1.15.17. A solução deve ser capaz de realizar inspeção de tráfego SSL e SSH;
- 1.15.18. A solução deverá receber atualizações de um serviço baseado em cloud;
- 1.15.19. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos;
- 1.15.20. A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS;
- 1.15.21. A solução deve suportar funcionalidade de GeoIP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade.

1.16. ADMINISTRAÇÃO E RELATÓRIOS

- 1.16.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;
- 1.16.2. Suportar, no mínimo, **40.000 usuários autenticados** com serviços ativos e identificados passando por este dispositivo de segurança em um único dispositivo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo. Está comprovação poderá ser exigida em testes sobre o ambiente de produção com o fornecimento do produto para comprovação deste e demais itens;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.16.3. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;
- 1.16.4. Fornecer gerência remota, com interface gráfica nativa, através interface WEB;
- 1.16.5. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;
- 1.16.6. Fornecer interface gráfica para no mínimo 05 usuários:
 - Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração;
- 1.16.7. O gerenciamento local do equipamento deve permitir/Possuir:
 - Criação e administração de políticas;
 - Administração de políticas de IPS, Antivírus e *Anti-Spyware*;
 - Política de Filtro de Dados e Filtro de URLs.
 - Monitoração de logs;
 - *Debugging*;
 - Captura de pacotes.
- 1.16.8. Deverá possuir solução de gerenciamento centralizado, possibilitando o gerenciamento das caixas em alta disponibilidade;
- 1.16.9. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos gateways de segurança;
- 1.16.10. Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado;
- 1.16.11. Deverá possuir relatórios de utilização dos recursos por aplicações, URL, Ameaças, etc.;
- 1.16.12. Prover mecanismo de visualização de eventos em tempo real das funções de segurança, com uma prévia sumarização para fácil visualização de no mínimo as seguintes informações:
 - Aplicações mais utilizadas;
 - Usuários com maior atividade;
 - Estatísticas de uso;
 - Principais aplicações por taxa de transferência de bytes;
 - Principais hosts por número de ameaças identificadas;
 - Prover mecanismo de consulta às informações registradas integrado à interface de administração;
 - Possibilitar o armazenamento de seus registros (log e/ou eventos).



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.16.13. Prover uma visualização sumarizada de todas as aplicações, ameaças e URLs que passaram pela solução;
- 1.16.14. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;
- 1.16.15. Deverá possuir mecanismo "*drill-down*" para visualização de relatório do tráfego em até os últimos 7 dias;
- 1.16.16. Nas opções de "*drill-down*", ser possível identificar o usuário que fez determinado acesso;
- 1.16.17. Deverá possibilitar a criação de diferentes perfis de administração separando pelo menos: Leitura, Alterações, Relatórios e Monitoração;
- 1.16.18. Deverá ser possível de forma granular, assinar permissões para os administradores criarem outros usuários, alterarem configurações, ler configurações, etc.;
- 1.16.19. Deverá ser possível administrar o firewall localmente ou remotamente sem causar problemas de sincronismo de configurações;
- 1.16.20. Deverá possuir interface ethernet "*Out-of-Band*" para gerenciamento: SSH; HTTPS.
- 1.16.21. Possuir controle de número máximo de sessões TCP, prevenindo a exaustão de recursos do *appliance* e permitindo a definição de um percentual do número total de sessões disponíveis que podem ser utilizadas para uma determinada conexão definida por regra de acesso;
- 1.16.22. Possuir suporte ao protocolo SNMP versões 2 e 3;
- 1.16.23. Gerar alertas automáticos via:
 - E-mail;
 - SNMP;
 - Syslog.
- 1.16.24. Possuir roteamento RIP e OSPF, com configuração pela interface gráfica;
- 1.16.25. Suportar *Rollback* de configuração para a última configuração salva;
- 1.16.26. Suportar *Rollback* de Sistema Operacional para a última versão local;
- 1.16.27. Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;
- 1.16.28. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;
- 1.16.29. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;
- 1.16.30. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.16.31. Ser capaz de visualizar, de forma direta no console do *appliance* e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas;
- 1.16.32. Permitir a visualização de estatísticas do uso de CPU do *appliance* o através da interface gráfica remota em tempo real;
- 1.16.33. Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas;
- 1.16.34. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes;
- 1.16.35. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;
- 1.16.36. Possuir mecanismo que permita a realização de cópias de segurança (backups);
- 1.16.37. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;
- 1.16.38. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;
- 1.16.39. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;
- 1.16.40. Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;
- 1.16.41. Possibilitar a geração de pelo menos os seguintes tipos de relatórios, mostrados em formato HTML, PDF e CSV:
 - Máquinas mais acessadas;
 - Serviços mais utilizados;
 - Usuários que mais utilizaram serviços;
 - URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web);
 - Categorias Web mais acessadas;
 - Maiores emissores e receptores de e-mail;
 - Aplicativos mais utilizados.
 - Maiores emissores e receptores de e-mail;
 - detecção de intrusos;
 - intrusos bloqueados e alvos, para vírus e *spywares* bloqueados, alvos e detectados.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.16.42. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML:
- Máquinas acessadas X serviços bloqueados;
 - Usuários X URLs acessadas;
 - Usuários X categorias Web bloqueadas.
- 1.16.43. Permitir o envio dos relatórios, através de e-mail para usuários predefinidos;
- 1.16.44. Possuir relatórios pré-definidos na solução e permitir a criação de relatórios customizados;
- 1.16.45. Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP;
- 1.16.46. Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática;
- 1.16.47. Disponibilizar download dos relatórios gerados;
- 1.16.48. **Tempo de retenção de dados para relatórios: 5 anos, no mínimo;**

1.17. LOG E AUDITORIA

- 1.17.1. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;
- 1.17.2. **Tempo de retenção de log: 5 anos, no mínimo;**
- 1.17.3. Prover mecanismo de consulta às informações registradas integrado à interface de administração;
- 1.17.4. Possibilitar o armazenamento de seus registros (log e/ou eventos) em servidor apartado de X-Log, resumizando os dados e gerando relatórios gerenciais de acesso, quantidade de ataques e malwares identificados ou bloqueados;
- 1.17.5. Possibilitar a recuperação dos registros de log e/ou eventos armazenados em máquina remota, através de protocolo criptografado, de forma transparente através da interface gráfica;
- 1.17.6. Possibilitar a análise dos seus registros (log e/ou eventos) por pelo menos um programa analisador de log disponível no mercado;
- 1.17.7. Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP;
- 1.17.8. Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;

- 1.17.9. Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado.

2. SOLUÇÃO SOFTWARE DE ENDPOINT (ANTIVÍRUS) PARA, NO MÍNIMO, 150 USUÁRIOS/COMPUTADORES.

2.1. REQUISITOS GERAIS

- 2.1.1. Será fornecida e instalada a solução software de *Endpoint* (antivírus) para, **até 150 usuários / computadores** da rede de dados do CRA-SP, sendo até 30% deles servidores, com console fornecida em uma das seguintes opções:

- *Appliance* virtual (Microsoft Hyper-V), instalado no ambiente já existente disponibilizado pelo Conselho
- Ou ambiente em *Cloud Computing* do próprio fabricante da solução.

- 2.1.2. Prover segurança para estações de trabalho, sejam físicas ou em ambiente virtualizado;

- 2.1.3. Possuir console central única de gerenciamento. As configurações do *Antivírus*, *AntiSpyware*, *Firewall*, Detecção de intrusão controle de Dispositivos e Controle de Aplicações deverão ser realizadas através da mesma console;

- 2.1.4. O Produto deverá ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pela console de gerenciamento;

- 2.1.5. O produto deverá possuir no mínimo os seguintes módulos:

- Console de Gerenciamento fornecendo funcionalidades de gestão;
- Módulos para estações físicas, laptops e servidores;
- Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;
- Módulo para dispositivos móveis no mínimo para tablets e smartphones com sistema operacional iOS e Android;
- Utilizar o conceito de heurística.

- 2.1.6. Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (*anti-exploit*);

- 2.1.7. Oferecer tecnologia nativa no intuito de eliminar ameaças do tipo *Ransomware*;

- 2.1.8. Oferecer inventário de softwares;

- 2.1.9. Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

2.1.10. Oferecer proteção por base de assinaturas.

2.2. CONSOLE DE GERENCIAMENTO

2.2.1. INSTALAÇÃO E CONFIGURAÇÃO:

- Caso seja fornecida a solução por *appliance* virtual, esta deve rodar e ser compatível com os servidores Microsoft Windows Server 2012, na plataforma denominada *Microsoft Hyper-V*;
- Deverá ser fornecido com base de dados embutido no Console WEB, sem a necessidade de baixar para máquina do administrador da Console;
- Permitir instalação remota via console WEB de gerenciamento para ambientes;
- O mecanismo de varredura deverá estar disponível para download separadamente;
- A solução deverá permitir a inclusão de um módulo de balanceamento para casos em vários servidores tenham a mesma função (para alta disponibilidade, recuperação de desastres, performance entre outras);
- Deve ser totalmente em português.

