



PROCURADORIA GERAL DO ESTADO

ÍNDICE

1. DO OBJETO	2
2. DA JUSTIFICATIVA	2
3. DO DETALHAMENTO DO OBJETO	4
4. DOS LOCAIS PARA A PRESTAÇÃO DO SERVIÇO	5
5. DO QUANTITATIVO DOS PRODUTOS	7
6. DAS ESPECIFICAÇÕES, COMPOSIÇÕES E CARACTERÍSTICAS TÉCNICAS DOS SERVIÇOS DE PROTEÇÃO CORPORATIVA DE ENDPOINT	7
7. DA IMPLANTAÇÃO DOS SERVIÇOS DE PROTEÇÃO CORPORATIVA DE ENDPOINT	22
8. DOS SERVIÇOS ESPECIALIZADOS DE SUSTENTAÇÃO DOS SOFTWARES CORPORATIVOS de ANTIVÍRUS.....	23
9. DO PRAZO DE VIGÊNCIA	27
10. DO PRAZO DE EXECUÇÃO DE PLANEJAMENTO, FORNECIMENTO E IMPLANTAÇÃO DOS SERVIÇOS.....	27
11. DA ENTREGA, TESTES DE CONFORMIDADE E ACEITE DOS SOFTWARES E DOS SEUS COMPLEMENTOS	28
12. ACORDO DE NÍVEL DE SERVIÇO - ANS (MANUTENÇÃO E SUPORTE TÉCNICO REMOTO DOS PRODUTOS)	30
13. DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE	32
14. DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA.....	33
15. QUALIFICAÇÃO TÉCNICA	35
16. DA FISCALIZAÇÃO	35
17. DAS CONDIÇÕES DE PAGAMENTO	37
18. DA GARANTIA CONTRATUAL	38
19. DAS SANÇÕES ADMINISTRATIVAS	38
20. DA VISTORIA.	39
21. DAS CONSIDERAÇÕES FINAIS	39



PROCURADORIA GERAL DO ESTADO

TERMO DE REFERÊNCIA AQUISIÇÃO DE LICENCIAMENTO DE ANTIVÍRUS

1. DO OBJETO

- 1.1 Contratação de empresa especializada para prestar serviços de proteção corporativa de *endpoint*, incluindo a implantação, a sustentação e o fornecimento de softwares corporativos de antivírus com atualizações de versões, conforme condições, quantidades e exigências estabelecidas neste instrumento, para atendimento das necessidades da Procuradoria Geral do Estado – PGE/RJ.

2. DA JUSTIFICATIVA

- 2.1 Com o crescimento da rede de computadores da PGE-RJ interligada à internet, bem como o uso massivo de sistemas, serviços web e/ou de dispositivos de armazenamento externo, que se conectam aos dispositivos de computação através de interface física, como a USB ou uma rede sem fio, se faz necessário ter uma solução tecnológica que proteja esses equipamentos/dispositivos, dos acessos indevidos, pragas virtuais, roubo de informações entre outros, a fim de que o serviço-fim da Instituição seja prestado ao Estado e ao cidadão, de forma segura e confiável.

Atualmente, a PGE possui um contrato vigente de fornecimento de licenças e serviços de suporte e manutenção dos softwares corporativos de antivírus, instalada no seu ambiente tecnológico, cujo prazo não poderá mais ser prorrogado. Desta forma, sem a cobertura dessa fundamental ferramenta tecnológica, nosso ambiente de TI ficará parcialmente desprotegido e vulnerável às ameaças virtuais.

Objetivando evitar a ocorrência de tal situação supra de falta de contrato, torna-se imprescindível a contratação de um novo serviço de proteção corporativa de *endpoint*, a fim de substituir o atual. Ademais, foi analisado o modelo atual de gestão dos serviços e a qualidade prestada ao usuário final da tecnologia, o que nos permitiu concluir há necessidade de melhoramento e especialização da gestão desse tipo de serviço pelo alto impacto que pode causar a organização. Um dos motivos identificados está relacionado a falta de profissionais especialistas nessa tecnologia no quadro de pessoal da PGE, em parte pela dificuldade de treinamento, mas também pela rápida evolução desse tipo de tecnologia para fazer frente aos inúmeros ataques e invasões a sites e redes de computadores, que parte são reportados publicamente na mídia e nos websites especializados



PROCURADORIA GERAL DO ESTADO

(ex. www.cert.Br).

Outro ponto importante a se observar, é a Lei Geral de Proteção de Dados Pessoais (LGPD) - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, que entrará em vigor em 2021, que torna obrigatório a definição de mecanismos formais que visem auxiliar no controle sobre o tratamento de dados nas instituições conforme abaixo:

"Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

"Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. "

"Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

"Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término."

Por fim, justifica-se a duração contratual pelo período de 38 (trinta e oito) meses, devido ao alto impacto e à alta complexidade de ativação dos serviços na rede corporativa. Tal ativação implica na remoção do atual antivírus e instalação do novo em todos os equipamentos de processamento conectados à rede da PGE-RJ, o que implicará na mobilização das equipes de infraestrutura de TI e do atendimento ao usuário, gerando custos administrativo, técnico e operacional, para a execução durante meses, dessas atividades, cujas características fazem com que o processo de ativação seja demorado. Por essa razão, períodos curtos de contratos dessa natureza, podem acarretar riscos tecnológicos à segurança das informações/equipamentos e dispositivos, além dos altos custos para substituição da arquitetura/serviços, sempre que houver mudança de tecnologia.



PROCURADORIA GERAL DO ESTADO

3. DO DETALHAMENTO DO OBJETO

3.1 O objeto a ser contratado abrangerá (a/o):

3.1.1 Fornecimento dos softwares corporativos de proteção de *endpoint* com atualização de versão, contemplando as licenças de uso perpétua de softwares/agentes (Produtos):

3.1.1.1 Todos os produtos/softwares ofertados deverão estar na linha de comercialização do fabricante, sem data de descontinuidade definida na época da realização da licitação.

3.1.1.2 Deve ser disponibilizado para a CONTRATANTE todas as novas versões dos produtos (update e upgrade), bem como as atualizações da base de assinaturas no regime 24x7(vinte e quatro horas durante sete dias na semana).

3.1.2 Execução dos serviços de implantação completa da solução supramencionada, contemplando a transferência de conhecimento, instalação, configuração, customização dos softwares/ agentes nos dispositivos de computação da PGE e remoção dos softwares existentes de antivírus para que não haja a possibilidade de conflitos entre eles:

3.1.2.1 Transferência de conhecimento tecnológico na modalidade hands-on, através de capacitação da equipe técnica da CONTRATANTE, que terá as atribuições de acompanhar e fiscalizar a execução do Contrato;

3.1.2.2 Remoção completa dos softwares e agentes de antivírus instalados nos dispositivos de computação da Rede (antigo). Essa atividade pode ser remota ou presencial

3.1.3 Execução dos serviços de sustentação dos softwares, compreendendo a operação, monitoramento e o suporte técnico no regime 8x5 (oito horas durante cinco dias na semana):

3.1.3.1 O Suporte técnico para dirimir dúvidas, propor medidas preventivas, analisar e resolver problemas técnicos e de segurança.

3.1.3.2 A operação e o monitoramento para controlar, administrar, gerar relatórios, manter os serviços ativos e operacionais, atualizar o(s) produto(s)/softwares na(s) última(s) versão(ões) estáveis disponibilizadas pelo fabricante.



PROCURADORIA GERAL DO ESTADO

4. DOS LOCAIS PARA A PRESTAÇÃO DO SERVIÇO

4.1 Os serviços de implantação dos softwares corporativos de antivírus, bem como a remoção de softwares e agente existentes serão, preferencialmente prestados remotamente (off site), porém na impossibilidade técnica desta mobilidade, eles deverão ser executados presencialmente nos seguintes locais, conforme tabela de endereços abaixo:

Unidades da PGE	Produtos e Agentes com (Conexão Rede de Dados PGE))	Endereços
SEDE	Produtos e Agentes(Servidores, Desktop e Notebook.)	Rua do Carmo, 27 - Centro - Rio de Janeiro, RJ
PR01 – NITERÓI	Agente - Desktop	Rua Visconde de Sepetiba, 935 / 7º andar - Centro - Niterói, RJ
PR02 - DUQUE DE CAXIAS	Agente - Desktop	Avenida Brigadeiro Lima e Silva, 1939 / 6º e 7º andares - Vinte de Agosto - Duque de Caxias, RJ
PR03 - NOVA IGUAÇU	Agente - Desktop	Rua Comendador Soares, 194 / 2º andar - Ed. São Paulo Business Center - Centro - Nova Iguaçu, RJ
PR04 - BARRA DO PIRAÍ	Agente - Desktop	Rua Dona Guilhermina, 100 - Chácara Farani - Barra do Piraí, RJ
PR05 - VOLTA REDONDA	Agente - Desktop	Avenida Paulo de Frontin, 590 / Salas 1001 a 1013 - 10º andar - Aterrado - Volta Redonda, RJ
PR06 - ANGRA DOS REIS	Agente - Desktop	Rua do Comércio, 10 - Sobreloja - Centro - Angra dos Reis, RJ
PR07 - PETRÓPOLIS	Agente - Desktop	Rua do Imperador, 288 / Salas 30 a 35 - Shopping Dom Pedro II - Centro - Petrópolis, RJ
PR08 - NOVA FRIBURGO	Agente - Desktop	Rua Dante Laginestra, 49 - Centro - Nova Friburgo, RJ
PR09 – MACAÉ	Agente - Desktop	Avenida Nossa Senhora da Glória, 999 / 1º andar - Cavaleiros - Macaé, RJ
PR10 – CAMPOS	Agente - Desktop	Rua Gastão Machado, 66 - Parque Tomás Coelho - Campos dos Goytacazes, RJ
PR11- ITAPERUNA	Agente - Desktop	Avenida Zulamith Bittencourt, 300 / Sala 104 - 4º andar - Ed. Residencial Ajala - Centro - Itaperuna, RJ
PR12 - CABO FRIO	Agente - Desktop	Rua Domingos Ribeiro, 62 - Passagem - Cabo Frio, RJ
PR13 - SÃO GONÇALO	Agente - Desktop	Rua Coronel Serra, 1000 / 7º andar - Zé Garoto - São Gonçalo, RJ
PG-13 - BRASÍLIA	Agente - Desktop	SAF/S, Quadra 02, Lote 04, Sala 304 - Cond. Via Esplanada - Brasília, DF
CONVENTO DO CARMO	Agente - Desktop	Praça XV de Novembro, 101 (Antigo Convento do Carmo), Centro, Rio de Janeiro/RJ – CEP: 20010-010
Secretarias de Estado	(Conexão somente pela Internet do órgão)	Endereço
SETRAB	Agente - Desktop	Avenida Nilo Peçanha, nº 50, 33º andar – Centro, Rio de Janeiro, RJ
SEAP	Agente - Desktop	Praça Cristiano Ottoni, S/N (Edifício Dom Pedro II), 5º andar, sala 520 – Centro, Rio de Janeiro, RJ



PROCURADORIA GERAL DO ESTADO

SES	Agente - Desktop	Rua México, nº 128, 5º andar, sala 528 – Centro, Rio de Janeiro, RJ
SEDEC	Agente - Desktop	Praça da República, nº 45 – Centro, Rio de Janeiro, RJ
SEPLAG	Agente - Desktop	Avenida Erasmo Braga, nº 118, 4º andar – Centro, Rio de Janeiro, RJ
SETUR	Agente - Desktop	Rua Uruguaiana, nº 118, 5º andar – Centro, Rio de Janeiro, RJ
SEASDH	Agente - Desktop	Praça Cristiano Ottoni, S/N (Edifício Dom Pedro II), 6º andar, sala 647 – Central do Brasil, Centro, Rio de Janeiro, RJ
SEEDUC	Agente - Desktop	Avenida Professor Pereira Reis, nº 119 – Santo Cristo, Rio de Janeiro, RJ
SETRANS	Agente - Desktop	Avenida Nossa Senhora de Copacabana, 493, 11º andar – Copacabana, Rio de Janeiro, RJ
SESEG	Agente - Desktop	Praça Cristiano Ottoni, S/N (Prédio da Central do Brasil), 4º andar – Centro, Rio de Janeiro, RJ
SEAPEC	Agente - Desktop	Alameda São Boaventura, nº 770 – Fonseca, Niterói, RJ
SEC	Agente - Desktop	Rua da Quitanda, nº 86, 8º andar – Centro, Rio de Janeiro, RJ
SEDEIS	Agente - Desktop	Av. Rio Branco, nº 110 – 20º, 21º e 22º andares – Centro, Rio de Janeiro, RJ
SEELJE	Agente - Desktop	Avenida Presidente Vargas, nº 409, 21º andar – Centro, Rio de Janeiro, RJ

Obs. Os dispositivos de computação instalados nas Assessorias Jurídicas das Secretarias de Estado, não estão integrados ao AD e nem conectados à Rede PGE. Ou seja, eles estão conectados separadamente nas redes locais das Secretarias de Estado que tem acesso à internet.