2.3. CARACTERÍSTICAS GERAIS

2.3.1. Licenciamento flexível;

2.3.2. Arquitetura simples de atualização, com um simples clicar de botão todas as funções e serviços devem ser atualizadas;

2.3.3. Permitir que o administrador escolha qual o pacote será atualizado;

2.3.4. As notificações devem ser destacadas como item não lida, enviar e-mail para o administrador, no mínimo, enviar notificações:

- Problemas com licenças;
- Alertas de Surto de vírus;
- Máquinas desatualizadas;
- Eventos de *anti-malware*.

2.4. PAINEL PARA MONITORAMENTO

2.4.1. Baseado em “portlets” configuráveis com no mínimo as seguintes especificações:

- Nome;
- Tipo de relatório;
- Alvo do relatório.

2.4.2. Deverá disponibilizar “*portlets*” para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

2.5. INVENTÁRIO DA REDE

2.5.1. Possuir no mínimo as integrações abaixo:

- Múltiplos domínios do Active Directory;
- Múltiplos VMWare vCenters;
- Múltiplos Citrix Xen Servers.

2.5.2. Possuir a possibilidade de definição de sincronização com o Active Directory em horas;

2.5.3. Deverá ser compatível com Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM;

2.5.4. Descoberta de rede para máquinas em grupo de trabalho;

2.5.5. Possuir busca em tempo real pelo menos com os seguintes filtros:

- Nome;
- Sistema Operacional;
- Endereço IP.

2.5.6. Possibilitar a instalação remota e desinstalação remota do antivírus;

2.5.7. Possibilitar a configuração de pacotes de instalação do produto de antivírus;

2.5.8. Possuir tarefas remotas e configuráveis de Scan;

2.5.9. Possuir tarefa de reinicialização remota de estação ou servidor;

2.5.10. Assinar políticas para no mínimo os níveis:

- Computador;
- Máquina Virtual.

2.5.11. Possuir a propriedade detalhada de objetos gerenciados para:

- Nome;
- IP;
- Sistema Operacional;
- Grupo;
- Política Assinada;
- Último status de malware.

2.6. POLÍTICAS

2.6.1. Modelo único para todos os equipamentos, seja físico ou virtual;

2.6.2. Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar;

2.6.3. Deverá configurar as funcionalidades como escaneamento do Antivírus, firewall de duas vias de detecção de intrusão, controle de acesso à rede, controle de aplicação, controle de acesso web, criptografia (*Android*), localização de dispositivo (*Mobile*), autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

2.7. RELATÓRIOS

2.7.1. Deverá apresentar as seguintes funcionalidades:

- Relatório para cada serviço de segurança;
- Facilidade de usar e visualização simplificada;
- Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;
- Filtros de agendamento de relatórios;
- Arquivo com todas as instâncias de relatório agendados;
- Exportar o relatório nos formatos .pdf e/ou .csv;
- Oferecer possibilidade de criar relatórios de maneira dinâmica no dashboard da solução.

2.8. USUÁRIOS

2.8.1. Deverá apresentas no mínimo as seguintes funcionalidades:

- Administração baseada em regras;
- Disponibilizar tipos de usuários pré-definidos como no mínimo:
 - ✓ Administrador – Gerente dos componentes da solução;
 - ✓ Administrador de rede - Gerente dos serviços de segurança;
 - ✓ Relatório – Monitora e cria relatórios.
- Deverá ser possível customizar um tipo de usuário:
- Deverá permitir a integração do usuário com o Active Directory para autenticação da console de gerenciamento.

2.9. LOGS

2.9.1. Registrar as ações do usuário no console de gerenciamento;

2.9.2. Detalhar cada ação do usuário;

2.9.3. Permitir busca complexa baseada em ações do usuário, intervalos de tempo.

2.10. CERTIFICADO DE SEGURANÇA

2.10.1. Deverá prover o acesso via HTTPS;

2.10.2. Deverá permitir a importação de certificados digitais;

2.10.3. O gerenciamento e a comunicação com dispositivos móveis devem ser feitos de forma segura utilizando certificados digitais.

2.11. PROTEÇÃO PARA ESTAÇÕES DE TRABALHO E SERVIDORES FÍSICOS

2.11.1. Deverá apresentar no mínimo:



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- Deverá permitir a configuração do scan do antivírus do cliente como:
 - ✓ Scan local;
 - ✓ Scan Híbrido;
 - ✓ Scan Central.
- Deverá permitir a instalação customizada do antivírus com no mínimo:
 - ✓ Instalar o antivírus sem o controle de acesso à internet; (Windows Workstation);
 - ✓ Instalar o antivírus sem o módulo de firewall; (Windows Workstation).
- Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho:
 - ✓ Windows 10 64Bits;
 - ✓ Windows 8.1 64Bits;
 - ✓ Windows 8 64Bits;
 - ✓ Windows 7 64Bits;
 - ✓ Windows XP (SP3) apenas o módulo de antivírus.
- Deverá suportar no mínimo os seguintes sistemas operacionais para servidores:
 - ✓ Windows Server 2012R2;
 - ✓ Windows Server 2012;
 - ✓ Windows Server 2008 R2;
 - ✓ Windows Server 2008;
 - ✓ Windows Server 2003 R2 apenas o módulo de antivírus;
 - ✓ Windows Server 2003 com SP1 apenas o módulo de antivírus.
- Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux:
 - ✓ Red Hat Enterprise Linux;
 - ✓ Cent OS 5.6 ou superior;
 - ✓ Ubuntu 10.04 LTS ou superior;
 - ✓ SUSE Linux Enterprise Server 11 ou superior;
 - ✓ OpenSUSE 11 ou superior;
 - ✓ Fedora 15 ou superior;
 - ✓ Debian 5.0 ou superior.

2.12. GERENCIAMENTO E INSTALAÇÃO REMOTA

2.12.1. Deverá permitir ao administrador customizar a instalação;

2.12.2. A instalação deverá ser possível executar com no mínimo das seguintes maneiras:

- Executar o pacote de antivírus diretamente na estação de trabalho;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- Instalar remotamente, distribuído via console de gerencia web.
- 2.12.3. Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação;
- 2.12.4. A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações:
- Nome;
 - IP;
 - Sistema Operacional;
 - Política Aplicada.
- 2.12.5. Através da console o administrador poderá ser capaz de enviar uma política única para configurar o antivírus;
- 2.12.6. A console de gerenciamento deverá incluir sessão de log com as seguintes informações:
- Login;
 - Edição;
 - Criação;
 - Log-out.
- 2.12.7. Ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits;
- 2.12.8. Deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;
- 2.12.9. O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário à distribuição em um agente separado.

2.13. PROTEÇÃO PARA ESTAÇÕES E SERVIDORES VIRTUAIS

2.13.1. PROTEÇÃO DE ANTIVÍRUS DEDICADO PARA AMBIENTES VIRTUAIS:

- Deverá ter a disponibilidade de ser integrado com o VMWare e oferecer a escaneamento sem instalar o produto na máquina virtual;
- Hyper-V;
- A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare;
- Deverá proteger em tempo real e agendado as máquinas virtuais Linux;
- O produto deverá oferecer agente para virtualização dos seguintes produtos:
 - ✓ Citrix Xen Server;
 - ✓ Microsoft Hyper-V;
 - ✓ Red Hat Virtualization;
 - ✓ Oracle KVM;
 - ✓ KVM.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

2.13.2. FUNÇÕES GERAIS

- Deverá ter métodos de detecção de vírus, Spyware, rootkits e outros mecanismos de segurança;
- Deverá reportar o estado atual das VMs no mínimo, protegida/desprotegida;
- Requisitos Mínimos do Sistema e Plataformas de Virtualização:
 - ✓ VMware vSphere ESX 5.0 ou superior;
 - ✓ VMware vCenter Server 4.1 ou superior;
 - ✓ VMWare Tools 8.6.0 ;
 - ✓ Citrix XenDesktop 5.0 ou superior;
 - ✓ Xen Server 5.5 ou superior;
 - ✓ Citrix VDI-in-a-Box 5;
 - ✓ Microsoft Hyper-V Server 2008 R2, 2012
 - ✓ Oracle VM 3.0;
 - ✓ Red Hat Enterprise Virtualization 3.0.
- Requisitos do Sistema e Sistemas Operacionais desktops:
 - ✓ Windows 10
 - ✓ Windows 8;
 - ✓ Windows 7;
 - ✓ Windows XP.
- Sistemas Operacionais Servidores:
 - ✓ Windows Server 2012 R2
 - ✓ Windows Server 2012
 - ✓ Windows Server 2008 R2
 - ✓ Windows Server 2008
 - ✓ Windows Server 2003 R2 Instalação apenas do módulo de antivírus;
 - ✓ Windows Server 2003 com SP1 Instalação apenas do módulo de antivírus;
 - ✓ Linux Red Hat Enterprise;
 - ✓ CentOS 5.6 ou superior;
 - ✓ Ubuntu 10.04 LTS ou superior;
 - ✓ SUSE Linux Enterprise Server 11 ou superior;
 - ✓ OpenSUSE 11 ou superior;
 - ✓ Fedora 15 ou superior;
 - ✓ Debian 5.0 ou superior.

2.14. COMPONENTES E FUNCIONALIDADE DO ANTIVÍRUS GERAL

2.14.1. Deverá fazer escaneamento em tempo real automático;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 2.14.2. Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão;
- 2.14.3. Escaneamento de comportamento heurístico;
- 2.14.4. Deverá escanear em tempo real qualquer informação localizada em mídias de armazenamento como:
- CD/DVD;
 - Discos Externos;
 - Pen-Drivers;
 - Deverá permitir a escolha e configuração de pastas a serem escaneada;
 - Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção:
 - ✓ Baseada em Assinaturas;
 - ✓ Baseada em Heurística;
 - ✓ Baseada em monitoramento contínuo de processos.
- 2.14.5. Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL na Estações de trabalho;
- 2.14.6. O cliente do antivírus deverá ter o módulo de *Antiphishing* que deverá ter a opção de verificar links pesquisados com os sites de pesquisas *Search Advisor* na Estações de trabalho;
- 2.14.7. Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser instalado/desinstalado nas estações de trabalho;
- 2.14.8. O módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho.

2.15. QUARENTENA

- 2.15.1. Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;
- 2.15.2. Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;
- 2.15.3. Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;
- 2.15.4. Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;
- 2.15.5. Deverá permitir escanear a quarentena após a atualização das atualizações de assinaturas.
- 2.15.6. Restauração remota, com configuração de localidade e deleção;
- 2.15.7. Criação e exclusão para arquivos restaurados.

2.16. CONTROLE DE USUÁRIO

- 2.16.1. Deverá ter módulo de controle de usuário integrando com as seguintes características:
- Bloqueio de acesso à internet;
 - Bloqueio de acesso a aplicações definidas pelo administrador.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

2.17. CONTROLE DO DISPOSITIVO

2.17.1. Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;

2.17.2. Através do módulo de controle de dispositivo deverá ser possível controlar:

- Bluetooth;
- CDROM/DVDROM;
- IEEE 1284.4;
- IEEE 1394;
- Windows Portable;
- Adaptadores de Rede;
- Adaptadores de rede Wireless;
- Discos Externos.

2.17.3. Deverá permitir regras de definição de bloqueio/desbloqueio;

2.17.4. Deverá permitir regras de exclusão.

2.18. ATUALIZAÇÕES

2.18.1. Após a atualização o administrador deverá ter a capacidade de adira uma reinicialização;

2.18.2. Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;

2.18.3. Permitir atualizações de assinatura de hora em hora;

2.18.4. Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada.

2.19. SEGURANÇA PARA SMARTPHONES

2.19.1. REQUISITOS MÍNIMOS DO SISTEMA OPERACIONAL PARA SMARTPHONE

- Android 2.2 ou superior e iOS

2.19.2. RECURSOS

- Permitir atribuir dispositivo com usuário do Active Directory;
- A ativação do dispositivo da console de gerenciamento deverá ser através de um QR code;
- Os pacotes de instalação devem estar disponíveis nas lojas dos Sistemas Operacionais;
- Deverá permitir no mínimo as seguintes ações:
 - ✓ Impor bloqueio de tela e autenticação;
 - ✓ Desbloquear o dispositivo;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- ✓ Restaurar as configurações de fábrica;
- ✓ Localiza o Dispositivo;
- ✓ Análise de dispositivos para o Sistema Operacional Android;
- ✓ Criptografia de memória do dispositivo para o Sistema Operacional Android.

2.20. CONFIGURAÇÕES DE SEGURANÇA

- Caso o dispositivo não esteja em conformidade com as políticas estabelecidas deverá ser possível as ações abaixo:
 - ✓ Ignorar;
 - ✓ Bloquear acesso;
 - ✓ Bloquear o dispositivo;
 - ✓ Restaurar as configurações de fábrica;
 - ✓ Remover o dispositivo do console de gerenciamento.
- Deverá permitir o uso de senha. A senha pode ser configurada conforme necessidade do administrador com no mínimo os seguintes recursos:
 - ✓ Senha simples ou complexa;
 - ✓ Números e caracteres;
 - ✓ Comprimento mínimo;
 - ✓ Caracteres especiais mínimos;
 - ✓ Período de expiração da senha;
 - ✓ Definir restrição de reutilização de senha;
 - ✓ Definir o número de tentativas de entradas de senha incorretas;
 - ✓ Período de bloqueio do dispositivo.

2.21. CRIPTOGRAFIA

1.1.2. Deverá oferecer:

- Possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou *on-premise* com módulo de Criptografia presente na mesma Console do Antivírus.
- Deverá utilizar quando necessários serviços de criptografia SEM agentes nativos da estação de trabalho seja baseada em Windows (*BitLocker*) ou Mac (*FileVault*);
- Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;
- Deverá ser compatível com Mac OS X Mountain, Mavericks, Yosemite, Sierra.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ANEXO III - AMBIENTE COMPUTACIONAL DO CONSELHO

1.2. AMBIENTE DE INSTALAÇÃO DAS SOLUÇÕES:

1.2.1. Atualmente, a possui a infraestrutura de rede interna do Conselho é composta por:

• SWITCHES MARCA / MODELO:

- ✓ SWITCH DELL NETWORKING PowerConnect 6248P, 10/100/1000;
- ✓ SWITCH DELL NETWORKING N2024P, L2, POE+, 24X 1GBE + 2X 10GBE, SFP+ FIXED PORTS, STACKING, IO TO PSU AIR, AC"
- ✓ SWITCH DELL EMC N3048P, POE+, 48X 1 GBT, 2X SFP+ 10GBE, 2 PORTAS COMBINADAS GBE SFP, L3, STACKING, 1X PSU AC".

• LINKS DE INTERNET:

SERVIÇO	DESCRIÇÃO
LINK DE INTERNET DEDICADO: - Principal; - Operadora: WCS.	LINK DE INTERNET DEDICADO – FIBRA ÓPTICA: - IP fixo (04 disponíveis): 187.62.218.234 - Velocidade mínima garantida: 100 Mbps; - Conexão dedicada à Internet full-duplex; - Meio físico: Fibra óptica - Dupla Abordagem em Anel. - 24x7 (horas/dias) ininterruptamente;
LINK DE INTERNET DEDICADO: - Secundário; - Operadora: Valesat.	LINK DE INTERNET DEDICADO - SECUNDÁRIO: - IP fixo (04 disponíveis): 177.73.182.202; - Velocidade mínima garantida: 50 Mbps; - Conexão dedicada à Internet full-duplex; - Meio físico: Rádio Digital; - Utilizado para: Link Backup e Balanceamento de tráfego com outros links. - 24x7 (horas/dias) ininterruptamente;

IMPORTANTE: A solução deverá ser capaz de gerenciar todos os atuais links de internet em uso no CRA-SP, além de permitir o crescimento até pelo menos, 700 MB, considerando o tráfego full duplex;

1. DADOS GERAIS DA REDE DO CRA-SP:

1.1. NÚMERO DE USUÁRIOS: em torno de 120 usuários;

1.2. NÚMERO DE COMPUTADORES: em torno de 150 dispositivos, entre desktops, notebooks e servidores.

1.3. SEGUIMENTAÇÕES DE REDE E VLANS:



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 192.168.1.X – Rede principal;
- 192.168.2.X – Rede de telefonia IP;
- 10.36.1.X – Rede Wireless;
- 192.168.10.X – Rede de circuito de CFTV e câmeras IP.

1.4. SISTEMAS OPERACIONAIS:

- SERVIDORES:
 - ✓ Microsoft Windows 2003 Server;
 - ✓ Microsoft Windows 2008 Server;
 - ✓ Microsoft Windows 2012 Server – Standard e Datacenter;
 - ✓ Linux CentOS e Ubuntu;
- WORKSTATIONS:
 - ✓ Microsoft Windows XP;
 - ✓ Microsoft Windows 7;
 - ✓ Microsoft Windows 10.
- SERVIDORES VIRTUALIZADOS:
 - ✓ Plataforma: Microsoft Hyper-V.

1.5. SERVIÇOS DE MENSAGEIRA E COLABORAÇÃO:

- Google G Suite Business;
- Microsoft Outlook;
- Protocolos: SMTP e IMAP;

1.6. FERRAMENTA DE AUTOMAÇÃO DE ESCRITÓRIO;

- MS Office;