4.2 O local de prestação dos serviços poderá sofrer alterações no decorrer da execução do Contrato, conforme solicitação da CONTRATANTE, na forma do art. 65 da Lei n.º 8.666/93.



PROCURADORIA GERAL DO ESTADO

5. DO QUANTITATIVO DOS PRODUTOS

5.1 A contratação contempla a prestação dos serviços de proteção de *endpoint* incluindo o fornecimento, a implantação e a sustentação da solução corporativos de antivírus.

5.2 Os quantitativos estão descritos na tabela abaixo:

Serviços	Item	Descrição	Qtd.	Unidade	Valor Unitário (36 meses)
Solução de Proteção Corporativa de <i>endpoin</i>	1.	Fornecimento e Sustentação dos softwares corporativos de Antivírus com atualização	36	Mensal	
	1.1	Licença de Software para Servidor de Administração e Console central da solução.	01	Un.	
	1.2	Licença(s) de Software para Windows, MacOS	2.042	Un.	
	1.3	Licença(s) de Software para Servidores (Físicos e Virtualizados) Windows e Linux.	140	Un.	
	2.	Implantação dos softwares	15	Un	
	2.1	Na Rede da PGE (sede, regionais e especializada de Brasília-DF)	01	Un.	
	2.2	Na Assessorias Jurídicas das Secretarias Estaduais.	14	Un.	
		Total dos Serviços durante 36 meses (total dos itens 1 e 2)	36	Mensal	

Obs. Os valores pagos dos serviços de fornecimento e sustentação dos softwares serão parcelados em 36 vezes e os de implantação por unidade finalizada e aprovada pela Comissão de fiscalização.

6. DAS ESPECIFICAÇÕES, COMPOSIÇÕES E CARACTERÍSTICAS TÉCNICAS DOS SERVIÇOS DE PROTEÇÃO CORPORATIVA DE ENDPOINT

SERVIÇOS DE PROTEÇÃO CORPORATIVA DE ENDPOINT

6.1 REQUISITOS GERAIS:

6.1.1. O fornecimento completo, na modalidade de serviços, de softwares e acessórios necessários a implantação e a sustentação da Proteção Corporativa de Endpoint que deverá ser on premise;

6.1.1.1. Todos os softwares inclusos nos serviços deverão possuir suporte oficial do fabricante, sendo de responsabilidade da CONTRATADA fazer toda a gestão e administração, de tal forma que mantenha a solução operacional e nas últimas versões



PROCURADORIA GERAL DO ESTADO

estáveis dos produtos, em conformidade com o Acordo de Nível de Serviços e condições descritos neste instrumento.

- 6.1.1.2. A solução deverá ser toda de um único fabricante.
- 6.1.1.3. Os serviços de proteção corporativa de endpoint on premise deverão atender integralmente os requisitos especificados neste Termo de Referência, devendo ser fornecida com todas as licenças que forem necessárias para a entrega funcional e operacional da solução.
- 6.1.2. A prestação de serviços especializados desde o planejamento até a implantação completa dos softwares corporativos de antivírus nos endpoints, incluindo, a migração ou melhoria das regras de segurança existente para a nova solução, a fim de aperfeiçoar a proteção atual dos ativos de rede.
- 6.1.3. Os softwares de antivírus deverão, no mínimo, prover Controle de Aplicações, Firewall de host, HIPS, IDS, EDR (Endpoint Detection and Response) e Controle de Dispositivos integrados em único agente, gerenciado por uma única console;
- 6.1.4. HIPS (Host Intrusion Prevention System)
 - 6.1.4.1. Deverá possuir perfis pré-determinados, baseados em performance e segurança;
 - 6.1.4.2. Deverá possuir regras para proteger contra ameaças do tipo Ransomware;
 - 6.1.4.3. Deverá possuir regras contra exploit, vulnerabilidades e genéricas protegendo contra ameaças conhecidas ou desconhecidas;
 - 6.1.4.4. Deverá ser possível configurar o modo de detecção, possibilitando apenas detectar ou bloquear os eventos que violem as regras, de modo que o administrador possa optar por qual ação tomar;
 - 6.1.4.5. Deverá ser possível configurar o modo de detecção, possibilitando atuar no modo em linha para proteção contra ataques e modo escuta para monitoração e alertas;
 - 6.1.4.6. Deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;
 - 6.1.4.7. Deverá detectar conexões maliciosas, com a possibilidade de bloquear esta conexão.
 - 6.1.4.8. A opção de detecção e bloqueio deverá ter a possibilidade de ser implementada de forma global (todas as regras) e apenas para uma regra ou grupos de regras;
 - 6.1.4.9. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede;



PROCURADORIA GERAL DO ESTADO

- 6.1.4.10. Os arquivos quarentenados devem ser possíveis de ser restaurados pela console central ou direto no endpoint;
- 6.1.4.11. Os arquivos quarentenados devem ser criptografados para evitar execução acidental e devem ser acessados com ferramenta provida pelo fabricante;
- 6.1.4.12. Possibilidade de adicionar manualmente arquivos na quarentena do cliente com opção de restrições na console de gerenciamento;
- 6.1.4.13. Forma automática de envio dos arquivos da área de isolamento central para o fabricante, via protocolo seguro, onde este será responsável por gerar a vacina, automaticamente, sem qualquer tipo de intervenção do administrador;
- 6.1.4.14. Recebimento utilizando o mesmo método e aplicação da vacina recém-criada nas estações infectadas;
- 6.1.5. EDR (Endpoint Detection and Response):
 - 6.1.5.1. A solução deve ter a capacidade de implementar técnicas de EDR (Endpoint Detection and Response), possibilitando detecção e investigação nos endpoints com atividades suspeitas;
 - 6.1.5.2. Deverá possuir proteção contra exploração de vulnerabilidades baseada em agente;
 - 6.1.5.3. Deverá detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional;
 - 6.1.5.4. Deverá realizar auditoria automática do servidor protegido (agendada e manual), detectando o tipo e versão do sistema operacional, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem exploração das vulnerabilidades existentes no sistema operacional;
 - 6.1.5.5. Deverá possuir regras de defesa para blindagem de vulnerabilidades e ataques que explorem os sistemas operacionais supracitados e regras para aplicações/serviços padrões de mercado, incluindo Microsoft IIS, DNS, SQL Server, Microsoft Exchange, Oracle Database, PostgreSQL, Adobe Acrobat, Tomcat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, Red Hat Jboss, JAVA, PHP, Wordpress, Weblogic, soluções de backup, bibliotecas linux, e Web Server Apache;
 - 6.1.5.6. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;
 - 6.1.5.7. Deverá apresentar informações de proteção contra vulnerabilidades, contendo links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante e CVE relacionado;



PROCURADORIA GERAL DO ESTADO

- 6.1.5.8. Para evitar falso positivos com spywares a solução deve permitir um modo de avaliação onde o administrador seja notificado, porém as aplicações não são bloqueadas, permitindo criar uma whitelist antes de habilitar o bloqueio;
- 6.1.5.9. A Solução deve permitir conter surtos de malware na rede isolando o endpoint infectado, a partir de política criada na console de gerenciamento centralizado;
- 6.1.5.10. O administrador deve ser notificado sobre surto na rede, por e-mail e através da console de gerenciamento centralizada;
- 6.1.5.11. A ação de isolamento do endpoint deve ser executada de forma automatizada e/ou pelo administrador na console de gerenciamento centralizado;
- 6.1.5.12. Entre as ações tomadas pela contenção de surtos deve ser possível:
 - 6.1.5.12.1. Limitar ou negar acesso a pastas compartilhadas;
 - 6.1.5.12.2. Bloquear portas;
 - 6.1.5.12.3. Negar escrita em arquivos e pastas;
 - 6.1.5.12.4. Negar execução de arquivos executáveis (.exe)
 - 6.1.5.12.5. Deve ser possível notificar o usuário com uma mensagem customizada;
- 6.1.5.13. A solução deve possuir detecção de comportamento e análise de scripts, bloqueado ameaças conhecidas e potencialmente perigosas;
- 6.1.5.14. A funcionalidade de EDR e cliente de antivírus devem ser integradas em um único agente, não havendo a necessidade de instalar mais de um componente no endpoint;
- 6.1.5.15. A funcionalidade de EDR deve fazer detecção através do comportamento;
- 6.1.5.16. Deve ser possível fazer o correlacionamento de eventos entre computadores na rede (IoC Scanning);
- 6.1.5.17. O EDR deve permitir coletar informações forenses do endpoint tais como:
 - 6.1.5.17.1. Dumps de memória;
 - 6.1.5.17.2. Estado do sistema operacional
 - 6.1.5.17.3. Processos iniciados;
 - 6.1.5.17.4. Conexões estabelecidas;
 - 6.1.5.17.5. Registro modificado;
 - 6.1.5.17.6. Tentativas de conexão com um host remoto
 - 6.1.5.17.7. Tentativa de login com sucesso;
 - 6.1.5.17.8. Tentativa de login com falha;



PROCURADORIA GERAL DO ESTADO

- 6.1.6. A solução de EndPoint deverá suportar, no mínimo:
- 6.1.6.1. Arquiteturas de 32-bits e 64-bits;
 - 6.1.6.2. Proteção por base de assinaturas (vacinas) e uso da inteligência na nuvem do fabricante;
- 6.1.7. A solução de EndPoint deverá possuir agentes para os seguintes sistemas operacionais clientes:
- 6.1.7.1.1. Windows 10 ou superior;
 - 6.1.7.1.2. Mac OS X 10.3,12,13,14+
- 6.1.8. A solução de EndPoint deverá suportar as seguintes plataformas servidores:
- 6.1.4.4.1 Windows Server 2012 r2/2016/2019 (Todas edições);
 - 6.1.4.4.2 Red Hat Enterprise Linux Server 7x e superior
 - 6.1.4.4.3 CentOS Server 7x e superior.
- 6.1.9. A solução de EndPoint deverá suportar seguintes plataformas de virtualização:
- 6.1.4.4.4 Microsoft Hyper-V 2012 r2, 2016 e 2019;
 - 6.1.4.4.5 VMware ESXi 6.0 e 6.5;
 - 6.1.4.4.6 VMware vShpere 6.0, 6.5 e 6.7.
- 6.1.10. A solução de EndPoint deverá permitir testar arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção;
- 6.1.11. A solução deve ter a capacidade de instalação/atualização dos softwares e garantir o pleno funcionamento em dispositivo de computação com, no mínimo 4Gb de memória RAM;
- 6.1.12. A solução para o dispositivo de computação deverá possuir funcionalidades específicas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos com a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.
- 6.1.13. A solução de EndPoint deverá suportar deverá possuir solução contra a ação de ransomwares para (Servidores Virtuais) funcionalidades específicas para prevenção contra a ação de ransomwares, tais como a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração e também proteção para os dados compartilhados, bloquear o acesso do invasor ao compartilhamento e notificar o administrador.
- 6.1.14. A solução deverá possuir filtro de reputação de websites e arquivos, ferramentas de varredura, detecção, análise e remoção de malwares, riskware, vírus de setor de boot, de arquivos, multipartite, stealth, polimórficos, vírus de macro, ransomwares, mineradores de



PROCURADORIA GERAL DO ESTADO

criptomoedas e demais formas de vírus e códigos maliciosos conhecidos, ameaças desconhecidas e ataques do tipo fileless (malware sem arquivo).