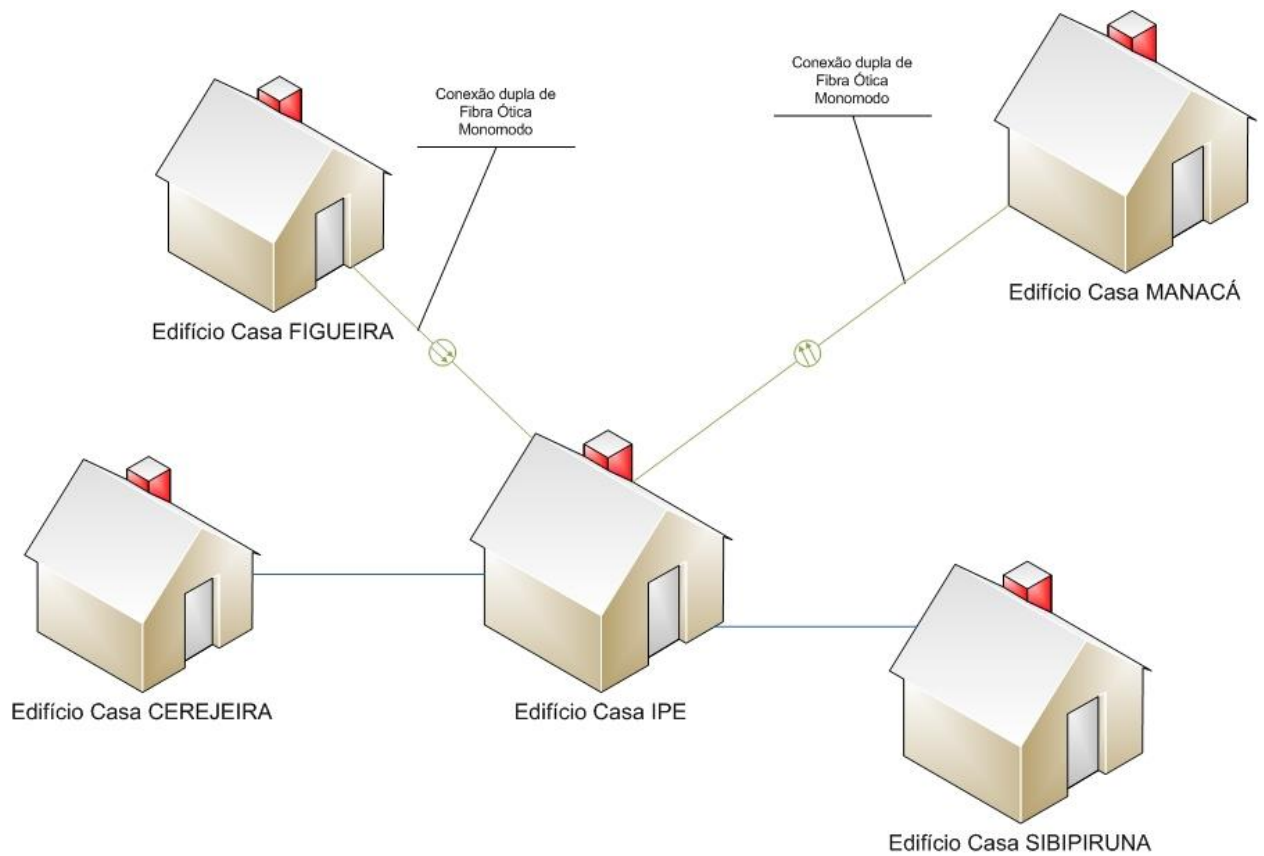
1.7. FERRAMENTAS DE BACKUP;

- NTBackup;
- Ferramentas nativas do sistema operacional Microsoft Windows.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ANEXO IV - COMPLEXO CRA-SP





CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ANEXO V – ROTEIRO DE HOMOLOGAÇÃO DOS SERVIÇOS

1. Amostra dos serviços que será considerada como protótipo funcional da solução de Appliance UTM para Segurança de Borda;

2. CONDIÇÕES PARA HOMOLOGAÇÃO DA CONTRATAÇÃO:

2.1. Este roteiro será utilizado pela equipe técnica do CONSELHO com a finalidade de apurar a real adequação das principais funcionalidades da solução fornecida pela CONTRATADA classificada em primeiro lugar na Licitação.

2.2. Este roteiro baseia-se integralmente nas funcionalidades mínimas especificadas no Documento Técnico.

2.3. A CONTRATADA deverá comprovar todas as funcionalidades deste roteiro, sem exceção, por meio da instalação da “amostra” de um *Appliance* na sede do CONSELHO.

2.4. A CONTRATADA será desqualificada tecnicamente nos seguintes casos:

1.1.1. Caso a CONTRATADA não observe os prazos máximos estabelecidos para a disponibilização da amostra dos serviços, a saber, 10 dias corridos a partir do primeiro dia útil subsequente à data de realização da Licitação ou da data de convocação;

1.1.2. Caso a CONTRATADA não consiga comprovar tecnicamente um ou mais itens do presente roteiro dentro do período de análise técnica a ser realizado pela equipe técnica do CONSELHO, ou seja, dentro do período de 15 dias corridos após a entrega da amostra dos serviços pela CONTRATADA.

2. ROTEIRO DE AFERIÇÕES E TESTES PARA HOMOLOGAÇÃO DA AMOSTRA DE SERVIÇOS:

2.1. Configuração de Filtragem de Pacotes e Configuração:

2.1.1. A CONTRATADA deverá configurar as regras de filtragem de pacotes para permitir a comunicação apenas entre máquinas pertencentes à rede do CONSELHO e serviços pré-determinados, descartando qualquer outro pacote que não tenha sido explicitamente permitido por estas regras.

2.1.2. A CONTRATADA deverá fornecer acesso remoto à console de administração da amostra dos serviços fornecida, via HTTPS e SSH, para consulta, pela equipe técnica do CONSELHO, da tela de exibição, em tempo real, dos pacotes aceitos e rejeitados informando, pelo menos, endereço e porta de origem, endereço e porta de destino, ação tomada (ALLOW, DROP ou REJECT) e número da regra utilizada. Esta tela deverá permitir a utilização de filtros para qualquer um dos campos exibidos.

2.2. Utilização de IDS/IPS Ativo:

2.2.1. A CONTRATADA deverá habilitar os serviços de IDS/IPS ativo, que deverá identificar e neutralizar tentativas de ataques e/ou invasões originadas, pela equipe técnica do CONSELHO, de fora da rede do CONSELHO;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

2.2.2. O IDS/IPS ativo deverá também identificar e neutralizar comunicações suspeitas, com conteúdo malicioso, entre as duas localidades protegidas pelos *appliances* instalados na amostra dos serviços;

2.2.3. Todas as atividades maliciosas e ações tomadas pelo IDS/IPS ativo deverão poder ser visualizadas, por meio de relatórios, pela equipe técnica do CONSELHO, que deverá também conseguir aplicar filtros nestes relatórios utilizando, pelo menos, os seguintes critérios: período de apuração, origem do ataque (IP ou rede), destino do ataque (IP ou rede) e tipo de ataque;

2.3. Controle de Banda e Qualidade de Serviço (QOS);

2.3.1. A CONTRATADA deverá configurar o controle de banda que priorize o tráfego de origem, destino e/ou serviço determinados pela equipe técnica do CONSELHO, comprovado mediante relatório e gráficos.

2.4. Backup e Restore de Configurações;

2.4.1. A equipe técnica do CONSELHO deverá conseguir realizar, remotamente, um back-up das configurações do(s) Firewall(s) por meio da solução de monitoramento que replique suas configurações para todos os firewalls de borda salvando-o em uma pasta compartilhada de qualquer computador pertencente à rede do CONSELHO. Também deverá ser possível realizar o agendamento de back-ups em rede;

2.4.2. Todos os back-ups realizados serão restaurados e deverão funcionar perfeitamente.

2.5. VPN Site-to-Site

2.5.1. A CONTRATADA deverá configurar uma VPN Client no Appliance UTM instalado na amostra dos serviços;

2.5.2. A equipe técnica do CONSELHO deverá conseguir comunicar por meio desta VPN.

2.6. Regras para acesso a serviços de terceiros;

2.6.1. A CONTRATADA deverá configurar e garantir o funcionamento de todas as regras para os serviços descritos no ANEXO 01 A – AMBIENTE COMPUTACIONAL, são eles:

- PUBLICAÇÃO PÁGINAS NA WEB:
- ACESSO A REDE INTERNA (PÁGINAS):
- NAVEGAÇÃO USUÁRIOS REDE LOCAL:
- REGRAS PARA ACESSO A SERVIÇOS DE TERCEIROS:



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ANEXO VI - SERVIÇO DE SUPORTE TÉCNICO E ATUALIZAÇÃO DE VERSÕES

1. REQUISITOS GERAIS:

- 1.1. Os serviços descritos a seguir são aplicáveis a todos os itens das soluções, sejam eles associados ao *Firewall*, ao *Endpoint* e outros;
- 1.2. O atendimento poderá ser feito pela CONTRATADA de modo **remoto** ou **presencial (on site)**. No entanto, **caso o atendimento remoto não esteja sendo efetivo**, a critério do CONSELHO, **poderá este último exigir o comparecimento de técnico da CONTRATADA à sede do CONSELHO em São Paulo/SP, na sede do Conselho**. Seguindo os seguintes critérios:
 - O envio de técnico à sede do CONSELHO não afetará os níveis mínimos de serviço estabelecidos na abertura do chamado em função da prioridade estabelecida;
 - Se entender que o atendimento presencial não está sendo efetivo, o CONSELHO poderá solicitar a substituição do técnico enviado, aplicando-se à substituição os níveis mínimos de serviço da abertura do chamado;
 - A contagem dos prazos não será interrompida para comparecimento presencial ou substituição de técnicos.
 - **Todos os custos relativos a deslocamento, hospedagem e diárias, ficarão a cargo da CONTRATADA.**
 - O CONSELHO definirá modelo para que a CONTRATADA possa realizar atendimento remoto da Solução. Caso opte pela utilização de administração remota, a CONTRATADA deverá arcar com quaisquer custos extraordinários (rede dedicada de dados, aquisição de certificados digitais, clientes VPN, clientes de serviços de terminal, entre outros) que se fizerem necessários para a montagem do ambiente.
- 1.3. O horário de atendimento deverá cobrir, no mínimo, o período de expediente do Conselho, descrito no item **“HORÁRIOS E LOCAL DA PRESTAÇÃO DOS SERVIÇOS”** do **ANEXO 01 – PROJETO BÁSICO**, deste edital;
- 1.4. A CONTRATADA será responsável perante o CONSELHO pela disponibilidade e níveis mínimos de serviço do suporte técnico e do direito de atualização de versão durante a vigência do contrato;
- 1.5. A CONTRATADA será responsável, durante a vigência contratual, pela prestação de suporte técnico à versão da Solução instalada no CONSELHO, mesmo que o suporte do fabricante para essa versão tenha sido descontinuado;
- 1.6. A CONTRATADA deverá providenciar o cadastramento inicial do CONSELHO junto ao fabricante para a abertura de chamados de suporte técnico e para permitir o recebimento de atualização de versões e pacotes de correções.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 1.7. Deverão ser disponibilizados pela CONTRATADA quando for solicitado, relatórios de demandas para todos os eventos de suporte técnico e disponibilização de novas versões ou correções, contendo, quando for o caso, informações sobre o tempo de atendimento (início, fim, suspensões, intercorrências, etc.).
- 1.8. Os tempos máximos para conclusão dos chamados associados a cada prioridade de chamado são estabelecidos no Erro! Fonte de referência não encontrada.;
- 1.9. Toda informação referente ao CONSELHO, que o serviço de suporte técnico vier a tomar conhecimento por necessidade da prestação dos serviços, não poderá ser divulgada a terceiros sem consentimento expresso do CONSELHO, mais detalhamentos sobre confidencialidade e segurança da informação, estão descritos no **ANEXO 01 G – REQUISITOS DE SEGURANÇA DA INFORMAÇÃO**;
- 1.10. O serviço de suporte abrangerá, principalmente, os seguintes serviços:

ITEM	DESCRIÇÃO
1	Aplicações de atualizações (<i>update</i> e <i>upgrade</i>), além do fornecimento de versões ou releases mais recentes dos softwares disponibilizadas pelos fabricantes dos produtos;
2	Aplicações de correções de novos “ <i>patches</i> ” e versões;
3	Auxílio remoto para criação / alteração de configurações, regras ou políticas de segurança, como também a emissão de relatórios e análise de logs;
4	Correções ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades da solução, isto abrange problemas de hardware, software e quaisquer recursos que compõem a solução
5	Dúvidas relacionadas à prestação de serviços, além de funcionalidades da solução e operação dos módulos dos produtos;
6	Realizar atividades e o acompanhamento de Adição / remoção de usuário
7	Realizar atividades e o acompanhamento de Alteração / liberação sites e demais serviços web;
8	Realizar atividades e o acompanhamento de Configuração de <i>Client-to-Lan</i> ;
9	Realizar atividades e o acompanhamento de Configuração de VPN Lan-to-Lan, DMZ, VPN e outros serviços de Firewall e rede;
10	Realizar atividades e o acompanhamento de Mudança e alteração de regras de Controle URL
11	Realizar atividades e o acompanhamento de mudança e alteração de regras de Firewall
12	Realizar atividades e o acompanhamento de Mudança e alteração de regras de IPS;
13	Realizar atividades e o acompanhamento de Mudança e alteração regras Firewall de Aplicação;
14	Problemas relacionados aos serviços de migração de dados e instalação e customização de sistemas;
15	Análise de incidentes de segurança e aplicações de correções e prevenções a ameaças;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

16	Instalações e configurações clientes em equipamentos da rede do Conselho;
17	Análises e ações corretivas, sejam no Firewall ou Endpoint, quanto a bloqueios ou mal funcionamento de serviços executados a partir de dispositivos da rede do Conselho;
18	Análises e ações corretivas, sejam no <i>Firewall</i> ou <i>Endpoint</i> , sobre a performance de escaneamentos (<i>scans</i>) executados pelos de equipamentos da rede do Conselho;

- 1.11. Somente com autorização do CONSELHO os chamados poderão ser encerrados;
- 1.12. A qualquer momento, os chamados poderão ser cancelados pelo CONSELHO. A CONTRATADA somente poderá cancelar chamados com ciência e anuência do CONSELHO;
- 1.13. Caso a CONTRATADA seja obrigada a interromper atendimento em razão de agendamento de atendimento a ser feito pelo CONSELHO, as interrupções serão descontadas dos prazos de atendimento.

2. SOBRE A CENTRAL DE ATENDIMENTO:

- 2.1. A Contratada deverá disponibilizar, através da sua Central de Atendimento e Operações (SOC), número telefônico e correio eletrônico para abertura de chamados, em português, nos dias, **24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco dias) por ano;**
- 2.2. A CONTRATADA deverá ter estrutura de suporte próprio com operação, via SOC, durante toda vigência contratual, para atendimento presencial na sede do Conselho em São Paulo/SP (se necessário), dentro do SLA definido neste certame;
- 2.3. A SOC deverá ser o principal ponto de contato entre a equipe técnica do CRA-SP e a CONTRATADA;
- 2.4. Esta estrutura deverá ser suficiente para realizar todas as atividades de Suporte Técnico e sanar quaisquer problemas;
- 2.5. Deve a CONTRATADA possuir sistema de chamados próprio para gerenciamento dos chamados abertos, permitindo acompanhamento, aferição dos tempos dos chamados até seu encerramento, com detalhamento de todas as ocorrências, e acesso à base de conhecimento. Durante o atendimento, deve ser registrado, no mínimo, o momento da abertura, de início de atendimento, de encerramento e demais ações realizadas pelo fabricante;
- 2.6. Deve a CONTRATADA permitir o cadastramento mínimo de dez usuários indicados pelo CONSELHO para abertura e gerenciamento de chamados;
- 2.7. Os chamados de suporte poderão ser abertos via telefone ou via e-mail, no **regime 24x7;**
- 2.8. **A CONTRATADA deverá informar ao CONSELHO número de telefone (custo de ligação local ou gratuita) e/ou endereço da página web para a abertura dos chamados técnicos junto ao fabricante e as credenciais de acesso necessárias para sua utilização;**



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 2.9. Todas as solicitações devem ser registradas e a elas atribuídos nº de protocolo para identificação e acompanhamento das ocorrências, sendo o registro feito em sistema WEB específico para este fim, além disto:
- Os membros da equipe técnica do CRA-SP devem ser cadastrados e receberem credencias de acesso ao sistema Web para acompanhamento das ocorrências;
- 2.10. Os chamados cadastrados serão classificados de acordo com os níveis de prioridade definidos no Erro! Fonte de referência não encontrada.. Os chamados poderão ter sua severidade alterada a qualquer tempo, a critério do CONSELHO, considerando alterações das condições de impacto no negócio ou a conveniência da administração;
- 2.11. O serviço de suporte do fabricante pode possuir níveis diferentes de prioridade de chamado em relação aos anteriormente definidos, desde que uniformes para todos os clientes do software e aprovados pelo CONSELHO. Caso haja níveis diferentes de prioridade, deve a licitante apresentá-los em sua proposta comercial, especificando quais prioridades do fabricante correspondem a quais prioridades estabelecidas no Erro! Fonte de referência não encontrada., de forma a permitir o julgamento da proposta pelo CONSELHO e a posterior aferição dos níveis de serviço durante a execução do contrato;
- 2.12. O atendimento de chamados será do tipo “on site”, mediante manutenção corretiva nas dependências do Conselho em São Paulo / SP, e deverá cobrir todo e qualquer defeito apresentado, incluindo:
- O fornecimento e a substituição de equipamentos;
 - Peças e/ou componentes;
 - Ajustes, reparos e correções necessárias para recolocar a solução em seu perfeito estado de funcionamento, sejam estas para hardware quanto para o software.
- 2.13. A abertura de chamado feita pela CONTRATADA junto a fabricante de hardware e / ou software, decorrente de demanda aberta pelo CONSELHO, **não representará interrupção na contagem dos prazos de atendimento**. Em casos excepcionais, desde que configurado e comprovado defeito sobre o qual a CONTRATADA não possua domínio de modificação, o tempo de resolução do chamado pelo fabricante poderá ser considerado para fins de avaliação de impacto no tempo de atendimento e resolução do incidente;
- 2.14. Para os chamados de prioridade alta (nível-3), uma vez iniciado o atendimento, este deve prosseguir ininterruptamente, inclusive fora do horário comercial, até que tenham sido concluídos ou estabelecida solução de contorno que permita retornar à Solução ao estado normal de utilização;

3. TROUBLESHOOTING



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 3.1. Para os casos de problemas mais complexos relacionados a lentidão e/ou mau funcionamento de serviços, sejam eles do *Firewall* ou *Endpoint*, a equipe técnica da contratada irá, em conjunto com a equipe técnica do Conselho, executar uma série de procedimentos para análises e verificações de rede, "*Troubleshooting*", para apontar de forma assertiva o agente causador do problema apresentado.