- 6.1.15. Deve ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas (zero-day) e suspeitas consultando modelos e características na nuvem do fabricante;
- 6.1.16. A solução de EndPoint deverá suportar ter capacidade de instalar remotamente, automaticamente e em modo silencioso, para os dispositivos de computação (Windows (Desktops e Servers) e Linux Servers);
- 6.1.17. A solução de EndPoint deverá suportar ter capacidade de remover automaticamente qualquer software de antivírus que estiver presente nos dispositivos de computação acima;
- 6.1.18. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições/assinaturas até o momento da expiração da licença.

6.2 SERVIDOR DE ADMINISTRAÇÃO

6.2.1 Compatibilidade:

- 6.2.1.1 Microsoft Windows Server 2012/2016/2019 (Todas edições);
- 6.2.1.2 Microsoft Hyper-V 2012 r2, 2016 e 2019;
- 6.2.1.3 VMware ESXi 6.0 e 6.5;
- 6.2.1.4 VMware vSphere 6.0, 6.5 e 6.7.

6.2.2 Características:

- 6.2.2.1 Administração gráfica deve ser acessada via WEB (HTTPS) e/ou através de uma Console de gerência centralizada que poderá ser instalada em mais de um desktop com acesso simultâneo;
- 6.2.2.2 Console deve ser baseada no modelo cliente/servidor;
- 6.2.2.3 Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
- 6.2.2.4 Console deve ser totalmente integrada com suas funções e módulos;
- 6.2.2.5 Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
- 6.2.2.6 Deve permitir, através da console de gerenciamento, visualizar o número total de licenças instaladas e não instaladas;
- 6.2.2.7 Através da solução de gerência, deve ser possível verificar qual licença está aplicada;
- 6.2.2.8 A console de gerência centralizada deve permitir gerar relatórios, visualizar eventos,



PROCURADORIA GERAL DO ESTADO

gerenciar políticas e criar painéis de controle;

- 6.2.2.9 Capacidade de gerenciar (Windows e Mac) e servidores (Windows e Linux) protegidos pela solução antivírus;
- 6.2.2.10 Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
- 6.2.2.11 Capacidade de atualizar os pacotes de instalação com as últimas versões de vacinas;
- 6.2.2.12 A comunicação entre o cliente e o servidor de administração deve ser criptografada;
- 6.2.2.13 Deve possuir integração com Microsoft Active Directory;
- 6.2.2.14 Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;
- 6.2.2.15 Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção automaticamente;
- 6.2.2.16 Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção automaticamente;
- 6.2.2.17 Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o agente e o antivírus automaticamente;
- 6.2.2.18 Se possuir um antivírus diferente deverá remover automaticamente e instalar o novo.
- 6.2.2.19 Capacidade de definir políticas de configurações diferentes por grupos de dispositivos de computação, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
- 6.2.2.20 Nas informações da política deve conter informações como nome, status, dono da política, horário e data da última alteração;
- 6.2.2.21 A gerencia central deverá mostrar compliance dos dispositivos gerenciáveis, com informações das máquinas:
- 6.2.2.22 Se o agente/antivírus está instalado;
- 6.2.2.23 Se o agente/antivírus está iniciado;
- 6.2.2.24 Se o agente/antivírus está atualizado;
- 6.2.2.25 Minutos/horas desde a última conexão da máquina com o servidor administrativo;
- 6.2.2.26 Minutos/horas desde a última atualização de vacinas;



PROCURADORIA GERAL DO ESTADO

- 6.2.2.27 Data e horário da última verificação executada na máquina;
- 6.2.2.28 Versão do antivírus instalado na máquina;
- 6.2.2.29 Se é necessário reiniciar o dispositivo de computação para aplicar mudanças;
- 6.2.2.30 Data e horário de quando a máquina foi ligada;
- 6.2.2.31 Quantidade de vírus encontrados (contador);
- 6.2.2.32 Nome do dispositivo de computação;
- 6.2.2.33 Domínio ou grupo de trabalho do dispositivo de computação;
- 6.2.2.34 Data e horário da última atualização de vacinas;
- 6.2.2.35 Sistema operacional com Service Pack;
- 6.2.2.36 Usuário (s) logado (s) naquele momento ou último logon com data e hora;
- 6.2.2.37 Endereço IP;
- 6.2.2.38 Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
- 6.2.2.39 Deve permitir bloquear com senha as configurações do antivírus instalado de maneira que o usuário não consiga alterá-las;
- 6.2.2.40 Manter conectadas as máquinas clientes ao servidor administrativo mesmo que haja:
 - 6.2.2.40.1 Alteração de Gateway Padrão;
 - 6.2.2.40.2 Alteração de Subrede;
 - 6.2.2.40.3 Alteração de Domínio;
 - 6.2.2.40.4 Alteração de Servidor DHCP;
 - 6.2.2.40.5 Alteração de Servidor DNS;
 - 6.2.2.40.6 Resolução de Nome;
- 6.2.2.41 Disponibilidade de endereço de conexão SSL; Capacidade de configurar políticas móveis para que quando um dispositivo de computação cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- 6.2.2.42 Capacidade de herança de tarefas e políticas na estrutura hierárquica dos dispositivos gerenciados;
- 6.2.2.43 Multicast, tecnologia para distribuição local de software, economizando tráfego em escritórios remotos;
- 6.2.2.44 Capacidade de eleger automaticamente qualquer dispositivo de computação cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;



PROCURADORIA GERAL DO ESTADO

- 6.2.2.45 Geração de relatórios e gráficos nos formatos html, pdf, xml ou csv;
- 6.2.2.46 Os relatórios devem conter informações de efetividade, nome/tipo do vírus, canais de infecção, principais usuários que receberam ameaças, vírus e spyware;
- 6.2.2.47 Capacidade de gerar traps SNMP para monitoramento de eventos; Capacidade de enviar e-mails para contas específicas em caso de algum evento;
- 6.2.2.48 Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
- 6.2.2.49 Capacidade de realizar atualização incremental de vacinas nos dispositivos de computação clientes;
- 6.2.2.50 Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo: e Nome do vírus; e Nome do arquivo infectado; Data e hora da detecção; Nome da máquina ou endereço IP e Ação realizada.
- 6.2.2.51 Capacidade de diferenciar máquinas virtuais de máquinas físicas.
- 6.2.2.52 Deve permitir pesquisas baseados nos seguintes critérios: Nome parcial ou completo dos dispositivos de computação, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina, nome do usuário (login usuário do AD), IP e range de IPS (subnet);
- 6.2.2.53 A solução deverá permitir a geração de relatórios contendo informação de diferentes intervalos de tempo (semanas ou meses) similares aos especificados abaixo:
 - 10 principais ameaças detectadas;
 - 10 principais ataques detectados;
 - Os 10 equipamentos com maiores detecções;
 - Os 10 usuários com mais detecções;
 - As 10 principais origens com mais detecções;
 - Resumo das repostas de detecção;
 - Número de ameaças por criticidade.
- 6.2.2.54 Deve ter a possibilidade de exportar/importar configurações dos softwares através da console de gerenciamento;
- 6.2.2.55 Deve permitir integração com Active Directory para acesso a console de administração;



PROCURADORIA GERAL DO ESTADO

6.3 PROTEÇÃO ANTIMALWARE OTIMIZADA PARA VIRTUALIZAÇÃO

6.3.1 Compatibilidade:

6.3.1.1 Microsoft Windows Server 2012/2016/2019 (Todas edições);

6.3.1.2 Microsoft Windows 10 64bits (build 1909);

6.3.1.3 Microsoft Hyper-V 2012 r2, 2016 e 2019;

6.3.1.4 VMware ESXi 6.0 e 6.5;

6.3.1.5 VMware vSphere 6.0, 6.5 e 6.7.

6.3.1.6 Red Hat Enterprise Linux Server 7x e superior (64Bits)

6.3.1.7 CentOS Server 7x e superior (64Bits).

6.3.2 Requer softwares corporativos de Antivírus especialmente otimizada para funcionar em conjunto com soluções de virtualização, por agentless ou contendo um agente otimizado e com requisitos reduzidos de recursos;

6.3.3 Deverá funcionar tanto em "Virtual Servers" quanto em "Virtual Desktops";

6.3.4 A solução de antimalware deve fazer uso de assinaturas, machine learning e detecção de comportamento para identificar malwares;

6.3.5 Possuir Prevenção de Intrusão do Host (HIPS);

6.3.6 Anti-malware para Windows e Linux, mínimo para versões acima;

6.3.7 Deverá ter controle sobre as máquinas que estão em um mesmo hypervisor de modo que as mesmas não executem o scan de maneira simultânea para não afetar a performance do sistema;

6.3.8 Deverá suportar scan no momento em que um arquivo é acessado;

6.3.9 Deverá suportar scan de todos os arquivos de uma máquina virtual permitindo inclusive programar a frequência desse scan;

6.3.10 Deverá descobrir e importar máquinas virtuais, tanto as que estejam rodando quanto as que se encontram paradas;

6.3.11 Deverá possuir proteção por IDS/IPS de ataque a infraestrutura;

6.3.12 Deverá possuir prevenção de malware contra exploração de vulnerabilidades de softwares, reconhecendo padrões de comportamento suspeito ou típico, interrompendo o exploit em andamento e impedindo que qualquer código malicioso seja executado.

6.3.13 A solução deverá contar com um "cache" que permita otimizar os recursos evitando assim escanear arquivos que tenham sido analisados anteriormente e não tenham sofrido alterações;

6.3.14 O componente deverá ser administrado por uma console única. Esta console deverá



PROCURADORIA GERAL DO ESTADO

implementar políticas, aplicar atualizações, programar tarefas automáticas, obter informações e gerar relatórios de atividades dos usuários e ameaças identificadas;

- 6.3.15 Deverá contar com scan que executem análise de antivírus offline;
- 6.3.16 Deverá fazer a gestão e alocação de máquinas virtuais automaticamente para os scan com base na carga, pré-configuração ou a ranges de IP;
- 6.3.17 Os softwares não devem requerer que o hypervisor seja reiniciado em nenhum passo do processo de instalação da solução;
- 6.3.18 Deverá se conectar a uma base de reputação global de ameaças onde obtenha informações de novas vulnerabilidades e novos conteúdos maliciosos e proveja inteligência para detecção eficiente de ataques;
- 6.3.19 Deverá contar com políticas de exclusão do scan de determinados, pastas, arquivos e programas;
- 6.3.20 A solução deverá baixar atualizações e engines de análise periodicamente de maneira automática e aplicar aos demais componentes da solução;
- 6.3.21 A solução deverá definir uma política por máquina virtual;
- 6.3.22 A console de administração deverá armazenar os logs de atividades;
- 6.3.23 Deverá ser possível o controle de monitoramento web com verificação de URL
- 6.3.24 Deve ser possível automatizar a geração dos relatórios e seu envio através de correio eletrônico de maneira programada pelo administrador através da console de administração central;
- 6.3.25 A solução deverá permitir a geração de relatórios contendo informação de diferentes intervalos de tempo (semanas ou meses) similares aos especificados abaixo:
 - 10 principais ameaças detectadas;
 - 10 principais ataques detectados;
 - Os 10 equipamentos com maiores detecções;
 - Os 10 usuários com mais detecções;
 - As 10 principais origens com mais detecções;
 - Resumo das repostas de detecção;
 - Número de ameaças por criticidade."