4. ATUALIZAÇÃO DE VERSÕES:

- 4.1. O direito de atualização de versão do software será fornecido durante o período de vigência do contrato e deverá abranger toda a solução e todos os softwares de apoio fornecidos pela CONTRATADA;
- 4.2. A atualização de versão deve contemplar o fornecimento de todos os novos *releases* dos softwares fornecidos, bem como o fornecimento dos releases corretivos;
- 4.3. Além do suporte técnico fornecido pelos fabricantes da Solução e softwares de apoio, caberá à CONTRATADA, durante a vigência contratual, prestar apoio ao CONSELHO durante a atualização de versão. O apoio consistirá na presença de técnicos da CONTRATADA para, juntamente com pessoal técnico do CONSELHO, executar atualização de versão. O apoio consistirá ainda na solução de problemas detectados após a implantação da nova versão, inclusive os relacionados às customizações efetuadas, sejam pelo CONSELHO ou pela CONTRATADA;
- 4.4. O serviço de suporte técnico e atualização de versão é o fornecido pelo fabricante do software e / ou hardware, que segue termo de suporte próprio e padronizado, aplicável a todos os clientes do software que contratam este serviço;
- 4.5. O suporte técnico e direito de atualização de versão deverão ser adquiridos pela CONTRATADA junto aos fabricantes da solução e dos softwares de apoio fornecidos pela CONTRATADA, em nome do CONSELHO, com termo inicial do serviço idêntico à data de emissão das licenças as quais se refere. **Deverá o documento comprobatório da contratação do suporte, emitido pelo fabricante, fazer menção às licenças abrangidas pelo suporte. Não será aceito suporte contratado para licenças que não as entregues ao CONSELHO nem suporte com data de início anterior à data de emissão das licenças;**
- 4.6. O serviço de suporte técnico e direito de atualização de versão deverão abranger todo o ambiente de execução e período de contrato.

5. REPOSIÇÃO DE HARDWARE EM CASO DE FALHAS:



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- 5.1. A CONTRATADA deverá disponibilizar a substituição imediata “Spare Part”, do(s) equipamento(s) obedecendo ao nível de SLA (*Service Level Agreement*) Acordo de Nível de Serviços;
- 5.2. Uma vez detectada a necessidade da troca do *appliance*, a CONTRATADA deverá efetuar a substituição do equipamento na sede do Conselho e todas as atividades e configurações necessárias para a restauração de todos os serviços que compõe a solução em até **02 (duas) horas corridas**;
- 5.3. Todos os custos e logística para o deslocamento da equipe técnica do Conselho, será responsabilidade da CONTRATADA.

6. EQUIPE TÉCNICA DA CONTRATADA

- 1.1. A licitante deverá possuir Certificação emitida pelo fabricante do Produto UTM-Firewall ofertado;
- 1.2. A CONTRATADA deverá comprovar que possui em seu quadro de funcionários no mínimo **01 (um) profissionais com certificação oficial do fabricante** do produto UTM ofertado;
- 1.3. A equipe técnica da CONTRATADA que manterá relacionamento direto com o CONSELHO deverá ser formada pelos perfis descritos nesta seção. Outros perfis poderão ser agregados à equipe a critério da CONTRATADA. Em função do contato direto, deverão exercer suas atividades no local de execução do contrato, conforme definido no Edital.
- 1.4. Um **preposto**, que será a pessoa formalmente indicada pela CONTRATADA para representá-la técnica e operacionalmente durante a execução do contrato. Esse profissional será o principal ponto de contato com o CONSELHO, devendo ser alocado ao longo de todo o contrato. No caso da CONTRADA decidir indicar uma nova pessoa, o CONSELHO deverá ser informado.
- 1.5. São responsabilidades do preposto:
 - Gestão operacional do contrato;
 - Requisição e alocação de todos os recursos necessários, inclusive aqueles eventualmente fornecidos pelo CONSELHO, como acessos, informações, recursos materiais, entre outros;
 - Gestão das pessoas alocadas à equipe técnica e administrativa da CONTRATADA;
 - Gestão em todas as dimensões previstas no manual de gerenciamento de projetos PMBoK (quarta edição), incluindo o registro de atas de reunião e outras documentações necessárias;
 - Revisão, ajustes e entrega de todos os produtos previstos no Edital;
 - Entrega de documentação, papéis de trabalho e bases de dados;
 - Gestão de qualidade de serviços, para assegurar o atendimento dos níveis de serviços estabelecidos e, em caso de desvios, identificar e aplicar medidas corretivas efetivas;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- Participar, quando convocado pelo CONSELHO, de reuniões de alinhamento de expectativas contratuais.
- 1.6. Profissionais no papel de **técnicos de implantação**, em quantidade definida pela CONTRATADA, com responsabilidade de instalação da Solução e de todo serviço de implantação, descrito no ITEM 2: SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DE TODOS OS EQUIPAMENTOS E AMBIENTE DE REDE, descrita no ANEXO 01 – TERMO DE REFERENCIA, deste edital. A alocação destes profissionais será por todo o prazo definido no planejamento da implantação, devendo possuir, no mínimo, as seguintes qualificações:
- **Certificado oficial do fabricante, em vigência, voltado para as áreas de implantação nas quais os profissionais atuarão;**
 - **Experiência mínima de um 01 (ano) em implantação da Solução CONTRATADA;**
 - A comprovação deve ser por meio de atestado expedido por pessoa jurídica de direito público ou privado onde o sistema foi implantado.
- 1.7. **Comprovação de capacidade técnico-profissional.**
- Na reunião de abertura e em todas as ocasiões em que a CONTRATADA promover alteração na equipe, deverá relacionar, com nome completo, identidade, CPF, comprovantes de experiência exigidas no Edital, comprovantes de qualificação técnica e tipo de vínculo com a CONTRATADA, os componentes de sua equipe técnica, alocados nos papéis anteriormente descritos, que venham a ter contato direto com o CONSELHO.
 - Essa relação, acompanhada dos documentos comprobatórios e respectivas cópias digitalizadas, deverá ser entregue ao CONSELHO na reunião de abertura e na data em que a CONTRATADA propuser a alteração da equipe. Após conferência no ato de entrega, o CONSELHO devolverá os documentos originais.
- 1.8. **Recusa e substituição de profissionais**
- O CONSELHO poderá recusar a participação de profissional no projeto ou exigir a substituição de profissional que, a seu critério, não possuam qualificações técnicas necessárias, possua comportamento inadequado a prestação dos serviços para o CONSELHO, ou cuja qualificação demonstrada mostre-se aquém do necessário para garantir a qualidade dos produtos a serem entregues e dos serviços desempenhados.
 - A substituição de profissionais deverá ser precedida da comprovação de que os substitutos cumprem os requisitos mínimos exigidos no Edital, devendo haver anuência da parte do CONSELHO.
 - A substituição de profissionais, por iniciativa da CONTRATADA ou exigência do CONSELHO, não poderá acarretar prejuízos ao CONSELHO, sejam eles de ordem financeira ou relativos a prazos e à qualidade dos serviços prestados. O prazo máximo para substituição será de cinco dias úteis.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ANEXO VII – NÍVEIS MÍNIMOS DE SERVIÇO (SLA)

1. Os serviços terão atendimento garantido nos horários, descritos no item **“HORÁRIOS E LOCAL DA PRESTAÇÃO DOS SERVIÇOS”**, deste edital;
2. Todas as demandas encaminhadas pelo Conselho à CONTRATADA, serão classificados de acordo com os requisitos de Níveis de serviço, que são critérios objetivos e mensuráveis estabelecidos com a finalidade de aferir e avaliar fatores relacionados à solução CONTRATADA, principalmente qualidade, desempenho e disponibilidade;
3. Para mensurar esses fatores serão utilizados os indicadores do quadro adiante, com respectivos limites:

TIPO DO PROBLEMA	CRITICIDADE	PRAZO MÁXIMO DE ATENDIMENTO	PRAZO MÁXIMO DE SOLUÇÃO
Erros ou falhas	Emergencial	01 (uma) hora	04 (quatro) horas
	Falha intermitente	04 (quatro) horas	08 (oito) horas
	Importante (normal)	04 (quatro) horas	24 (vinte e quatro) horas
Dúvidas e ações operacionais	Emergencial	01 (uma) hora	04 (quatro) horas
	Falha intermitente	04 (quatro) horas	24 (vinte e quatro) horas
	Importante (normal)	06 (seis) horas	36 (trinta e seis) horas
Solicitação de mudança ou visitas programadas	Crítico	Negociado entre as partes	
	Grave		
	Importante		

4. Todos os valores associados a horas na tabela acima, devem ser interpretados como **HORAS ÚTEIS**;
5. Os prazos de atendimento serão calculados em horas dentro do horário de expediente do Conselho, descrito no item **“HORÁRIOS E LOCAL DA PRESTAÇÃO DOS SERVIÇOS”**, deste edital;
6. Os prazos descritos na tabela acima, começam a ser contados a partir do por início do atendimento. Entende-se por **INÍCIO DO ATENDIMENTO**, o primeiro contato (seja por e-mail, telefone ou qualquer outra forma);
7. Para efeito de apuração do prazo de atendimento de um chamado, será considerada como **“DATA E HORA DA ABERTURA DO CHAMADO”** a data e hora que a CONTRATADA recebeu o pedido e como **“DATA E HORA DA ENTREGA”** a data em que o Conselho recebeu a informação da solução do problema;
8. Para a abertura do chamado, a equipe de suporte da CONTRATADA, deverá registrar a ocorrência, informar formalmente ao solicitante e demais envolvidos ao processo de atendimento, e dar prosseguimento no tratamento do problema reportado;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

9. Entende-se como “**PRAZO MÁXIMO DE ATENDIMENTO**”, o intervalo entre o início do atendimento e o registro formal da demanda;
10. Entende-se como “**PRAZO MÁXIMO DE SOLUÇÃO**”, o intervalo entre o registro formal da demanda e o término integral do atendimento;
11. Entende-se por “**TÉRMINO INTEGRAL DO ATENDIMENTO**”, a apresentação ou aplicação da solução e homologação do usuário requisitante;
12. A classificação dos chamados quanto ao **TIPO DE PROBLEMA** e **GRAU** é de responsabilidade do Conselho, que é quem deverá informar à CONTRATADA sobre as prioridades de cada demanda. Esta deverá obedecer às seguintes definições:

13. TIPOS DE PROBLEMAS:

- | | |
|---|---|
| 13.1. ERROS OU FALHAS: | <ul style="list-style-type: none">• Todo e qualquer incidente que gere mau funcionamento de um ou vários recursos das soluções implementadas;• Qualquer recurso, seja ele de hardware ou software, que passe a funcionar de forma incorreta ou de modo diferente do que estava previsto. |
| 13.2. DÚVIDAS E AÇÕES OPERACIONAIS: | <ul style="list-style-type: none">• Auxílio em procedimentos operacionais executadas pela equipe técnica do Conselho. |
| 13.3. SOLICITAÇÃO DE MUDANÇA OU VISITAS PROGRAMADAS: | <ul style="list-style-type: none">• Manutenção e/ou atualizações de firmware, versões ou softwares em geral;• Manutenções ou configurações em geral que podem ser programas. |

14. CRITICIDADE:

- | | |
|---------------------------|---|
| 14.1. EMERGENCIAL: | <ul style="list-style-type: none">• Falha no sistema, fora de operação e necessidade de troca do equipamento;• Perda parcial ou total de funcionalidade do produto;• Impacto geral na organização ou nos sistemas relacionados;• Prejudica a prestação dos serviços;• Impede o cumprimento de obrigações legais do Conselho com |
|---------------------------|---|



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

prazos estabelecidos e inadiáveis e compromete a imagem do Conselho.

- 14.2. **FALHA INTERMITENTE:**
- Falhas intermitentes em serviços suportados que torne o ambiente lento ou com baixa erros que se repetem;
 - Falhas em alguma funcionalidade da solução, mas sem interrupções.
- 14.3. **IMPORTANTE (NORMAL):**
- Problemas que não resultem em impactos mais sérios ao Conselho;
 - Problemas que podem ser contornados através de outros procedimentos, mas que requerem atendimento técnico.
 - Problemas que resultem em impactos isolados no ambiente.

15. A CONTRATADA disponibilizará ferramenta on-line para que o CONSELHO possa acompanhar as solicitações, seus prazos, as entregas e as previsões de atendimento;
16. Quaisquer problemas que venham a comprometer o alcance dos níveis de serviços estabelecidos devem ser imediatamente comunicados à Conselho, que colaborará com a CONTRATADA na busca da melhor solução para os problemas;
17. Os prazos máximos de atendimento das solicitações somente poderão ser ajustados com autorização expressa do CONTRATANTE;
18. A classificação das solicitações pelo TIPO e CRITICIDADE é de responsabilidade do CONTRATANTE, de acordo com as definições acima, no momento do pedido da solicitação. Caso esta não o faça, fica a critério de a CONTRATADA classificá-las;

19. CRITÉRIOS DE AVALIAÇÃO:

- 19.1. Os serviços prestados pela CONTRATADA serão mensalmente avaliados;
- 19.2. Esta avaliação será feita a partir de dados obtidos na ferramenta on-line que a CONTRATADA disponibilizará ao Conselho para acompanhamento dos serviços;
- 19.3. Poderão ser aplicadas sanções a CONTRATADA, conforme desempenho insatisfatório;
- 19.4. Desempenho insatisfatório correspondente ao não atendimento dos NÍVEIS MÍNIMOS DE SERVIÇO (SLA) e o Conselho, por intermédio de seus responsáveis pela Fiscalização do Serviço e do Contrato, aplicará as penalidades, garantida a prévia defesa (art. 87, §2º, da Lei nº 8.666/93):

- Para **01 (UM) MÊS DE DESEMPENHO INSATISFATÓRIO** poderá ser aplicada a penalidade de **ADVERTÊNCIA**;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

- Para **02 (DOIS) MESES SEGUIDOS DE DESEMPENHO INSATISFATÓRIO** poderá ser aplicada a penalidade de **MULTA DE 5% DO VALOR DO CONTRATO**;
- Para **03 (TRÊS) MESES SEGUIDOS DE DESEMPENHO INSATISFATÓRIO** poderá ser aplicada a penalidade de **RESCISÃO UNILATERAL DO CONTRATO**.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ANEXO VIII - REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

1. A Solução de TI deverá observar a Norma Brasileira ABNT NBR ISO/IEC 27002, código de prática para a gestão da segurança da informação;
2. A Solução de TI deverá estar aderente às normas de segurança estabelecidas pela CONSELHO, constantes na sua **Política de Segurança de Tecnologia da Informação**;
3. Os requisitos de segurança definidos no Edital e em normas de segurança da CONTRATADA aplicam-se, no que for cabível, à toda a Solução CONTRATADA, incluindo todos softwares de apoio e todos os produtos que vierem a ser utilizados durante a vigência do contrato.

4. CONTROLE DE ACESSO

- 4.1. As soluções descritas neste certame, deve possuir recursos para integração às soluções de controle de acesso baseadas em LDAP ou *Active Directory*;
- 4.2. As soluções deverão apresentar funcionalidades de controle de acesso (logs de acesso), com o objetivo de gerenciar e monitorar todas as operações do sistema, por meio de:
 - Acesso seletivo a funcionalidades da Solução CONTRATADA, com visibilidade dos itens de menu de acordo com o perfil de acesso;
 - Acesso seletivo a visualização e edição de campos de interfaces;
 - Acesso seletivo a tabelas e campos da base de dados;
 - Acesso seletivo a registros de banco de dados.
- 4.3. As soluções deverão permitir que o gestor da informação ajuste os perfis de acesso quando existirem mudanças na classificação de informações ou nas regras de controle de acesso a dados;
- 4.4. As soluções deverão permitir e prover ao CONSELHO perfil especial com privilégio de acesso a todas as tabelas e logs da Solução implantada;
- 4.5. As soluções deverão prover mecanismos de segurança e controle de acesso que impeçam a visualização e edição informações de negócio do CONSELHO por usuários que não tiverem com as devidas permissões de acesso ao conteúdo, sempre com registro de log de auditoria.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ANEXO IX – TERMO DE CONFIDENCIALIDADE

1. COMPROMISSO DE SIGILO

- 1.1. A empresa licitante interessada em participar do processo licitatório deverá apresentar **termo de compromisso de sigilo** que resguarde a confidencialidade das informações a que eventualmente tenham acesso em decorrência de suas atividades durante a vistoria e verificação da amostra;
- 1.2. Após firmado o contrato de prestação de serviços, a CONTRATADA deve providenciar que **os profissionais que atuarem em função do contrato estejam obrigados**, antes de iniciarem seu trabalho, **a conhecer, aceitar e assinar termo de compromisso de sigilo que resguarde a confidencialidade das informações** a que eventualmente tenham acesso em decorrência de suas atividades contratuais. Esses termos de responsabilidade devem estar à disposição do CONSELHO, que pode solicitar sua apresentação a qualquer tempo;
- 1.3. A CONTRATADA deve manter atualizada relação de funcionários que poderão atuar junto ao CONSELHO na execução do contrato. Em caso de desligamento, a CONTRATADA deve imediatamente retirar todas as credenciais que permitam ao funcionário fazer qualquer acesso à Solução provida e informar o fato à CONSELHO.
- 1.4. No mesmo termo, haverá também o compromisso de o profissional da empresa observar todas as regras de segurança estabelecidas pela CONTRATADA.

2. DO TRATAMENTO DE DADOS

- 2.1. A CONTRATADA e o Conselho, concordam que o tratamento dos dados fornecidos/recebidos por qualquer das partes pela outra parte em razão deste Contrato deverá ser realizado em consonância à legislação brasileira, inclusive no tocante às diretrizes previstas na Lei nº 13.709/2018 (“Lei Geral de Proteção de Dados”), sendo certo que deverão ser verificados e respeitados todos os tipos de dados previstos na legislação aplicável, conforme cada caso concreto em questão (inclusive com condutas para anonimizar os dados, caso exigido por lei e/ou se fizer necessário);
- 2.2. As partes apenas tratarão os tipos de dados relacionados com as categorias de titulares de dados para efeitos do presente Contrato e para os fins específicos de cada caso, ou conforme instruções fornecidas, por escrito, pela outra Parte, não devendo tratar, transferir, modificar, aditar ou alterar os dados nem divulgar ou permitir a divulgação dos dados a terceiros de forma que não esteja de acordo com as instruções documentadas e/ou aprovadas, por escrito, pela outra Parte, a menos que o tratamento seja autorizado ou exigido por qualquer lei aplicável à



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

qual Parte estiver sujeita, em cujo caso a Parte deverá, na medida do permitido por essa lei, informar, por escrito, a outra Parte desse requisito legal antes de tratar esses dados.