6.4 CARACTERÍSTICAS DOS DISPOSITIVOS WINDOWS

- 6.4.1 **Antivírus** de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;



PROCURADORIA GERAL DO ESTADO

- 6.4.2 Antivírus de Web (verificação de sites e downloads contra vírus);
- 6.4.3 O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
- 6.4.4 A solução de antimalware deve fazer uso de assinaturas, machine learning e detecção de comportamento para identificar malwares;
- 6.4.5 Multicast, tecnologia para distribuição local de software, economizando tráfego em escritórios remotos;
- 6.4.6 Deverá possuir Firewall com IDS;
- 6.4.7 Deverá possuir Autoproteção (contra-ataques aos serviços/processos do antivírus);
- 6.4.8 Controle de dispositivos externos;
- 6.4.9 Controle de acesso a sites por categoria;
- 6.4.10 Controle de acesso a sites por usuários;
- 6.4.11 Controle de execução de aplicativos;
- 6.4.12 Capacidade de escolher quais recursos serão instalados, tanto na instalação local quanto na instalação remota;
- 6.4.13 As vacinas devem ser atualizadas pelo Servidor de Administração e disponibilizada para os dispositivos automaticamente em período de tempo definido;
- 6.4.14 Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
- 6.4.15 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 6.4.16 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "SMTP") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 6.4.17 Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
- 6.4.18 Capacidade de parar automaticamente varreduras agendadas;
- 6.4.19 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- 6.4.20 Capacidade de verificar somente arquivos novos e alterados;
- 6.4.21 Capacidade de verificar objetos usando heurística;



PROCURADORIA GERAL DO ESTADO

- 6.4.22 Capacidade de agendar uma pausa na verificação;
- 6.4.23 Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
- 6.4.24 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 6.4.25 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - a) Perguntar o que fazer, ou;
 - b) Bloquear acesso ao objeto;
- 6.4.26 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
- 6.4.27 Caso positivo de desinfecção:
 - a) Restaurar o objeto para uso automaticamente.
- 6.4.28 3.5.6.30 Caso negativo de desinfecção:
 - b) Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).
- 6.4.29 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 6.4.30 Capacidade de verificar tráfego nos browsers: Microsoft Edge, Internet Explorer, Google Chrome, Firefox e Opera;
- 6.4.31 Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
- 6.4.32 Deve ter suporte total ao protocolo IPv6;
- 6.4.33 Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
 - a) Perguntar o que fazer, ou;
 - b) Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
 - c) Permitir acesso ao objeto.
- 6.4.34 Na verificação de tráfego web deve realizar a verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real,
- 6.4.35 Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
- 6.4.36 Deve ser possível análise de ações de cada aplicação em execução no dispositivo de computação, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;



PROCURADORIA GERAL DO ESTADO

- 6.4.37 Deve possuir a função SCAN CACHE, otimizando o scan nas máquinas armazenando informações dos arquivos que já são conhecidos como bons otimizando o uso de recurso;
- 6.4.38 Deve ser possível alterar o período que o cache será armazenado para que seja criada uma nova base de assinaturas;
- 6.4.39 Deve ser possível análise de macro VBA executada, procurando por sinais de atividade maliciosa;
- 6.4.40 Deve ser possível a análise de qualquer tentativa de edição, exclusão ou gravação do registro automaticamente;
- 6.4.41 Deve ser possível bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group;
- 6.4.42 Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
- 6.4.43 Deve possuir IDS/IPS, proteção contra port scans. A base de dados de análise deve ser atualizada juntamente com as vacinas;
- 6.4.44 O Firewall deve conter, no mínimo, dois conjuntos de regras:
 - a) Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; e
 - b) Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- 6.4.45 Capacidade de liberar acesso a um dispositivo externo por usuários e/ou grupo do AD (Active Directory), por período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
- 6.4.46 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
- 6.4.47 Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc), com possibilidade de configuração por usuário e grupos de usuários do AD;
- 6.4.48 Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);
- 6.4.49 Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do



PROCURADORIA GERAL DO ESTADO

registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

6.4.50 Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web; e

6.4.51 Capacidade de, caso o dispositivo de computação cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

6.5 CARACTERÍSTICAS MAC OS X:

6.5.1 Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

6.5.2 Capacidade de instalação local e remota;

6.5.3 Deve possuir suportes a notificações utilizando o Growl;

6.5.4 Capacidade de voltar para a base de dados de vacina anterior;

6.5.5 Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;

6.5.6 Possibilidade de desabilitar automaticamente varreduras agendadas quando o dispositivo de computação estiver funcionando a partir de baterias (notebooks);

6.5.7 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

6.5.8 Capacidade de verificar somente arquivos novos e alterados;

6.5.9 Capacidade de verificar objetos usando heurística;

6.5.10 Capacidade de agendar uma pausa na verificação;

6.5.11 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

6.5.11.1 Perguntar o que fazer, ou

6.5.11.2 Bloquear acesso ao objeto;

6.5.11.3 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);

6.5.12 Caso positivo de desinfecção:

6.5.12.1 Restaurar o objeto para uso;

6.5.12.2 Caso negativo de desinfecção:

6.5.12.3 Mover para quarentena ou apagar (de acordo com a configuração pré-



PROCURADORIA GERAL DO ESTADO

estabelecida pelo administrador);

6.5.12.4 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

6.5.13 Capacidade de verificar arquivos de formato de e-mail;

6.5.14 Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

7 DA IMPLANTAÇÃO DOS SERVIÇOS DE PROTEÇÃO CORPORATIVA DE ENDPOINT

7.1 Os serviços serão executados on site, preferencialmente, nas dependências da CONTRATANTE em dias úteis (segunda a sexta-feira), no horário de 9h às 18h. Contudo, a CONTRATANTE a seu critério pode autorizar a realização dos serviços na modalidade off site, conforme a conveniência e a possibilidade técnica de realizar o serviço/atividade usando VPN (Acesso remoto).

7.2 Deve ser implementado todo o ciclo de proteção de endpoints, desde o bloqueio automático de ameaças até a resposta a incidentes, incluindo tecnologias complementares com recursos avançados de defesa.

7.3 Toda a documentação técnica específica, acesso ao repositório oficial, arquivos de configuração dos softwares e todo o material gerado em função da prestação dos serviços deverão ser entregues à CONTRATANTE.

7.4 A CONTRATADA deverá apresentar, em até 5 (cinco) dias após o término de cada OS, um relatório contendo, no mínimo:

6.3.1 A descrição das atividades realizadas durante o serviço e a apresentação das evidências de conclusão das atividades ou/e relatório técnico;

7.5 A equipe técnica designada pela CONTRATANTE acompanhará a execução dos serviços de operação assistida realizada pelos profissionais da CONTRATADA, toda a vez que for implantada uma nova versão do software.

7.6 A equipe técnica designada pela CONTRATANTE deverá receber, avaliar, homologar e aprovar os serviços entregues pela CONTRATADA e, quando aprovados, emitir o TERMO DE ACEITE DO SERVIÇO.

7.7 Na execução dos serviços deverão ser respeitados os prazos estabelecidos, padrões de qualidade e critérios de aceitação definidos neste instrumento.

7.8 A CONTRATADA deverá executar no mínimo, os seguintes serviços para a Implantação dos



PROCURADORIA GERAL DO ESTADO

softwares corporativos de antivírus:

- 7.8.1 Capacitação dos técnicos da CONTRATANTE na utilização de funcionalidade dos softwares e na gestão dos serviços;
- 7.8.2 Realizar Reunião Técnica para identificação de necessidade de melhoria dos serviços;
- 7.8.3 Executar as atividades de Instalação, configuração, customização e atualização dos softwares/módulos de gerência e configuração;
- 7.8.4 Executar as atividades de Instalação, configuração, customização e atualização dos agentes nos dispositivos de computação da Rede PGE;
- 7.8.5 Executar as atividades de Instalação, configuração e atualização nos dispositivos de computação das Assessorias Jurídicas;
- 7.8.6 Executar as atividades de Customização e modelagem do ambiente segundo a necessidade da contratante;
- 7.8.7 Executar as atividades de diagnósticos e manutenção corretiva e preventiva – A ser realizada após a instalação - correção problemas (travando, falhas genéricas, não atualizando, etc..).
- 7.8.8 Executar as atividades de Health Check - Ampla Análise do Ambiente que visa apontar falhas e pontos de melhorias. Análise do hardware, sistema operacional, políticas, segurança, disponibilidade, carga (quantidade e tipo de acesso), operação (manutenções), disaster recovery.

8 DOS SERVIÇOS ESPECIALIZADOS DE SUSTENTAÇÃO DOS SOFTWARES CORPORATIVOS de ANTIVÍRUS

- 8.1 **Suporte Técnico:** são os serviços remotos contínuos especializados, compreendendo o atendimento a dúvidas, análise e diagnóstico de problemas ou defeitos ocorridos no funcionamento dos produtos objetos desta contratação prestados diretamente pelo fabricante ou autorizada.
- 8.2 Atualização do(s) Software(s)(update e upgrade): são os serviços remotos especializados de atualizações, correções e novas versões de softwares, contendo novas funcionalidades, atualizações de funcionalidades existentes, updates e upgrades dos softwares, implementadas e distribuídas pela fabricante da solução aos seus clientes, incluindo, dentre outras: correções de erros de versões, novas funções, melhorias e novas versões, incluindo atualização da base de assinaturas(vacina); adaptações em função da descontinuidade de versões existentes ou do



PROCURADORIA GERAL DO ESTADO

advento de novas versões de componentes de software de terceiros e de sistemas operacionais suportado pelo produto, de forma a manter o(s) software(s) de Antivírus operante(s), integrado(s) e atualizado(s).

- 8.3 A CONTRATADA, através do fabricante, deverá garantir que todas as novas versões dos softwares, independentes de nova denominação comercial, deverá ser disponibilizada à PGE/RJ, para que esta, a seu critério, promova o upgrade na sua instalação.
- 8.4 A CONTRATADA, através do fabricante, deverá garantir que todas as novas atualizações das bases de assinaturas, independentes de nova denominação comercial, deverá ser disponibilizada automaticamente à PGE/RJ, para que esta, a seu critério, promova a atualização.
- 8.5 Toda documentação técnica, acessos ao repositório oficial, arquivos de configuração e manuais de instalação e do usuário, deverão ser entregues juntamente com as novas versões.
- 8.6 A CONTRATANTE exercerá o papel de fiel depositário dos arquivos de configuração e documentação da solução de antivírus implantada na PGE, conforme item supramencionado, com direito total e irrestrito de utilização interna para suporte, apenas, assegurado o direito de propriedade intelectual e comercial da CONTRATADA. Em caso de descontinuidade dos softwares, falência ou extinção da Empresa, a CONTRATANTE passa a ter o direito de contratar terceiros para continuar a prestação dos serviços, ainda que haja necessidade de disponibilização daqueles itens, mediante termos de confidencialidade, em ambiente interno da CONTRATANTE, de forma que impossibilite extração, cópia e/ou envio indevido dos arquivos dos sistemas e da documentação técnica específica.
- 8.7 Os softwares, base de assinaturas e documentação poderão ser entregues por meio de área restrita na web, registrada pelo fornecedor, e em conta especificamente identificada para a CONTRATANTE com permissão de acesso para download.
- 8.8 A CONTRATADA garante à CONTRATANTE que as mídias digitais nas quais os softwares (upgrades, updates e/ou novas versões) porventura forem gravados estão livres de defeitos materiais sob uso normal, e de qualquer rotina alienígena (vírus) voltada para a danificação ou degradação, tanto de dados quanto de hardware ou software.
- 8.9 A prestação de serviços especializados de manutenção, suporte técnico, administração, operação e monitoramento da solução tecnológica, a fim de garantir o correto funcionamento dos mesmos:
 - 8.9.1 Os serviços poderão ser prestados na forma remota ou presencial;
 - 8.9.2 Os serviços de manutenção preventiva e corretiva compreendem: a execução de aperfeiçoamentos e ajustes nas especificações originais, a correção de eventuais falhas de



PROCURADORIA GERAL DO ESTADO

softwares que possam surgir durante a execução dos serviços, as aplicações de atualizações de produtos e serviços;

8.9.3 Os serviços de administração, operação e monitoramento compreendem toda a gestão da solução que garanta o pleno funcionamento da mesma nos mais altos níveis de segurança, desempenho de conectividade e funcionalidade de todo o ambiente tecnológico da PGE/RJ.

8.10 Ao final da vigência do Contrato, a CONTRATADA deve garantir a transferência tecnológica para a CONTRATANTE de toda a documentação e conhecimento técnico que garantam a continuidade dos serviços na mesma plataforma de software implantada ou em outra compatível, sem quaisquer custos adicionais.

8.11 Todos os serviços prestados devem estar em conformidade com o Acordo de Nível de Serviços e condições descritos neste instrumento.

8.12 A CONTRATADA deverá disponibilizar, a partir da data constante do Memorando de Início de Serviço, o número do Identificador de Suporte ao Cliente (CSI) ou similar, números de telefone fixo ou móvel, endereços de correio eletrônico ou área em sítio da *web* para viabilizar a abertura dos chamados técnicos;

8.13 O suporte técnico para resolver problemas de bugs de softwares será realizado sempre que solicitada pela CONTRATANTE por meio da abertura de chamado técnico, acionando diretamente a CONTRATADA, observando o tempo de início do atendimento e a severidade da ocorrência prevista na tabela própria dos níveis de serviços contratados, descritos neste instrumento:

8.13.1 A resolução de chamados de Suporte Técnico que necessitem intervenção direta nos ambientes da CONTRATANTE deverá ser precedida de planejamento e deverá ocorrer, preferencialmente, em horário comercial, de 09h às 18h.

8.13.2 O suporte técnico compreenderá todos os procedimentos destinados a recolocar em estado de operação os produtos tais como: desinstalação, reconfiguração ou reinstalação decorrente de falhas no *Software*, atualização da versão de *Software*, correção de defeitos, ajustes e reparos necessários, cobertos pela garantia mínima exigida no presente instrumento, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados.

8.13.3 Nos atendimentos aos chamados técnicos abertos deverá ser disponibilizado suporte técnico personalizado por um Analista designado como especialista no *software*, via atendimento de suporte remoto.

8.13.4 Suporte especializado deverá atender os seguintes requisitos técnicos:



PROCURADORIA GERAL DO ESTADO

- 8.13.4.1 Permitir a abertura, acompanhamento e validação de chamados através de e-mail e/ou website (portal do cliente) e telefone (0800) no regime 8x5x365, com atendimento em português;
- 8.13.4.2 Possuir processo de escalção funcional, mapeamento e documentação, com os seguintes níveis de atendimento: N1, N2 e N3, conforme melhores práticas descritas pelo ITIL;
- 8.13.4.3 Possuir canal com os fabricantes envolvidos na solução dos incidentes, bem como ser responsável pela abertura e acompanhamento dos chamados junto aos mesmos;
- 8.13.4.4 Possuir os processos de gerenciamento de incidentes, requisição, eventos, problemas, mudanças, incidentes críticos e atendimento aos usuários VIPs mapeados e documentados de acordo com as melhores práticas descritas pelo ITIL;
- 8.13.4.5 O suporte será em formato de dupla custódia, mantendo os administradores de tecnologia da CONTRATANTE com total controle da plataforma, o qual somente irá atuar em casos emergenciais, porém a responsabilidade pela operação diária da solução será da CONTRATADA;
- 8.13.4.6 Assegurar o atendimento presencial previamente acordado nas seguintes situações:
 - 8.13.4.6.1 Migração de versionamento de softwares;
 - 8.13.4.6.2 Incidentes massivos ou desastres;
 - 8.13.4.6.3 Inacessibilidade, ocasionado pela CONTRATADA, da console de gerenciados.
 - 8.13.4.6.4 Suporte técnico de 2º nível quanto a dúvidas de customização e configuração dos softwares e console de gerenciamento.
- 8.13.5 A Manutenção Preventiva deverá atender os seguintes requisitos técnicos:
 - 8.13.5.1 Atualizar os softwares das respectivas consoles de gerenciamento;
 - 8.13.5.2 Realizar os ajustes e melhorias constantes, de acordo com as melhores práticas dos fabricantes; mantê-las documentadas e acessíveis no website (portal do cliente);
 - 8.13.5.3 Propor melhorias no ambiente de forma proativa, periodicamente; mantê-las documentadas no website (portal do cliente) e submetê-las para a aprovação da CONTRATANTE;
- 8.13.6 Na abertura de chamados técnicos serão fornecidas pela CONTRATANTE, informações como:
 - 8.13.6.1 Anormalidade observada;
 - 8.13.6.2 Nome do responsável pela solicitação do serviço;
 - 8.13.6.3 Sistema/versão/módulo/item;



PROCURADORIA GERAL DO ESTADO

8.13.6.4 Natureza do problema;

8.13.6.5 Descrição da natureza enfrentada; e

8.13.6.6 Severidade do chamado, a ser definida conforme tabela própria dos níveis de serviços contratados, descritos neste instrumento.

8.13.7 A CONTRATADA, após a realização dos serviços, deverá apresentar um Relatório de Atendimento, contendo:

8.13.7.1 Identificação do chamado;

8.13.7.2 Data e hora do início e término do atendimento com a solução do chamado técnico;

8.13.7.3 Identificação do defeito; e

8.13.7.4 As providências adotadas, origem do problema outras informações pertinentes.

8.13.8 Após concluído o atendimento, a CONTRATADA comunicará à comissão de fiscalização do contrato e solicitará autorização para o respectivo fechamento. Caso a comissão de fiscalização não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela CONTRATADA. Nesse caso, a GTI informará as pendências relativas ao chamado aberto.

9 DO PRAZO DE VIGÊNCIA

9.1 O prazo de vigência do Contrato será de 38 (trinta e oito) meses, contados a partir da data constante do Memorando de Início de Serviço, desde que posterior à data de publicação do extrato do Contrato no Diário Oficial do Estado do Rio de Janeiro (DOERJ), valendo esta data de publicação como termo inicial de vigência, caso seja posterior à data convencionada neste item.

9.2 O prazo de vigência do Contrato poderá ser prorrogado, para o serviço de Consultoria sob demanda, observando-se o limite previsto no art. 57, inciso II, da Lei n.º 8.666/93, desde que, a proposta da CONTRATADA seja mais vantajosa para a CONTRATANTE.

10 DO PRAZO DE EXECUÇÃO DE PLANEJAMENTO, FORNECIMENTO E IMPLANTAÇÃO DOS SERVIÇOS

10.1 A partir da reunião de início do Contrato (kick-off) e da emissão do Memorando de Início de Serviços pela PGE/RJ, as etapas macro de planejamento, fornecimento e implantação dos softwares devem ser iniciadas e concluídas no prazo de 60 (sessenta) dias, conforme detalhamento do item correspondente abaixo:



PROCURADORIA GERAL DO ESTADO

11 DA ENTREGA, TESTES DE CONFORMIDADE E ACEITE DOS SOFTWARES E DOS SEUS COMPLEMENTOS

11.1 A CONTRATADA fornecerá a especificação técnica, os manuais de instalação e operação do software em meio digital, bem como as mídias de instalação.

11.2 O software e complementos serão recusados se entregues com as especificações técnicas diferentes das contidas neste instrumento e na proposta da CONTRATADA.

11.3 A CONTRATADA fornecerá os softwares bem como: a documentação técnica, os manuais de instalação e operação da solução em meio digital. Além disso, as licenças de uso da solução devem ser adequadas quantitativamente e qualitativamente para o ambiente computacional da PGE;

11.4 Os softwares e todos os seus elementos deverão ser instalados, configurados e otimizados, segundo as melhores práticas do fabricante em termos de desempenho, disponibilidade e segurança, por técnico certificado e capacitado supracitado, de modo a garantir total interoperabilidade no ambiente computacional da PGE.

11.5 Cronograma de Execução:

11.5.1 A execução do objeto será iniciada a partir da Entrega do Memorando de Início de Serviços e conforme o cronograma definido na tabela abaixo.

11.5.2 A CONTRATADA deverá garantir a qualidade e a estabilidade dos serviços prestados em todas as etapas utilizando as melhores práticas de mercado, de tal forma que a CONTRATANTE tenha uma solução viável do ponto de vista técnico com alto grau de segurança, escalabilidade, usabilidade e desempenho:

ATIVIDADES E PRAZOS DE IMPLANTAÇÃO DOS SERVIÇOS			
ITEM	DESCRIÇÃO DAS ATIVIDADES	MÉTRICA	PRAZO MÁXIMO (Em dias)
01	Reunião de início dos serviços – Apresentação do Preposto, a composição da equipe de trabalho, a Metodologia de Trabalho, os recursos necessários para iniciar os serviços, pontos de atenção da Comissão de Fiscalização e modelo de ordem de serviço.	Prazo, em dias úteis, a contar da data designada no Memorando de Início de Serviço.	01
02	I – A CONTRATADA elabora e entrega <u>relatório executivo sumário de diagnóstico e viabilidade técnica</u> à CONTRATANTE	Prazo, em dias consecutivos, após a entrega do(s) produto(s) descrito(s) no Item anterior.	05



PROCURADORIA GERAL DO ESTADO

ATIVIDADES E PRAZOS DE IMPLANTAÇÃO DOS SERVIÇOS			
ITEM	DESCRIÇÃO DAS ATIVIDADES	MÉTRICA	PRAZO MÁXIMO (Em dias)
03	A CONTRATANTE Aprova o(s) produto(s) descrito(s) no item anterior emitindo a Ordem de Serviço para autorizar a CONTRATADA a iniciar o fornecimento dos produtos e licenças de uso, remoção dos antivírus existentes e implantação dos novos softwares de Antivírus na Rede PGE.	Prazo, em dias consecutivos, após a entrega do(s) produto(s) descrito(s) no Item anterior.	03
04	A CONTRATADA fornece os produtos e licenças de uso dos novos Softwares de Antivírus na Rede PGE (SEDE, Especializada de Brasília e Regionais) e Assessorias Jurídicas.	Prazo, em dias consecutivos, após a entrega do(s) produto(s) aprovado(s) descrito(s) no Item anterior.	15
05	A CONTRATADA executa as atividades de remoção dos antivírus existentes e implanta os novos Softwares de Antivírus na Rede PGE (SEDE, Especializada de Brasília e Regionais).	Prazo, em dias consecutivos, após a entrega do(s) produto(s) aprovado(s) descrito(s) no Item anterior.	20
06	A CONTRATADA finaliza o processo de capacitação dos técnicos da CONTRATANTE.	Prazo, em dias consecutivos, após a entrega do(s) produto(s) descrito(s) no Item 03.	05
07	A CONTRATADA executa as atividades de remoção dos antivírus existentes e implanta os agentes/produtos dos novos Softwares de Antivírus nos dispositivos de computação das Assessorias Jurídicas das Secretarias de Estado.	Prazo, em dias consecutivos, após a entrega do(s) produto(s) do item 4.	10
08	CONTRATANTE Aprova o(s) produto(s) descrito(s) nos itens anteriores.	Prazo, em dias consecutivos, após a entrega do(s) produto(s) descrito(s) no Item anterior.	01
09	Inicia os Serviços Sustentação e Atualização dos softwares (Update e Upgrade) corporativos de antivírus nos <i>endpoints</i> .	Prazo, em dias consecutivos, após a entrega do(s) produto(s) aprovado(s) descrito(s) no Item anterior.	Até o final do contrato.



PROCURADORIA GERAL DO ESTADO

OBS. Os itens 4-7 poderão sofrer alterações cronológicas entre si ou podem ser executados paralelamente segundo disponibilidade de recursos da CONTRATADA e aprovado pela CONTRATANTE.

12 ACORDO DE NÍVEL DE SERVIÇO - ANS (MANUTENÇÃO E SUPORTE TÉCNICO REMOTO DOS PRODUTOS)

12.1 Procuradoria Geral do Estado – PGE/RJ adotará Acordo de Nível de Serviços – ANS como instrumento para avaliação e controle da qualidade e desempenho dos serviços prestados pela CONTRATADA, segundo os critérios indicados nos itens subsequentes.

12.2 O ANS tem por:

12.2.1.1 FINALIDADE: garantir que a prestação dos serviços esteja condizente com as Especificações Técnicas inerentes à contratação;

12.2.1.2 INDICADORES: a regularidade no cumprimento dos prazos das Ordens de Serviços e Suporte Técnico;

12.2.1.3 META A CUMPRIR: a realização de 100% (cem por cento) dos serviços com resultado satisfatório dentro dos prazos estabelecidos;

12.2.1.4 INSTRUMENTOS DE MEDIÇÃO: registro da abertura de chamado técnico, relatório das atividades executadas pela CONTRATADA, fichas de acompanhamento de Contrato ou e-mails, todos emitidos pela Fiscalização do Contrato e Termo de Entrega/Aceite das atividades executadas.

12.3 FORMA DE ACOMPANHAMENTO E PONTUAÇÃO: A contagem do prazo de atendimento terá início a partir da abertura do chamado na Central de Atendimento disponibilizada pela CONTRATADA, até o momento da comunicação da solução definitiva do problema e aceite pela equipe técnica da Gerência de Tecnologia da Informação (GTI) da PGE/RJ.

12.4 Os pagamentos mensais poderão sofrer descontos em razão do não cumprimento aos prazos estipulados para o atendimento com solução aos chamados, conforme a severidade da ocorrência e segundo a faixa de pontuação, na forma fixada nos quadros abaixo:

QUADRO I – CLASSIFICAÇÃO DAS OCORRÊNCIAS

OCORRÊNCIA	TEMPO DE RESPOSTA	SEVERIDADE	ESFORÇO EXIGIDO
NÃO ENTREGOU O RELATÓRIO EXECUTIVO DA VISTORIA PRÉVIA	ATÉ UM DIA, APÓS A DATA DE ENTREGA PREVISTA NO MEMORANDO DE INICIO DE SERVIÇO.	CRÍTICA (ALTO IMPACTO)	TOTAL EMPENHO DA CONTRATADA, INCLUSIVE COM RECURSOS EXTRAS, SE NECESSÁRIO
AMBIENTE INOPERANTE (INDISPONIBILIDADE NO USO DO SOFTWARE)	ATÉ 4 (QUATRO) HORAS, PARA ATENDIMENTO COM SOLUÇÃO DO PROBLEMA, A	CRÍTICA (ALTO IMPACTO)	TOTAL EMPENHO DA CONTRATADA, INCLUSIVE



PROCURADORIA GERAL DO ESTADO

	PARTIR DO RECEBIMENTO DO CHAMADO PELA EQUIPE TÉCNICA DA CONTRATADA		COM RECURSOS EXTRAS, SE NECESSÁRIO
FALHA SIMULTÂNEA OU NÃO (AMBIENTE OPERANDO COM RESTRIÇÕES)	ATÉ 6 (SEIS) HORAS, PARA ATENDIMENTO COM SOLUÇÃO DO PROBLEMA, A PARTIR DO RECEBIMENTO DO CHAMADO PELA EQUIPE TÉCNICA DA CONTRATADA	NORMAL (MÉDIO IMPACTO)	EMPENHO NECESSÁRIO DA CONTRATADA, DE ACORDO COM A QUANTIDADE DE RECURSOS DISPONÍVEIS
PERDA DE EFICÁCIA EM ALGUMA(S) FUNCIONALIDADE(S), COMPROMETENDO O FUNCIONAMENTO DO SISTEMA	ATÉ 2 (DOIS) DIAS ÚTEIS, PARA ATENDIMENTO COM SOLUÇÃO DO PROBLEMA, A PARTIR DO RECEBIMENTO DO CHAMADO PELA EQUIPE TÉCNICA DA CONTRATADA	BAIXA (BAIXO IMPACTO)	EMPENHO DA CONTRATADA, DE ACORDO COM OS RECURSOS PERTINENTES
NÃO ENTREGOU OS SERVIÇOS PREVISTOS NA ORDEM DE SERVIÇO	ATÉ A DATA DE ENTREGA PREVISTA NA ORDEM DE SERVIÇO EMITIDA PELO REPRESENTANTE DA CONTRATANTE	NORMAL (MÉDIO IMPACTO)	EMPENHO NECESSÁRIO DA CONTRATADA, DE ACORDO COM A QUANTIDADE DE RECURSOS DISPONÍVEIS
NÃO ENTREGOU OS SERVIÇOS PREVISTOS NA ORDEM DE SERVIÇO CLASSIFICADOS COMO CRÍTICOS	ATÉ A DATA DE ENTREGA PREVISTA NA ORDEM DE SERVIÇO EMITIDA PELO REPRESENTANTE DA CONTRATANTE	CRÍTICA (ALTO IMPACTO)	TOTAL EMPENHO DA CONTRATADA, INCLUSIVE COM RECURSOS EXTRAS, SE NECESSÁRIO
NÃO FOI APROVADO OS ENTREGÁVEIS PELA COMISSÃO DE FISCALIZAÇÃO	ATÉ DOIS DIAS, PARA ATENDIMENTO COM SOLUÇÃO DO PROBLEMA, A PARTIR DA IDENTIFICAÇÃO OU O RECEBIMENTO DO CHAMADO COM PEDIDO DE AJUSTE DA CONTRATANTE.	CRÍTICA (ALTO IMPACTO)	TOTAL EMPENHO DA CONTRATADA, INCLUSIVE COM RECURSOS EXTRAS, SE NECESSÁRIO
APÓS ABERTURA DO CHAMADO DE SUPORTE TÉCNICO CRÍTICO, A CONTRATADA/FABRICANTE NÃO ATENDEU DENTRO DO TEMPO DE ATENDIMENTO PREVISTO	ATÉ 6 (SEIS) HORAS, PARA ATENDIMENTO, A PARTIR DO RECEBIMENTO DO CHAMADO PELA EQUIPE TÉCNICA DA CONTRATADA	CRÍTICA (ALTO IMPACTO)	TOTAL EMPENHO DA CONTRATADA, INCLUSIVE COM RECURSOS EXTRAS, SE NECESSÁRIO
APÓS ABERTURA DO CHAMADO DE SUPORTE TÉCNICO NORMAL, A CONTRATADA/FABRICANTE NÃO ATENDEU DENTRO DO TEMPO DE ATENDIMENTO PREVISTO	ATÉ 2 (DOIS) DIAS ÚTEIS, PARA ATENDIMENTO, A PARTIR DO RECEBIMENTO DO CHAMADO PELA EQUIPE TÉCNICA DA CONTRATADA	BAIXA (BAIXO IMPACTO)	EMPENHO DA CONTRATADA, DE ACORDO COM OS RECURSOS PERTINENTES

QUADRO II – PONTUAÇÃO

SEVERIDADE	PONTUAÇÃO	CRITÉRIO
CRÍTICA (ALTO IMPACTO)	02 (DOIS) PONTOS A CADA OCORRÊNCIA	PONTUAÇÃO POR NÚMERO DE ATENDIMENTOS FORA DO PRAZO DESCRITO NO QUADRO I, CONFORME REGISTROS NO SISTEMA DE ATENDIMENTO DA PGE/RJ, SEM JUSTIFICATIVA ACEITA PELA FISCALIZAÇÃO. O ATENDIMENTO CONCLUÍDO, MAS NÃO ACEITO PELA GTI, COMO APTO A ATENDER À DEMANDA DO USUÁRIO, TAMBÉM SERÁ CONSIDERADO COMO FORA DO PRAZO ESTABELECIDO.
NORMAL (MÉDIO IMPACTO)	1,5 (UM PONTO E MEIO) A CADA OCORRÊNCIA	
BAIXA (BAIXO IMPACTO)	01 (UM) PONTO A CADA OCORRÊNCIA	



PROCURADORIA GERAL DO ESTADO

12.5 PERIODICIDADE DA APLICAÇÃO DO ANS: Mensal.

12.5.1 **INÍCIO DA MEDIÇÃO:** O ANS terá aplicação inicial (contagem da pontuação) no segundo mês de vigência do Contrato.

12.5.2 **MECANISMO DE CÁLCULO:** Somatório dos pontos, aferidos na forma do Quadro II, o que implicará, eventualmente, em ajustes nos pagamentos mensais, na forma abaixo descrita:

12.5.2.1 Até 2 pontos = recebimento de 100% do valor da fatura de serviços;

12.5.2.2 De 3 a 9 pontos = recebimento de 98% do valor da fatura de serviços;

12.5.2.3 De 10 a 15 pontos = recebimento de 96% do valor da fatura de serviços;

12.5.2.4 Acima de 15 pontos = recebimento de 94% do valor da fatura de serviços.

12.5.3 OBSERVAÇÕES:

12.5.3.1 As penalidades contratuais decorrentes da inexecução dos serviços poderão ser aplicadas independentemente dos descontos aplicados por força do Acordo de Nível de Serviços;

12.5.3.2 Mensalmente, após o último dia do mês, a Comissão de Fiscalização do Contrato da PGE/RJ deverá elaborar relatório, informando à CONTRATADA o resultado da medição dos serviços, mediante aplicação do Acordo de Nível de Serviço, apurado até o segundo dia útil do mês subsequente;

12.5.3.3 O Setor Financeiro da PGE/RJ receberá junto com Nota Fiscal do mês, quando e se for o caso, Relatório contendo a pontuação.

13 DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

A CONTRATANTE deverá:

13.1 Acompanhar e fiscalizar a execução do Contrato por meio de representantes especialmente designados, nos termos do art. 67 da Lei nº 8.666/93 e do Decreto Estadual nº 45.600/2016.

13.2 Manter a CONTRATADA informada acerca da composição da Comissão de Fiscalização, cientificando-lhe para fins de propiciar que seus Prepostos possam reportar eventuais falhas ou problemas detectados, bem como, possam apresentar-lhes os faturamentos correspondentes às prestações executadas.

13.3 Disponibilizar o local e os meios adequados para a execução dos serviços.

13.4 Efetuar os pagamentos nas condições e preços pactuados, especialmente no que diz respeito aos eventuais descontos decorrentes de desconformidades apuradas na prestação dos serviços, ficando esclarecido que estes somente serão aplicados a contar do segundo mês de vigência do Contrato.



PROCURADORIA GERAL DO ESTADO

- 13.5 Prestar as informações e esclarecimentos necessários à execução do objeto contratual pela CONTRATADA.
- 13.6 Documentar e notificar por escrito a CONTRATADA, a ocorrência de eventuais imperfeições, falhas ou irregularidades no curso da execução dos serviços, fixando prazo para a sua correção ou regularização.
- 13.7 Não permitir que pessoas estranhas à CONTRATADA examinem ou provoquem qualquer alteração nos serviços do presente objeto.
- 13.8 Observar e pôr em prática as recomendações técnicas feitas pela CONTRATADA relacionadas às condições de funcionamento, quando julgar pertinente ou oportuno.
- 13.9 Receber provisória e definitivamente o objeto do Contrato nas formas definidas.

14 DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

- 14.1 Prestar os serviços contratados nos termos da legislação vigente e aplicável, bem como, nos termos explicitados no presente instrumento;
- 14.2 Elaborar o Plano de Trabalho, de acordo com as condições estabelecidas pela CONTRATANTE;
- 14.3 Prestar os serviços somente após o recebimento da respectiva Ordem de Serviço – OS emitida pela CONTRATANTE, na qual deverá estar registrada a concordância de, no mínimo, 2 (dois) membros da Comissão de Fiscalização do Contrato;
- 14.4 Cumprir todos os requisitos de segurança da informação, respeitando a preservação do sigilo, da integridade, dos direitos autorais e dos aspectos legais concernentes aos documentos que lhe forem entregues para a prestação dos serviços;
- 14.5 Manter atualizados os números de telefone, os endereços de correio eletrônico ou a área em sítio da web para a abertura de chamados;
- 14.6 Prestar garantia de suporte técnico e atualização dos Softwares, durante todo o período de vigência do Contrato;
- 14.7 Disponibilizar canais de acesso 8X5 (Oito horas, cinco dias na semana), por meio de número de telefone e/ou Internet, para a abertura de chamados técnicos, objetivando a resolução de problemas e dúvidas quanto aos serviços, produtos e funcionamento dos Softwares e permitir a utilização de estrutura de pesquisa em base de conhecimento de solução de problemas e documentos técnicos da CONTRATADA;
- 14.8 Dar garantias técnicas dos serviços executados, durante todo o período de vigência do Contrato;
- 14.9 Comunicar à CONTRATANTE, por escrito, no prazo máximo de 5 (cinco) dias úteis que antecedem o prazo de vencimento das entregas, quaisquer anormalidades que ponham em risco



PROCURADORIA GERAL DO ESTADO

o êxito e o cumprimento dos prazos da execução dos serviços, propondo as ações corretivas necessárias para a execução dos mesmos;

- 14.10 Submeter à aprovação da CONTRATANTE qualquer alteração que se tornar essencial à continuação da execução ou prestação dos serviços;
- 14.11 Arcar com todas as despesas referentes à prestação dos serviços, tais como: despesas com viagens, fretes, seguros, taxas, transportes e embalagens, bem como, os encargos trabalhistas, previdenciários, comerciais e salários dos seus empregados, para entrega do serviço no prazo estipulado;
- 14.12 Comprovar que os responsáveis pelos serviços de consultoria, manutenção e suporte técnico possuam a qualificação técnica necessária do fabricante dos produtos e a experiência comprovada em atividades similares, as quais irão executar, a fim de atender as especificações técnicas contidas neste instrumento, de forma a garantir a máxima qualidade na prestação;
- 14.13 Manter seus funcionários ou representantes credenciados, devidamente identificados, quando da execução de qualquer serviço nas dependências da CONTRATANTE, referente ao objeto contratado, observando as normas de segurança (interna e de conduta);
- 14.14 Indicar o preposto para, em todas as questões relativas ao cumprimento dos serviços, representar a CONTRATADA, de forma a garantir a presteza e a agilidade necessária ao processo decisório, o qual será o responsável da CONTRATADA pela execução deste Contrato e deverá se reportar à CONTRATANTE, indicando seu cargo, endereço com CEP, número de telefone comercial e celular e endereço eletrônico;
- 14.15 Responder integralmente pelos danos causados ao patrimônio da PGE ou de terceiros por seus empregados, direta ou indiretamente, em decorrência de ação ou omissão de seus empregados ou de seus prepostos, devendo ser adotadas, dentro do prazo de 48 (quarenta e oito) horas, as providências necessárias ao integral ressarcimento, não se excluindo ou reduzindo essa responsabilidade;
- 14.16 Designar o preposto para representar administrativamente a CONTRATADA sempre que necessário, o qual deverá estar habilitado a responder qualquer indagação pela CONTRATADA;
- 14.17 Arcar com os ônus resultantes de quaisquer ações, demandas, custos e despesas decorrentes de contravenções, seja por culpa sua ou de quaisquer de seus empregados ou prepostos, obrigando-se, outrossim, a quaisquer responsabilidades decorrentes de ações judiciais ou extrajudiciais de terceiros, que lhe venham a ser exigidas por força da lei, ligadas ao cumprimento do Contrato a ser firmado;



PROCURADORIA GERAL DO ESTADO

- 14.18 Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com a CONTRATANTE;
- 14.19 Responder por todos os vícios e defeitos dos Softwares e dos serviços prestados durante toda a vigência do contrato, contados a partir do aceite definitivo da prestação (atesto);
- 14.20 Manter, durante toda a duração do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas para contratação;
- 14.21 Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados, não podendo invocar posteriormente, desconhecimento para cobrança de serviços extras;
- 14.22 Aceitar, nas mesmas condições pactuadas, os acréscimos ou supressões que se fizerem necessários no objeto, até o limite previsto no parágrafo 1º do art. 65 da Lei nº 8.666/93.

15 QUALIFICAÇÃO TÉCNICA

A licitante vencedora da fase de lances deve apresentar:

- 15.1 Para fins de comprovação da qualificação técnica, deverão ser apresentados os seguintes documentos:
- 15.1.1 Um ou mais atestados de capacidade técnica, emitidos por pessoa jurídica de direito público ou privado, que comprove (m) aptidão pertinente e compatível em características, quantidades e prazos com o objeto da licitação, na forma do artigo 30, § 4º, da Lei Federal nº 8.666/93 que indiquem nome, função, endereço, telefone, e-mail ou telefax de contato do (s) atestador (es), ou qualquer outro meio para eventual contato pelo ÓRGÃO LICITANTE.
- 15.1.2 Poderá ser apresentado mais de um atestado de capacidade técnica, sendo aceito o seu somatório, desde que reste demonstrada a execução concomitante do objeto.
- 15.1.3 A aptidão técnico-operacional para o desempenho de atividade pertinente e compatível em características e quantidades com o objeto desta licitação poderá ser demonstrada pela execução pretérita de, no mínimo, 50% (cinquenta por cento) do quantitativo relativo às parcelas do objeto: Item 01 no quadro descritivo do Item 5 – Do Quantitativo dos Produtos.

16 DA FISCALIZAÇÃO



PROCURADORIA GERAL DO ESTADO

- 16.1 O Contrato deverá ser executado fielmente, de acordo com as cláusulas avançadas, nos termos do instrumento convocatório, do cronograma de execução e da legislação vigente, respondendo o inadimplente pelas consequências da inexecução total ou parcial.
- 16.2 A PGE/RJ manterá, desde o início dos serviços, a seu critério exclusivo, uma Comissão de Fiscalização constituída por 03 (três) membros designados para acompanhamento e controle dos trabalhos.
- 16.3 A CONTRATADA deverá sujeitar-se à fiscalização do órgão CONTRATANTE quanto ao acompanhamento do cumprimento das obrigações pactuadas, prestando-lhe todos os esclarecimentos solicitados, como também, o atendimento às reclamações consideradas procedentes respeitando as exigências quanto à execução dos serviços, horários, qualidade e quantidade dos materiais e providenciar a imediata correção de deficiências constatadas quanto à execução dos serviços contratados.
- 16.4 A CONTRATADA deverá facilitar, por todos os meios ao seu alcance, a ampla ação da Fiscalização, permitindo o acesso aos serviços em execução, bem como, atendendo prontamente às solicitações que lhe forem efetuadas.
- 16.5 A atuação ou a eventual omissão da Fiscalização durante a realização dos trabalhos não poderá ser invocada para eximir a CONTRATADA da responsabilidade pela execução dos serviços.
- 16.6 A Fiscalização tem autonomia para exercer, dentre outras, as seguintes atividades:
- 16.6.1 Exercer rigoroso controle sobre o cronograma de rotinas de execução dos serviços, fazendo com que sejam cumpridas as obrigações assumidas pela CONTRATADA, nos termos estabelecidos no presente instrumento;
 - 16.6.2 Solucionar as dúvidas e questões pertinentes à prioridade ou sequência dos serviços em execução, bem como, às interferências e interfaces dos trabalhos da CONTRATADA com as atividades das unidades desta PGE/RJ;
 - 16.6.3 Paralisar ou solicitar o refazimento de qualquer serviço que não seja executado em conformidade com as normas técnicas ou qualquer disposição aplicável ao objeto do Contrato;
 - 16.6.4 Aprovar partes, etapas ou a totalidade dos serviços executados, verificar e atestar as respectivas medições, bem como, conferir, certificar e encaminhar para pagamento as faturas emitidas pela CONTRATADA, especialmente, no que diz respeito aos eventuais descontos decorrentes de desconformidades apuradas na prestação dos serviços;
 - 16.6.5 Avaliar eventuais acréscimos ou supressões de serviços necessários ao perfeito atendimento do objeto do Contrato;



PROCURADORIA GERAL DO ESTADO

16.6.6 Relatar à CONTRATADA, para análise de possível substituição, os casos em que qualquer de seus empregados embarace ou dificulte a ação da Fiscalização ou cuja presença no local dos serviços seja considerada prejudicial ou inadequada ao andamento dos trabalhos

17 DAS CONDIÇÕES DE PAGAMENTO

17.1 Após a aceitação definitiva dos produtos e serviços, a CONTRATANTE autorizará a CONTRATADA a realizar a emissão da Nota Fiscal/Fatura, conforme tabela abaixo:

ITENS	DESCRIÇÃO	UNIDA DE	PRAZO	CONDIÇÕES DE PAGAMENTO
01	Serviços de Fornecimento, implantação e sustentação dos softwares com atualização (updates/upgrades)	Mensal	Até 30 dias consecutivos da implantação dos softwares	O pagamento será mensal em 36 parcelas, mediante a emissão da fatura que deverá ocorrer após a entrega do relatório técnico consolidado e aceite total da execução dos serviços pela Comissão de Fiscalização da PGE.

17.2 A CONTRATADA deverá indicar na Nota Fiscal/Fatura o número do Contrato (empenho) firmado com a CONTRATANTE.

17.3 Satisfeitas as obrigações previstas nas cláusulas contratuais e cumpridos os requisitos constantes dos itens anteriores, a CONTRATADA deverá encaminhar as faturas à Comissão de Fiscalização da PGE/RJ para pagamento.

17.4 A Comissão de Fiscalização do Contrato terá o prazo de até 15 (quinze) dias para atestar a nota fiscal e encaminhá-la para pagamento.

17.5 Os pagamentos serão efetuados por meio de crédito em conta corrente da instituição financeira contratada pelo Estado do Rio de Janeiro – atualmente o Banco Bradesco S/A –, cujo número e agência deverão ser informados pela CONTRATADA até a assinatura do Contrato.

17.6 No caso de a CONTRATADA estar estabelecida em localidade que não possua agência da instituição financeira contratada pelo Estado do Rio de Janeiro, ou caso, verificada pelo Órgão Gestor a impossibilidade de a CONTRATADA, em razão de negativa expressa da instituição financeira contratada pelo Estado do Rio de Janeiro, abrir ou manter conta corrente naquela instituição financeira, o pagamento poderá ser feito mediante crédito em conta corrente de outra instituição. Nesse caso, eventuais ônus financeiros e/ou contratuais adicionais serão suportados exclusivamente pela CONTRATADA. O prazo para pagamento das faturas será de 30 (trinta) dias, contados da data da entrada do documento de crédito na repartição competente, isenta de



PROCURADORIA GERAL DO ESTADO

erros, previamente atestado por servidores que não o ordenador de despesas, designados para a Fiscalização do Contrato:

17.6.1 O pagamento referente ao item concernente aos serviços de consultoria (UST) será realizado nos moldes estabelecidos na Ordem de Serviços, após a conclusão dos trabalhos planejados e do respectivo aceite pela Comissão de Fiscalização da PGE/RJ;

17.6.2 Caso se faça necessária a reapresentação de qualquer fatura por culpa da CONTRATADA, o prazo de 30 (trinta) dias ficará suspenso, prosseguindo a sua contagem a partir da data da respectiva reapresentação.

17.7 Os pagamentos eventualmente realizados com atraso, desde que não decorram de ato ou fato atribuível à CONTRATADA, sofrerão a incidência de atualização financeira pelo Índice Nacional de Preços ao Consumidor – INPC, calculado e divulgado pelo Instituto Brasileiro de Geografia e Estatísticas – IBGE, e juros moratórios de 0,5% ao mês, calculado pro rata die;

17.8 Os pagamentos devidos à CONTRATADA não excederão os valores apresentados em sua proposta comercial e observarão eventuais descontos decorrentes da aplicação do Acordo de Nível de Serviço – ANS previsto neste instrumento.

18 DA GARANTIA CONTRATUAL

18.1 Exigir-se-á da CONTRATADA, no prazo máximo de 10 (dez) dias consecutivos, contados da data constante do Memorando de Início de Serviços, uma garantia, a ser prestada durante toda a vigência do Contrato, em qualquer das modalidades previstas no parágrafo 1º do art. 56 da Lei n.º 8.666/93, no montante de 5 % (cinco por cento) do valor do Contrato, a ser restituída após sua execução satisfatória.

18.2 A garantia prestada não poderá se vincular a outras contratações, salvo após sua liberação.

18.3 Caso o valor do Contrato seja alterado, de acordo com o art. 65 da Lei n.º 8.666/93, a garantia deverá ser complementada no prazo de 72 (setenta e duas) horas, mantendo o percentual de 5% (cinco por cento) do valor do Contrato.

18.4 Nos casos em que valores de multas eventualmente aplicadas venham a ser descontados da garantia, seu valor original deverá ser recomposto no prazo máximo de 72 (setenta e duas) horas, sob pena de rescisão administrativa do Contrato.

19 DAS SANÇÕES ADMINISTRATIVAS

19.1 A inexecução dos serviços, total ou parcial, a execução imperfeita, a mora na execução ou qualquer inadimplemento ou infração contratual, sujeitará a CONTRATADA, sem prejuízo da



PROCURADORIA GERAL DO ESTADO

responsabilidade civil ou criminal que couber, às sanções previstas na Lei n.º 8.666/93 e demais normas pertinentes, assegurados, nos termos da lei, a ampla defesa e o contraditório.

19.2 A multa administrativa prevista no inciso II do art. 87 da Lei n.º 8.666/93, corresponderá ao valor de até 5% (cinco por cento) do Contrato, aplicada de acordo com a gravidade da infração e proporcionalmente às parcelas não executadas, e poderá ser aplicada cumulativamente a qualquer outra penalidade, não possuindo caráter compensatório, e o seu pagamento não exime a responsabilidade por perdas e danos das infrações cometidas.

19.3 Nas reincidências específicas, a multa corresponderá ao dobro do valor da que tiver sido inicialmente imposta, observando-se sempre o limite de 20% (vinte por cento), conforme preceitua o artigo 87 do Decreto n.º 3.149/80.

20 DA VISTORIA

20.1 É facultado aos interessados vistoriar as dependências da PGE/RJ, com o objetivo de conhecer o local e as condições para a prestação dos serviços, objeto desta contratação.

20.2 A opção pela vistoria constitui direito e ônus do interessado, com vistas à elaboração precisa e técnica de sua proposta, mas que não ostenta caráter eliminatório do certame para fins de exame de habilitação. Se, facultativamente, o interessado resolver não vistoriar os locais onde serão prestados os serviços, objeto da contratação, no caso de não contratação, não poderá alegar desconhecimento das condições dos locais como pretexto para eventual inexecução total ou parcial do Contrato ou atrasos em sua implementação.

20.3 O agendamento para a realização da vistoria poderá ser feito com a Gerência de Tecnologia da Informação da PGE/RJ, por meio dos telefones (21) 2332-9401, no horário de 10h às 12h e 14h às 17h.

21 DAS CONSIDERAÇÕES FINAIS

21.2 Antes de apresentar a proposta, a CONTRATADA deverá realizar todos os levantamentos essenciais, de modo a não incorrer em omissões que jamais poderão ser alegadas ao tempo do fornecimento em favor de eventuais pretensões de acréscimos de preços, alteração de data de entrega ou alteração de qualidade.

21.3 O preço total proposto deverá considerar a consecução do objeto da presente contratação, englobando todos os custos diretos e indiretos.

21.4 Cabe à CONTRATADA consultar com antecedência os seus fornecedores quanto aos prazos de entrega, não cabendo, portanto, a justificativa de atraso do fornecimento devido ao não cumprimento da entrega por parte dos fornecedores.



PROCURADORIA GERAL DO ESTADO

21.5 Os casos omissos serão analisados pela Procuradoria Geral do Estado, à luz da legislação vigente, subsidiando posteriores decisões administrativas.

Rio de Janeiro, 10 de junho de 2020.



PROCURADORIA GERAL DO ESTADO

ANEXO I

TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO

PROCESSO ADMINISTRATIVO N.º	
PROCESSO LICITATÓRIO	
OBJETO	
CONTRATO N.º	

A **PGE-RJ**, com sede no Rio de Janeiro-RJ, inscrito no CNPJ sob o nº _____, e a **Empresa** _____, estabelecida à _____, CEP: _____, inscrita no CNPJ sob o nº _____, doravante denominada simplesmente **CONTRATADA**, representada neste ato pelo **Sr** _____, (cargo) _____, (nacionalidade) - _____, (estado civil) _____, (profissão) _____, portador da Cédula de Identidade nº _____, e do CPF nº _____, residente e domiciliado em _____, e, sempre que em conjunto referidas como **PARTES** para efeitos deste **TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO**, doravante denominado simplesmente **TERMO**.

CONSIDERANDO que, em razão do atendimento à exigência do Contrato Nº XX/20XX, celebrado pelas **PARTES**, doravante denominado **CONTRATO**, cujo objeto é a <objeto do Contrato>, mediante condições estabelecidas pelo **CONTRATANTE**;

CONSIDERANDO que o presente **TERMO** vem para regular o uso dos dados, regras de negócio, documentos, informações, sejam elas escritas ou verbais ou de qualquer outro modo apresentada, tangível ou intangível, entre outras, doravante denominadas simplesmente de **INFORMAÇÕES**, que a **CONTRATADA** tiver acesso em virtude da execução contratual;

CONSIDERANDO a necessidade de manter sigilo e confidencialidade, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da **PGE/RJ** de que a **CONTRATADA** tomar conhecimento em razão da execução do **CONTRATO**, respeitando todos os critérios estabelecidos aplicáveis às **INFORMAÇÕES**;

A **PGE** estabelece o presente **TERMO** mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA - DO OBJETO



PROCURADORIA GERAL DO ESTADO

O objeto deste **TERMO** é prover a necessária e adequada **PROTEÇÃO ÀS INFORMAÇÕES** da **PGE/RJ**, principalmente aquelas classificadas como **CONFIDENCIAIS**, em razão da execução do **CONTRATO** celebrado entre as PARTES.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

Parágrafo Primeiro: As estipulações e obrigações constantes do presente instrumento serão aplicadas a todas e quaisquer **INFORMAÇÕES** reveladas pela **PGE/RJ**.

Parágrafo Segundo: A **CONTRATADA** se obriga a manter o mais absoluto sigilo e confidencialidade com relação a todas e quaisquer **INFORMAÇÕES** que venham a ser fornecidas pela **PGE/RJ**, a partir da data de assinatura deste **TERMO**, devendo ser tratadas como **INFORMAÇÕES CONFIDENCIAIS**, salvo aquelas prévia e formalmente classificadas com tratamento diferenciado pela **PGE/RJ**.

Parágrafo Terceiro: A **CONTRATADA** se obriga a não revelar, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que nenhum de seus diretores, empregados e/ou prepostos faça uso das **INFORMAÇÕES** da **PGE/RJ**.

Parágrafo Quarto: A **PGE/RJ**, com base nos princípios instituídos na Segurança da Informação, zelará para que as **INFORMAÇÕES** que receber e tiver conhecimento sejam tratadas conforme a natureza de classificação informada pela **CONTRATADA**.

CLÁUSULA TERCEIRA - DAS LIMITAÇÕES DA SEGURANÇA DADE

Parágrafo Único: As obrigações constantes deste **TERMO** não serão aplicadas às **INFORMAÇÕES** que:

- I.** Sejam comprovadamente de domínio público no momento da revelação ou após a revelação, exceto se isso ocorrer em decorrência de ato ou omissão das PARTES;
- II.** Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente **TERMO**;
- III.** Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo Estadual, somente até a extensão de tais ordens, desde que as PARTES cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.



PROCURADORIA GERAL DO ESTADO

CLÁUSULA QUARTA - DAS OBRIGAÇÕES ADICIONAIS

Parágrafo Primeiro: A **CONTRATADA** se compromete a utilizar as **INFORMAÇÕES** reveladas exclusivamente para os propósitos da execução do **CONTRATO**.

Parágrafo Segundo: A **CONTRATADA** se compromete a não efetuar qualquer cópia das **INFORMAÇÕES** sem o consentimento prévio e expresso da **PGE/RJ**.

- I. O consentimento mencionado no Parágrafo segundo, entretanto, será dispensado para cópias, reproduções ou duplicações para uso interno das **PARTES**.

Parágrafo Terceiro: A **CONTRATADA** se compromete a cientificar seus diretores, empregados e/ou prepostos da existência deste **TERMO** e da natureza confidencial das **INFORMAÇÕES** da **PGE/RJ**.

Parágrafo Quarto: A **CONTRATADA** deve tomar todas as medidas necessárias à proteção das **INFORMAÇÕES** da **PGE/RJ**, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela **PGE/RJ**.

Parágrafo Quinto: Cada **PARTE** permanecerá como única proprietária de todas e quaisquer **INFORMAÇÕES** eventualmente reveladas à outra parte em função da execução do **CONTRATO**.

Parágrafo Sexto: O presente **TERMO** não implica a concessão, pela parte reveladora à parte receptora, de nenhuma licença ou qualquer outro direito, explícito ou implícito, em relação a qualquer direito de patente, direito de edição ou qualquer outro direito relativo à propriedade intelectual.

- I. Os produtos gerados na execução do **CONTRATO**, bem como as **INFORMAÇÕES** repassadas à **CONTRATADA**, são única e exclusiva propriedade intelectual da **PGE/RJ**.

Parágrafo Sétimo: A **CONTRATADA** firmará acordos por escrito com seus empregados e consultores ligados direta ou indiretamente ao **CONTRATO**, cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente instrumento.

Parágrafo Oitavo: A **CONTRATADA** obriga-se a não tomar qualquer medida com vistas a obter, para si ou para terceiros, os direitos de propriedade intelectual relativos aos produtos gerados e às **INFORMAÇÕES** que venham a ser reveladas durante a execução do **CONTRATO**.

CLÁUSULA QUINTA - DO RETORNO DE INFORMAÇÕES



PROCURADORIA GERAL DO ESTADO

Parágrafo Único: Todas as **INFORMAÇÕES** reveladas pelas PARTES permanecem como propriedade exclusiva da parte reveladora, devendo a esta retornar imediatamente assim que por ela requerido, bem como todas e quaisquer cópias eventualmente existentes.

- I. A **CONTRATADA** deverá devolver, íntegros e integralmente, todos os documentos a ela fornecida, inclusive as cópias porventura necessárias, na data estipulada pela **PGE/RJ** para entrega, ou quando não mais for necessária a manutenção das Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias.
- II. A **CONTRATADA** deverá destruir quaisquer documentos por ela produzidos que contenham Informações Confidenciais da **PGE/RJ**, quando não mais for necessária a manutenção dessas Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades previstas neste Termo.

CLÁUSULA SEXTA - DA VIGÊNCIA

Parágrafo Único: O presente **TERMO** tem natureza irrevogável e irretroatável, permanecendo em vigor desde a data de sua assinatura até 5 (cinco) anos após o término do Contrato.

CLÁUSULA SÉTIMA - DAS PENALIDADES

Parágrafo Único: A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na **RESCISÃO DO CONTRATO** firmado entre as PARTES. Neste caso, a **CONTRATADA**, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela **PGE/RJ**, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

CLÁUSULA OITAVA - DAS DISPOSIÇÕES GERAIS

Parágrafo Primeiro: Este **TERMO** constitui vínculo indissociável ao **CONTRATO**, que é parte independente e regulatória deste instrumento.



PROCURADORIA GERAL DO ESTADO

Parágrafo Segundo: O presente **TERMO** constitui acordo entre as PARTES, relativamente ao tratamento de **INFORMAÇÕES**, principalmente as **CONFIDENCIAIS**, aplicando-se a todos e quaisquer acordos futuros, declarações, entendimentos e negociações escritas ou verbais, empreendidas pelas PARTES em ações feitas direta ou indiretamente.

Parágrafo Terceiro: Surgindo divergências quanto à interpretação do pactuado neste **TERMO** ou quanto à execução das obrigações dele decorrentes, ou constatando-se nele a existência de lacunas, solucionarão as PARTES tais divergências, de acordo com os princípios da legalidade, da equidade, da razoabilidade, da economicidade, da boa-fé, e, as preencherão com estipulações que deverão corresponder e resguardar as **INFORMAÇÕES** da **PGE/RJ**.

Parágrafo Quarto: O disposto no presente **TERMO** prevalecerá sempre em caso de dúvida, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos legais conexos relativos à **CONFIDENCIALIDADE DE INFORMAÇÕES**.

Parágrafo Quinto: A omissão ou tolerância das PARTES, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo.

CLÁUSULA NONA - DO FORO

Parágrafo Único: Fica eleito o foro da _____, em _____-RJ, para dirimir quaisquer dúvidas oriundas do presente **TERMO**, com renúncia expressa a qualquer outro, por mais privilegiado que seja. E, por assim estarem justas e estabelecidas as condições, a **CONTRATADA** assina o presente **TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO**, em 2 (duas) vias de igual teor e um só efeito, na presença de duas testemunhas.

Rio de Janeiro/RJ, ____ de _____ de 20 ____.

Representante da Gerência de Tecnologia da
Informação
Cargo

Nome do Diretor/representante legal da
empresa
Cargo