2.3. As Partes declaram e garantem que **tratarão todos os dados como estritamente confidenciais** e que informarão todos os seus funcionários, representantes, contratados e/ou subcontratados envolvidos no tratamento dos dados acerca da natureza confidencial desses dados. As Partes tomarão medidas razoáveis para garantir a confiabilidade de qualquer funcionário, representante, contratado e/ou subcontratado que possa ter acesso aos dados, assegurando em cada caso que o acesso seja estritamente limitado àquelas pessoas ou partes que precisem acessar os respectivos dados, conforme estritamente necessário para os fins estabelecidos neste Contrato, no contexto dos deveres dessa pessoa ou parte perante as Partes.

2.4. As Partes assegurarão que todas essas pessoas ou partes envolvidas no tratamento de dados:

- (i) tenham realizado treinamento adequado em relação às Leis Geral de Proteção de Dados;
- (ii) estejam sujeitas a compromissos de confidencialidade (dos quais uma cópia deve ser fornecida a pedido do Controlador);
- e (iii) estejam sujeitas a autenticação de usuário e processos de login ao acessar os dados.

2.5. Sem prejuízo de quaisquer outras normas de segurança acordadas pelas Partes, as Partes deverão implementar medidas técnicas e organizacionais apropriadas para garantir um nível de segurança dos dados adequado ao risco, tomando todas as medidas necessárias de acordo com as diretrizes Leis Geral de Proteção de Dados, incluindo, mas sem limitação, os artigos 46 a 49 desta lei. Ao avaliar o nível adequado de segurança, o Operador levará em consideração, em particular, os riscos apresentados pelo tratamento, especialmente de destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados transmitidos, armazenados ou de outra forma tratados. As medidas técnicas e organizacionais incluirão, em todo caso, medidas razoáveis para:

- Assegurar que os dados possam ser acessados somente por pessoas autorizadas para os fins estabelecidos neste Contrato;
- Proteger os dados contra destruição acidental ou ilegal, perda ou alteração acidental, armazenamento, tratamento, acesso ou divulgação não autorizados ou ilegais;
- Identificar vulnerabilidades no que diz respeito ao tratamento de dados em sistemas utilizados para prestar serviços à outra Parte; e
- Dentre outras condutas pertinentes previstas na Lei Geral de Proteção de Dados.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

2.6. As Partes reconhecem que os requisitos de segurança estão em constante mudança e que a segurança efetiva requer avaliação frequente e melhorias regulares em medidas de segurança desatualizadas. As Partes avaliarão, portanto, de forma contínua, as medidas técnicas e organizacionais implementadas de acordo com esta Cláusula, restringindo, suplementando e melhorando essas medidas, a fim de manter a conformidade com as Leis Geral de Proteção de Dados.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ANEXO X - MODELO DE PROPOSTA COMERCIAL

Fornecedor:

CNPJ:

Endereço:

Bairro

Telefone:

E-mail:

Inscrição Estadual:

Cidade:

Estado:

Fax:

Pelo presente apresentamos proposta comercial para fornecimento de solução integrada de segurança de perímetro no padrão *Next Generation Firewall* – NGFW/UTM, conforme especificações constantes no ANEXO 01 – TERMO DE REFERÊNCIA deste edital do Pregão nº/2020 e demais anexos.

O projeto se dará através dos itens abaixo:



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

DISCRIMINAÇÃO DOS CUSTOS - RESUMO				
ITEM	DETALHAMENTO		DIVISÃO DO ORÇAMENTO EM PORCENTUAIS (%) LIMITES SOBRE VALOR GLOBAL	CUSTOS
PROJETO DE IMPLANTAÇÃO (A)	Serviço de implantação da solução, contemplando: - instalação e configuração de todos os equipamentos, softwares e demais recursos que compõem a solução, no ambiente de rede do CRA-SP; - Serviço de treinamento das soluções contratadas.	Implantação	5%	R\$ -
OPERAÇÃO EM PRODUÇÃO E SUPORTE TÉCNICO CONTINUO (B)	Dispositivo (Appliance) de controle de acesso lógico no padrão UTM (Gerenciamento Unificado de Ameaças), com Licenciamento de todos os softwares e recursos acerca da solução;	Mensal	95%	R\$ -
	Solução software de Endpoint para, no mínimo, 150 usuários/computadores, contemplando: - Licenciamento de software; - Implantação; - Operação.	Mensal		
	Serviço de monitoramento remoto, 24x7: - NOC (Network Operations Center), próprio e especializado; - Plataforma/Software próprio para monitoramento dos principais hosts e serviços de rede do CRA-SP.	7x24		
	Serviço de suporte técnico especializado "on site": - Gestão de incidentes e suporte técnico especializado com SLA; - Workshop de segurança para usuário final; - Consultoria para política de segurança; - Análise de vulnerabilidade; - Visita semestral de especialista; - Consultoria para serviço de análise de vulnerabilidade e teste de penetração (pentest).	Horário Expediente CRA-SP		
VALOR GLOBAL (A + B)			100%	R\$ -

- a) VALOR GLOBAL DO CONTRATO PARA 36 MESES: R\$ (.....)
- b) **Prazo de entrega:** conforme edital e seus anexos;
- c) **Local de entrega:** conforme edital e seus anexos;
- d) **Forma de Pagamento:** Conforme contrato.
- e) **Validade da proposta:** 60 (sessenta) dias contados da data da sessão pública.



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

.....de.....de 2020.

Assinatura do representante legal

Cargo:

Carteira de identidade n.º:

CPF n.º

**PREENCHIDA EM PAPEL TIMBRADO DA EMPRESA E ASSINADA POR SEUS
REPRESENTANTES LEGAIS OU PROCURADOR (es) DEVIDAMENTE HABILITADO (s)**



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ANEXO XI – MODELO DE COMPROVANTE DE QUALIFICAÇÃO TÉCNICA

A (nome da empresa cliente da licitante), situada no (endereço) declara que a empresa (nome da empresa licitante) forneceu o sistema aplicativo e os serviços de implantação, migração de dados e a consultoria em desenvolvimento ou customização do Sistema Integrado de Recursos Humanos e Folha de Pagamento, como também todo Treinamento e Suporte técnico necessário, conforme as especificações abaixo:

- Serviços realizados:
 - Escopo detalhado:
 - Caracterização do contratante (órgão da Administração Pública ou Empresa Privada):
 - Número de usuários da rede computacional:
 - Data de início da implantação:
 - Data de término da implantação:
 - Data de início da operação da solução em ambiente de produção:
 - Descrição resumida dos serviços realizados:
 - Implantação:
 - Treinamento:
 - Suporte técnico:
 - Descrição resumida do ambiente tecnológico:
 - Arquitetura de ambiente de rede:
 - Software gerenciador de banco de dados utilizado:
 - Plataforma/Software próprio para monitoramento:
-, ... de 2020.

Assinatura do representante legal _____

Cargo:

**PREENCHIDA EM PAPEL TIMBRADO DA EMPRESA E ASSINADA POR SEUS
REPRESENTANTES LEGAIS OU PROCURADOR (es) DEVIDAMENTE HABILITADO
(s)**



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ANEXO XII - DECLARAÇÕES

Ao
CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO
Rua Estados Unidos, 889 – Jd. América
São Paulo – SP

Para fins de participação no Pregão nº/2020, a licitante
declara:

1. PLENO ATENDIMENTO AOS REQUISITOS DE HABILITAÇÃO

Sob as penas da Lei, conhecer e aceitar as condições constantes do certame e que atende plenamente aos requisitos necessários para a habilitação.

2. REGULARIDADE PERANTE O MINISTÉRIO DO TRABALHO

Sob as penas da lei, que, nos termos do parágrafo 6º do artigo 27 da Lei n.º 6.544, de 22 de novembro de 1989, e Lei Federal n.º 9.854 de 27 de outubro de 1999, encontra-se em situação regular perante o Ministério do Trabalho, no que se refere à observância do disposto no artigo 7º da Constituição Federal.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz (). x.

3. FATO IMPEDITIVO

Sob as penas da lei, que, até a presente data, inexistem fato(s) impeditivo(s) para sua habilitação, obrigando-se a comunicar a superveniência de qualquer fato impeditivo.

1. ELABORAÇÃO INDEPENDENTE DA PROPOSTA

Sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

a) a proposta apresentada para participar do Pregão Eletrônico nº ____, foi elaborada de maneira INDEPENDENTE pela (nome da empresa) _____ e o conteúdo da proposta não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº ____, por qualquer meio ou por qualquer pessoa;

b) a intenção de apresentar a proposta elaborada para participar do Pregão Eletrônico nº ____, não foi informada, discutida ou recebida de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº ____, por qualquer meio ou por qualquer pessoa;

c) que não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de outro participante potencial ou de fato do Pregão Eletrônico nº ____, quanto a participar ou não do referido certame;

d) que o conteúdo da proposta apresentada para participar do Pregão Eletrônico nº ____ não será, no todo ou em parte, direta ou indiretamente comunicado ou discutido com qualquer outro participante potencial ou de fato do Pregão Eletrônico nº ____, antes da adjudicação do objeto do certame;



CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

e) que o conteúdo da proposta apresentada para participar do Pregão Eletrônico nº____, não foi, no todo ou em parte, direta ou indiretamente informado, discutido ou recebido de qualquer integrante do CRA-SP antes da abertura oficial das propostas;

f) que está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

....., ... de 2020.

ASSINATURA DO REPRESENTANTE LEGAL:

Nome/Cargo:

Carteira de identidade n.º:

CPF n.º

EMPRESA:

CNPJ: