

Equipe Responsável	
Elaboração	
Divisão de Gestão de Planejamento e Contratação de Infraestrutura de TIC <b>DPCI</b>	Natália Barbosa Ramos 359.394
Aprovação Motivada	
<p>Considerando que o Termo de Referência elaborado se apresenta de forma conveniente e oportuna para atender a demanda exposta no <b>Estudo Técnico</b>, encaminho este Termo para aprovação. Os elementos para que as empresas especifiquem seus preços estão no Termo de Referência e o valor da estimativa será incluído oportunamente no processo, após pesquisa ao mercado pela área competente.</p>	
Divisão de Planejamento de Infraestrutura de TIC <b>DIPL</b>	Carlos Alberto Quintanilha Neto 340.294
Divisão de Gestão de Treinamento e Desenvolvimento <b>DIGT</b>	Raquel Goncalves Losekann 348.830
Divisão de Sustentação de Plataformas de Segurança <b>DSPS</b>	Felipe Queto de Souza Pinto 363.979
Departamento de Gestão Técnica de Infraestrutura de TIC <b>DEGI</b>	Sonia da Silva Pereira Garcia 286.800
Departamento de Planejamento e Serviços de Infraestrutura de TIC <b>DEPS</b>	Carlos Wagner da Silva 346.241
Departamento de Segurança Operacional de Infraestrutura de TIC <b>DESO</b>	Marcelo Andre Ferreira Silva 335.622
Superintendência de Planejamento e Gestão Técnica de Infraestrutura de TIC <b>SUPI</b>	Leandro Cianconi de Paiva Rodas 352.926
Superintendência de Gestão de Data Center <b>SUGD</b>	Bruno Manhaes de Souza 335.991

## **Sumário**

- [1. OBJETO](#)
- [2. DOCUMENTAÇÃO OBRIGATÓRIA](#)
- [3. PROVA DE CONCEITO](#)
- [4. PLANEJAMENTO](#)
- [5. ENTREGA](#)
- [6. INSTALAÇÃO](#)
- [7. ORIENTAÇÃO TÉCNICA](#)
- [8. CONDIÇÕES GERAIS PARA PRESTAÇÃO DOS SERVIÇOS DE GARANTIA](#)
- [9. ATUALIZAÇÃO DE LICENÇA DE \*SOFTWARE\*](#)
- [10. SUPORTE TÉCNICO](#)
- [11. REGISTRO E ATENDIMENTO DE OCORRÊNCIAS](#)
- [12. PRAZO PARA SOLUÇÃO DAS OCORRÊNCIAS](#)
- [13. RELATÓRIOS](#)
- [14. ACESSO AO SITE DO FABRICANTE](#)
- [15. USO DA LÍNGUA PORTUGUESA](#)
- [16. SIGILO E INVIOABILIDADE](#)
- [17. REMANEJAMENTO DE PRODUTOS](#)
- [18. SANÇÕES ADMINISTRATIVAS](#)
- [19. AVALIAÇÃO DO FORNECEDOR](#)
- [20. OBRIGAÇÕES DA CONTRATADA](#)
- [21. OBRIGAÇÕES DA CONTRATANTE](#)
- [22. FATURAMENTO](#)
- [23. PAGAMENTO](#)
- [24. VIGÊNCIA CONTRATUAL](#)
- [25. GESTÃO CONTRATUAL](#)
- [26. ANEXOS](#)

## 1. OBJETO

1.1. Trata o presente processo da aquisição de **Solução de Firewalls de Rede** com garantia pelo período de **60 (sessenta) meses**, para instalação nos *Data Centers* da Dataprev, incluindo prestação dos serviços de capacitação e orientação técnica a serem utilizadas **sob demanda**.

1.2. A contratação deverá considerar os itens definidos abaixo, a saber:

LOTE ÚNICO			
ITEM	DESCRIÇÃO / PRODUTO	QUANTIDADE TOTAL	UNIDADE
1	a) Solução de Firewall de Rede <i>on-premises</i> com garantia, suporte e atualização de conteúdo de segurança para 60 meses (Tipo I).	6	Equipamento
	b) Solução de Firewall de Rede <i>on-premises</i> com garantia, suporte e atualização de conteúdo de segurança para 60 meses (Tipo II).	6	Equipamento
	c) Gerenciamento Centralizado da Solução de Firewall de Rede <i>on-premises</i> com garantia, suporte e atualização de conteúdo de segurança para 60 meses.	1	Solução
	d) Serviço de Instalação para solução de Gerenciamento Centralizado	1	Serviço
	e) Serviço de Instalação para a solução de Firewall de Rede	12	Serviço
	f) Orientação Técnica	640	Hora
	g) Capacitação Técnica	2	Turma

1.3. Esta contratação será realizada na modalidade de **Pregão**.

1.4. Será permitida a formação de consórcio de empresas para esta contratação.

1.5. Quaisquer equipamentos e/ou componentes (*hardware* e *software*) necessários ao pleno funcionamento da solução, mesmo que não solicitados explicitamente, deverão ser incluídos no fornecimento.

1.6. Os equipamentos que constituem a solução a ser fornecida deverão ser novos e com versão de *software* atualizada, não sendo aceitos equipamentos remanufaturados.

1.7. Os produtos que compõem a solução não devem estar com término de comercialização (*End-of-Sale*) anunciado, isto é, devem estar em produção e serem comercializados pelo fabricante no momento da assinatura do Pedido de Compra / Contrato. Após ser anunciado o término da comercialização (*End-of-Sale*) dos produtos que o compõem a solução, o suporte (*End-of-Support*) deverá permanecer por, no mínimo, o período de vigência da garantia.

1.8. A especificação técnica da **Solução de Firewalls de Rede** a ser adquirida está contida no **ANEXO I – ESPECIFICAÇÃO TÉCNICA** deste **Termo de Referência**.

1.9. As condições gerais de Capacitação Técnica estão contidas no **ANEXO V – CAPACITAÇÃO TÉCNICA** deste **Termo de Referência**.

## 2. DOCUMENTAÇÃO OBRIGATÓRIA

2.1. A **LICITANTE** deverá encaminhar os seguintes documentos para efeitos de classificação e habilitação:

No mínimo, 01 (um) atestado de capacidade técnica (declaração ou certidão), conforme **ANEXO III – MODELO DE ATESTADO OU DECLARAÇÃO DE CAPACIDADE TÉCNICA**, emitido por empresa pública ou privada, contendo identificação da empresa e nome completo do responsável pela emissão, comprovando o perfeito cumprimento das obrigações relativas ao fornecimento de **Solução de Firewalls de Rede**, com características técnicas e complexidade similares ao objeto especificado neste **Termo de Referência** informando o período de serviços superior a **12 (doze)** meses e o local da prestação dos serviços de instalação, suporte técnico, capacitação e orientação técnica. Caso seja necessário, a **LICITANTE** vencedora poderá apresentar mais de um atestado, a fim de comprovar a capacidade nos serviços citados.

2.1.1. A **DATAPREV** poderá realizar diligência/visita técnica a fim de complementar informações ou de comprovar a veracidade do(s) Atestado(s) de Capacidade Técnica apresentado(s) pela **LICITANTE** convocada, quando poderá ser requerida cópia do(s) contrato(s), nota(s) fiscal(is) ou qualquer outro documento que comprove inequivocamente que o serviço apresentado no(s) atestado(s) foi prestado.

2.1.2. Proposta técnica comercial, que deve obrigatoriamente:

a) Informar sobre a concordância com todos os termos descritos neste **Termo de Referência**;

b) Ser elaborada utilizando a Planilha de Formação de Preços, **ANEXO II** deste **Termo de Referência**;

c) Informar que os valores apresentados incluem os impostos federais, estaduais e municipais, taxas e todos os demais custos envolvidos no escopo desta contratação, tais como frete, embalagem, seguro etc.;

d) Descrever a arquitetura da solução ofertada, relacionado todos os itens de *hardware* e/ou *software* que a comporão, informando suas respectivas quantidades, modelo e fabricante, além de suas características técnicas, em conformidade com o solicitado no **ANEXO I – ESPECIFICAÇÃO TÉCNICA**;

e) Ser apresentado em papel timbrado da empresa e assinada pelo responsável pelo contrato.

**2.1.3.** A **LICITANTE** deverá apresentar documentação que comprove a homologação e a certificação da Agência Nacional de Telecomunicações (ANATEL) para os equipamentos ofertados.

### 3. PROVA DE CONCEITO

**3.1.** Concluída a etapa de lances do pregão e identificado o **LICITANTE**, provisoriamente em primeiro lugar, a partir da solicitação do pregoeiro na sessão pública, a **DATAPREV** dará início à fase de **Prova de Conceito da Solução de Firewalls de Rede**.

**3.1.1.** A prova de conceito compreende:

a) **Definição de Ambiente:** A **LICITANTE**, provisoriamente em primeiro lugar, deverá se reunir com a equipe técnica da **DATAPREV**, no Rio de Janeiro, em local a ser definido pela **DATAPREV** ou por videoconferência, no **prazo máximo de 10 (dez) dias úteis** após solicitação formal da **DATAPREV**, descrita no **subitem 3.1**.

A data da reunião deverá ser agendada em comum acordo com a **DATAPREV**.

Nesta reunião:

- A **LICITANTE** deverá informar todos os requisitos necessários ao dimensionamento adequado da infraestrutura física do ambiente a ser disponibilizado pela **DATAPREV** (tamanho da sala, quantidade de pontos elétricos, quantidade de pontos de rede, temperatura ideal etc.), para que a solução apresentada pela **LICITANTE** possa ser avaliada;

- Deverá ser definida a lista de produtos que serão entregues na etapa seguinte.

Caso a reunião não ocorra por problema único e exclusivo da **LICITANTE**, a Prova de Conceito acontecerá no ambiente padrão de teste da **DATAPREV**. Nesta situação é vedada à **LICITANTE** reivindicar qualquer adaptação na infraestrutura oferecida pela **DATAPREV**.

b) **Entrega e Instalação:** A **LICITANTE** deverá entregar e instalar a quantidade mínima de equipamentos e licenças de *software* que contemple todas as funcionalidades especificadas para a **Solução de Firewalls de Rede** no endereço abaixo, no **prazo máximo de 20 (vinte) dias úteis**, contados a partir do dia seguinte à realização da reunião descrita na alínea “a” ou o fim do prazo para sua realização, o que ocorrer primeiro, em horário comercial (9:00 às 18:00 horas). A **LICITANTE** deverá disponibilizar 01 (um) técnico que se responsabilizará pela montagem da solução. A **LICITANTE** deverá apresentar a documentação técnica da **Solução de Firewalls de Rede**, contemplando informações detalhadas de todos os itens e modelos que compõe a solução, conforme descrito **ANEXO I – ESPECIFICAÇÃO TÉCNICA**.

**Departamento de Planejamento e Serviços de Infraestrutura de TIC – DEPS**

**Endereço: Rua Professor Álvaro Rodrigues, 460, Botafogo – Rio de Janeiro – CEP 22280-040.**

- A **LICITANTE** deverá prover todo o ambiente necessário (componentes de *hardware* e *software*), no endereço acima, para comprovação do atendimento às funcionalidades do **ANEXO I – ESPECIFICAÇÃO TÉCNICA**. O provimento do ambiente utilizado exclusivamente para os testes da etapa de prova de conceito inclui o fornecimento dos acessórios como: gerador de tráfego para os testes de *throughput*, o simulador de WAN, *switches*, roteadores, transceptores, cabos e demais recursos requeridos para conexão remota. A critério da **DATAPREV**, a composição do ambiente necessário poderá ser realizada em conjunto.

- A **DATAPREV** fornecerá para a prova de conceito a energia elétrica, climatização e rack de 19 polegadas para a instalação dos equipamentos que serão de responsabilidade da **LICITANTE**.

c) **Comprovação:** esta etapa será realizada por um **período máximo de 20 (vinte) dias úteis**, com **carga diária de 6 (seis) horas**, a contar do dia seguinte à conclusão do prazo para a etapa de Entrega e Instalação (alínea “b”), conforme informado pelo pregoeiro em sessão pública. A partir do primeiro dia desta etapa, a **LICITANTE** deverá:

- Entregar o **ANEXO I – ESPECIFICAÇÃO TÉCNICA** preenchido, informando no campo próprio, a página da documentação técnica que referência o requisito a ser avaliado. Caso existam requisitos não descritos na documentação técnica que sejam atestados exclusivamente por meio de testes na Prova de Conceito, o respectivo campo do **ANEXO I – ESPECIFICAÇÃO TÉCNICA** deverá ser preenchido com o texto “COMPROVAÇÃO PRÁTICA”.

- Disponibilizar 01 (um) técnico que se responsabilizará pela comprovação das funcionalidades e requisitos em conformidade com o **ANEXO I – ESPECIFICAÇÃO TÉCNICA**, por meio de testes práticos ou por comandos de configuração. A aprovação das funcionalidades existentes na **Solução de Firewalls de Rede** apresentada pela **LICITANTE** serão efetuadas pela Equipe Técnica da **DATAPREV**.

Durante a realização da etapa da Comprovação da Prova de Conceito, se a **LICITANTE** identificar a necessidade de realizar alteração de versão de S.O. (Sistema operacional) de algum dispositivo entregue, poderá realizar tal procedimento de substituição de versão, uma única vez. Todo e qualquer ônus, oriundo dessa atualização é de responsabilidade exclusiva da LICITANTE, podendo a **DATAPREV** exigir nova comprovação de funcionalidades já testadas com a versão anterior de S.O. (Sistema operacional). A entrega do **ANEXO I – ESPECIFICAÇÃO TÉCNICA** devidamente preenchido não exclui a necessidade de comprovação do atendimento aos requisitos por meio de testes práticos ou por comandos de configuração durante a realização da **Prova de Conceito**. No entanto, os itens destacados no **ANEXO I – ESPECIFICAÇÃO TÉCNICA** com o termo “aceita-se documentação”, não necessitarão de comprovação prática na Prova de Conceito.

Todos os requisitos descritos no **ANEXO I – ESPECIFICAÇÃO TÉCNICA** devem poder ser validados concomitantemente sem prejuízo de funcionalidade ou desempenho, conforme necessidade da **DATAPREV**.

d) **Local e Horário da Prova de Conceito:** a prova acontecerá no local de entrega do equipamento durante o horário comercial (9:00 às 18:00 horas), respeitando a carga horária diária de 6 (seis) horas. Os horários de início e intervalos serão definidos em comum acordo entre a **LICITANTE** e a Equipe Técnica da **DATAPREV**.

- 3.2. Caso a **LICITANTE** não atenda as condições definidas nas alíneas “b” ou “c” do **subitem 3.1.1** deste **Termo de Referência**, ou seja, se porventura a **Solução de Firewalls de Rede** for entregue/instalado fora do prazo estabelecido, ou caso seja constatado o não atendimento a qualquer item de caráter técnico, a **LICITANTE** será **DECLASSIFICADA**.
- 3.3. Todos os itens do **ANEXO I – ESPECIFICAÇÃO TÉCNICA** deverão ser documentados com evidências sobre o atendimento à Especificação Técnica, incluindo os itens onde exige-se testes práticos, e aqueles onde aceita-se documentação.
- 3.3.1. Os documentos de evidência deverão ser gerados individualmente para cada item, em formato .pdf, organizados em pastas, e o nome do arquivo deverá identificar o respectivo item. (Ex: “Item 1.1\Evidencias - Item 1.1.pdf”).
- 3.3.2. Arquivos de imagens deverão ser salvos separadamente nas respectivas pastas, para que a resolução seja mantida no arquivo original, devido à perda de qualidade na compactação do documento PDF.
- 3.3.3. Os documentos de evidências de todos os itens da especificação técnica (comprovação prática obrigatória e dispensada) deverão ser apresentados durante o período da etapa de Comprovação. Não serão aceitos documentos entregues após o prazo estabelecido no **subitem 3.1.1 c)**.
- 3.3.4. Os documentos de evidências deverão conter:
- a) Cabeçalho de identificação da licitante e do processo;
  - b) Código do Item e descrição da Especificação Técnica;
  - c) Para os itens de Comprovação Prática:
    - Forma de comprovação: Texto descritivo sobre a forma e defesa do atendimento ao item;
    - Evidências: Captura da tela do manual ou documentação técnica do fabricante, captura de telas do software e/ou fotos do equipamento utilizados na comprovação do item, contendo data e hora de forma a apresentar cronologicamente a demonstração do item. Deve-se ainda apresentar legenda para cada captura de tela/foto e uma breve explicação textual do que foi realizado;
    - Referências e anexos (manuais e documentos técnicos do fabricante), com indicação das páginas do documento utilizado na comprovação.
  - d) Para os itens em que é dispensada comprovação prática (aceita-se documentação):
    - Forma de comprovação: Texto descritivo com a defesa de atendimento ao item;
    - Conteúdo: Captura da tela do manual ou documentação técnica do fabricante que comprova atendimento ao item;
    - Referências e anexos (manuais e documentos técnicos do fabricante), com indicação das páginas do documento utilizado na comprovação.
- 3.4. Concluída a **Prova de Conceito** da **Solução de Firewalls de Rede** e verificado o atendimento de todas as condições supracitadas no **subitem 3.1.1**, não havendo, portanto, anormalidades e/ou sanados todos os problemas detectados, a **DATAPREV** emitirá em **até 10 (dez) dias úteis**, o **Termo de Aprovação** da **Prova de Conceito** da **Solução de Firewalls de Rede**.
- 3.5. A realização da **Prova de Conceito** poderá ser acompanhada por todos os **LICITANTES** e demais interessados neste processo.
- 3.6. Solicitações excepcionais de alteração dos prazos descritos nas alíneas “a”, “b” e “c” do **item 3.1.1** poderão ser avaliadas a critério da **DATAPREV** quando objetivamente apresentadas e justificadas.
- 3.7. Os equipamentos utilizados nesta **Prova de Conceito**, caso sejam aprovados, podem ser entregues como parte da oferta do objeto da contratação, desde que atendam às exigências deste **Termo de Referência**. Porém, ao término da Prova de Conceito, devem ser retirados pela **LICITANTE** e somente entregues novamente após a assinatura do **Pedido de Compra/Contrato**. A **DATAPREV** não permite que os produtos da Prova de Conceito sejam mantidos nas dependências da **DATAPREV**, após o término da Prova de Conceito.
- 3.8. Todos os itens da Solução de Firewalls de Rede que forem submetidos à Prova de Conceito deverão ser iguais aos que serão fornecidos posteriormente, na etapa de Entrega, conforme **item 5** deste Termo de Referência.

#### 4. PLANEJAMENTO

- 4.1. A **CONTRATADA** deverá se reunir com o **Gestor Técnico** do contrato, conforme descrito no **subitem 25.1** deste **Termo de Referência**, e com a Equipe Técnica responsável pelo gerenciamento da implantação da solução, no Rio de Janeiro, em local a ser definido pela **DATAPREV** ou por videoconferência, no prazo máximo de **10 (dez) dias úteis** contados a partir do dia seguinte à assinatura do Contrato / Pedido de Compra (PC). A data da reunião deverá ser agendada em comum acordo com a **DATAPREV**.

Nesta reunião a **CONTRATADA** deverá:

- 4.1.1. Apresentar as características dos produtos fornecidos, além de tratar das informações sobre o planejamento e cronograma da sua instalação, além de esclarecer todos os questionamentos técnicos. A **DATAPREV** definirá, com o apoio da equipe técnica da **CONTRATADA** de que forma os produtos deverão ser instalados e configurados. A **CONTRATADA** e a **DATAPREV**, em comum acordo, deverão fazer um planejamento das atividades de instalação antes de iniciar a instalação propriamente dita, conforme descrito nos **subitens 4.4.2 e 4.5.2** deste **Termo de Referência**.
- 4.1.2. Apresentar quem será o gestor do projeto e o profissional técnico que atuará como coordenador de todas as atividades de instalação e implementação dos produtos adquiridos
- 4.1.3. Agendar visitas técnicas de pré-instalação aos sites da **DATAPREV** (DCRJ, DCSP e DCDF) para definição do posicionamento dos equipamentos, da instalação elétrica e demais requisitos necessários à instalação física dos equipamentos. Como produto dessas visitas técnicas, a **CONTRATADA** deverá elaborar um relatório detalhado, por local de instalação. Tal relatório deverá fazer parte do **Plano de Instalação de Conectividade de Rede e Infraestrutura**.
- 4.1.4. Apresentar os parâmetros a serem utilizados pelo sistema que registrará os chamados descritos no **item 11** deste **Termo de Referência**. Os parâmetros serão analisados pela **DATAPREV** para identificação das adequações necessárias a serem realizadas pela **CONTRATADA** para que atenda a todas as exigências descritas neste **Termo de Referência**.

4.2. Após a realização desta primeira reunião, caso existam questionamentos direcionados à **DATAPREV** e/ou à **CONTRATADA**, será disponibilizado um prazo de até 05 (cinco) dias úteis, contados a partir do dia seguinte à realização da reunião, para as respostas.

4.3. A instalação da solução contratada deverá ocorrer nos três *Data Centers*, contemplando *hardware* e *software*, além da replicação das configurações e políticas de segurança existentes na solução de *firewall* a ser substituída, e será realizada em duas etapas:

- Instalação de Conectividade de Rede e Infraestrutura;
- Instalação de Serviços.

4.3.1. A solução de Firewall a ser substituída é composta por:

Função	DCRJ	DCDF	DCSP
06 Firewalls Palo Alto, modelo PA-5250 (software e hardware) para a função de firewall externo	2 appliances físicos operando em HA	2 appliances físicos operando em HA	2 appliances físicos operando em HA
06 Firewalls Palo Alto, modelo PA-5220 (software e hardware) para a função de firewall interno	2 appliances físicos operando em HA	2 appliances físicos operando em HA	2 appliances físicos operando em HA
Gerência da solução, denominado de Panorama. (gerência centralizada)	1 appliance virtual (VM)	1 appliance virtual (VM)	N/A

4.4. Como produto da reunião descrita no **subitem 4.2** deste **Termo de Referência**, a **CONTRATADA** deverá encaminhar, por meio eletrônico, em **5 (cinco) dias úteis** após a realização da reunião de Planejamento e esclarecimento de possíveis dúvidas remanescentes, o **Plano de Instalação de Conectividade de Rede e Infraestrutura**.

4.4.1. No prazo de **até 5 (cinco) dias úteis**, a partir do recebimento formal do **Plano de Instalação de Conectividade de Rede e Infraestrutura**, a **DATAPREV** deverá se manifestar sobre sua aprovação. Caso seja necessário, será concedido à **CONTRATADA** um novo prazo de **até 5 (cinco) dias úteis** para eventuais ajustes e reapresentação da documentação reprovada. As versões definitivas dos planos supracitados serão as versões aprovadas pela Equipe Técnica da **DATAPREV**.

4.4.2. O **Plano de Instalação de Conectividade de Rede e Infraestrutura** dos produtos a serem fornecidos deverá conter, de forma detalhada:

- Descrição dos equipamentos e *software* que deverão ser instalados;
- Pré-requisitos para a instalação: deverão ser descritos todos os recursos e condições que deverão ser providos pela **DATAPREV**, necessários para que a **CONTRATADA** possa realizar os serviços de instalação;
- Relação dos especialistas certificados da **CONTRATADA** alocados nos processos de instalação;
- Relatórios das visitas técnicas de pré-instalação;
- Visão geral da arquitetura da solução que será implantada;
- Descrição de como será feito o serviço de instalação, com descrição dos pré-requisitos de *hardware* e *software* para cada *Data Center*.
- Definição de cronograma detalhado, incluindo datas de início e conclusão de cada fase da instalação da conectividade de rede e da infraestrutura.
- Necessidade de atualização de versões dos produtos a serem fornecidos.
- Definição do comprimento adequado de cada cabo e dos tipos de conectores para fibra (SL/LC) conforme exigidos no **Anexo I - Especificação Técnica**. Não será aceita a entrega de cabos sem a anuência prévia da **DATAPREV** quanto aos comprimentos dos mesmos.

4.5. A **CONTRATADA** deverá elaborar e entregar o **Plano de Instalação de Serviços** em **até 5 (cinco) dias úteis**, contados após a aprovação do **Plano de Instalação de Conectividade de Rede e Infraestrutura**, conforme **item 4.4.1** deste **Termo de Referência**.

4.5.1. No prazo de **até 5 (cinco) dias úteis**, a partir do recebimento formal do **Plano de Instalação dos Serviços**, a **DATAPREV** deverá se manifestar sobre sua aprovação. Caso seja necessário, será concedido à **CONTRATADA** um novo prazo de **até 5 (cinco) dias úteis** para eventuais ajustes e reapresentação da documentação reprovada. As versões definitivas dos planos supracitados serão as versões aprovadas pela Equipe Técnica da **DATAPREV**.

4.5.2. O **Plano de Instalação de Serviços** deverá conter, no mínimo, as seguintes informações:

- Descrição das configurações e políticas de segurança na nova infraestrutura, a partir da transposição das configurações e políticas de todas as funcionalidades de segurança existentes na solução de *Firewall* de Rede Palo Alto, que se encontrarem em produção.
- Relação dos especialistas certificados da **CONTRATADA** alocados.
- Testes de funcionalidade e validação das configurações e políticas implantadas para garantir que a proteção será mantida, minimamente, como instalada na solução Palo Alto.
- Definição de cronograma detalhado, incluindo datas de início e conclusão de cada fase da instalação dos serviços
- Entrega da documentação final incluindo os procedimentos realizados.

4.6. Após a aprovação do **Plano de Instalação de Conectividade de Rede e Infraestrutura** elaborado pela **CONTRATADA**, conforme **subitem 4.4.1** deste **Termo de Referência**, a **DATAPREV** realizará a preparação da infraestrutura, no prazo de **até 20 (vinte) dias úteis**.

A **DATAPREV** comunicará a **CONTRATADA** sobre a conclusão da preparação da infraestrutura para que se inicie a implantação da solução.

4.7. A **CONTRATADA** deverá se reunir com o **Gestor Administrativo** do contrato, conforme descrito no **subitem 25.2** deste **Termo de Referência**, no Rio de Janeiro, em local a ser definido pela **DATAPREV** ou por videoconferência, no prazo máximo de 10 (dez) dias úteis contados a partir do dia seguinte à assinatura do Contrato / Pedido de Compra (PC). A data da reunião deverá ser agendada em comum acordo com a **DATAPREV**. Esta será considerada a Reunião de Abertura Contratual onde serão discutidos os aspectos relevantes para a Gestão Contratual.

4.8. Nesta reunião a **CONTRATADA** deverá apresentar quem será o gestor do contrato por parte da **CONTRATADA** para tratar de questões comerciais e/ou contratuais.

## 5. ENTREGA

5.1. Os componentes de *software* e *hardware* que integram a solução definida no **ANEXO I – ESPECIFICAÇÃO TÉCNICA**, deverão ser disponibilizados ao **Gestor Técnico** do contrato, conforme descrito no **subitem 25.1** deste **Termo de referência** e deverão ser entregues no prazo máximo de **35 (trinta e cinco) dias úteis**, a contar do dia seguinte à assinatura do Contrato / Pedido de Compra, nos endereços a seguir:

ENDEREÇOS
<ul style="list-style-type: none"><li>• <b>Data Center Rio de Janeiro (DCRJ)</b> Rua Cosme Velho, 06, Cosme Velho, Rio de Janeiro – RJ – CEP 22241-900 E</li><li>• <b>Data Center São Paulo (DCSP)</b> Rua Dr. Manoel Vitorino, 343, Brás, São Paulo – SP – CEP 03017-020 E</li><li>• <b>Data Center Distrito Federal (DCDF)</b> Setor de Autarquias Sul, quadra 1, bloco E/F, Brasília – DF – CEP 70070-931</li></ul>

5.2. Os volumes contendo os componentes de *hardware* deverão estar identificados externamente, com os dados discriminados na documentação de Registro de Entrega / Nota Fiscal, na qual deverá constar necessariamente o número de série de todos os componentes que estiverem sendo entregues.

5.3. Junto aos produtos fornecidos, a **CONTRATADA** deverá entregar ao **Gestor Técnico** do contrato, conforme descrito no **subitem 25.1** deste **Termo de Referência**, as documentações descritas abaixo:

- Documentação do Registro de Entrega por meio de Ofício/Nota Fiscal da **CONTRATADA**;
- Ofício da **CONTRATADA** relacionando os itens discriminados na documentação de Registro de Entrega com os produtos de *hardware* e/ou *software* objeto desta contratação e que estão descritos na proposta técnica comercial validada pela **DATAPREV**, de forma que seja possível verificar a correlação entre os itens, conforme definido no **ANEXO I – ESPECIFICAÇÃO TÉCNICA**, e aqueles representados na documentação de Registro de Entrega. Esta correlação não poderá ser feita por códigos e sim pela descrição de cada *hardware* e/ou *software*, com a respectiva quantidade;
- Documentação técnica, original do fabricante, preferencialmente em língua portuguesa, que abranja configuração, instalação e gerenciamento dos produtos adquiridos. Na ausência de publicação em português da documentação original do fabricante, será aceito apenas material em inglês;
- Informar o *Stock Keeping Unit* (SKU);
- Detalhamento dos valores unitários de cada componente por modelo de equipamento descritos no **subitem 1.2**.

5.4. A conferência dos produtos adquiridos será realizada com base na documentação descrita nas **alíneas “a” e “b”** do **subitem 5.3**, conforme descrito abaixo:

- Para os itens de *software*, a **DATAPREV** validará os produtos recebidos em **até 07 (sete) dias úteis**, contados a partir do recebimento da formalização de entrega dos itens pela **CONTRATADA**.
- Para os itens de *hardware*, os volumes entregues serão abertos pela **CONTRATADA** na presença da **DATAPREV**, em **até 07 (sete) dias úteis**, contados a partir da sua solicitação formal, que em conjunto conferirão o seu conteúdo.

Constatada a ocorrência de divergência entre os componentes entregues e o descrito na documentação das **alíneas “a” e “b”** do **subitem 5.3**, fica a **CONTRATADA** obrigada a providenciar a sua correção ou sua substituição, a critério da **DATAPREV**. Os produtos não serão considerados entregues até que todas as pendências sejam sanadas.

5.5. Os produtos serão considerados entregues e o **Termo de Recebimento** será emitido pela **DATAPREV** em **até 10 (dez) dias úteis**, contados a partir da ocorrência dos fatos abaixo:

- A **CONTRATADA** realizar a entrega da documentação constante no **subitem 5.3** deste **Termo de Referência**.
- A **DATAPREV** realizar a conferência dos produtos descritos no **subitem 5.4** deste **Termo de Referência**.

## 6. INSTALAÇÃO

6.1. A **CONTRATADA** deverá realizar a instalação “assistida” de todo componente de *hardware* e *software*, incluindo sua configuração e interligação física (cabeamento) e lógica à rede de dados da **DATAPREV**, que será acompanhada por analistas da **DATAPREV**. Todo processo de instalação deverá atender ao especificado nos **Planos de Instalação** aprovados pela **DATAPREV**, conforme descrito nos **subitens 4.4.1 e 4.5.1** deste **Termo de Referência**.

6.1.1. A instalação deve ser realizada por profissionais especializados, em conformidade com as certificações oficiais da solução contratada.

6.1.2. As certificações exigidas no **subitem 6.1.1** devem estar válidas durante o período de prestação dos serviços de instalação e configuração.

6.2. O prazo para conclusão da instalação dos equipamentos será de **60 (sessenta) dias úteis**, contados a partir do dia seguinte à ocorrência dos fatos abaixo:

- Aprovação da versão definitiva dos **Planos de Instalação** descritos nos **itens 4.4.2 e 4.5.2**;

- Emissão do Termo de Recebimento dos itens de *hardware* e *software*;

- Conclusão da preparação da infraestrutura pela **DATAPREV**.

**6.3.** A **CONTRATADA** deverá providenciar a aplicação de todas as correções e atualizações de *software* liberados até a data da instalação, incluindo a atualização de *firmware* dos componentes de *hardware* que compõem a solução, salvo solicitação da **DATAPREV** por outra versão. A **CONTRATADA** deverá encaminhar documento, em meio eletrônico, que comprove a aplicação das atualizações em todos os produtos instalados.

**6.4.** Constatada a ocorrência de divergência na especificação técnica ou qualquer outro defeito de operação durante a instalação dos equipamentos, fica a **CONTRATADA** obrigada a providenciar a sua correção ou, a critério da **DATAPREV**, a substituição dos produtos adquiridos.

**6.5.** É de responsabilidade da **CONTRATADA** toda e qualquer despesa, independentemente da sua natureza, decorrente dos serviços de instalação aqui mencionados.

**6.6.** Padrão de requisitos físicos nos Data Centers da **DATAPREV**:

- **Energia elétrica** – Corrente alternada (AC). Frequência de rede com 60 Hz.
  - **Brasília e Rio de Janeiro:** Tensão nominal de 380V Trifásico ou 220V Monofásico. Corrente do circuito de distribuição com máximo de 30A. Padrão de tomada utilizado nos *Data Centers* é do tipo **Pial** (Referência 56407).
  - **São Paulo:** Tensão nominal de 380V Trifásico ou 220V Monofásico. Corrente do circuito de distribuição com máximo de 32A. Padrão de tomada utilizado no *Data Center* é **Steck** (N3276).
- **Climatização** – faixa de operação ampliada (Classe 2): 10° a 35° C / 20% a 80% RH (umidade).
- **Espaço Físico** – acomodação em rack padrão de 19" com máxima carga pontual de 545 kg e máxima carga distribuída de 1.479 Kg/m2
- **Cabeamento** - O cabeamento UTP deverá ser fornecido na cor cinza. O cabeamento em fibra deverá ser fornecido na cor aqua.

**6.7.** Concluídas a instalação e a configuração dos produtos adquiridos, a **CONTRATADA** deverá comunicar formalmente à **DATAPREV** sobre a conclusão dos serviços e entregar o Caderno de Testes de acordo com o **Anexo VI – MODELO DE CADERNO DE TESTE**. A **DATAPREV** terá o prazo de **até 10 (dez) dias úteis** para verificar a conformidade da instalação e das configurações realizadas com as condições constantes neste **Termo de Referência**.

**6.7.1.** Caso sejam constatadas anormalidades ou sejam detectados problemas durante a verificação de conformidade realizada pela **DATAPREV**, esta comunicará formalmente os problemas detectados e que a instalação não foi concluída. A **CONTRATADA** terá um novo prazo de **10 (dez) dias úteis**, contados a partir do dia seguinte à confirmação de recebimento da comunicação, para sanar os problemas/anormalidades detectados, sem prejuízo do prazo descrito no **subitem 6.2** deste **Termo de Referência**, sujeitando-se a **CONTRATADA** às penalidades previstas.

**6.8.** Os serviços de instalação deverão ocorrer em dias úteis, no horário compreendido entre 9:00h e 18:00h, salvo definição contrária, realizada em comum acordo entre a **DATAPREV** e a **CONTRATADA** e deverão ser agendados previamente com a **DATAPREV**.

**6.9.** Os produtos adquiridos serão considerados instalados e o **Termo de Aceite de Instalação** será emitido pela **DATAPREV** em **até 10 (dez) dias úteis**, contados a partir da ocorrência dos fatos a seguir:

- a) As atualizações serem aplicadas e a documentação comprobatória ser entregue à **DATAPREV** pela **CONTRATADA**, conforme descrito no **subitem 6.3** deste **Termo de Referência**.
- b) A **DATAPREV** receber da **CONTRATADA** o **Caderno de Testes** devidamente preenchido, conforme descrito no **subitem 6.7** deste **Termo de Referência**;
- c) A **CONTRATADA** enviar as evidências da instalação conforme definido nos **Planos de Instalação** descritos nos **itens 4.4.2 e 4.5.2**;
- d) A **DATAPREV** receber o comunicado da **CONTRATADA** informando a conclusão dos serviços de instalação e configuração, conforme descrito no **subitem 6.7** deste **Termo de Referência**.
- e) A **DATAPREV** concluir a verificação da conformidade da instalação e das configurações realizadas com as condições constantes neste **Termo de Referência** e que não existem anormalidades ou foram sanados todos os problemas detectados, conforme descrito nos **subitens 6.7 e 6.7.1** deste **Termo de Referência**.

## 7. ORIENTAÇÃO TÉCNICA

**7.1.** As atividades de orientação técnica objetivam otimizar a utilização dos produtos adquiridos e o desenvolvimento ou aperfeiçoamento de competências, por meio do repasse de conhecimento de forma ordenada e seu escopo compreende:

- Apoio na definição da melhor metodologia para o uso adequado da solução contratada;
- Apoio nas definições de alterações de topologia e configurações da solução, em função de revisões de arquitetura de rede;
- Diagnóstico / orientação quanto à análise do desempenho da solução;
- Apoio no planejamento e desenvolvimento de API's permitindo a integração via API REST para automação de processos com aplicações terceiras;
- Apoio na integração com demais ferramentas da Dataprev como SIEM e *log* centralizado;
- Apoio no planejamento da ativação das funcionalidades de *Firewall* de Rede;
- Apoio na resolução de problemas;
- Orientações nas customizações das regras *default* da ferramenta;



- Apoio no desenvolvimento de configurações específicas para mitigar ameaças ao ambiente da Dataprev;
- Orientações de administração e gestão do ambiente;
- Apoio na configuração das funcionalidades de Antivírus, ajustando a integração com as aplicações da Dataprev;
- Apoio na realização de *health check* da solução de *Firewall* de Rede;
- Apoio nos serviços de configuração da solução, fora do escopo de suporte, que seja necessário engajar serviços de um técnico profissional especializado;
- Orientações para automatização de processos para a gestão da ferramenta, como inventário de IPs protegidos e certificados digitais.

**7.2.** As atividades de orientação técnica serão realizadas, a critério da **DATAPREV**, em qualquer um dos *Data Centers* (Rio de Janeiro, São Paulo e Brasília), a partir da assinatura do Contrato / Pedido de Compra, durante toda a vigência contratual.

**7.3.** Estas atividades devem ter produtos definidos (planos, procedimentos, laudos, pareceres técnicos, guias, padrões etc.), escopo, prazo de entrega e as respectivas horas alocadas para a execução, previamente aprovadas pela **DATAPREV**, para fins de contabilização e posterior faturamento. Estas informações devem estar devidamente registradas nas respectivas Ordens de Serviço, autorizadas pelo **Gestor Técnico** do contrato, conforme descrito no **subitem 25.1** deste **Termo de Referência**.

**7.4.** A **CONTRATADA** deverá disponibilizar **640 (seiscentos e quarenta) horas** de orientação técnica *on site*, a serem realizadas por profissionais especializados na solução fornecida, em conformidade com a(s) certificação(ões) descrita(s) no **subitem 7.4.2**. Essas horas serão utilizadas, sob demanda, de acordo com as necessidades da **DATAPREV**.

**7.4.1.** A critério da **DATAPREV**, as atividades referentes às horas de orientação técnica poderão ser despendidas nas dependências da **CONTRATADA**.

**7.4.2.** O profissional que prestará o serviço de orientação técnica deverá ser especializado, e deverá comprovar que possui certificação do fabricante atestando as habilidades técnicas necessárias para desempenhar as atividades de orientação técnica para a solução fornecida.

**7.4.3.** A(s) certificação(ões) exigida(s) no **subitem 7.4.2** deve(m) estar válida(s) durante o período de prestação dos serviços de orientação técnica.

**7.5.** Os serviços de Orientação Técnica serão prestados em conformidade com as Ordens de Serviços (OS) a serem emitidas para sua execução. As Ordens de Serviço deverão ser executadas de acordo com planejamento realizado pela equipe da **DATAPREV** em conjunto com a equipe da **CONTRATADA**, obedecendo cronograma estabelecido.

**7.6.** A **CONTRATADA** deverá disponibilizar os seguintes canais de atendimento para abertura das Ordens de Serviço: *Website* e telefone (preferencialmente, 0800).

Cada solicitação de orientação técnica deverá conter, no mínimo, o registro das informações abaixo:

- Número do chamado (na abertura da OS; a ser fornecido pela **CONTRATADA**);
- Número da Ordem de Serviço (a ser fornecido pela **DATAPREV**);
- Identificação do atendente;
- Identificação do solicitante;
- Data e hora da solicitação;
- Descrição da demanda.

As informações sobre os canais de atendimento para abertura das **Ordens de Serviço** deverão ser apresentadas à **DATAPREV** no prazo **máximo de 10 (dez) dias úteis**, contados a partir do dia seguinte à assinatura do **Contrato / Pedido de Compra (PC)**.

**7.7.** As solicitações de serviço deverão ser retornadas no prazo máximo de **4 (quatro) horas** úteis após o seu respectivo registro, entendido este retorno como um contato inicial para fins de definição do escopo e forma de tratamento da demanda apresentada. Neste retorno, deverá ser agendada uma reunião presencial ou uma audioconferência para definição do número de horas necessárias e cronograma de execução da respectiva Ordem de Serviço.

**7.8.** A **CONTRATADA** terá o prazo **máximo de 3 (três) dias úteis**, contados a partir do dia seguinte ao registro da solicitação de abertura da Ordens de Serviço (OS) pela **DATAPREV**, para se reunir com o solicitante, presencialmente ou por meio de audioconferência, com a finalidade de definir o escopo e a forma de tratamento da demanda apresentada. Nesta reunião, a **CONTRATADA** obterá os insumos necessários para realizar a definição do número de horas e do cronograma de execução da respectiva Ordem de Serviço (OS). A data da reunião deverá ser agendada em comum acordo com a **DATAPREV**.

**7.9.** A **CONTRATADA** terá o **prazo máximo de 3 (três) dias úteis**, contados a partir do dia seguinte à realização da reunião descrita no **subitem 7.8** para encaminhar ao solicitante, por meio eletrônico, o número de horas e o cronograma de execução da respectiva Ordem de Serviço (OS). Após alinhamentos entre a **CONTRATADA** e a **DATAPREV**, possíveis negociações e aprovação do número final de horas e cronograma de execução da respectiva Ordem de Serviço (OS), a **DATAPREV** emitirá o documento de **abertura** da Ordem de Serviço (OS), que deverá ser assinado por responsáveis da **CONTRATADA** e pelo gestor técnico da **DATAPREV**, conforme descrito no **subitem 25.1** deste **Termo de Referência**.

**7.10.** Todas as funções e atividades desempenhadas pela **CONTRATADA** deverão ter como preocupação primária a transferência do conhecimento à equipe técnica da **DATAPREV** designada a acompanhar cada atividade. Caso a **DATAPREV** entenda ser necessário, poderá solicitar, mediante Ordem de Serviço específica, a realização de *workshops*, que não se caracterizam como capacitação, mas como apresentação e debate sobre as atividades planejadas ou executadas abrangendo tópicos específicos da tecnologia envolvida.

**7.11.** Entende-se por transferência de conhecimento, a passagem de conhecimento para os técnicos da **DATAPREV**, de todas as atividades desenvolvidas, relativas a cada Ordem de Serviço executada, visando aprimorar os conhecimentos da tecnologia utilizada e maximizar a utilização das funcionalidades.

**7.12.** Os registros de solicitação de serviços poderão ser realizados em horário comercial (9:00 às 18:00 horas), de segunda a sexta-feira, excluídos os feriados nacionais.

7.13. Os serviços solicitados serão realizados em horário comercial (9:00 às 18:00 horas), de segunda a sexta-feira, excluídos os feriados nacionais, salvo definição contrária, realizada em comum acordo entre a **DATAPREV** e a **CONTRATADA**.

7.14. Concluída a realização dos serviços solicitados na OS (Ordem de Serviço), a **CONTRATADA** deverá comunicar este fato formalmente à **CONTRATANTE**. A **DATAPREV** terá o prazo de **10 (dez) dias úteis**, contados a partir da formalização da conclusão, para realizar a avaliação das entregas e validar o consumo de horas, de acordo com:

- A documentação técnica entregue, conforme padrões previamente acordados entre as partes;
- O atingimento dos resultados já estipulados;
- A disponibilização dos entregáveis.

7.15. Após a **DATAPREV** finalizar a avaliação das entregas e a validação do consumo de horas, atestando que o serviço foi realizado em conformidade com o solicitado, emitirá o documento de aceite da respectiva OS (Ordem de Serviço), que deverá conter as informações relacionadas à sua execução, incluindo o número efetivo de horas utilizadas, e ser assinado por responsáveis da **CONTRATADA** e pelo Gestor Técnico da **DATAPREV**, conforme descrito no item 25.1 deste **Termo de Referência**.

7.16. Somente o Gestor Técnico, descrito no subitem 25.1 deste **Termo de Referência**, poderá oficializar, junto à **CONTRATADA**, as solicitações de OS (Ordem de Serviço).

7.17. OS's (Ordens de Serviço) aprovadas para execução e formalizadas, não poderão sofrer acréscimos em seu conteúdo previamente negociado sem a anuência do Gestor Técnico, conforme descrito no subitem 25.1 deste **Termo de Referência**.

7.18. Em casos excepcionais, as Ordens de Serviço poderão sofrer redução no conteúdo, previamente negociado, desde que a atividade específica ainda não tenha sido iniciada.

## 8. CONDIÇÕES GERAIS PARA PRESTAÇÃO DOS SERVIÇOS DE GARANTIA

8.1. A garantia dos produtos adquiridos deverá considerar o período de **60 (sessenta) meses** a partir da data de emissão do **Termo de Aceite** dos produtos e contemplar a prestação dos seguintes serviços:

- Atualização de versão das licenças de *software*;
- Suporte Técnico.

8.2. A prestação dos serviços relacionados à garantia não deve imputar qualquer custo adicional à **DATAPREV**.

8.3. A modalidade de atendimento deverá ser **em regime 24x7** (24 horas por dia x 7 dias da semana), de segunda a domingo, incluindo os feriados.

8.3.1. Para os itens aferidos em horas úteis, o regime será 8x5 (8 horas por dia x 5 dias da semana), de segunda a sexta (9:00 às 17:00 horas, sem interrupções), excluindo os feriados nacionais

8.4. A **CONTRATADA** deverá notificar **formalmente** à **DATAPREV** sobre a descontinuidade comercial e sobre o término do suporte técnico dos produtos objeto deste **Termo de Referência** com antecedência mínima de **6 (seis) meses** da descontinuidade.

## 9. ATUALIZAÇÃO DE LICENÇA DE SOFTWARE

9.1. Durante o período de garantia, a **CONTRATADA** deverá disponibilizar para a **DATAPREV** todas as atualizações do *software*, (atualização de versões, *releases* e *patches*), *firmware* ou microcódigos dos *hardwares* adquiridos, sem nenhum ônus adicional à **DATAPREV**.

9.2. A **CONTRATADA** deverá notificar aos contatos indicados pelo Gestor Técnico do contrato, conforme descrito no subitem 25.1, sobre a liberação de novas versões e correções de *software* (*patches*) dos produtos objeto deste **Termo de Referência**. Os avisos poderão ser encaminhados por e-mail, utilizando mecanismo automático de notificação.

9.3. A solução de segurança deve ser fornecida com licenças de uso **perpétuo**, ou seja, não devem parar de funcionar mesmo após o período de garantia, permitindo continuar com todas as suas funcionalidades ativas após o período de garantia, mesmo que sem a possibilidade de atualização tecnológica, no mínimo, para as seguintes funcionalidades:

- *Firewall*;
- Alta disponibilidade;
- VPN (*Client-to-Site* e *Site-to-Site*);
- Gerência centralizada;
- Gerência de *Logs*.

9.4. Para as funcionalidades não descritas no item 9.3, serão aceitas licenças no modelo de **subscrição** sem exigência de manutenção das funcionalidades após o período de garantia, ou perpétua.

9.5. Caso as condições de licenciamento do *software* fornecido sejam alteradas pelo fabricante durante o período de garantia, as funcionalidades e os quantitativos definidos não deverão ser prejudicados. Nas situações em que a alteração na forma de licenciamento implique em perdas qualitativas e/ou quantitativas, licenças complementares deverão ser fornecidas à **DATAPREV**, sem custo adicional.

## 10. SUPORTE TÉCNICO

10.1. Durante o período de garantia, a **CONTRATADA** deverá prover o serviço de suporte técnico para os produtos adquiridos, que deverá ser prestado nas modalidades:

- **On site (presencial)**: para chamados relacionados aos produtos de *hardware*;
- **Remoto**: para as demais situações, conforme descrito no subitem 10.4 deste **Termo de Referência**.

10.2. Entende-se por **Suporte Técnico On site (presencial)** a disponibilização de soluções destinadas a corrigir problemas originados por falhas, incluindo a

atualização de versão, *patches* de correção, configurações, reinstalação e demais procedimentos necessários objetivando o retorno do ambiente operacional (*disaster recovery*). A **CONTRATADA** obriga-se e compromete-se a não utilizar material de reposição improvisado. As peças e/ou equipamentos que vierem a ser substituídos deverão ser novos e originais do fabricante.

**10.3.** Os serviços de **Suporte Técnico On site (presencial)** serão prestados por técnicos devidamente habilitados e credenciados pela **CONTRATADA**, no local onde os equipamentos encontram-se instalados. A **CONTRATADA** deverá informar quem será o responsável pelo centro de suporte e assistência técnica durante o período contratual.

**10.4.** Entende-se por **SUPORTE TÉCNICO REMOTO** as seguintes atividades para tratamento de problemas relacionados à solução:

- a) Orientações sobre uso, configuração, instalação dos produtos contratados e para identificação da versão de software mais adequada, conforme perfil de necessidade apontada pela **DATAPREV**.
- b) Questões sobre compatibilidade e interoperabilidade dos produtos adquiridos (*hardware* e *software*);
- c) Interpretação da documentação dos produtos contratados;
- d) Orientações para identificar a causa de uma falha de *software* e/ou *hardware*;
- e) Para os casos de defeitos de *software* conhecidos, devem ser fornecidas as informações sobre a correção ou a própria correção. No caso de fornecidas as informações sobre a correção, a critério da Dataprev, pode ser demandado à **CONTRATADA** o acompanhamento na realização dos procedimentos sugeridos;
- f) No caso de defeitos de software não conhecidos, a assistência técnica da **CONTRATADA** deverá enviar as informações sobre a falha ao fabricante do produto para que o mesmo forneça a solução. A **CONTRATADA** deverá informar o número do chamado aberto junto ao fabricante, bem como uma estimativa de prazo para solução da falha. Quando fornecidas pelo fabricante as informações sobre a correção, a **CONTRATADA** deverá fornecer estas informações sobre a correção ou a própria correção. No caso de fornecidas as informações sobre a correção, a critério da **DATAPREV**, pode ser demandado à **CONTRATADA** o acompanhamento na realização dos procedimentos sugeridos;
- g) Orientação para solução de problemas de "*performance*" e "*tuning*" das configurações dos produtos suportados;
- h) Orientação quanto às melhores práticas para implementação dos produtos suportados;
- i) Apoio na recuperação de ambientes em caso de panes ou perda de dados;
- j) Apoio para execução de procedimentos de atualização para novas versões dos produtos de *software* instalados;

**10.5.** As atividades relacionadas ao **SUPORTE TÉCNICO REMOTO** devem ser realizadas por meio de contato telefônico, troca de mensagens eletrônicas e videoconferência por meio de ferramenta homologada pela **DATAPREV**, sendo vedada a utilização de acesso remoto. Caso a **CONTRATADA** opte por solucionar o problema reportado pela **DATAPREV** por meio de atendimento **on site** (presencial), isso não deve imputar qualquer ônus adicional à **DATAPREV**. Em caráter excepcional, a área de Segurança da Informação da **DATAPREV** poderá autorizar a utilização de acesso remoto por meio de ferramenta homologada pela **DATAPREV** após avaliar sua necessidade devido a situações emergenciais que representem grande impacto para **DATAPREV**.

**10.6.** O fato de qualquer um dos produtos adquiridos não utilizar a última versão disponibilizada de qualquer *software* instalado originalmente, incluindo *firmwares*, não poderá ser utilizado pela **CONTRATADA** como argumento para postergar eventual suporte técnico, a menos que tenha sido objeto de notificação e que seja apresentada documentação correlacionando a falha detectada com a versão de *software* instalada.

**10.7.** Durante o período de garantia contratual, a **CONTRATADA** deverá prover o serviço de suporte técnico com o apoio de profissionais técnicos especializados, que possuam as certificações do fabricante da solução contratada.

**10.7.1.** As certificações exigidas no **subitem 10.7** devem estar válidas durante o período de prestação dos serviços de manutenção e suporte.

## 11. REGISTRO E ATENDIMENTO DE OCORRÊNCIAS

**11.1.** Para atendimento aos serviços de garantia dos produtos adquiridos, a **CONTRATADA** deverá oferecer atendimento por meio de Centro de Suporte e Assistência Técnica, que poderá pertencer ao fabricante dos produtos ou à **CONTRATADA** (parceira formalmente designada pelo fabricante dos produtos adquiridos como habilitada a prestar os serviços de suporte e assistência técnica).

**11.2.** No **prazo máximo de 10 (dez) dias úteis**, contados a partir do dia seguinte à assinatura do Contrato / Pedido de Compra (PC), a **CONTRATADA** deverá apresentar à **DATAPREV**:

- As informações sobre os canais de atendimento para abertura dos chamados: número de telefone (preferencialmente 0800) e endereço de *website*;
- As informações referentes ao centro de suporte e assistência técnica responsável pelo atendimento aos serviços de garantia: se pertence ao fabricante dos produtos ou à própria **CONTRATADA**, endereço, telefone, e-mail e contato.
- As informações referentes a ferramenta de abertura de chamados que poderão ser efetuadas, a critério da **DATAPREV**, com a entrega de um manual de utilização e/ou a realização de Workshop, a ser agendado, para as áreas de operação da ferramenta.

**11.3.** A **CONTRATADA** deverá providenciar o registro de toda e qualquer solicitação de suporte técnico, independentemente de sua natureza, cabendo à DATAPREV o devido acompanhamento. À **DATAPREV** serão disponibilizados os seguintes canais de atendimento para abertura dos chamados:

*Website* e telefone (preferencialmente 0800)

Onde cada chamado deverá conter, no mínimo, o registro das informações abaixo:

- Número do registro/ocorrência (a ser fornecido pela **CONTRATADA**);
- Identificação do atendente;
- Identificação do solicitante;

- Data e hora da solicitação;
- Nível de severidade da ocorrência (a ser fornecido pela **DATAPREV**);
- Descrição da ocorrência;
- Classificação da ocorrência:
  - Suporte Técnico Remoto: incidente
  - Suporte Técnico Remoto: esclarecimento de dúvidas
  - Suporte Técnico *On Site* (presencial): incidente

11.4. No provimento deste serviço por meio de telefone, a **CONTRATADA** fica obrigada a permitir o recebimento de ligações de terminais fixos e móveis.

11.5. Para os atendimentos por meio de telefone, o **tempo máximo** de espera deverá ser de **até 03 (três) minutos**.

11.6. No provimento deste serviço por meio de *Website*, deverá ser possível que a **DATAPREV** indique uma lista de produtos por meio de arquivo anexo ou diretamente na página, em um único registro. Neste caso, a data e hora do registro serão consideradas como horário da abertura do chamado para todos os produtos listados.

11.7. Caso a **CONTRATADA** opte por prestar os serviços de garantia dos produtos adquiridos por meio de Centro de Suporte e Assistência Técnica próprio, deverá possuir acesso direto, por meio de telefonema ou via correio eletrônico, ao Centro de Suporte e Assistência Técnica do fabricante.

11.8. Independentemente da forma que a **CONTRATADA** utilize para prestar os serviços de garantia dos produtos adquiridos (por meio de Centro de Suporte e Assistência Técnica **do fabricante** dos produtos ou de centro de suporte e assistência técnica **próprio**), à **DATAPREV** deverá ser permitido acompanhar, por meio de *Website*, o andamento de todos os chamados abertos por meio de telefone e de *Website*. Este acesso ao Centro de Suporte e Assistência Técnica deverá:

- Estar disponível **24 (vinte e quatro) horas por dia, 7 (sete) dias por semana**, todos os dias do ano;
- Permitir realizar filtro por chamados encerrados em determinado intervalo de tempo, relacionados a um contrato específico;
- Permitir realizar filtro por chamados com status "aberto", com sua data de abertura no intervalo de tempo informado, relacionados a um contrato específico;
- Permitir a apuração do tempo total de atendimento do chamado e o tempo em que ficou sob a responsabilidade da **CONTRATADA**;
- Exibir as informações do andamento dos chamados de forma completa, clara e precisa, permitindo identificar objetivamente as transições de responsabilidade entre **DATAPREV** e **CONTRATADA** pelas ações a serem realizadas;
- Exibir as informações de data e hora de forma padronizada, incluindo o fuso horário a ser considerado.

11.9. O horário de abertura de chamado será determinado conforme abaixo:

- Para chamados abertos pelo canal **Telefone** (preferencialmente 0800) → o horário da abertura do chamado será a data e hora da ligação realizada pelo profissional da **DATAPREV** informando do problema ocorrido. Caso a atendente não possa informar o número do chamado neste momento, deverá, **obrigatoriamente**, informar um número de protocolo que registre a data e hora da ligação realizada.
- Para chamados abertos pelo canal **Website** → o horário da abertura do chamado será a data e hora do acesso ao *Website* para registro do problema ocorrido. No momento do registro, a página *web* deverá informar o número do chamado. Caso isso não seja possível, deverá informar um número de protocolo que registre a data e hora do acesso realizado.

11.10. O horário de abertura do chamado marcará o início da contagem do prazo de solução das ocorrências, independentemente do retorno da **CONTRATADA**. O horário de abertura de chamado será determinado conforme descrito no **subitem 11.9** deste **Termo de Referência**.

11.11. O serviço de registro de chamados deverá ser disponibilizado de acordo com a modalidade de atendimento estabelecida no **subitem 8.4** deste **Termo de Referência**.

11.12. Não deverá haver qualquer limitação para o número de solicitações de suporte técnico remoto.

11.13. Não deverá haver qualquer limitação para o número de técnicos da **DATAPREV** autorizados a abrir chamados técnicos.

## 12. PRAZO PARA SOLUÇÃO DAS OCORRÊNCIAS

12.1. Deverão ser considerados os seguintes prazos e níveis de severidade para os chamados de **Suporte Técnico**:

PRAZOS PARA SOLUÇÃO DAS OCORRÊNCIAS REGISTRADAS (a partir do registro da ocorrência)	
SEVERIDADE INFORMADA	TEMPO PARA SOLUÇÃO
1	4 horas corridas
2	24 horas corridas
3	72 horas corridas
4	24 horas úteis

Os níveis de severidade são descritos abaixo:

- Severidade 1** – quando ocorre a perda ou paralisação de atividades exercidas ou de serviços relevantes prestados pela **DATAPREV**, configurando-se como emergência. Uma solicitação de serviço de **Severidade 1** pode possuir uma ou mais das seguintes características:
  - Dados corrompidos;
  - Uma função crítica não está disponível;

- O sistema se desliga repentinamente, causando demoras excessivas e intermitências para utilização de recursos;
- O sistema falha repetidamente após tentativas de reinicialização;
- O sistema continua em execução permanente (congelado) necessitando ser reiniciado.

- b) **Severidade 2** – Quando se verifica uma grave perda de funcionalidades em programas ou sistemas da **DATAPREV**, inexistindo alternativas de contorno, sem, no entanto, interromper em sua totalidade a prestação do serviço;
- c) **Severidade 3** – Quando se verifica uma perda de menor relevância de funcionalidades em programas ou sistemas da Dataprev, causando apenas inconveniências para a devida prestação dos serviços pela **DATAPREV**;
- d) **Severidade 4** – Quando se verifica como necessária a prestação de informações, aperfeiçoamentos ou esclarecimentos sobre documentação ou funcionalidades de programas, porém sem prejudicar diretamente a operação dos programas ou sistemas da **DATAPREV**.

**12.1.1.** Para contabilização de horas úteis, será considerado regime 8x5 (8 horas por dia x 5 dias da semana), de segunda a sexta (9:00 às 17:00 horas, sem interrupções), excluindo os feriados nacionais.

**12.2.** O nível de severidade será atribuído pela **DATAPREV** no momento da abertura do chamado.

**12.3.** Para abertura de chamados pela **DATAPREV** na **ferramenta**, deverá ser permitido que a **DATAPREV** registre o nível de severidade que será atribuído ao chamado, e este só poderá ser alterado com a anuência da **DATAPREV**.

**12.4.** No atendimento dos chamados, para efeitos de apuração do tempo gasto pela **CONTRATADA** para a disponibilização da solução, serão desconsiderados os períodos em que a **DATAPREV** estiver responsável por executar ações necessárias para a análise e solução da ocorrência.

**12.5.** Considerando que as soluções das ocorrências de software, pela sua natureza, podem envolver atividades relacionadas ao desenvolvimento de *patches* específicos, admite-se, para todos os casos, a adoção de solução de contorno (*workaround*), respeitados os prazos definidos para cada severidade informada, sem prejuízo da disponibilização da solução definitiva cabível. Neste caso, a partir do encerramento do chamado original, com a disponibilização da solução de contorno, a **CONTRATADA** deverá abrir uma nova ocorrência para provimento da solução definitiva imediatamente, na qual deverá constar, **obrigatoriamente**, um novo campo contendo o número do chamado original (encerrado com a solução de contorno). O prazo máximo para disponibilização da solução definitiva será:

<b>PRAZOS PARA SOLUÇÃO DEFINITIVA</b> <b>(a partir do encerramento do chamado original, com a disponibilização da solução de contorno)</b>	
<b>SEVERIDADE INFORMADA</b>	<b>TEMPO PARA SOLUÇÃO</b>
<b>1</b>	<b>15 dias corridos</b>
<b>2</b>	<b>30 dias corridos</b>
<b>3</b>	<b>45 dias corridos</b>

**12.6.** Considerando a solução de ocorrências de hardware, a substituição dos módulos ou equipamentos defeituosos deverá utilizar módulos ou equipamentos novos e originais, recomendados pelo fabricante, dentro do prazo máximo de **12 (doze) horas corridas**, contadas a partir da expiração do prazo de solução. Após a substituição, a **CONTRATADA** deverá entregar um documento onde constem as descrições e os números de série dos módulos ou equipamentos defeituosos e dos novos (de substituição).

**12.6.1.** Os HDs/Mídias substituídos não serão retirados pela **CONTRATADA**, devendo ficar em posse da **DATAPREV**.

**12.6.2.** As peças defeituosas só poderão ser retiradas da **DATAPREV** após sanitização ou destruição de mídia.

**12.7.** Para fins de cálculo do período decorrido para solução da ocorrência de software, será contabilizado o prazo entre a formalização e o fechamento efetivo da ocorrência – seja essa solução de caráter definitivo ou provisório com a disponibilização de solução de contorno (*workaround*).

**12.8.** Para fins de cálculo do período decorrido para solução da ocorrência de hardware, será contabilizado o prazo entre a formalização e o fechamento efetivo da ocorrência. Nos casos em que houver a substituição do módulo ou equipamento defeituoso para a solução da ocorrência, o seu fechamento efetivo se dará somente após a entrada em operação do novo módulo ou equipamento (de substituição).

**12.9.** Entende-se como substituição do módulo ou equipamento defeituoso, a desativação e remoção física do módulo ou equipamento defeituoso, seguida da ativação física e lógica do módulo ou equipamento novo (de substituição), reestabelecendo completamente o serviço que atendia antes da ocorrência.

**12.10.** Em caso de impossibilidade da disponibilização de solução de contorno ou definitiva das ocorrências de *software*, dentro dos prazos estabelecidos, a **CONTRATADA** deverá, ainda dentro destes prazos, emitir um parecer com previsão de novo prazo, contendo o histórico de maior abrangência possível das atividades desenvolvidas desde a abertura do respectivo chamado.

**12.11.** Após avaliação deste parecer inicial, a **DATAPREV** decidirá sobre a **periodicidade da emissão de pareceres ou laudos posteriores**, até o fechamento do atendimento, sem prejuízo da aplicação das penalidades previstas pelo descumprimento dos prazos estabelecidos nos **subitens 12.1 e 12.5** deste **Termo de Referência**.

## 13. RELATÓRIOS

**13.1.** Durante todo o período de prestação dos serviços relacionados à garantia, a **CONTRATADA** deverá apresentar, mensalmente, um arquivo contendo o registro de todas as ocorrências de suporte técnico do período mensal de prestação de serviços encerrado. O **Relatório Mensal de Atendimento** e seus anexos, descritos no **subitem 13.1.1**, deverá ser encaminhado para os Gestores Administrativo e Técnico conforme descrito no **item 25** deste **Termo de Referência** em **até 7 (sete) dias úteis**, contados a partir do dia seguinte **ao fim do período mensal de prestação de serviços** e deverá estar no formato “.PDF”, devidamente assinado pelo gestor do contrato por parte da **CONTRATADA** (descrito no **subitem 4.1.2**), acompanhado da versão editável, em formato “.XLS” (para ambiente MS Windows) ou outro formato definido em comum acordo. O relatório deverá conter as seguintes informações de cada ocorrência:

- a) Número do registro/ocorrência;
- b) Identificação do atendente;

- c) Identificação do solicitante (**DATAPREV**);
- d) Data e hora da solicitação (considerando o fuso horário de Brasília);
- e) Nível de severidade da ocorrência (estabelecido pela **DATAPREV**);
- f) Descrição da ocorrência;
- g) Data e hora da solução (considerando o fuso horário de Brasília);
- h) Data e hora do fechamento da ocorrência (considerando o fuso horário de Brasília);
- i) Identificação do responsável (**DATAPREV**) pelo fechamento;
- j) Duração da ocorrência (no formato hh:mm);
- k) Tempo de atendimento sob responsabilidade da **CONTRATADA** (no formato hh:mm);
- l) Tempo de atendimento sob responsabilidade da **DATAPREV** (no formato hh:mm);
- m) Tipo de Suporte Técnico prestado:
  - Remoto
  - *On Site* (presencial)
- n) Classificação da ocorrência:
  - Suporte Técnico Remoto: incidente
  - Suporte Técnico Remoto: esclarecimento de dúvidas
  - Suporte Técnico *On Site* (presencial): incidente
- o) Subclassificação da ocorrência:
  - *Hardware*
  - *Software*
  - *Hardware e Software*
- p) Tipo de fechamento da ocorrência:
  - Solução de contorno
  - Solução definitiva
- q) Informar o número do chamado original (quando o chamado for originário de outro onde se tiver feito uso da solução de contorno).

**13.1.1. A CONTRATADA deverá encaminhar à DATAPREV, como anexos do Relatório Mensal de Atendimento, descrito no subitem 13.1 deste Termo de Referência:**

- a) Documento contendo as seguintes informações para cada registro/ocorrência:
  - Número do registro/ocorrência;
  - Descrição detalhada da causa da ocorrência;
  - Descrição detalhada da solução da ocorrência;
  - Resumo de cada interação ocorrida durante o atendimento, identificando claramente as transições de responsabilidade pelas ações entre **DATAPREV** e a **CONTRATADA**, contemplando data e hora de início e fim destas interações (considerando o fuso horário de Brasília), demonstrando assim a memória de cálculo para se chegar aos tempos finais apresentados sob responsabilidade da **DATAPREV** e sob responsabilidade da **CONTRATADA**.
- b) Cópias dos Relatórios de Visita, descritos no **subitem 13.3** deste **Termo de Referência**.

**13.1.2. O atraso no envio do Relatório Mensal de Atendimento, descrito no subitem 13.1 deste Termo de Referência, implicará no atraso da análise técnica de suas informações. Tal análise serve de subsídio para a realização da medição do serviço prestado pela CONTRATADA no respectivo período.**

**13.1.3. O Relatório Mensal de Atendimento, descrito no subitem 13.1 deste Termo de Referência, deve considerar formatação realizada pela CONTRATADA de forma a contemplar todas as informações exigidas descritas em fonte com tamanho que permita a sua impressão legível no formato A4, em orientação "paisagem".**

**13.2. Durante todo o período de prestação dos serviços relacionados à orientação técnica, a CONTRATADA deverá apresentar, mensalmente, um arquivo contendo o registro de todas as OS's (Ordens de Serviço) abertas e/ou fechadas relacionadas aos serviços de Orientação Técnica no período mensal de prestação de serviços encerrado. O Relatório Mensal de OS deverá ser encaminhado para os Gestores Administrativo e Técnico, conforme descrito no item 25 deste Termo de Referência, em até 7 (sete) dias úteis, contados a partir do dia seguinte ao fim do período mensal de prestação de serviços e deverá estar no formato XLS (para ambiente MS Windows) ou outro formato definido em comum acordo. O relatório deverá conter as seguintes informações de cada OS (Ordem de Serviço):**

- a) Número de registro/ chamado;
- b) Número da OS (Ordem de Serviço);
- c) Identificação do atendente;
- d) Identificação do solicitante;
- e) Data e hora da solicitação (considerando fuso horário de Brasília);
- f) Descrição dos serviços solicitados;
- g) Data e hora da reunião de definição do escopo da demanda (considerando fuso horário de Brasília);

- h) Data e hora da conclusão do serviço (considerando fuso horário de Brasília);
- i) Número de horas consumidas para execução do serviço, detalhadas por atividades desempenhadas, visando garantir o repasse do conhecimento e das melhores práticas para as equipes da **DATAPREV**;
- j) Identificação do responsável **DATAPREV** pela aprovação do serviço executado e consequente conclusão da OS (Ordem de Serviço).
- 13.3.** Ao término de cada atendimento *on site*, o técnico da **CONTRATADA** deverá preencher um **Relatório de Visita**, contendo data e hora do chamado, início e término do atendimento, identificação do equipamento/módulo defeituoso, as providências adotadas, peças substituídas e as observações pertinentes. O **Relatório de Visita** deve ser assinado pelo técnico da **CONTRATADA** responsável pelo atendimento e por um técnico da **DATAPREV**.
- 13.4.** O período mensal de prestação de serviços será definido pelo **Gestor Administrativo**, conforme descrito no **subitem 25.2** deste **Termo de Referência**, e informado à **CONTRATADA** na **Reunião de Abertura Contratual**, definida no **subitem 4.1** deste **Termo de Referência**.

#### 14. ACESSO AO SITE DO FABRICANTE

- 14.1.** Deverá ser garantido à **DATAPREV** o pleno acesso ao *site* do fabricante dos produtos adquiridos que constituem o objeto deste **Termo de Referência** para:
- a) Consultar quaisquer bases de dados disponíveis para usuários.
- b) Efetuar *downloads* de quaisquer atualizações de *software* ou documentações.
- 14.2.** Caso haja diferentes níveis de acesso no *site*, deverá obrigatoriamente ser ofertado o nível com maior grau de privilégios.

#### 15. USO DA LÍNGUA PORTUGUESA

- 15.1.** Em todas as atividades de suporte técnico, capacitação técnica e orientação técnica deverá ser empregada a língua portuguesa falada e escrita do Brasil. Serão admitidas as seguintes exceções a esta exigência:
- a) O uso de termos técnicos em inglês, nas conversações ou correspondências;
- b) O acesso a *sites* com conteúdo na língua inglesa, para consulta às bases de conhecimento ou *download* de componentes de *software*;
- c) A utilização de material original do fabricante em inglês, na realização da capacitação técnica, somente nos casos de ausência da publicação em português.
- d) Outros casos, com o aceite da **DATAPREV**.
- 15.2.** A abertura, o acompanhamento e o atendimento das ocorrências deverão ser feitos em língua portuguesa.
- 15.3.** Todos os relatórios constantes do **item 13** deste **Termo de Referência** deverão ser apresentados com conteúdo em língua portuguesa.

#### 16. SIGILO E INVIOABILIDADE

- 16.1.** A **CONTRATADA** deverá assinar **TERMO DE SIGILO** que se encontra no **ANEXO IV**, a fim de garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso, durante a prestação dos serviços de suporte técnico, orientação técnica e capacitação técnica.
- 16.2.** A **CONTRATADA** deverá prestar esclarecimentos à **DATAPREV** sobre eventuais atos ou fatos noticiados que se refiram à mesma.

#### 17. REMANEJAMENTO DE PRODUTOS

- 17.1.** A totalidade ou parte dos produtos adquiridos poderá eventualmente ser remanejado para outra localidade, em uma das três cidades nas quais a **DATAPREV** mantém *Data Centers* (Rio de Janeiro, Brasília ou São Paulo), sem prejuízo do atendimento nas condições descritas neste **Termo de Referência**, mediante prévia comunicação à **CONTRATADA**.
- 17.2.** Todas as despesas relativas ao eventual remanejamento e reinstalação serão de responsabilidade da **DATAPREV**.

#### 18. SANÇÕES ADMINISTRATIVAS

- 18.1.** Será aplicada multa pelo descumprimento dos prazos relacionados no **item 4 – Planejamento** deste **Termo de Referência**, causado pela **CONTRATADA**. O descumprimento de cada prazo implicará em uma nova multa, aplicadas cumulativamente conforme o caso.
- O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo:
- a) Para atrasos de até 10 (dez) dias corridos → multa de 0,1% (um décimo por cento) ao dia do valor total do respectivo Pedido de Compras / Contrato;
- b) Para atrasos superiores a 10 (dez) dias corridos → a multa descrita na alínea "a" será substituída por multa de 0,25% (vinte e cinco centésimos por cento) ao dia, até o limite máximo de 5% (cinco por cento) do valor total do respectivo Pedido de Compras / Contrato.
- 18.2.** Será aplicada multa pelo atraso causado pela **CONTRATADA** na **entrega dos produtos adquiridos**, conforme descrito no **subitem 5.1** deste **Termo de Referência**.
- O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo:
- a) Para atrasos de até 15 (quinze) dias corridos → multa de 0,2% (dois décimos por cento) ao dia do valor total dos produtos adquiridos;
- b) Para atrasos superiores a 15 (quinze) dias corridos → a multa descrita na alínea "a" será substituída por multa de 0,5% (cinco décimos por cento) ao dia, até o limite máximo de 10% (dez por cento) do valor total dos produtos adquiridos.
- 18.3.** Será aplicada multa pelo atraso causado pela **CONTRATADA** na **instalação dos produtos adquiridos**, conforme descrito no **subitem 6.2** deste **Termo de Referência**.

O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo:

- a) Para atrasos de até 10 (dez) dias corridos → multa de 0,2% (dois décimos por cento) ao dia do valor total do item Instalação;
- b) Para atrasos superiores a 10 (dez) dias corridos → a multa descrita na alínea "a" será substituída por multa de 0,5% (cinco décimos por cento) ao dia, até o limite máximo de 10% (dez por cento) do valor total do item Instalação.

**18.3.1.** Caso a **CONTRATADA** descumpra os prazos descritos nos **subitens 6.2 e 6.7.1** deste **Termo de Referência**, simultaneamente, a multa descrita no **subitem 18.3**, alíneas "a" e "b", será substituída por multa de 2% (dois por cento) ao dia, até o limite máximo de 10% (dez por cento) do valor total do item Instalação, pelo atraso, causado pela **CONTRATADA**, na instalação dos produtos adquiridos.

- 18.4.** Será aplicada multa de 0,1% (um décimo por cento) ao dia, até o limite máximo de 1% (um por cento) do valor de cada turma do item Capacitação, pelo descumprimento dos prazos relacionados no **Anexo V – Capacitação Técnica** deste **Termo de Referência**, causado pela **CONTRATADA**, exceto as alterações de prazos ocorridas de comum acordo entre a **CONTRATADA** e a **DATAPREV**. O descumprimento de cada prazo implicará em uma nova multa, aplicadas cumulativamente conforme o caso.
- 18.5.** Será aplicada multa de 1% (um por cento) ao dia, até o limite máximo de 10% (dez por cento) do valor de cada turma do item Capacitação, pelo atraso, causado pela **CONTRATADA**, na **realização de cada turma da capacitação**, conforme descrito no **Anexo V – Capacitação Técnica** deste **Termo de Referência**. O descumprimento do prazo de cada turma implicará em uma nova multa, aplicadas cumulativamente conforme o caso.
- 18.6.** Será aplicada multa de 1% (um por cento) do valor de cada turma do item Capacitação, pela indisponibilização de material didático ou disponibilização de modelo diferente do validado ou incompatível com a solução configurada na **DATAPREV**.
- 18.7.** Será aplicada multa de 3% (três por cento) do valor de cada turma do item Capacitação, pela interrupção de treinamento por indisponibilidade, instabilidade da solução ou por uso incompatível de infraestrutura física e tecnológica com o disposto neste **Termo de Referência**.
- 18.8.** Será aplicada multa de 5% (cinco por cento) do valor de cada turma do item Capacitação caso o resultado alcançado com a aplicação da avaliação da **Capacitação Técnica** seja considerado **INSATISFATÓRIO**, após reaplicação da turma conforme descrito no **Anexo V – Capacitação Técnica** deste **Termo de Referência**.
- 18.9.** Será aplicada multa de 7% (sete por cento) do valor de cada turma do item Capacitação/de cada produto de EAD especificado no Plano de Capacitação pela não entrega do conteúdo programático na qualidade e/ou na totalidade prevista.
- 18.10.** Será aplicada multa, calculada com base no valor caucionado em garantia do cumprimento das obrigações contratuais, de 1% (um por cento) ao dia, até o limite máximo de 3% (três por cento), pelo atraso, causado pela **CONTRATADA**, no cumprimento dos prazos relacionados nos **subitens 7.7 e 7.9 - Orientação Técnica** deste **Termo de Referência**, para cada abertura de Ordem de Serviço realizada pela **DATAPREV**. O descumprimento de mais de um prazo para uma mesma Ordem de Serviço implicará em uma nova multa, aplicadas cumulativamente conforme o caso.
- 18.11.** Será aplicada multa de 1% (um por cento) ao dia, até o limite máximo de 10% (dez por cento) do valor da respectiva Ordem de Serviço, pelo atraso, causado pela **CONTRATADA**, na **conclusão das Ordens de Serviço**, conforme descrito no **subitem 7.5** deste **Termo de Referência**. O descumprimento do prazo de cada Ordem de Serviço implicará em uma nova multa, aplicadas cumulativamente conforme o caso.
- 18.12.** Será aplicada multa pelo atraso, causado pela **CONTRATADA**, no fornecimento das informações sobre os canais de atendimento, conforme descrito nos **subitens 7.6 e 11.2** deste **Termo de Referência**. O descumprimento de cada prazo implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo:

- a) Para atrasos de até 10 (dez) dias corridos → multa de 0,05% (cinco centésimos por cento) ao dia do valor total do respectivo Pedido de Compras / Contrato;
- b) Para atrasos superiores a 10 (dez) dias corridos → a multa descrita na alínea "a" será substituída por multa de 0,1% (um décimo por cento) ao dia, até o limite máximo de 2% (dois por cento) do valor total do respectivo Pedido de Compras / Contrato.

**18.13.** Será aplicada multa pelo atraso, causado pela **CONTRATADA**, no **fornecimento das informações sobre a descontinuidade dos produtos**, conforme descrito no **subitem 8.5** deste **Termo de Referência**.

O cálculo do valor da multa variará de acordo com o número de dias de atraso, conforme descrito abaixo

- a) Para atrasos de até 15 (quinze) dias corridos → multa de 0,5% (cinco décimos por cento) ao dia do valor caucionado em garantia do cumprimento das obrigações contratuais;
- b) Para atrasos superiores a 15 (quinze) dias corridos → a multa descrita na alínea "a" será substituída por multa de 1% (um por cento) ao dia, até o limite máximo de 6% (seis por cento) do valor caucionado em garantia do cumprimento das obrigações contratuais.

- 18.14.** Será aplicada multa, calculada com base no valor caucionado em garantia do cumprimento das obrigações contratuais, de 0,1% (um décimo por cento) à hora, até o limite máximo de 6% (seis por cento), pelo atraso, causado pela **CONTRATADA**, no **cumprimento dos prazos para solução de ocorrências**, conforme descrito no **subitem 12.1** deste **Termo de Referência**, para cada chamado registrado pela **DATAPREV**. O descumprimento de mais de um prazo para um mesmo chamado implicará em uma nova multa, aplicadas cumulativamente conforme o caso.
- 18.15.** Será aplicada multa, calculada com base no valor caucionado em garantia do cumprimento das obrigações contratuais, de 1% (um por cento) ao dia, até o limite máximo de 6% (seis por cento), pelo atraso, causado pela **CONTRATADA**, no **fornecimento da solução definitiva para as ocorrências de software e hardware**, conforme descrito no **subitem 12.5 e 12.6** deste **Termo de Referência**. O descumprimento do prazo de cada chamado registrado pela **DATAPREV** implicará em uma nova multa, aplicadas cumulativamente conforme o caso.
- 18.16.** Será aplicada multa, calculada com base no valor caucionado em garantia do cumprimento das obrigações contratuais, de 1% (um por cento) ao dia até o limite de 3% (três por cento), pelo atraso, causado pela **CONTRATADA**, no fornecimento de qualquer um dos **relatórios**, conforme descrito no **item 13** deste **Termo de Referência**.
- 18.17.** Será aplicada multa, calculada com base no valor caucionado em garantia do cumprimento das obrigações contratuais, de 0,05% (cinco centésimos por cento) ao dia, até o limite máximo de 1% (um por cento), pelo atraso nas respostas as comunicações formais encaminhadas pela **DATAPREV**.
- 18.18.** Será aplicada multa de 0,25% (vinte e cinco centésimos por cento) à 10% (dez por cento) do valor total do respectivo Pedido de Compras / Contrato



pelos inadimplementos contratuais relacionados às situações não previstas nos subitens anteriores.

**18.19.** As multas constantes nesse item poderão ser aplicadas cumulativamente conforme o caso e são meramente moratórias, não isentando a **CONTRATADA** o ressarcimento por perdas e danos pelos prejuízos a que der causa.

**18.20.** As multas calculadas sobre o valor caucionado em garantia do cumprimento das obrigações contratuais serão aplicadas sobre o valor total pago mensalmente pela **DATAPREV** para a garantia dos itens que compõem a contratação da **Solução de Firewall de Rede**.

Caso o valor total pago mensalmente pela **DATAPREV** para a garantia seja insuficiente para o débito das multas devidas pela **CONTRATADA** no referido mês, o valor devido deverá ser descontado integralmente do valor caucionado em garantia do cumprimento das obrigações contratuais.

**18.21.** À **CONTRATADA** será garantido o direito à apresentação de defesa prévia, no prazo de **10 (dez) dias úteis**, contados a partir do dia seguinte à confirmação de recebimento da notificação de multa. Cabe à **DATAPREV** a solução final e definitiva da questão.

## 19. AVALIAÇÃO DO FORNECEDOR

**19.1.** Objetivando a contínua melhoria do processo de gestão, ao longo da vigência contratual, a **DATAPREV** realizará, trimestralmente, a Avaliação de Desempenho de Fornecedores, o que permitirá a adoção de eventuais ajustes no modelo de atendimento.

**19.2.** Serão avaliados os seguintes critérios:

- **Comunicação:** Avaliação qualitativa da comunicação do fornecedor, como: clareza na informação, formas de solicitações e questionamentos à **DATAPREV**, educação e nível de formalidade no atendimento, e tempo de resposta às solicitações da **DATAPREV**;
- **Confiabilidade:** Prestação correta (isenta de falhas e erros) do serviço / atendimento, comprovando a eficácia das medidas preventivas e/ou corretivas adotadas;
- **Organização:** Demonstra planejamento, integração e controle das atividades, cumprindo os prazos acordados, disponibilidade de pessoal com domínio dos serviços e conhecimento das atividades.

**19.3.** Para os critérios descritos acima serão atribuídas notas de 0 (zero) a 10 (dez), cuja média resultará em um dos conceitos abaixo:

**Péssimo** (de 0 a 4,9) / **Regular** (de 5 a 7,4) / **Bom** (de 7,5 a 8,9) / **Ótimo** (de 9 a 10)

**19.4.** Trimestralmente, a **CONTRATADA** será informada do conceito médio obtido no período e registrado no sistema interno de gestão da **DATAPREV**, resultando este que deverá balizar eventuais ações corretivas que se fizerem necessárias.

## 20. OBRIGAÇÕES DA CONTRATADA

**20.1.** Em até **20 (vinte) dias úteis**, contados a partir do dia seguinte à assinatura do Pedido de Compra / Contrato, a **CONTRATADA** deverá comprovar possuir mão de obra qualificada de profissionais certificados pelo fabricante para realizar os serviços de **instalação** em conformidade com o exigido no **subitem 6.1.1** deste **Termo de Referência**.

Caso seja necessário, a **CONTRATADA** poderá apresentar documentação de mais de um profissional, a fim de comprovar as certificações nas tecnologias exigidas.

**20.2.** Em até **20 (vinte) dias úteis**, contados a partir do dia seguinte à assinatura do Pedido de Compra / Contrato, a **CONTRATADA** deverá comprovar possuir mão de obra qualificada de pelo menos 1 (um) profissional certificado para realizar os serviços de **orientação técnica**, em conformidade com o exigido no **subitem 7.4.2** deste **Termo de Referência**.

Caso seja necessário, a **CONTRATADA** poderá apresentar documentação de mais de um profissional, a fim de comprovar as certificações nas tecnologias exigidas.

**20.3.** Em até **20 (vinte) dias úteis**, contados a partir do dia seguinte à assinatura do Pedido de Compra / Contrato, a **CONTRATADA** deverá comprovar possuir mão de obra qualificada de pelo menos 1 (um) profissional certificado para apoiar as atividades de suporte técnico, em conformidade com o exigido no **subitem 8.6** deste **Termo de Referência**.

Caso seja necessário, a **CONTRATADA** poderá apresentar documentação de mais de um profissional, a fim de comprovar as certificações nas tecnologias exigidas.

**20.4.** O vínculo jurídico-legal do(s) profissional(is) citado(s) no(s) **subitens 20.1 a 20.3** deste **Termo de Referência** com a **CONTRATADA** ou com o **FABRICANTE** pode ser: empregatício, societário ou contratual. A **CONTRATADA** deverá, conforme a situação, fornecer a documentação exigida abaixo:

- **Situação 1:** Vínculo empregatício (o profissional é funcionário da **CONTRATADA**):
  - I – Cópia autenticada dos certificados do fabricante ou certificados em formato digital contendo a chave e/ou link para validação de titularidade junto a certificadora;
  - II – Carteira Profissional (páginas de qualificação, foto e Contrato de Trabalho).
- **Situação 2:** Vínculo societário (o profissional é sócio da **CONTRATADA**):
  - I – Cópia autenticada dos certificados do fabricante ou certificados em formato digital contendo a chave e/ou link para validação de titularidade junto a certificadora;
  - II – Contrato Social da empresa.
- **Situação 3:** Vínculo contratual (o profissional presta serviços para a **CONTRATADA** ou para o **FABRICANTE**):
  - I – Cópia autenticada dos certificados do fabricante ou certificados em formato digital contendo a chave e/ou link para validação de titularidade junto a certificadora;
  - II – Contrato firmado entre o profissional e a **CONTRATADA** ou entre o profissional e o **FABRICANTE** para a prestação de serviços.

**20.5.** Durante a vigência contratual, caso a **CONTRATADA** queira apresentar um novo profissional com a certificação para atender à exigência descrita nos **subitens 20.1, 20.2, 20.3** deste **Termo de Referência**, deverá entregar a documentação descrita no **subitem 20.4** deste **Termo de Referência**.

**20.6.** Em até **20 (vinte) dias úteis**, contados a partir do dia seguinte à assinatura do Pedido de Compra / Contrato, a **CONTRATADA** deverá apresentar declaração do fabricante comprovando o atendimento às exigências descritas no **subitem 1.7** deste **Termo de Referência**.

20.7. Caso a **CONTRATADA** opte por oferecer atendimento por meio do centro de suporte e assistência técnica do fabricante dos produtos, conforme **subitem 11.1** deste **Termo de Referência**, deverá estar ciente da abertura e andamento de todo e qualquer chamado de suporte técnico realizado pela **DATAPREV**.

20.8. Independentemente da **CONTRATADA** optar por oferecer atendimento por meio de centro de suporte e assistência técnica próprio ou do fabricante dos produtos, conforme **subitem 11.1** deste **Termo de Referência**, será responsabilizada pelo descumprimento dos prazos para solução das ocorrências, descritos nos **subitens 12.1 e 12.5** deste **Termo de referência**. Desta forma, arcará com as devidas sanções decorrentes de tais descumprimentos, conforme descrito nos **subitens 18.14 e 18.15** deste **Termo de Referência**.

20.9. Em **até 20 (vinte) dias úteis**, contados a partir do dia seguinte à assinatura do Pedido de Compra / Contrato, caso a **CONTRATADA** opte por oferecer atendimento por meio do centro de suporte e assistência técnica próprio, deverá apresentar declaração do fabricante dos produtos adquiridos comprovando ser sua parceira formalmente designada como habilitada a prestar os serviços de suporte e assistência técnica destes produtos, e que possui acesso direto ao seu centro de suporte e assistência técnica, conforme **subitens 11.1 e 11.7** deste **Termo de Referência**.

20.10. Caso a **CONTRATADA** descumpra o estabelecido nos **subitens 20.1 à 20.9** deste **Termo de Referência**, a **DATAPREV** poderá cancelar o contrato por não atendimento sem arcar com qualquer ônus. Caberão à **CONTRATADA** as sanções devidas por não atendimento ao contrato.

20.11. Todos os prazos estabelecidos em dias úteis neste **Termo de Referência** devem considerar somente os feriados nacionais.

## 21. OBRIGAÇÕES DA CONTRATANTE

21.1. A **DATAPREV** deverá fiscalizar e acompanhar a prestação do serviço, comunicando à **CONTRATADA** toda e qualquer deficiência e/ou irregularidade relacionada com a entrega do objeto, diligenciando nos casos que exigirem providências corretivas.

## 22. FATURAMENTO

22.1. **Produtos de hardware/software**: mediante o envio pela **DATAPREV** do Relatório de Medição do produto fornecido pela **CONTRATADA**, após a emissão do respectivo **Termo de Aceite de Instalação** conforme **subitem 6.9** deste **Termo de Referência**.

22.2. **Instalação de hardware/software**: mediante o envio pela **DATAPREV** do Relatório de Medição do serviço prestado pela **CONTRATADA**, após a emissão do respectivo **Termo de Aceite de Instalação** conforme **subitem 6.9** deste **Termo de Referência**.

22.3. **Garantia**: Mensal, mediante o envio pela **DATAPREV** do Relatório de Medição do serviço prestado pela **CONTRATADA**. Dar-se-á em **60 (sessenta) parcelas mensais** após a emissão do respectivo **Termo de Aceite da Instalação** conforme **subitem 6.9** deste **Termo de Referência**.

22.3.1. Os chamados de suporte, descritos no **subitem 11.3** deste **Termo de Referência**, serão analisados mensalmente, após o envio do Relatório Mensal de Atendimento pela **CONTRATADA**, conforme descrito no **subitem 13.1** deste **Termo de Referência**. Tanto os chamados quanto as possíveis sanções decorrentes do descumprimento dos prazos para a solução de ocorrências relacionadas aos mesmos, conforme descritos nos **subitens 12.1 e 12.5** deste **Termo de Referência**, deverão ser refletidos no Relatório de Medição do mês subsequente a conclusão do processo administrativo equivalente.

22.4. **Capacitação**: mediante o envio pela **DATAPREV** do Relatório de Medição do serviço prestado pela **CONTRATADA**, após conclusão de cada turma considerada **SATISFATÓRIA**.

22.5. **Orientação Técnica**: mediante o envio pela **DATAPREV** do Relatório de Medição do serviço prestado pela **CONTRATADA**. Dar-se-á de acordo com as horas efetivamente utilizadas, em conformidade com o fechamento das Ordens de Serviços concluídas no período.

22.6. A **CONTRATADA** deverá enviar a documentação de cobrança diretamente à Unidade Centralizada de Recebimento – UCR, situada na Rua Cosme Velho, 6, Cosme Velho – Rio de Janeiro/RJ – CEP 22241-900, dentro do horário comercial, indicando o número do Pedido de Compra/Contrato, o número de medição descrito no Relatório de Medição e o período de prestação de serviço (quando for o caso).

## 23. PAGAMENTO

23.1. **15 (quinze) dias** após recebimento da fatura pela **DATAPREV**.

23.2. O reajuste de preço do contrato, quando factível, observará a variação do Índice de Custo da Tecnologia da Informação (ICTI).

## 24. VIGÊNCIA CONTRATUAL

24.1. A vigência contratual será de **72 (setenta e dois) meses** a partir da assinatura do pedido de compras/contrato, na forma do artigo 71, inciso I da Lei 13.303.

24.1.1. **12 (doze) meses** para as etapas de planejamento, entrega e instalação das licenças e equipamentos de hardware a contar:

- Início: assinatura do Contrato/Pedido de Compras (PC);
- Término: Emissão do **Termo de Aceite de Instalação**.

24.1.2. **60 (sessenta) meses** para a execução da garantia, suporte técnico e atualização, a contar da emissão do **Termo de Aceite de Instalação** da solução contratada;

24.1.3. **60 (sessenta) meses** para a execução da orientação técnica e capacitação, a contar assinatura do Pedido de Compras (PC)/Contrato.

24.2. **Prorrogável**, conforme previsto no art. 71 da Lei 13.303/2016.

## 25. GESTÃO CONTRATUAL

25.1. **Gestão Técnica** – Divisão de Gestão Técnica dos Recursos de TIC – DIGR.

25.2. **Gestão Administrativa** – Divisão de Gestão Administrativa de Contratos de TIC – DGTI.

## 26. ANEXOS

- ANEXO I – ESPECIFICAÇÃO TÉCNICA
- ANEXO II – PLANILHA DE FORMAÇÃO DE PREÇOS
- ANEXO III – MODELO DE ATESTADO OU DECLARAÇÃO DE CAPACIDADE TÉCNICA
- ANEXO IV – TERMO DE SIGILO
- ANEXO V – CAPACITAÇÃO TÉCNICA
- ANEXO VI – MODELO CADERNO DE TESTE

## ANEXO I – ESPECIFICAÇÃO TÉCNICA

Os itens que **NÃO** necessitarão de comprovação prática na prova de conceito, com execução na presença dos técnicos da Dataprev, estarão destacados neste anexo, com o termo “**Aceita-se documentação**”. Não serão aceitos vídeos previamente elaborados como comprovações práticas.

### 1. DESCRIÇÃO TÉCNICA DA SOLUÇÃO (sem necessidade de comprovação em Prova de Conceito – Item 1 e seus subitens)

A solução a ser fornecida deverá atender aos requisitos de segurança da informação por meio da entrega de componentes e funcionalidades de **Firewall de Próxima Geração (NGFW)**.

Todos os elementos da solução, sejam físicos ou virtualizados, deverão ser instalados *on-premises* e possuir capacidade de processamento compatível com os requisitos dessa especificação técnica para cada equipamento/modelo em *appliance* único — não sendo utilizados valores em *cluster* ou com uso de balanceador de carga — sem perda de desempenho, mesmo com a ativação simultânea de todos os recursos descritos. Serviços de *sandbox* e inteligência artificial poderão ser em nuvem ou utilizar recursos da nuvem do fornecedor.

Serão requeridos 2 (dois) tipos de equipamentos de *firewall* físicos, Tipo I e Tipo II, uma plataforma de gerência centralizada e armazenamento de logs, cujos requisitos se encontram definidos nesta especificação técnica.

Serão instalados 2 (dois) clusters da solução nos *Data Centers* de Rio de Janeiro, São Paulo e Distrito Federal, denominados respectivamente como Firewall Externo (Tipo I) e Firewall Interno (Tipo II), totalizando 6 (seis) *clusters*. Cada *cluster* da solução será composto por 2 (dois) equipamentos de *firewall* físicos para alta disponibilidade (HA).

#### 1.1. Requisitos Gerais de Segurança

A solução deverá permitir a **configuração e aplicação de políticas de segurança integradas**, com suporte aos seguintes recursos e funcionalidades:

##### 1.1.1. Regras de Firewall

- 1.1.1.1. Por protocolo (por exemplo: TCP, UDP, ICMP);
- 1.1.1.2. Por endereçamento (origem e destino – IP e sub-redes);
- 1.1.1.3. Por aplicação (identificação e controle de aplicações específicas mesmo em portas não padrão ou tráfego criptografado);
- 1.1.1.4. Por usuário.

##### 1.1.2. Filtro de URL (*Web Filtering*)

- 1.1.2.1. Possibilidade de restringir ou permitir o acesso a categorias de sites com base em política organizacional e listas dinâmicas de reputação.

##### 1.1.3. Identificação e Autenticação de Usuários

- 1.1.3.1. Integração com serviços de diretório (por exemplo: OpenLDAP, Active Directory) para definição de políticas com base em identidade de usuário.

##### 1.1.4. Prevenção contra Ameaças Avançadas (*Threat Prevention*)

Funcionalidades que combinem inteligência de ameaças, análise heurística, inspeção profunda de pacotes (DPI) e serviços em nuvem para identificar e bloquear ataques modernos, incluindo *exploits* e *ransomwares*.

###### 1.1.4.1. Sistema de Prevenção contra Intrusão (IPS)

- 1.1.4.1.1. Mecanismos de detecção e bloqueio de tráfego malicioso baseado em assinaturas, anomalias e análise comportamental.

###### 1.1.4.2. Antimalware / Antivírus

- 1.1.4.2.1. Capacidade de inspecionar e bloquear arquivos e tráfego contendo códigos maliciosos.

###### 1.1.4.3. Proteção contra Bots (Anti-bot) / Spyware (Anti-spyware)

- 1.1.4.3.1. Capacidade de identificar dispositivos comprometidos que se comuniquem com redes de comando e controle (C&C), bloqueando essas conexões.

##### 1.1.5. Proteção DoS (Anti-DDoS)

- 1.1.5.1. Capacidade de detectar e mitigar ataques de negação de serviço distribuídos (DDoS), localmente, garantindo a continuidade dos serviços e a integridade da rede, mesmo sob ataque.

##### 1.1.6. Integração com SIEM (*Security Information and Event Management*)/SOAR (*Security Orchestration, Automation and Response*)

- 1.1.6.1. Capacidade de enviar *logs* e alertas para sistemas de orquestração e correlação de eventos.

##### 1.1.7. Virtualização / *Multitenancy* (NGFW Virtual)

- 1.1.7.1. Suporte a múltiplas instâncias virtuais (*firewalls* virtualizados) com políticas isoladas.

##### 1.1.8. *Sandboxing*

- 1.1.8.1. Capacidade de isolar e analisar arquivos suspeitos em ambiente controlado antes de permitir sua entrada na rede, contando com a inspeção profunda de pacotes (DPI).

##### 1.1.9. Gerência Centralizada

- 1.1.9.1. Capacidade de permitir o gerenciamento e a administração dos *firewalls* NGFW da solução, sejam físicos ou virtualizados, a partir de uma

console centralizada, bem como a implementação e operação das políticas de segurança, fornecendo recursos para monitoração em tempo real do status e desempenho dos equipamentos gerenciados.

## 1.2. Aplicabilidade das Funcionalidades, Atualizações e Licenciamento

- 1.2.1. Todos os recursos listados acima deverão estar disponíveis e plenamente operacionais através dos dispositivos da solução, incluindo:
  - 1.2.1.1. *Firewalls* físicos (*clusters* - HA);
  - 1.2.1.2. Instâncias de *firewalls* virtualizados em *firewalls* físicos;
  - 1.2.1.3. Plataforma de gerência centralizada (*Appliances* virtuais - HA).
- 1.2.2. Durante a vigência do contrato devem ser fornecidas todas as atualizações, de sistemas operacionais, *software*, *patches* (correções).
  - 1.2.2.1. Devem ser fornecidas também todas aquelas requeridas para as funcionalidades dependentes de atualizações publicadas pelo fabricante, como: bases de conhecimento, assinaturas de ataques, de aplicações, vulnerabilidades e evasão de dados.
- 1.2.3. A solução de segurança deve ser fornecida com licenças de uso **perpétuo**, ou seja, não devem parar de funcionar mesmo após o período de garantia, no mínimo, para as seguintes funcionalidades:
  - 1.2.3.1. *Firewall*;
  - 1.2.3.2. Alta disponibilidade;
  - 1.2.3.3. VPN (*Site-to-Site*);
  - 1.2.3.4. VPN (*Client-to-Site*), no mínimo com as funções básicas para o Cliente para Sistemas operacionais Windows e MacOS;
  - 1.2.3.5. Gerência centralizada;
  - 1.2.3.6. Gerência de *Logs*.
- 1.2.4. Para as demais funcionalidades não explicitadas nos subitens do item 1.2.3, serão aceitas licenças no modelo de subscrição ou perpétua.
- 1.2.5. Todo licenciamento perpétuo contemplado na solução (*firewalls* e plataforma de gerência) deve permitir continuar com todas as suas funcionalidades ativas após o período de garantia, mesmo que sem a possibilidade de atualização tecnológica.
- 1.2.6. A solução deve ser licenciada para um número de usuários compatível com os requisitos dessa especificação técnica.
- 1.2.7. A solução deve ser licenciada para a funcionalidade de Filtro de URL (*Web Filtering*) somente para o equipamento Tipo I.
- 1.2.8. A solução deve ser licenciada para a criação de, no mínimo, 50 mil regras no total ou no mínimo 25 mil regras em cada política de controle de acesso.
- 1.2.9. Todos os equipamentos devem ser novos, de primeiro uso, não sendo aceitos equipamentos remanufaturados.
- 1.2.10. Todos os componentes de *hardware* e *software* da solução devem ser do mesmo fabricante.
- 1.2.11. Os equipamentos que compõem a solução devem estar homologados pela Anatel.
  - 1.2.11.1. A homologação da ANATEL deverá ser feita para os equipamentos em nome do fabricante da solução.
- 1.2.12. A solução ofertada não poderá ser composta por solução de *software* livre.

## 1.3. Distribuição de Instalação nos Data Centers

- 1.3.1. Todos os componentes de *firewall* serão instalados nos *Data Centers* da Dataprev do Rio de Janeiro, São Paulo e Distrito Federal
- 1.3.2. Todos os componentes da plataforma de gerência serão instalados nos *Data Centers* da Dataprev do Rio de Janeiro e Distrito Federal.
- 1.3.3. Cada *Data Center* contará com dois *clusters* de alta disponibilidade para proteção, respectivamente, de redes de borda dos *Data Centers* (interface externa) e segmentação de redes internas da Dataprev.

## 2. HARDWARE DO APPLIANCE DE FIREWALL NGFW

### 2.1. Características de fornecimento (sem necessidade de comprovação em Prova de Conceito – item 2.1 e seus subitens)

- 2.1.1. Os equipamentos componentes da solução de *firewall* NGFW devem implementar no mesmo conjunto de dispositivos de *hardware*, no momento da entrega, todas as funcionalidades e características exigidas nesta especificação técnica, sem a necessidade posterior de inclusão de nenhum componente, módulo ou dispositivo extras, não sendo aceitas soluções que requeiram a combinação de diferentes produtos para compor os dispositivos de segurança de rede.
- 2.1.2. Cada *appliance* deverá ser instalado em *rack* de 19 (dezenove) polegadas (fornecido pela Dataprev), incluindo todos os acessórios necessários para a instalação do *appliance* no *rack*.
- 2.1.3. Cada *appliance* deve possuir altura máxima de 4U.
- 2.1.4. Deve ser fornecido cabo de energia para cada fonte, tendo comprimento mínimo de 1,80 m (um metro e oitenta centímetros), como os seguintes padrões de tomada:
  - 2.1.4.1. Para os *Data Centers* de Brasília e Rio de Janeiro, fornecer o padrão de tomada o **Pial 3P+T** (Referência 56407).
  - 2.1.4.2. Para o *Data Center* de São Paulo, fornecer o padrão de tomada **Steck 2P+T** (N3276).
- 2.1.5. Deve vir acompanhado de todos os acessórios indispensáveis para a sua perfeita instalação e funcionamento.
- 2.1.6. Deverá ser fornecido cabo de console compatível com a porta de console do equipamento, caso não seja uma interface Ethernet com conector RJ-45.
- 2.1.7. Deverão ser fornecidos todos os cabos, de até 10 metros e conectores ópticos necessários para todas as interfaces e portas do equipamento, sendo que o comprimento adequado de cada cabo e os tipos de conectores para fibra (SC/LC) serão especificados pela Contratante durante a etapa de planejamento da instalação de conectividade de rede e Infraestrutura.
- 2.1.8. Para interface 1000BASE-T deverá ser adotado cabeamento CAT6A e para interfaces ópticas deverá ser adotado cabeamento composto por fibras de diâmetro 50µm/125µm, homologados pela Anatel, com conector LC (*Lucent Connector*).
  - 2.1.8.1. O cabeamento UTP deverá ser fornecido na cor cinza.
  - 2.1.8.2. O cabeamento em fibra deverá ser fornecido na cor aqua.
- 2.1.9. Os cabos deverão ser certificados, fornecidos já conectorizados e deverão ser testados conforme especificação do fabricante.
  - 2.1.9.1. O certificado poderá ser emitido pelo fabricante, fornecedor do cabo ou pela contratada.
- 2.1.10. Deverão ser fornecidos, no mínimo, todos os transceptores relativos a todas as interfaces exigidas na especificação técnica.
- 2.1.11. O sistema operacional/*firmware* dos *appliances* fornecidos deve, dentro das características solicitadas, ser a versão atual mais estável no momento da instalação.
  - 2.1.11.1. Não será permitido atendimento de requisitos da especificação técnica através de promessa de versões futuras.
  - 2.1.11.2. Não serão aceitas versões de teste, versões experimentais, versões personalizadas para clientes específicos ou que não tenham sido publicadas no *website* oficial do fabricante.
- 2.1.12. Na data da proposta, nenhum dos componentes da solução ofertada poderá estar listado no *website* do fabricante em listas de *end-of-life*, *end-of-support* e/ou *end-of-sale*.
- 2.1.13. Deve ser destinado ao uso normal, em ambiente tropical, com umidade relativa na faixa de 20% a 80% (sem condensação).
- 2.1.14. Deve suportar temperatura ambiente de armazenamento entre 0°C e 50°C.
- 2.1.15. Deve operar entre temperaturas de 0°C a 40°C.
- 2.1.16. Deve possuir configurações de CPU e memória (RAM e *Flash*) suficientes para a implementação de todas as funcionalidades descritas nesta especificação.

### 2.2. Características de hardware – Firewall NGFW

- 2.2.1. A plataforma de *hardware* deve permitir a instalação/substituição de discos SSD sem exigir a troca do equipamento.
- 2.2.2. Cada equipamento deve possuir discos SSD (*Solid-State Drive*) redundantes com capacidade de, no mínimo, 240 GB, funcionando em RAID 1.
- 2.2.3. O equipamento deve possuir no mínimo 2 (duas) fontes de energia internas, para Corrente Alternada (AC – *Alternating Current*), com chaveamento automático, capacidade de operação em 100V a 240V, e de frequência entre 50 e 60 Hz, conforme a seguir (**Aceita-se documentação**):
  - 2.2.3.1. As fontes de energia redundantes devem permitir utilização de circuitos elétricos distintos com, no mínimo, 1 (um) input de alimentação em cada fonte.

- 2.2.3.2. As fontes de energia devem ser do tipo substituível (*hot-swap*), permitindo instalação e substituição sem a necessidade de qualquer interrupção no funcionamento normal do equipamento.
- 2.2.3.3. O equipamento deverá dispor de fontes de energia redundantes, capazes de manter integralmente todas as suas operações em caso de falha de uma das fontes, independentemente da quantidade de interfaces em uso, considerando-se a capacidade máxima especificada e com todas as funcionalidades habilitadas. **(Aceita-se documentação)**.
- 2.2.4. Deve possuir LED de diagnóstico que forneçam informações de alimentação e atividade do equipamento.
- 2.2.5. Para facilitar o manuseio de cabos e conexões, todas as placas de rede, interfaces e portas devem estar localizadas no painel frontal do equipamento.
- 2.2.6. O equipamento deve possuir módulos de ventilação redundantes, substituíveis, *hot-swap*, permitindo que fluxo de ar (exaustão) ocorra em direção à parte traseira do *rack*. **(Aceita-se documentação)**.

### 2.3. Interfaces

2.3.1. O *appliance* deve possuir interfaces exclusivas para:

2.3.1.1. **Console**, para acesso à interface de linha de comando do *appliance*.

2.3.1.2. **Gerenciamento/administração**

2.3.1.2.1. Deve possuir no mínimo, 1 (uma) interface de gerenciamento/administração OOB (*out-of-band*) que deve ser 1000Base-T, sendo uma conexão de rede dedicada e separada das interfaces de dados, usada exclusivamente para acessar, gerenciar e administrar o *firewall* de forma segura, mesmo quando a rede principal está indisponível.

2.3.1.3. **Sincronismo/alta disponibilidade**

2.3.1.3.1. Devem possuir, no mínimo, 2 (duas) interfaces de sincronismo/alta disponibilidade, devendo ser, no mínimo, de 10 Gbps;

2.3.1.4. **Tráfego de dados de produção**

2.3.1.4.1. Cada equipamento componente dos *clusters* de alta-disponibilidade deve possuir, no mínimo, o seguinte conjunto de interfaces, dedicadas ao tráfego de produção:

#### Para equipamentos que suportam *breakout*

2.3.1.4.2. Para equipamentos que suportam *breakout*, deve possuir, no mínimo, o seguinte conjunto de interfaces, dedicadas ao tráfego de produção:

Item	Tipo I	Tipo II
2.3.1.4.3	No mínimo, 2 (duas) interfaces 100GBase-F QSFP28, 16 (dezesesseis) interfaces 10GE SFP+	No mínimo, 2 (duas) interfaces 100GBase-F QSFP28, 8 (oito) interfaces 10GE SFP+

2.3.1.4.4. As interfaces de 100GBase-F devem permitir suporte a *breakout* em taxas de transmissão de 10 Gbps e 25 Gbps. **(Aceita-se documentação)**.

2.3.1.4.4.1. Para cada interface de 100GBase-F deverão ser fornecidos: cabo de *breakout* (4 x 25 Gbps) e transceptor de 100 Gbps, a serem utilizados conforme demanda. **(Aceita-se documentação)**.

#### Para equipamentos que não suportam *breakout*

2.3.1.4.5. Para equipamentos que não suportam *breakout*, deve possuir, no mínimo, o seguinte conjunto de interfaces, dedicadas ao tráfego de produção:

Item	Tipo I	Tipo II
2.3.1.4.6	No mínimo, 2 (duas) interfaces 100GBase-F QSFP28, 4 (quatro) interfaces de 25GBase-F SFP28 e 16 (dezesesseis) interfaces 10GE SFP+	No mínimo, 2 (duas) interfaces 100GBase-F QSFP28, 2 (duas) interfaces de 25GBase-F SFP28 e 8 (oito) interfaces 10GE SFP+

2.3.1.4.7. As interfaces de console, gerenciamento/administração e sincronismo/alta disponibilidade devem ser dedicadas e exclusivas para estas finalidades, ou seja, separadas das interfaces dedicadas ao tráfego de produção.

2.3.1.4.8. O *appliance* deve possuir LED de diagnósticos que forneçam informações e atividades de cada interface de dados e gerência.

### 3. RECURSOS E DESEMPENHO DOS EQUIPAMENTOS

3.1. Deve suportar os protocolos IPv4 e IPv6.

3.1.1. Deve implementar mecanismo de pilha dupla (*dual-stack*), para permitir o funcionamento simultâneo dos protocolos IPv4 e IPv6.

3.2. O *appliance* deve possibilitar a configuração dinâmica de interfaces por *software*, permitindo a definição de interfaces ativas/inativas.

3.3. Deve implementar VLANs compatíveis com o padrão IEEE 802.1Q e implementar VLAN *tagging* através de enlaces *trunk* com dispositivos de rede. Cada interface operando o protocolo IEEE 802.1Q deve suportar tráfego *tagged* e tráfego *non-tagged* simultaneamente. **(Aceita-se documentação)**.

3.3.1. Deve suportar pelo menos 4.094 VLANs (VLAN tags) 802.1Q. **(Aceita-se documentação)**.

3.4. Deve suportar o protocolo 802.3ad, *Link Aggregation Control Protocol* (LACP).

3.4.1. Suportar ao menos 128 VLANs por conjunto de links 802.3ad. **(Aceita-se documentação)**.

3.5. Deve implementar associação de portas 10 *Gigabit Ethernet*, compatível com o padrão IEEE 802.3ad, em grupo de até 4 portas (caso disponíveis), formando uma única interface lógica com as mesmas funcionalidades das interfaces originais.

3.6. Implementar associação das portas 25 *Gigabit Ethernet*, compatível com o padrão IEEE 802.3ad, no mínimo 2 portas formando uma única interface lógica com as mesmas funcionalidades das interfaces originais.

3.7. Deve permitir a inclusão de um texto de descrição na configuração de cada interface, possibilitando ao administrador identificar as regiões do ambiente de rede que serão alcançadas através de uma determinada interface.

3.8. Cada equipamento componente do *cluster* de alta-disponibilidade deve possuir a capacidade para suportar, no mínimo **(Aceita-se documentação)**:

Item	Recurso	Tipo 1	Tipo 2
a	<i>Throughput</i> de NGFW c/ <i>Threat Prevention</i>	55 Gbps	35 Gbps
b	<i>Throughput</i> de VPN IPsec	20 Gbps	10 Gbps
c	TLS Inspection <i>Throughput</i>	10 Gbps	5 Gbps
d	Conexões simultâneas	8.000.000	4.500.000

3.9. Para cálculo de *throughput* (vazão), as seguintes funcionalidades devem estar habilitadas:

- 3.9.1. NGFW c/ Threat Prevention:** Firewall, Application Control (Controle de Aplicações), IPS, Malware Protection (Proteção antimalware), Sandbox e log ativado. **(Aceita-se documentação).**
- 3.9.2. TLS Inspection Throughput:** inspeção profunda de pacotes (DPI), com threat prevention ativado e com suporte ao tráfego formado por um mix de diferentes versões de TLS (1.0, 1.1, 1.2, e 1.3) ativas simultaneamente com, no mínimo, 400.000 conexões simultâneas, para o equipamento Tipo 1. **(Aceita-se documentação).**
- 3.9.3. TLS Inspection Throughput:** inspeção profunda de pacotes (DPI), com threat prevention ativado e com suporte ao tráfego formado por um mix de diferentes versões de TLS (1.0, 1.1, 1.2, e 1.3) ativas simultaneamente com, no mínimo, 200.000 conexões simultâneas, para o equipamento Tipo 2. **(Aceita-se documentação).**
- 3.9.4. TLS Inspection Throughput:** inspeção profunda de pacotes (DPI), com threat prevention ativado para tráfego com criptografia TLS 1.2, considerando pacotes de 1500 bytes, não devendo ultrapassar 70% do consumo de CPU, no mínimo com 50.000 conexões simultâneas e chaves RSA 2048 bits, para o equipamento Tipo 1.
- 3.9.5. TLS Inspection Throughput:** inspeção profunda de pacotes (DPI), com threat prevention ativado para tráfego com criptografia TLS 1.3, considerando pacotes com 1500 bytes, não devendo ultrapassar 80% do consumo de CPU, no mínimo com 50.000 conexões simultâneas e chaves ECC 256 bits, para o equipamento Tipo 1.
- 3.9.6.** Todos os requisitos de desempenho especificados neste documento devem ser suportados com os appliances operando em modo cluster ativo/passivo, onde toda demanda de desempenho deve ser atendida com apenas um equipamento operando. **(Aceita-se documentação).**
- 3.10.** A solução de firewall deve suportar a configuração dos dispositivos de firewall físicos, em cluster de alta disponibilidade, na configuração ativo/ativo. **(Aceita-se documentação).**
- 3.10.1.** Os firewalls virtualizados nos appliances físicos devem obedecer ao ativo/ativo configurado nos firewalls físicos do cluster ao qual pertencem. **(Aceita-se documentação).**
- 3.11.** A solução de firewall deve suportar a configuração dos dispositivos de firewall físicos, em cluster de alta disponibilidade, na configuração ativo/passivo.
- 3.11.1.** Os firewalls virtualizados nos appliances físicos devem obedecer ao ativo/passivo configurado nos firewalls físicos do cluster ao qual pertencem.
- 3.12.** A solução deverá comutar automaticamente o tráfego entre equipamentos do cluster de alta disponibilidade, em caso de falha de um de seus dispositivos de firewall, tanto na configuração ativo/ativo quanto na configuração ativo/passivo. **(Aceita-se documentação somente para ativo/ativo).**
- 3.13.** A configuração dos dispositivos em alta disponibilidade (ativo/ativo e ativo/passivo) deve sincronizar entre os equipamentos, no mínimo **(Aceita-se documentação somente para ativo/ativo):**
- 3.13.1.** Sessões;
- 3.13.2.** Políticas de firewall, NAT, objetos de configuração (rede, nuvem e dinâmicos);
- 3.13.3.** Associações de segurança (SAs) das VPNs.
- 3.14.** A solução deve suportar roteamento baseado em políticas (Policy Based Routing), atendendo, no mínimo, aos seguintes critérios:
- 3.14.1.** Protocolo (TCP/UDP);
- 3.14.2.** Porta de destino;
- 3.14.3.** Endereçamento de origem.
- 3.15.** Deverá suportar a configuração de roteamento estático para IPv4 e IPv6.
- 3.16.** Deverá suportar a configuração de roteamento dinâmico para IPv4 e IPv6 para, no mínimo:
- 3.16.1.** BGP v4, com suporte a extensões de múltiplos protocolos, compatível com IPv4 e IPv6. **(Aceita-se documentação).**
- 3.16.2.** OSPF v2. **(Aceita-se documentação).**
- 3.16.3.** OSPF v3. **(Aceita-se documentação).**
- 3.16.4.** IGMP v2 e IGMP v3. **(Aceita-se documentação).**
- 3.17.** Deve possuir suporte a roteamento multicast (PIM-SM) **(Aceita-se documentação).**
- 3.18.** Permitir o roteamento nível 3 entre VLANs em suas subinterfaces.
- 3.19.** Permitir a inclusão manual de mapeamento ARP estático.
- 3.20.** O equipamento deve fornecer acesso a uma CLI (interface de linha de comando), sendo acessada localmente via porta de console.
- 3.21.** O hardware e o software do appliance devem ser obrigatoriamente do mesmo fabricante, não sendo aceito qualquer tipo de solução OEM composta de servidor de mercado com software embarcado ou pré-instalado. **(Aceita-se documentação).**
- 3.22.** O sistema operacional / firmware deve suportar a configuração das funções do sistema operacional através de:
- 3.22.1.** interface gráfica web utilizando navegadores disponíveis gratuitamente e protocolo HTTPS;
- 3.22.2.** CLI (interface de linha de comando), acessando localmente, via porta de console;
- 3.22.3.** Acesso remoto, via comunicação SSHv2.
- 3.23.** Deve ter a capacidade de atualização do sistema operacional / firmware via FTP, SCP, SFTP ou TFTP. **(Aceita-se Documentação).**
- 3.24.** Deve permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- 3.25.** Deve possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, traceroute, ping e log de eventos.
- 3.26.** O sistema operacional do dispositivo deverá permitir a utilização da ferramenta tcpdump, ou similar, para captura e monitoração de pacotes em quaisquer de suas interfaces de rede, permitindo que as capturas sejam armazenadas em formato pcap.
- 3.27.** Um sistema de backup/restore de todas as configurações do appliance, manual e automática, deve estar incluso e deve permitir ao administrador agendar backups das configurações em determinada data e hora, e exportá-los para um servidor remoto, suportando transferência de arquivos através de protocolo seguro SFTP (Secure File Transfer Protocol) ou SCP (Secure Copy Protocol).
- 3.28.** Deve suportar a restauração do sistema operacional para a última versão salva.
- 3.29.** Deve suportar sincronização do relógio interno via protocolo NTP.
- 3.30.** Deve suportar atualização automática do horário de verão com suporte a customização local, pelo fato de algumas cidades do Brasil não seguirem o padrão mundial. **(Aceita-se documentação).**
- 3.30.1.** Esta configuração deve ser realizada através de interface de configuração do sistema operacional, não sendo necessário instalar nenhum tipo de correção. **(Aceita-se documentação).**
- 3.31.** Os appliances devem ter, no mínimo, seu hardware ou sistema operacional, com a certificação Common Criteria. **(Aceita-se documentação).**
- 3.32.** A solução deverá prover integração do firewall ao serviço de autenticação da rede, permitindo, minimamente, a integração com serviços baseados em diretório nos padrões Open LDAP e Microsoft Active Directory.
- 3.32.1.** Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório Open LDAP e ao Microsoft Active Directory.
- 3.32.2.** Não será permitida a utilização de agentes instalados nos equipamentos dos usuários.
- 3.33.** A solução deve suportar a autenticação multifator (MFA) ou a integração com solução de MFA externa.
- 3.34.** Deve suportar SAML (Security Assertion Markup Language) para autenticação em bases e serviços de autenticação externos.

#### 4. REQUISITOS DE CONTROLE DE APLICAÇÕES (APPLICATION CONTROL)

- 4.1.** Os appliances devem possuir o recurso de Controle de Aplicações (Application Control).
- 4.2.** A solução deve ser capaz de identificar aplicações independentemente de porta, protocolo ou criptografia, utilizando múltiplos métodos como análise de assinatura, decodificação de protocolo e inspeção do payload dos pacotes (IPV4 e IPV6).
- 4.3.** Deve reconhecer, ao menos, 3.000 aplicações diferentes, incluindo, mas não se limitando a aplicações de redes sociais, mensagens instantâneas, P2P, acesso remoto, VOIP, e-mails, cloud storage, protocolos de rede e ferramentas de trabalho colaborativo. **(Aceita-se documentação).**
- 4.4.** A solução deve ser capaz de identificar funcionalidades específicas dentro de uma aplicação (ex.: permitir chat e bloquear vídeo dentro do mesmo serviço).
- 4.5.** A base de assinaturas de aplicações deve ser atualizada automaticamente e permitir atualização manual em horários configuráveis.
- 4.6.** Deve permitir a criação de assinaturas personalizadas diretamente pela interface do administrador ou ferramenta auxiliar do mesmo fabricante, para reconhecimento de aplicações proprietárias, sem necessidade de envolvimento do fabricante, mantendo a confidencialidade.

4.7. Deve identificar e controlar aplicações que utilizem táticas evasivas ou canais criptografados para se comunicar (ex.: Tor).

#### 4.8. Políticas de Controle e Ação

- 4.8.1. A solução deve permitir a aplicação de políticas com as ações: bloquear, permitir, alertar e limitar (*traffic shaping*) com base em aplicação identificada.
- 4.8.2. Deve ser possível criar grupos dinâmicos de aplicações com base em atributos como categoria, tipo de tecnologia (ex.: *client-server*, *browser-based*), ou nível de risco.
- 4.8.3. Deve permitir a personalização de mensagens de bloqueio e o redirecionamento dos usuários a portais informativos.
- 4.8.4. O processamento de controle de aplicações deve ocorrer localmente no equipamento, sem envio de dados pessoais para a nuvem do fabricante.

#### 5. REQUISITOS DE VIRTUALIZAÇÃO E MULTITENANCY (NGFW VIRTUAL)

- 5.1. A solução de *firewall* deve oferecer suporte nativo à virtualização, permitindo a criação de múltiplas instâncias lógicas (*firewalls* virtuais ou containers), com total isolamento de políticas, *logs*, interfaces e configurações administrativas.
- 5.2. Cada instância virtual deve operar de forma independente, permitindo personalização granular de regras de segurança, rotas e interfaces, sem afetar as demais instâncias em execução.
- 5.3. A criação e exclusão de *firewalls* virtuais deve ser realizada via interface gráfica e linha de comando.
- 5.4. As instâncias virtuais devem poder compartilhar recursos físicos de forma controlada permitindo definir limites para configuração de, no mínimo: quantidade de interfaces de rede; sessões ou conexões; e túneis VPN.
- 5.5. Deve permitir segmentação de ambientes por cliente, projeto, unidade organizacional ou serviço, garantindo *multitenancy* seguro, inclusive com autenticação e delegação administrativa por *tenant*.
- 5.6. Deve ser possível virtualizar os recursos de *hardware* e segurança do *appliance* físico em, no mínimo, 10 (dez) instâncias virtuais (*firewalls* virtualizados). **(Comprovar de forma prática, no mínimo, 1 (uma) instância de firewall virtualizado. Para as 10 (dez) instâncias virtuais, aceita-se documentação).**
- 5.7. Todas as funcionalidades de NGFW citados nessa especificação, devem poder ser usadas na(s) instância(s) virtual(ais) de *firewall*(s), que for(em) criada(s) no *appliance* físico. **(Aceita-se documentação).**

#### 6. INTEGRAÇÃO COM AMBIENTES DE NUVEM

- 6.1. A solução deve suportar integração nativa, no mínimo, com os principais provedores de nuvem pública e privada: AWS, Google Cloud Platform, VMware ESXi. **(Aceita-se documentação).**
- 6.2. O *firewall* deve manter sincronização contínua com os ambientes de nuvem, atualizando os objetos utilizados nas políticas em tempo real. **(Aceita-se documentação).**

#### 7. PROTEÇÃO DOS (ANTI-DDoS)

- 7.1. A solução deve ser capaz de detectar e mitigar ataques de DoS e DDoS diretamente, de forma local e autônoma, sem necessidade de redirecionamento de tráfego para serviços externos.
- 7.2. A solução deve monitorar o comportamento do tráfego de rede em tempo real, com capacidade de identificar padrões anômalos, no mínimo, a explosão de conexões (SYN flood), tráfego UDP malicioso e ICMP flood.
- 7.3. Deve permitir a configuração de limiares de tráfego por IP, protocolo ou tipo de conexão, com ações automáticas de mitigação (ex.: bloqueio, *rate-limit*, *drop*).
- 7.4. Deve registrar os eventos de detecção e resposta a ataques DoS/DDoS, com *logs* detalhados e alertas em tempo real por meio de SNMP e integração com o sistema de gerenciamento centralizado.

#### 8. GERENCIAMENTO CENTRALIZADO DA SOLUÇÃO

##### 8.1. Características de fornecimento (sem necessidade de comprovação em Prova de Conceito – item 8.1 e seus subitens)

- 8.1.1. A solução deve ser fornecida com, no mínimo, 01 (um) produto de gerenciamento centralizado, integrado a todos os dispositivos de *firewalls* e suas políticas de segurança, podendo ser composta por mais de um produto e *appliances* com diferentes funções, desde que estes atuem em conjunto para compor uma solução de gerenciamento centralizado que atenda a todas as características desta especificação técnica.
- 8.1.2. A solução de gerenciamento deve ser instalada em 2 *Data Centers* da Dataprev, fornecendo redundância ativo/passivo, ou seja, se o *appliance* de gerência localizado no Rio de Janeiro ficar indisponível, o *appliance* de gerência localizado no Distrito Federal, em sub-rede distinta, deverá ser capaz de controlar todos os *firewalls* da solução.
- 8.1.3. A solução deve suportar e estar licenciada para gerenciar todos os equipamentos de *firewall* fornecidos.
- 8.1.4. O *software* da solução de gerência deve ser, dentro das características solicitadas, a versão atual mais estável no momento da instalação.
- 8.1.5. Todas as soluções de *software* de gerência necessárias para o controle dos *firewalls* devem ser fornecidas pela Contratada.
- 8.2. As alterações realizadas em um servidor de gerência deverão ser replicadas para o servidor redundante mediante publicação das alterações realizadas.
- 8.3. A solução de gerência centralizada deve utilizar recursos de virtualização através de máquinas virtuais compatíveis com os virtualizadores VMWare, a serem fornecidos pela Dataprev. **(Aceita-se documentação).**
  - 8.3.1. O *software* de gerência deve ser do mesmo fabricante do *software* de *firewall*.
- 8.4. A Dataprev permitirá o consumo de recursos computacionais de sua infraestrutura, independentemente da quantidade de máquinas virtuais, limitado em cada *Data Center* a:
  - 8.4.1. 32 vCPUs; **(Aceita-se documentação).**
  - 8.4.2. 64 GB de memória RAM e; **(Aceita-se documentação).**
  - 8.4.3. 10 TB de armazenamento. **(Aceita-se documentação).**
- 8.5. Deve permitir que todos os *firewalls* sejam controlados de forma centralizada, utilizando apenas um servidor de gerência.
  - 8.5.1. A solução de gerenciamento deverá ser capaz de gerenciar a quantidade de *firewalls* descrita nesta especificação, bem como a capacidade de 10 (dez) instâncias virtuais (*firewall* virtualizados) para cada *firewall* físico. **(Aceita-se documentação).**
- 8.6. Deve suportar a criação e administração de políticas de segurança baseadas em objetos (Endereços - IPV4 / IPV6, faixa de IPs, grupo de endereços IP, redes, portas, protocolos, serviços, usuários, grupos de usuários, aplicações, grupos de aplicações, categorias de aplicações, categorias de URL, localização geográfica, zonas/interfaces e perfis de segurança das features de NGFW), permitindo sua utilização simultaneamente em diversas regras e configurações.
- 8.7. Deve suportar a criação de regras de *firewall* que sejam ativadas em datas e horários pré-definidos pelo administrador.
- 8.8. Um sistema de *backup/restore* de todas as configurações da solução de gerência deve estar incluso e deve permitir ao administrador agendar *backups* da configuração em uma determinada data/hora.
- 8.9. Deve ser permitido ao administrador transferir os *backups* para um servidor remoto, suportando FTP e protocolo seguro (SFTP ou SCP).
- 8.10. Caso os *appliances* de *firewall* percam comunicação com a solução de gerência, os *firewalls* deverão continuar tratando o tráfego corretamente, sem causar interrupção das comunicações.
- 8.11. Deve incluir um canal de comunicação seguro, com criptografia baseada em certificados, entre os servidores de gerência e todos os *firewalls* que fazem parte da solução.
- 8.12. A solução de gerência deve permitir a gerência através de interface *web* ou de *software* cliente, desde que todas as soluções de *software* necessárias sejam fornecidas.
- 8.13. A solução deve incluir uma ferramenta para gerenciar de forma centralizada as licenças de todos os *appliances* controlados pela estação de gerenciamento, permitindo ao administrador incluir e remover licenças nos *appliances* através dessa ferramenta. **(Aceita-se documentação).**
- 8.14. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de *software* dos *appliances*.
- 8.15. Deve incluir uma CA interna x.509, capaz de gerar certificados para os *gateways* e usuários, a fim de permitir fácil autenticação em VPNs.
- 8.16. Deve incluir a capacidade de confiar em CAs externas ilimitadas, inclusive com suporte a certificadoras suportadas pelo ICP-BR. **(Aceita-se documentação).**
- 8.17. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de certificado digital ou nome de usuário e senha.

- 8.18. No caso de usuário e senha, o usuário deverá poder se autenticar utilizando os seguintes esquemas: contas de usuários cadastrados no próprio servidor de gerência e contas de em serviço de diretório *Open LDAP* e *Active Directory*. **(Aceita-se documentação para o Open LDAP).**
- 8.19. A solução deve permitir autenticação multifator (MFA).
- 8.20. Deve suportar sincronização do relógio interno via protocolo NTP. **(Aceita-se documentação).**
- 8.21. Deve suportar atualização automática do horário de verão, com suporte a personalização local, pelo fato de algumas cidades do Brasil não seguirem o padrão mundial. Esta configuração deve ser realizada através da interface de configuração do sistema operacional (GUI ou CLI). **(Aceita-se documentação).**
- 8.22. A solução deve suportar níveis de permissões de administração distintos, incluindo pelo menos os seguintes perfis: *read/write*, *read only*, gerenciamento de usuários (com exceção de administradores).
- 8.23. Deve registrar *login* ou tentativa de *login* de qualquer usuário.
- 8.24. Deve possuir interface gráfica para pesquisa de *logs* de todos os *firewalls* administrados, permitindo a utilização de filtros, no mínimo, para verificação de acessos e bloqueios realizados;
- 8.25. Deve permitir a localização das regras nas quais um determinado endereço IP, rede ou objetos estão sendo utilizados;
- 8.26. *Logs* de auditoria para configurações de regras e objetos devem ser visualizados em uma lista diferente da que exhibe os *logs* relacionados a tráfego de dados.
- 8.27. A solução deve possibilitar que todos os *logs* gerados e armazenados na solução de armazenamento de logs do item 15, sejam exportados diretamente para soluções centralizadas de *log* da Dataprev. Essa exportação deve ser compatível com Elastic e ferramenta SIEM, via *syslog* em formato CEF (*Common Event Format*) ou JSON (*JavaScript Object Notation*). **(Aceita-se documentação para a capacidade de integração com plataformas de SIEM e Elastic. Comprovar de forma prática a exportação via syslog nos formatos sugeridos).**
- 8.28. A solução deve possibilitar a monitoração dos equipamentos do *cluster* de alta disponibilidade de *firewall*, identificando:
- 8.28.1. Falha de *link* nas interfaces de rede dos seus equipamentos (físicos e virtuais);
- 8.28.2. Falha de componentes de *hardware* ou *software* essenciais ao funcionamento dos dispositivos. **(Aceita-se documentação).**
- 8.29. CONTROLE DE FLUXO E MUDANÇAS DE REGRAS
- 8.29.1. A solução de gerência deve prover uma ferramenta para controlar as mudanças realizadas numa base de regras.
- 8.29.2. Esta ferramenta deve ser capaz de rastrear visualmente mudanças realizadas na base de regras, destacando e enumerando todas as mudanças.
- 8.29.3. Deve ser capaz de gerar relatórios ou visualizações de todas as alterações feitas durante uma sessão de mudanças, a ser utilizado pelos administradores e auditores.
- 8.29.4. Deve ser capaz de gerar relatórios ou visualizações comparativas entre duas sessões diferentes, resumindo todas as alterações efetuadas.

## 9. REQUISITOS DE FIREWALL

- 9.1. Cada *firewall* deve suportar trabalhar simultaneamente em modo *bridge* e modo *gateway*, realizando controle *Stateful Inspection* em ambos os modos, em quaisquer interfaces. **(Aceita-se documentação).**
- 9.2. Deve utilizar *Stateful Inspection*. **(Aceita-se documentação).**
- 9.3. Deve suportar os seguintes tipos de NAT:
- 9.3.1. NAT de Origem;
- 9.3.2. NAT de Destino;
- 9.3.3. NAT estático (1:1);
- 9.3.4. NAT estático bidirecional 1:1;
- 9.3.5. NAT dinâmico (N:1);
- 9.3.6. Tradução de porta (PAT).
- 9.4. Deve suportar as seguintes configurações de NAT:
- 9.4.1. NAT de origem e NAT de destino, simultaneamente;
- 9.4.2. NAT para objetos dinâmicos, como: nomes de domínios, listas externas de endereços IPs e FQDN.
- 9.5. Para cada regra, a solução deve fornecer várias opções de evento, entre elas: Log, envio de SNMP *trap*, enviar um e-mail, enviar alerta para a interface de monitoração da gerência.
- 9.5.1. As opções podem ser simultâneas ou não, a critério do administrador.
- 9.6. Deve ser possível segmentar as regras de segurança através de rótulos, a fim de melhor organizar as políticas.
- 9.7. Deve possuir o mínimo de 3.000 aplicações pré-definidos, que deverão ser utilizados para decisão de liberação de tráfego. **(Aceita-se documentação).**
- 9.8. Deve permitir a definição dos tempos de expiração (*time-out*) de sessões e conexões, novas ou já estabelecidas, para os diferentes tráfegos, possibilitando sua customização por protocolo.
- 9.9. Deve incluir um mecanismo de busca a fim de tornar fácil a consulta de quais objetos de rede contém endereços IP específicos ou parte deles, e listar todas as regras nas quais um determinado objeto é utilizado.
- 9.10. Qualquer funcionalidade de controle de tráfego relativo a regras de acesso implementados para IPv4, também deve funcionar com IPv6. **(Aceita-se documentação).**
- 9.11. Deve ser possível realizar NAT de endereços IPv6 para endereço IPv4.
- 9.12. Deve permitir o encaminhamento e tratamento de segurança de *Jumbo Frames* (pacotes de 9.000 bytes).
- 9.13. Deve permitir a visualização de informações sobre a utilização de uma determinada regra, no mínimo, como a quantidade de vezes que ela permitiu uma determinada conexão, volume de tráfego em bytes, e a última data e hora que foi utilizada, mesmo que as regras não estejam configuradas para gerar *log*.
- 9.14. A solução deve incluir assistente virtual, podendo ser em nuvem, com recursos de IA, para consulta e análise de regras, políticas e configurações de IPS:
- 9.14.1. Deve oferecer sugestões automatizadas de configuração.
- 9.14.2. Deve permitir executar tarefas administrativas e operacionais com base no contexto do ambiente, como regras existentes, eventos recentes e configurações aplicadas.
- 9.14.3. Deve permitir a avaliação das configurações do *firewall* e identificar áreas para melhoria.
- 9.14.4. Deve fornecer informações sobre a saúde dos *firewalls*, bem como possibilitar a monitoração e a geração de alertas para falhas de *hardware*.
- 9.14.5. Caso a solução seja em nuvem, ou seja, necessária a comunicação com a nuvem do fabricante para atender as funcionalidades de IA, esta comunicação deve ser segura e criptografada.

## 10. PREVENÇÃO DE AMEAÇAS (THREAT PREVENTION)

### 10.1. Sistema de Prevenção de Intrusões (IPS)

- 10.1.1. A solução de *firewall* deve incluir IPS nativo e integrado, operando simultaneamente com as demais funcionalidades de segurança no mesmo *hardware*. **(Aceita-se documentação).**
- 10.1.2. Deve oferecer mecanismos de detecção como: análise heurística, assinaturas de vulnerabilidades, validação e decodificação de protocolos, detecção de anomalias, análise comportamental, fragmentação de pacotes e correlação de eventos. **(Aceita-se documentação).**
- 10.1.3. O IPS deve ser capaz de inspecionar sessões completas, independentemente do tamanho ou protocolo. **(Aceita-se documentação).**
- 10.1.4. Deve permitir inspeção direcionada por interface e sentido de tráfego, com políticas pré-definidas prontas para uso imediato.
- 10.1.5. Deve permitir a criação, personalização e desativação de assinaturas específicas, além de regras de exceção com base em IPs, serviços ou combinações.
- 10.1.6. As ações configuráveis por assinatura devem incluir: permitir, logar, bloquear e bloqueio temporário por IP.
- 10.1.7. Deve suportar modo passivo (detecção apenas), com geração de alertas sem bloqueio.
- 10.1.8. Devem estar disponíveis descrições técnicas por assinatura, incluindo código CVE, severidade, impacto e ação prevista.
- 10.1.9. O IPS deve ser capaz de capturar pacotes automaticamente para eventos específicos e permitir extração via logs para fins forenses.



- 10.1.10. Deve detectar e mitigar ataques de rede e aplicação, incluindo: serviços *web*, DNS, SMTP, IMAP, POP3, FTP, Microsoft Networking, SNMP, VoIP, peer-to-peer, SFTP, SSH, RDP, TCP *flood* e *hijacking*. **(Aceita-se documentação)**.
- 10.1.11. Deve possibilitar bloqueio de tráfego por geolocalização, com políticas configuráveis por país ou região. **(Aceita-se documentação)**.
- 10.1.12. Deve suportar atualização automatizada ou manual da base de assinaturas, com agendamento e possibilidade de desativação.

## Antimalware / Antivírus e Análise em Sandbox

### 10.2.1. Detecção e Prevenção de Ameaças Desconhecidas

- 10.2.1.1. A solução de *firewall* deve possuir módulo antimalware / antivírus integrado, com capacidade de bloquear arquivos maliciosos através de mecanismos avançados de detecção, prevenção e tratamento de ameaças conhecidas e desconhecidas e análise em ambiente controlado (*sandbox*), com capacidade de bloquear arquivos maliciosos.
- 10.2.1.2. As atualizações das assinaturas devem ocorrer de forma automática ou manual, com possibilidade de agendamento e desativação do mecanismo automático.
- 10.2.1.3. A solução de *firewall* deve oferecer mecanismos avançados de detecção de *malwares* desconhecidos (*zero-day*), por meio da análise comportamental em ambiente de *sandbox*. **(Aceita-se documentação)**.
- 10.2.1.4. A análise deve ocorrer antes da liberação do conteúdo ao destino, sem entrega parcial de arquivos suspeitos durante a verificação, garantindo proteção proativa contra ameaças emergentes.
- 10.2.1.5. O sistema deve ser capaz de detectar arquivos potencialmente maliciosos em comunicações Web (HTTP/HTTPS), e-mail (POP3, SMTP/TLS) e tráfego interno (protocolo SMB), FTP, independentemente do modo de operação do *firewall* (transparente ou camada 3). **(Aceita-se documentação)**.
- 10.2.1.6. O envio para análise em *sandbox* deve ocorrer de forma automática, com base em políticas pré-definidas, bem como sob demanda, por decisão do administrador.

### 10.2.2. Capacidade de Análise em Sandbox

- 10.2.2.1. O ambiente *sandbox* deve permitir execução e simulação realista dos arquivos analisados, minimamente, no sistema operacional Windows 10 ou superior.
- 10.2.2.2. Devem ser analisáveis, minimamente, arquivos dos seguintes tipos:
  - 10.2.2.2.1. Executáveis (.exe), lote (.bat), bibliotecas (.dll), pacotes Java (.jar), Linux (.elf);
  - 10.2.2.2.2. Documentos de escritório: Word (.doc, .docx), Excel (.xls, .xlsx), PowerPoint (.ppt, .pptx), PDFs (.pdf);
  - 10.2.2.2.3. Arquivos compactados ou criptografados: .zip, .rar, .7zip e gzip, incluindo varredura recursiva em arquivos aninhados.

### 10.2.3. Políticas de Seleção e Classificação

- 10.2.3.1 A seleção de arquivos para análise em *sandbox* deve ser baseada em políticas de segurança customizáveis, utilizando critérios como:
  - 10.2.3.11.1. Endereço IP de origem e destino;
  - 10.2.3.11.2. Usuário ou grupo de usuários;
  - 10.2.3.11.3. Aplicações, portas e protocolos;
  - 10.2.3.11.4. URLs e categorias de URL;
  - 10.2.3.11.5. Tipo e extensão de arquivo.
- 10.2.3.2. Os arquivos analisados devem ser classificados ao menos nas seguintes categorias:
  - 10.2.3.2.1. Malicioso;
  - 10.2.3.2.2. Não malicioso;
- 10.2.3.3. A solução deve registrar URLs extraídas de arquivos maliciosos e encaminhá-las para classificação automática na base de filtro de URLs. **(Aceita-se documentação)**.

### 10.2.4. Integração e Automação

- 10.2.4.1. A solução deve permitir envio automático de arquivos e links para análise *sandbox* por meio de API RESTful.
- 10.2.4.2. Deve permitir a emissão de relatórios técnicos detalhados contendo comportamento, chamadas de sistema, comunicação de rede e indicadores de comprometimento (IoCs).
- 10.2.4.3. Deve ser possível exportar os relatórios de análise *sandbox* em formatos legíveis e tabulados, como .txt, .csv ou .pdf, diretamente pela console de gerenciamento.

### 10.2.5. Gestão e Visibilidade

- 10.2.5.1. A solução deve manter *logs* detalhados das ameaças detectadas pelo antimalware / antivírus e *sandbox*, com identificação do país de origem e destino, aplicando controle geográfico. **(Aceita-se documentação)**.
- 10.2.5.2. A solução deve manter histórico das análises realizadas em *sandbox*, com interface para auditoria e consulta dos resultados, incluindo *timeline* de execução e ações observadas.
- 10.2.5.3. Deve permitir a análise forense de *malwares*, com captura de pacotes vinculados a eventos de detecção e exportação de dados para sistemas externos de SIEM ou análise.

### 10.2.6. Recursos Adicionais

- 10.2.6.1. O sistema deve possuir:
  - 10.2.6.1.1. Cache local ou distribuído de decisões anteriores (*hash/reputação*), para acelerar e reduzir redundância das análises (*AntiMalware/Antivirus* e *sandbox*).
  - 10.2.6.1.2. Possibilidade de consulta manual ou automática a essa base de reputação para arquivos previamente verificados (*AntiMalware/Antivirus* e *sandbox*).
- 10.2.6.2. A plataforma deve permitir compartilhamento de indicadores de comprometimento (IoCs) derivados da análise *sandbox* com mecanismos de *Threat Intelligence* da própria solução ou de terceiros.

### 10.2.7. Anti-Bot e Anti-Spyware

- 10.2.7.1. A solução deve detectar e bloquear comunicação com servidores de comando e controle (C&C), incluindo *callbacks* e padrões de *beaconing*.
- 10.2.7.2. Deve suportar detecção de *botnets* por IP, nome de domínio e análise de comportamento, mesmo que não constem em listas públicas.
- 10.2.7.3. Deve incluir mecanismo de detecção e prevenção de DNS *tunneling* e outras técnicas de exfiltração via canais encobertos, tais como, HTTP *tunneling*, ICMP *tunneling*, Cloud *exfiltration*. **(Requer comprovação de detecção para a técnica de DNS tunneling. Aceita-se documentação para as demais técnicas de exfiltração)**.
- 10.2.7.4. Deve identificar e bloquear *spyware* com base em assinaturas e comportamento, mesmo em tráfego criptografado (HTTPS).
- 10.2.7.5. Deve permitir aplicação de exceções e políticas específicas para segmentos de rede ou serviços, inclusive com *logs* detalhados por evento detectado.
- 10.2.8. A análise de links suspeitos deve ser suportada, permitindo que URLs detectadas como maliciosas (ex: *phishing*) sejam automaticamente categorizadas na base de filtragem de conteúdo da solução. **(Aceita-se documentação)**.

## 10.3. Threat Intelligence

- 10.3.1. A solução deve incluir serviço de *Threat Intelligence* nativo, mantido pelo fabricante, com base em fontes próprias e *feeds* externos validados.

(**Aceita-se documentação**).

10.3.2. Deve identificar ameaças emergentes e aplicar proteções automaticamente sem necessidade de reinício do equipamento. (**Aceita-se documentação**).

10.3.3. As decisões de bloqueio devem considerar reputação de IP/domínio, assinatura de *malware*, e comportamento em tempo real.

10.3.4. Os *logs* de eventos devem incluir dados enriquecidos com país de origem, categoria da ameaça e indicação de mitigação realizada.

#### 10.4. Filtragem de URLs (*Web Filtering*)

10.4.1. Para o equipamento **Tipo I**:

10.4.1.1. Deve ser capaz de filtrar acessos *web* por categoria (ex: redes sociais, jogos, conteúdo adulto, *downloads*, *proxies*, etc.), com atualização contínua da base.

10.4.1.2. Deve permitir bloqueio, alerta ou liberação por políticas com base em usuários, grupos, horários ou localidade geográfica.

10.4.1.3. O administrador deve poder criar listas personalizadas de URLs (permitidas e bloqueadas), com granularidade por domínio, caminho ou extensão.

10.4.1.4. Deve suportar inspeção de URLs em conexões HTTPS via decifração SSL/TLS.

10.4.1.5. A solução deve incluir visualização em tempo real do tráfego *web*, com *dashboards* de acesso por categorias e alertas de risco por atividade anômala.

#### 11. REQUISITOS DE VPN

11.1. Os recursos de VPN deverão ser gerenciados pela mesma solução de gerência dos equipamentos de *firewall*.

11.2. A solução de VPN deve suportar o estabelecimento de túneis VPN *Site-to-Site*, permitindo a utilização simultânea de pelo menos 100 túneis. (**Aceita-se documentação**).

11.3. A solução de VPN IPsec deve suportar:

11.3.1. Autenticação SHA-256 e SHA-512; (**Aceita-se documentação**).

11.3.2. Diffie-Hellman Group 14, Group 15 e Group 16; (**Aceita-se documentação**).

11.3.3. Algoritmo Internet Key Exchange (IKE), métodos IKEv1 e IKEv2; (**Aceita-se documentação**).

11.3.4. Algoritmo Advanced Encryption Standard (AES), com chaves de 128 e 256 bits (AES-128 e AES-256); (**Aceita-se documentação**).

11.3.5. Autenticação via certificado IKE PKI. (**Aceita-se documentação**).

11.4. Para o equipamento **Tipo I**:

11.4.1. A solução de VPN deve suportar conexões VPN utilizando os protocolos IPSec e SSL/TLS, simultaneamente, para acessos do tipo Remote Access (*Client-to-Site*).

11.4.2. Deve possuir servidor DHCP próprio e distribuir endereços IP para acessos do tipo *Remote Access (Client-to-Site)*.

11.4.3. Deve permitir que os usuários estabeleçam conexões VPN (*Client-to-Site*) através de um navegador padrão ou um *software* cliente instalado no próprio computador do usuário.

11.4.4. Os usuários poderão estabelecer conexão VPN utilizando os sistemas operacionais de versões mais recentes: Microsoft Windows, Linux (Ubuntu), macOS, Android e iOS. (**Comprovar de forma prática: Microsoft Windows 11 e macOS 15, para os demais, aceita-se documentação**).

11.4.5. Os usuários poderão estabelecer conexão VPN através de programa de *software* cliente a partir de sistemas operacionais de versões mais recentes: Microsoft Windows, Linux, macOS, Android e iOS. (**Comprovar de forma prática: Microsoft Windows 11 e macOS 15, para os demais, aceita-se documentação**).

11.4.6. Os usuários poderão se autenticar através de certificado digital ou nome de usuário e senha.

11.4.7. A solução deve permitir o estabelecimento de túneis VPN IPSec *Client-to-Site* **simultaneamente** de pelo menos **30.000 Usuários**. (**Aceita-se documentação**).

11.4.8. No caso de usuário e senha, a autenticação poderá ser realizada utilizando quaisquer dos seguintes esquemas: contas de usuários cadastrados no próprio servidor de gerência, TACACS+ e serviços de diretórios (*Open LDAP* e AD).

#### 12. CORRELAÇÃO DE EVENTOS DE SEGURANÇA

12.1. A solução de gerenciamento deve possuir uma ferramenta para análise de eventos de segurança, baseada nos *logs* gerados pelos módulos de *firewall* e IPS dos *appliances*.

12.2. A ferramenta de análise de eventos de segurança deve permitir ao administrador realizar o agrupamento de eventos baseado em quaisquer de seus parâmetros.

12.3. Deve incluir a opção de gerar automaticamente pequenos gráficos e tabelas, com os eventos, as origens e os destinos.

12.4. Deve incluir a opção de tomar ações pré-definidas disparadas por determinados alertas.

12.5. Deve permitir agendar a geração de relatórios pré-definidos de eventos de segurança em intervalos diários, semanais e mensais, incluindo Top eventos, Top origens, Top destinos, Top Serviços, Top origens e os seus principais eventos, Top destinos e seus principais eventos e Top serviços e seus principais eventos.

12.6. Deve permitir o uso de filtros customizáveis para selecionar alertas baseados nos seguintes parâmetros: origem, destino, serviço, tipo e nome do alerta.

12.7. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como endereços IP de origem e destino, serviço, tipo de evento, severidade do evento, nome do ataque, inclusive países de origem e de destino.

12.8. Deve exibir num mapa ou numa lista a distribuição por países dos diferentes eventos. (**Aceita-se documentação**).

12.9. Deve detectar ataques de DoS e correlacionar eventos das fontes.

#### 13. MONITORAÇÃO DOS APPLIANCES

13.1. Cada *appliance* deve suportar os padrões abertos de gerência de rede SNMP v2c e SNMP v3, incluindo a geração de *traps* SNMP para falhas de *hardware* e eventos, como alterações na configuração do equipamento, por exemplo.

13.2. Deve possuir suporte a MIB II, conforme RFC 1213. Caso a solução não possua suporte total a MIB II, deve suportar objetos semelhantes em sua MIB privativa. (**Aceita-se documentação**).

13.3. Implementar MIB privativa que forneça informações específicas sobre o funcionamento de seus módulos de proteção.

13.4. Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa. (**Aceita-se documentação**).

13.5. Todos os componentes e processos críticos devem gerar *logs* e permitir gravação dos *logs* em servidor remoto, através do protocolo *syslog*.

13.6. A solução de monitoramento deve incluir uma interface gráfica que forneça uma maneira simples de monitorar o estado dos *appliances*.

13.7. Deve prover, entre outras, as seguintes informações do sistema para cada *gateway*: sistema operacional, consumo de CPU, consumo de memória, atividade de rede, *throughput*, número de conexões simultâneas, novas conexões por segundo, número de pacotes por segundo.

#### 14. GERAÇÃO DE RELATÓRIOS

14.1. A solução deve incluir uma ferramenta para geração de relatórios. Esta ferramenta deve suportar pelo menos os seguintes filtros: IP de origem, IP de destino, serviço/protocolo, usuário, nome do ataque, número da regra, ID da regra, faixa de tempo e ação tomada. Deve ser possível utilizar mais de um filtro simultaneamente.

14.2. A ferramenta de geração de relatórios deve permitir personalizar um relatório e salvar essas alterações, para agilizar a coleta de informações necessárias para o administrador.

14.3. Deve permitir o agendamento de relatórios em intervalos diários, semanais e mensais.

14.4. Deve ser possível exportar os relatórios gerados para arquivos nos formatos CSV, HTML ou PDF.

14.5. Deve suportar a distribuição automática de relatórios por e-mail.

14.6. Deve permitir a geração de relatórios contendo, no mínimo, as seguintes informações:

- 14.6.1. Resumo gráfico de aplicações utilizadas;
- 14.6.2. Principais aplicações por volume de bytes trafegados;
- 14.6.3. Principais hosts por número de ameaças identificadas;
- 14.6.4. Principais ameaças ou ataques identificados;
- 14.6.5. O volume de sessões que foram bloqueadas pelo *gateway/cluster*;
- 14.6.6. As dez origens de conexões mais bloqueadas, seus destinos e serviços;
- 14.6.7. As dez regras mais usadas pelo *gateway/cluster*;
- 14.6.8. Os dez ataques à segurança mais detectados pelo *gateway/cluster* e determinação das suas principais fontes e os destinos;
- 14.6.9. Os dez serviços de rede mais utilizados;
- 14.6.10. Serviços que utilizaram mais tráfego criptografado;
- 14.6.11. Usuários VPN mais ativos em determinado horário;
- 14.7. Deve permitir visualizar informações a respeito das assinaturas utilizadas: código CVE ou equivalente, descrição, severidade, e tipo de ação executada;
- 14.8. Deve gerar relatórios sobre os eventos detectados, pelos seguintes critérios: volume de bytes trafegados, nível de risco e controle de aplicações.

#### 15. SOLUÇÃO DE ARMAZENAMENTO DE LOGS

- 15.1. Deverá armazenar *log* histórico e estar presente em cada um dos 3 *Data Centers* (RJ, SP e DF);
- 15.1.1. Deverá armazenar todos os *logs* gerados por todas as funcionalidades da solução de NGFW, definidos nesta especificação, tanto os *logs* de segurança, quanto *logs* de sistema. **(Aceita-se documentação)**;
- 15.2. A solução de armazenamento de *log* histórico, deverá ser apartada da solução de gerência e dos *appliances* de *firewall*;
- 15.3. Os *logs* devem ser transferidos de maneira segura entre os *appliances* e a solução de armazenamento de *log* histórico.
- 15.4. Os *logs* devem ser exportados diretamente dos *appliances* para os coletores respectivos em cada *Data Center*;
- 15.4.1. O armazenamento dos *logs* deve possuir capacidade mínima de 24 TB por cada *Data Center* (RJ, DF e SP). **(Aceita-se documentação)**.
- 15.5. Deve realizar o rotacionamento automático dos arquivos de *log*, por intervalo de tempo regular ou de acordo com o tamanho dos arquivos.
- 15.6. O armazenamento de *logs* deve utilizar recursos de virtualização através de máquinas virtuais compatíveis com os virtualizadores VMWare. **(Aceita-se documentação)**.
- 15.7. A Dataprev permitirá o consumo de recursos computacionais de sua infraestrutura, independentemente da quantidade de máquinas virtuais, limitado em cada *Data Center* a:
- 15.7.1. 32 vCPUs; **(Aceita-se documentação)**.
- 15.7.2. 128GB de memória RAM e; **(Aceita-se documentação)**.
- 15.7.3. 60 TB de armazenamento. **(Aceita-se documentação)**.

#### ANEXO II – PLANILHA DE FORMAÇÃO DE PREÇOS

LOTE ÚNICO									
ITEM	DESCRIÇÃO	QUANTIDADE TOTAL (A)	UNIDADE	PRODUTOS / SERVIÇOS		GARANTIA			
				VALOR UNITÁRIO (B)	SUBTOTAL A x B	VALOR UNITÁRIO MENSAL (C)	SUBTOTAL MENSAL A x C (D)	QTD. DE MESES (E)	SUBTOTAL 60 MESES D x E
1	a) Solução de Firewall de Rede on-premises com garantia, suporte e atualização de conteúdo de segurança para 60 meses (Tipo I).	6	Equipamento	R\$ -	R\$ -	R\$ -	R\$ -	60	R\$ -
	b) Solução de Firewall de Rede on-premises com garantia, suporte e atualização de conteúdo de segurança para 60 meses (Tipo II).	6	Equipamento	R\$ -	R\$ -	R\$ -	R\$ -	60	R\$ -
	c) Gerenciamento Centralizado da Solução de Firewall de Rede on-premises com garantia, suporte e atualização de conteúdo de segurança para 60 meses.	1	Solução de Gerenciamento Centralizado	R\$ -	R\$ -	R\$ -	R\$ -	60	R\$ -
	d) Serviço de Instalação para a solução de Gerenciamento Centralizado	1	Serviço	R\$ -	R\$ -				
	e) Serviço de Instalação para a solução de Firewall de Rede	12	Serviço	R\$ -	R\$ -				
	f) Orientação técnica	640	Hora	R\$ -	R\$ -				
	g) Capacitação técnica	2	Turma	R\$ -	R\$ -				
				TOTAL PRODUTOS / SERVIÇOS (F)	R\$ -	TOTAL MENSAL GARANTIA	R\$ -	TOTAL 60 MESES GARANTIA (G)	R\$ -
TOTAL (F + G)			R\$ -						

VALOR TOTAL DA CONTRATAÇÃO

R\$ -

Os valores apresentados incluem os impostos federais, estaduais e municipais, taxas e todos os demais custos envolvidos no escopo desta contratação, tais como: frete, embalagem, seguro etc.

#### ANEXO III – MODELO DE ATESTADO OU DECLARAÇÃO DE CAPACIDADE TÉCNICA

Atestamos (ou declaramos) que a empresa \_\_\_\_\_, inscrita no CNPJ (MF) nº \_\_\_\_\_, inscrição estadual/distrital nº \_\_\_\_\_, estabelecida no (a) \_\_\_\_\_, \_\_\_\_\_ (forneceu equipamentos/software, prestou serviços de instalação, serviços de suporte técnico, serviços de capacitação técnica e prestou serviços de orientação técnica) para a plataforma de \_\_\_\_\_ para este órgão (ou para esta empresa).

Atestamos (ou declaramos), ainda, que os compromissos assumidos pela empresa foram cumpridos integralmente e satisfatoriamente, nada constando em nossos arquivos que a desabone comercial ou tecnicamente.

Local e data

Assinatura e carimbo do emissor  
(com nº de matrícula ou do CPF)  
telefone de contato e e-mail

Observação: este documento deve ser emitido em papel timbrado que identifique o emissor.

ANEXO IV – TERMO DE SIGILO

PREGÃO ELETRÔNICO Nº XXX/2024  
PROCESSO Nº

TERMO DE SIGILO E PRIVACIDADE VINCULADO AOS CONTRATOS

Cláusula Primeira - OBJETO

Constitui objeto deste Termo o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela contratada, doravante denominada **PARTE RECEPTORA**, no que diz respeito ao trato de informações sigilosas, disponibilizadas pela contratante, doravante denominada **PARTE REVELADORA**, por força dos procedimentos necessários para a execução do objeto do Contrato Principal celebrado entre as partes.

Cláusula Segunda - CONCEITOS E DEFINIÇÕES

2.1 Para os efeitos deste TERMO aplicam-se os seguintes termos e definições:

2.1.1 Confidencialidade ou Sigilo

Propriedade de que a informação não seja revelada a pessoa física, sistema, órgão ou entidade não autorizados e credenciados.

2.1.2 Contrato de trabalho ou Contrato principal

Contrato celebrado entre as partes, ao qual este Termo de Sigilo se vincula.

2.1.3 Dado pessoal

Informação relacionada a pessoa natural identificada ou identificável (Lei nº 13.709/2018).

2.1.4 Dado pessoal sensível

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

2.1.5 Informação

Conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

2.1.6 Informação de acesso restrito

Aquelas que estão submetidas temporariamente à restrição de acesso público.

2.1.7 Informação sigilosa

Aquelas que estão submetidas à restrição de acesso público, cujo conhecimento e divulgação estão regidos por esse instrumento.

2.1.8 Informações de acesso restrito, sigilosas por legislação específica (não exaustivas):

I. Hipóteses de sigilo aplicáveis a informações de natureza patrimonial:

a) Segredo industrial (L. 9.279/1996);

- b) Direito autoral (L. 9.610/1998); e
- c) Propriedade intelectual de Software (L. 9.609/1998).

II. Hipóteses de sigilo decorrentes de direitos de personalidade:

- a) Sigilo Fiscal (Art. 198 da Lei nº 5.172/196);
- b) Sigilo bancário (Art. 1º da Lc nº 105/2001);
- c) Sigilo Comercial (§2º do art. 155 da Lei nº 6.404/1976);
- d) Sigilo Empresarial (Art. 169 da Lei nº 11.101/2005); e
- e) Sigilo Contábil (Art. 1.190 e 1.191 da Lei nº 5.869/1973).

III. Hipóteses de sigilo decorrentes de processos e procedimentos:

- a) Sigilo de inquérito policial (Art. 20 da Lei nº 3.689/1941);
- b) Segredo de justiça no processo civil (Art. 155 da Lei nº 5.869/1973); e
- c) Segredo de justiça no processo penal (§6º do art. 201 da Lei nº 3.689/1941).

2.1.9 Necessidade de conhecer

Condição pessoal inerente à função ou atividade, indispensável para que o colaborador tenha acesso a dados ou informações classificadas. De acordo com este princípio, os colaboradores só devem ter acesso às informações necessárias para o desenvolvimento de suas atividades dentro da empresa.

2.1.10 Tratamento ou processamento de dados pessoais

Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Cláusula Terceira - INFORMAÇÕES SIGILOSAS

§1º Serão consideradas como informações sigilosas, toda e qualquer informação, revelada a outra parte por razão da execução do contrato, contendo ou não marcação ou rótulo de grau de sigilo. O termo "informação" abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando, a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da contratante e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao Contrato Principal, doravante denominados **INFORMAÇÕES**, a que diretamente ou pelos seus empregados, a **PARTE RECEPTORA** venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do Contrato Principal celebrado entre as partes.

§2º A **PARTE RECEPTORA** compromete-se a não revelar, copiar, transmitir, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do Contrato Principal, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do Contrato Principal.

§3º As estipulações e obrigações contidas neste Termo não serão aplicadas a qualquer informação que seja comprovadamente de domínio público, exceto se decorrer de ato ou omissão do beneficiado ou tenha sido comprovada e legitimamente recebida de terceiros, estranhos ao presente instrumento ou ainda informações resultantes de pesquisa pelo beneficiado.

Cláusula Quarta - EXTENSÃO DA RESPONSABILIDADE

§1º A **PARTE RECEPTORA** se obriga a:

- a) Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das informações sigilosas por seus agentes, representantes ou por terceiros; e
- b) Comunicar à **PARTE REVELADORA** de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente.

Cláusula Quinta - DIREITOS E OBRIGAÇÕES

§1º A **PARTE RECEPTORA** se compromete e se obriga a utilizar a informação sigilosa revelada pela **PARTE REVELADORA** exclusivamente para os propósitos da execução do Contrato Principal, em conformidade com o disposto neste Termo.

§2º A **PARTE RECEPTORA** se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da **PARTE REVELADORA**

§3º A **PARTE RECEPTORA** se compromete a obter o aceite formal dos funcionários que atuarão direta ou indiretamente na execução do Contrato Principal sobre a existência deste Termo, bem como da natureza sigilosa das informações, a instruir sobre as formas de tratamento das informações a que terão acesso, e dar ciência à **PARTE REVELADORA** dos documentos comprobatórios quando solicitado.

§4º A **PARTE RECEPTORA** obriga-se a tomar todas as medidas necessárias a proteção da informação sigilosa, bem como para evitar e prevenir a revelação a terceiros.

§5º A **PARTE RECEPTORA** deve adotar Política de Segurança de Informação que comprove o atendimento dos requisitos de sigilo e segurança definidos no âmbito do contrato.

§6º A **PARTE RECEPTORA** deverá, quando requerido pela **PARTE REVELADORA**, proceder com o imediato descarte de forma irreversível, incluindo todas e quaisquer cópias eventualmente existentes em qualquer suporte de todas as informações sigilosas sob sua custódia referentes ao contrato principal.

## Cláusula Sexta - PROTEÇÃO DE DADOS PESSOAIS

- §1º Ambas as partes se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, em qualquer formato ou suporte, cooperando mutuamente para observar e seguir a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD).
- §2º Necessidades de coleta de consentimento para outras finalidades deverão ser identificadas e correr sob responsabilidade da **PARTE REVELADORA**.
- §3º São escopo de tratamento somente os dados pessoais indispensáveis para a execução do objetivo contratual, e conforme bases legais preestabelecidas e acordadas, cabendo à **PARTE RECEPTORA** observar estritamente a finalidade a que se destinam os dados pessoais a que venha a ter conhecimento
- §4º À **PARTE RECEPTORA** é vedada qualquer forma de compartilhamento de dados pessoais com terceiros fora do âmbito do contrato.
- §5º Ao término do contrato, a **PARTE RECEPTORA** deverá comprovar a cessação de acessos, uso e o descarte definitivo, conforme procedimentos a serem determinados pela **PARTE REVELADORA**
- §6º A **PARTE RECEPTORA** adotará todas as medidas de segurança necessárias para impedir o acesso não autorizado, divulgação, alteração ou destruição não autorizada dos dados pessoais, no que couber.

## Cláusula Sétima - DISPOSIÇÕES GERAIS

- §1º Surgindo divergências quanto a interpretação do acordo pactuado neste instrumento ou quanto a execução das obrigações dele decorrentes ou, se constatados casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade e da economicidade.
- §2º O disposto no presente Termo prevalecerá sempre em caso de dúvida, e salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

## Cláusula Oitava - DISPOSIÇÕES ESPECIAIS

Ao assinar o presente instrumento, a **PARTE RECEPTORA** manifesta sua concordância no sentido de que:

- a) O não exercício, por qualquer uma das Partes, de direitos assegurados neste instrumento não importará em renúncia aos mesmos, sendo considerado como mera tolerância para todos os efeitos de direito;
- b) Todas as condições, termos e obrigações ora constituídas serão regidas pela legislação e regulamentação brasileiras pertinentes;
- c) O presente Termo somente poderá ser alterado mediante termo aditivo firmado pelas partes;
- d) Teve acesso e compromete-se a seguir a Política de Segurança da Informação e Comunicações - POSIC e o Código de Ética e Integridade, disponíveis no Portal da DATAPREV;
- e) Alterações do número, natureza e quantidade das informações disponibilizadas para a **PARTE RECEPTORA** não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste Termo de Sigilo, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;
- f) O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a **PARTE RECEPTORA**, serão incorporados a este Termo, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas; e
- g) Este Termo não deve ser interpretado como criação ou envolvimento das Partes, ou suas afiliadas, nem em obrigação de divulgar informações sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

## Cláusula Nona-VIGÊNCIA

O presente Termo tem natureza irrevogável e irretroatável, permanecendo em vigor desde a data de início das atividades pertinentes ao Contrato Principal, mantendo-se em vigor por prazo indeterminado, a não ser que haja disposição em contrário por escrito, estipulada pela **PARTE REVELADORA** mesmo após o término do Contrato Principal ao qual está vinculado.

, de 2025.

EMPRESA DE TECNOLOGIA DA INFORMAÇÃO  
DA PREVIDÊNCIA - DATAPREV

PARTE RECEPTORA

## ANEXO V – CAPACITAÇÃO TÉCNICA

### 1 CAPACITAÇÃO TÉCNICA

#### 1.1. Planejamento

- 1.1.1. A **CONTRATADA** deverá se reunir com os gestores técnico e administrativo do contrato, gestor do projeto e com o órgão responsável por gestão de

treinamento e desenvolvimento, na cidade do Rio de Janeiro/RJ em local a ser definido pela **DATAPREV** ou remotamente, no prazo máximo de até **5 (cinco) dias úteis**, contados a partir do dia seguinte da solicitação formal da **DATAPREV**. A data da reunião deverá ser agendada em comum acordo entre a **CONTRATADA** e a **DATAPREV**.

I. Nesta reunião, a **CONTRATADA** deverá fazer alinhamento - junto à **Área de Gestão de Treinamento e Desenvolvimento da DATAPREV** dos itens referentes à capacitação técnica, tais como: conteúdo programático; perfil dos participantes; carga horária; cronograma de execução; infraestrutura; definição da plataforma interativa de web conferência ou ambiente virtual de aprendizagem (AVA); material didático; avaliação; e demais informações pertinentes ao processo de capacitação, incluindo plano de trabalho para entrega dos treinamentos à distância, quando aplicáveis (conforme modelo de plano de capacitação anexo a este termo)

**1.1.2. Em até 10 (dez) dias úteis**, após a realização da reunião, a **CONTRATADA** deverá encaminhar, por meio eletrônico, o **Plano de Capacitação**. Este deverá conter, para cada turma a ser executada: modalidade, instrutoria/tutoria, perfil do público-alvo, conteúdo programático, carga horária, cronograma de execução, ambiente virtual de aprendizagem (AVA) ou plataforma interativa de web conferência; e demais informações pertinentes ao processo de capacitação.

**1.1.3.** O cronograma de execução que integra o plano de capacitação deverá conter eventuais atividades predecessoras, como, por exemplo: homologação da solução, instalação, implementação, entrega de material didático e suas etapas de validação. **Ao menos uma das turmas deverá completar sua capacitação antes que a solução seja instalada na Dataprev.**

**1.1.4.** Em até **5 (cinco) dias úteis**, a partir do recebimento formal do **Plano de Capacitação**, a **DATAPREV** deverá se manifestar sobre sua aprovação. Caso seja necessário, será concedido à **CONTRATADA** um novo prazo de até **3 (três) dias úteis** para eventuais ajustes e reapresentação da documentação reprovada. A cada necessidade de ajuste, o prazo para retorno se repetirá para **CONTRATADA**. A versão definitiva do **Plano de Capacitação** será a versão aprovada pela **Área de Treinamento e Desenvolvimento e Gestor Técnico da DATAPREV**.

**1.1.5.** A **Área de Gestão de Treinamento e Desenvolvimento** terá ciência quanto à evolução do cronograma de instalação/implantação da solução ou ferramenta contratada e a qualquer tempo, mudanças nesse cronograma poderão ensejar modificações no Plano de Capacitação inicialmente validado. Nestes casos, a **CONTRATADA** deverá fazer nova reunião de alinhamento junto à **Área de Gestão de Treinamento e Desenvolvimento e com representantes da Área de Negócio da DATAPREV envolvida no projeto de implantação**, sempre que houver modificações no plano ou cronograma do(a) projeto/instalação que modifiquem prazos de homologação, instalação e/ou implementação a fim de repactuar novas datas sem prejuízo para os prazos estabelecidos no capítulo de Capacitação deste TR.

## **1.2. Da Infraestrutura do Treinamento online**

**1.2.1.** A **CONTRATADA** será responsável por providenciar a infraestrutura necessária para o treinamento online ao vivo.

**1.2.2.** Se, no decorrer das capacitações, forem identificados problemas nas versões dos módulos disponibilizadas no ambiente de treinamento, que contrariem os requisitos expressos neste **Termo de Referência** e afetem a qualidade do serviço, a **DATAPREV** poderá exigir a sua mudança ou imediata suspensão da turma devendo ser prontamente atendida pela **CONTRATADA**, sem ônus financeiro.

**1.2.3.** As funcionalidades da solução a serem treinadas deverão ser similares àquelas que estarão no ambiente de produção da **DATAPREV**, incluindo eventuais customizações e parametrizações.

**1.2.4.** Para os cursos oferecidos na modalidade online síncrona, a **CONTRATADA** deverá:

I. Utilizar plataforma de web conferência interativa compatível com a política de segurança da **DATAPREV**, preferencialmente Microsoft Teams ou ZOOM Pro. Qualquer outra plataforma poderá ser aprovada desde que esteja de acordo com as diretrizes de Segurança da Informação da **DATAPREV**;

II. Utilizar ferramentas de interação e colaboração online, de forma síncrona, durante o período do treinamento para atividades práticas e esclarecimentos de dúvidas, tais como chats, fóruns e aplicativos de colaboração;

III. Disponibilizar ferramentas colaborativas adicionais, necessárias para a metodologia de ensino com enfoque prático, respeitadas as políticas de segurança da **DATAPREV**;

IV. Possuir recursos para apuração de frequência online diária dos participantes;

V. Disponibilizar material didático e de apoio para download;

VI. Suportar e corrigir possíveis problemas técnicos, em termos de infraestrutura tecnológica, durante a realização do curso, garantindo a transmissão ininterrupta de aulas ao vivo;

VII. Dispor de canal de comunicação com os participantes para atender-lhes em suas solicitações no prazo de até 48 (*quarenta e oito*) horas;

VIII. Encaminhar todos os dados sobre o acesso ao curso, incluindo URL para as aulas ao vivo e laboratórios na plataforma para área de Gestão de Treinamento e Desenvolvimento ([digt@dataprev.gov.br](mailto:digt@dataprev.gov.br)) da **DATAPREV** com a antecedência de **10 (dez) dias corridos** da data de início do curso;

IX. Dispor de meios para efetuar a gravação das sessões online ao vivo e disponibilizá-las para a **CONTRATANTE** ao longo do período de vigência contratual.

## **1.3. Instrutoria**

**1.3.1.** A **CONTRATADA** deverá apresentar para Área de Gestão de Treinamento e Desenvolvimento da **DATAPREV** documentos com os dados e credenciais do instrutor, demonstrando possuir as qualificações e expertise necessárias para bem capacitar os usuários no manuseio da solução.

**1.3.2.** A entrega da documentação que comprova o atendimento da exigência do **subitem 1.3.1** deverá ser realizada com antecedência de até **15 (quinze) dias úteis** do início da realização da respectiva capacitação. A capacitação técnica só será realizada após a **CONTRATADA** apresentar a devida comprovação.

**1.3.3.** É vedada a alteração de instrutor sem prévia comunicação e concordância da **DATAPREV**, estando um eventual substituto sujeito ao mesmo processo de verificação descrito anteriormente.

**1.3.4.** A capacitação técnica deverá ser ministrada em língua portuguesa **obrigatoriamente**.

#### 1.4. Disciplinas e Composição das Turmas

**1.4.1 O total de 20 participantes deverá ser dividido em, no mínimo, duas turmas, fechadas para a Dataprev e ministradas em formato online síncrono** (aulas à distância e 'ao vivo'), realizadas de acordo com o cronograma de implementação da solução e conforme acordado no **Plano de Capacitação**.

DISCIPLINAS	CARGA HORÁRIA (por turma)	TOTAL DE TREINANDOS
Instalação, Configuração e Gerenciamento da solução	40 horas	20
Segurança de Redes	52 horas	

**1.4.2.** Será admitido treinamento com carga horária inferior, exclusivamente na hipótese de a **CONTRATADA** ofertar treinamento oficial do fabricante da solução, e desde que a ementa seja aprovada pela **DATAPREV**.

**1.4.3.** Fica a **CONTRATADA** ciente de que, a depender da ementa e das necessidades de conhecimento do público participante, poderá haver carga-horária adicional em até 20% da CH mínima.

**1.4.4.** A **CONTRATADA** deverá estar apta a iniciar a capacitação em até 30 (trinta) dias corridos após validação do Plano de Capacitação. Esse prazo não poderá ser excedido, podendo ser prorrogado a critério da **DATAPREV** em acordo com a **CONTRATADA**.

**1.4.5.** Os treinamentos ministrados com aulas ao vivo devem ser conduzidos por **sessões síncronas de até 04 (quatro) horas de duração por dia**, devendo o cronograma de aulas ser objeto de validação e parte integrante do **Plano de Capacitação**.

**1.4.6.** Os treinamentos ministrados com aulas ao vivo devem prever, necessariamente, a disponibilização de recursos de interação e colaboração adicionais necessários para a metodologia de ensino com enfoque prático, tendo em vista o esclarecimento de dúvidas, realização de atividades práticas via AVA/máquinas/laboratórios virtuais, dentre outras. Tais atividades complementares podem acontecer de forma síncrona ou não.

**1.4.7.** A capacitação técnica deverá abordar todos os componentes da solução fornecida, devendo ainda estar de acordo com a utilização da solução instalada no ambiente da **DATAPREV**, incluindo eventuais parametrizações e customizações. A ementa básica ministrada deverá conter, pelo menos, os seguintes tópicos:

##### **1.4.7.1 Introdução, instalação e configuração, gerenciamento e solução de problemas** (Duração estimada: 40 horas):

a) **Introdução:** Funcionamento da solução, conceitos e características das funcionalidades do produto, *design*, arquitetura da solução e seus modos de funcionamento.

b) **Instalação e configuração:** Instalação; configuração das interfaces de rede; implementação de *updates*; atualização de licenças do produto; configuração dos diversos modos de operação, configuração de alta disponibilidade e da gerência da solução; operações de certificados; configuração de políticas de firewall, NAT, roteamento estático, roteamento dinâmico, roteamento de pacotes baseadas em políticas para implantações multicaminhos e com balanceamento de carga, SSL VPN e VPN IPSEC.

c) **Gerenciamento:** Monitoramento de eventos; configuração e utilização da gerência centralizada do produto; geração de relatórios; agendamento de relatórios; configuração de envio automático de relatórios; configuração de eventos geradores de *logs*; preservação dos *logs*; exportação de *logs* para *syslog*; rastreamento de eventos identificando a origem e destino; desligamento programado; *backup/restore* de todas as configurações e das funcionalidades de gerência; configuração do uso de NTP; configuração para horário de verão; configuração da autenticação de usuários no servidor de gerência via conta local, LDAP e Microsoft Active Directory; criação de contas com permissões distintas de usuários de gerência; criação de filtros para customizar alertas; operação da solução; configuração de regras e políticas de segurança e configuração dos modos de operação; uso de GUI e CLI para administração.

d) **Solução de problemas:** Verificação de indisponibilidade da solução; monitoração de tráfego nas interfaces; monitoramento (*sniffing/tcpdump*); utilização de ferramentas para depuração e gerenciamento em primeiro nível, tais como *debug*, *traceroute*, *ping* e *log* de eventos, verificação de problemas na operação da solução e recuperação da configuração da solução utilizando técnicas de *disaster recovery*; inspeção de tráfego protegido por SSL/TLS.

##### **1.4.7.2 Segurança de Redes** (Duração estimada: 52 horas, sendo 10 horas dedicadas a práticas)

###### **1. Análise Forense de Redes (4 horas)**

- 1.1. Embasamento Legal
- 1.2. Evidências Voláteis
- 1.3. Leitura dos pacotes
- 1.4. Ferramenta TCPdump
- 1.5. Ferramenta Wireshark
- 1.6. Ferramentas auxiliares
- 1.7. Engenharia reversa
- 1.8. Atividade prática (1 hora)

###### **2. Detalhamento dos tipos de ameaças/vulnerabilidades (8 horas)**

- 2.1. Vírus
- 2.2. Worm
- 2.3. Cavalo de Troia
- 2.4. Trojans
- 2.5. Ransomware
- 2.6. Ataques DoS/DDoS (quantidade e formato)
- 2.7. Spam
- 2.8. Phishing
- 2.9. Vishing
- 2.10. Pharming
- 2.11. Whaling
- 2.12. Rootkit
- 2.13. Injeção de código (SQL, XML, DLL e LDAP)
- 2.14. Violação de dados



- 2.15. APIs inseguras
- 2.16. Credenciais comprometidas
- 2.17. Bombas lógicas
- 2.18. Ataques de camada 2
- 2.19. Ataques de DNS
- 2.20. Ataques de dia zero
- 2.21. OWASP Top 10:2025
- 2.22. Bugs de software
- 2.23. Senhas fracas
- 2.24. Senhas codificadas
- 2.25. Cifras de criptografia ausentes
- 2.26. Estouro de buffer
- 2.27. Travessia de caminho
- 2.28. Cross-Site Scripting – CSS
- 2.29. Cross-Site Request Forgery – CSRF
- 2.30. Time of Check (TOC) ou Time of Use (TOU)
- 2.31. Atividade prática (2 horas)

### **3. Análise Forense de Malware (6 horas)**

- 3.1. Exame das Propriedades Estáticas de um Malware
- 3.2. Análise Comportamental
- 3.3. Análise de Código
- 3.4. Processo de Patching de Código
- 3.5. Unpacking Malware
- 3.6. Análise de Código Ofuscado
- 3.7. Engenharia Reversa
  - 3.7.1. Compilers, Linkers e Loaders
  - 3.7.2. Assembly
  - 3.7.3. Registradores
  - 3.7.4. Instruções
  - 3.7.5. Fluxo de Controle
  - 3.7.6. Disassembly
  - 3.7.7. Anti-Engenharia Reversa
- 3.8. Estudos práticos de casos
  - 3.8.1. API Hooking
  - 3.8.2. Keyloggers
  - 3.8.3. Sniffers
  - 3.8.4. Spoofers
  - 3.8.5. Downloaders
  - 3.8.6. Comando & Controle via HTTP
  - 3.8.7. Forense de Memória
- 3.9. Atividade prática (2 horas)

### **4. Criptografia (3 horas)**

- 4.1. Hash
- 4.2. PKI
- 4.3. SSL
- 4.4. IPsec
- 4.5. NAT-T IPv4 para IPsec
- 4.6. Chave pré-compartilhada
- 4.7. Autorização baseada em certificado

### **5. E-mail seguro (2 horas)**

- 5.1. Chaves de domínio e assinatura DKIM
- 5.2. SPF e SIDF
- 5.3. DMARC
- 5.4. S/MIME

### **6. Tipos e componentes de VPN (3 horas)**

- 6.1. Interfaces de túnel virtual
- 6.2. IPsec baseado em padrões
- 6.3. DMVPN
- 6.4. GETVPN
- 6.5. FlexVPN
- 6.6. VPN site a site
- 6.7. VPN de acesso remoto
- 6.8. Atividade prática (2 horas)

### **7. Segurança de Rede (5 horas)**

- 7.1. Comparação de soluções de segurança de rede com prevenção de intrusão e de firewall
- 7.2. Tipos de firewalls (stateless, stateful, NGFW, WAF e WAAP)
- 7.3. Componentes, recursos e benefícios dos registros NetFlow e Flexible NetFlow
- 7.4. Segmentação de rede usando VLANs
- 7.5. Camada 2 e segurança de porta
- 7.6. DHCP snooping
- 7.7. Inspeção ARP dinâmica
- 7.8. Storm control
- 7.9. PVLANS para segregar tráfego de rede
- 7.10. Defesas contra ataques MAC, ARP, salto de VLAN, STP e DHCP
- 7.11. Configuração de controle de acesso por TACACS+ e RADIUS

### **8. Gerenciamento de Rede (4 horas)**

- 8.1. SNMPv3

- 8.2. NetConf
- 8.3. RestConf
- 8.4. Syslog seguro
- 8.5. NTP com autenticação

#### 9. Segurança de Conteúdo (2 horas)

- 9.1. Métodos de redirecionamento e captura de tráfego para web proxy
- 9.2. Recursos de segurança de e-mail, como filtragem de SPAM, filtragem antimalware, DLP, lista de bloqueio e criptografia de e-mail

#### 10. Acesso Seguro (4 horas)

- 10.1. Mecanismos de controle de acesso à rede: 802.1X, MAB e WebAuth
- 10.2. Acesso à rede com CoA (Change of Authorization))
- 10.3. Tunelamento DNS
- 10.4. HTTPS
- 10.5. SSH
- 10.6. SFTP
- 10.7. SCP
- 10.8. NTP

#### 11. Métodos de diagnóstico e solução de problemas (5 horas)

- 11.1. Caça a ameaças ao ambiente de uma organização utilizando a Pirâmide da Dor
- 11.2. MITRE ATT&CK
- 11.3. MITRE CAPEC
- 11.4. NIST Cybersecurity Framework (NIST CSF)
- 11.5. TaHiTI (Threat Intelligence and Directed Hunting)
- 11.6. Método de Análise e Solução de Problemas (MASP)/PASTA
- 11.7. Atividade prática (2 horas)

#### 12. Processo e documentação (6 horas)

- 12.1. Componentes necessários para um relatório de análise de causa raiz
- 12.2. Processo de execução de análise forense de dispositivos de rede (táticas, técnicas e procedimentos)
- 12.3. Processo de Solução de Problemas em Sete Etapas
- 12.4. Solução de problemas com modelos de camadas
- 12.5. Métodos Estruturados de Solução de Problemas
- 12.6. Regras YARA para identificação, classificação e documentação de malware
- 12.7. Atividade prática (1 hora)

1.4.8. As turmas de capacitação deverão ser realizadas durante a vigência contratual, conforme estabelecido no cronograma de execução aprovado pela **DATAPREV** na versão definitiva do **Plano de Capacitação**. Este cronograma poderá sofrer alterações, desde que essas sejam devidamente justificadas e realizadas em comum acordo entre a **CONTRATADA** e a **DATAPREV**.

1.4.9. Em projetos de implantação de tecnologias, as turmas de capacitação somente serão executadas após concluído o aceite da ferramenta e suas funcionalidades que serão objeto do treinamento, exceto nos casos previstos no **subitem 1.4.10**. Na hipótese de haver funcionalidades com pendências, a critério da **DATAPREV** a **CONTRATADA** deverá obrigatoriamente adicionar, ao plano de capacitação, turmas extras a serem executadas antes da entrada em produção da solução, com objetivo de complementar/sanar o gap de conhecimento das funcionalidades não treinadas.

1.4.10. A necessidade de qualificação da equipe que estará diretamente envolvida na gestão do projeto de implantação deverá ser sinalizada na reunião de alinhamento sobre o Plano de Capacitação, e nestes casos, o treinamento ocorrerá conforme cronograma que melhor atenda ao projeto, podendo inclusive ter uma ou mais turmas antes da instalação. Para tanto, a **CONTRATADA** deverá assegurar ambiente de treinamento para capacitação capaz de refletir todo o conteúdo da ementa aprovada pela **DATAPREV**. As funcionalidades a serem treinadas deverão ser similares às disponíveis no ambiente de produção.

1.4.11. As turmas deverão ser realizadas no horário compreendido entre 09h às 18h, de segunda a sexta-feira, sempre em turno parcial de 04 (quatro) horas de duração.

1.4.12. Conforme prática de mercado, as horas de intervalo para almoço dos treinandos não deverão ser computadas para fins de cálculo da carga horária.

#### 1.5. Material Didático

1.5.1. A **CONTRATADA** deverá fornecer o material didático de acompanhamento detalhado, original do desenvolvedor da ferramenta, quando cabível, **em português (Brasil)**, contendo todos os assuntos abordados na capacitação. Entende-se como material didático, apostilas, manuais, livros texto, dentre outros de semelhante natureza, destinados a facilitar ou complementar o aprendizado. Na ausência de publicação em **português (Brasil)**, será aceito apenas material em **inglês**, desde que acompanhado de versão sintética em português contendo as principais funcionalidades.

1.5.2. As apostilas ou manuais, deverão ser oferecidas em formato eletrônico, a critério da **DATAPREV**, com conteúdo oficial do fabricante e atualizado, de acordo com a versão da solução a ser ministrada.

1.5.3. Após a conclusão da capacitação, mediante solicitação formal da **DATAPREV**, a **CONTRATADA** deverá fornecer cópia da apresentação em formatos padrão de mercado (PDF, DOC, DOCX, PPT ou HTML).

1.5.4. A **CONTRATADA** deverá disponibilizar as videoaulas gravadas em ambiente AVA/LMS, ou plataforma de videoconferência pela internet, pelo tempo que durar a turma, salvo se comprovadamente impedida por fabricante em treinamentos oficiais.

1.5.5. Para os treinamentos online, a **CONTRATADA** deverá disponibilizar ao órgão responsável por gestão de treinamento e desenvolvimento, login de acesso temporário ao ambiente virtual de aprendizado (AVA), LMS ou plataforma de web conferência, anteriormente à liberação de acesso aos participantes, tendo em vista a realização de teste de desempenho e funcionalidades; validação técnica e pedagógica do material e conteúdo programático.

1.5.6. A **CONTRATADA** deverá disponibilizar à **DATAPREV** uma cópia do material didático e acesso ao ambiente virtual de aprendizagem (AVA) em

até **10 (dez) dias úteis** antes do início da capacitação para fins de validação técnica e pedagógica. Os prazos de validação por parte da **DATAPREV** não poderão ser inferiores a **05 (cinco) dias úteis**. As etapas de correções ou adequações na versão entregue deverão ser previstas e negociadas em comum acordo, devendo constar no cronograma do **Plano de Capacitação**. A cada necessidade de ajuste, o prazo para retorno da **CONTRATADA** não poderá exceder **05 (cinco) dias úteis**.

**1.5.7.** A validação técnica e pedagógica estará dispensada caso o material didático seja de treinamento oficial do fabricante da solução ou ferramenta contratada.

## 1.6. AVALIAÇÃO DA CAPACITAÇÃO ONLINE

**1.6.1.** Para os treinamentos online, seis fatores serão objetos de avaliação pelo formulário: Programa e Metodologia, Instrutoria, Material, Estrutura do Curso, Ambiente e Autoavaliação.

**1.6.2.** Cada fator é composto por um conjunto de itens que deverão ser avaliados por meio de notas atribuídas em uma escala de 1 (um) a 10 (dez), sendo 1 totalmente insatisfeito e 10 totalmente satisfeito. Para fins de avaliação geral da turma, será considerada a média obtida nos fatores que compõem a avaliação de reação, com exceção do fator Autoavaliação.

<b>Programa e Metodologia</b>	Avalia a percepção dos participantes em relação a importância do tema e se os objetivos do curso foram alcançados.
<b>Instrutoria</b>	Avalia a satisfação dos participantes com relação a atuação do instrutor durante a capacitação, tanto em relação ao seu conhecimento técnico do tema, quanto à sua habilidade didático-pedagógica e de interação com a turma.
<b>Material</b>	Avalia a satisfação dos participantes quanto ao material didático disponibilizado, a sua qualidade, clareza e organização;
<b>Estrutura do Curso</b>	Avalia a percepção dos participantes quanto a organização do curso, sequência do conteúdo apresentado e a carga horária;
<b>Ambiente</b>	Avalia a percepção de qualidade das interfaces gráficas e de adequação do ambiente tecnológico disponibilizado para o treinamento online, a disponibilidade e efetividade dos recursos de interação, colaboração e comunicação.
<b>Autoavaliação</b>	Avalia a percepção dos participantes quanto à aquisição de novos conhecimentos e habilidades por meio da capacitação oferecida, bem como, a segurança para a sua aplicação e relevância do conteúdo abordado.

**1.6.3.** Com base nas informações registradas pelos participantes no Formulário de Avaliação da **DATAPREV**, a **Área de Gestão de Treinamento e Desenvolvimento** deverá emitir o Relatório Consolidado da Avaliação de Reação.

**1.6.4.** O formulário de Avaliação de Reação, composto pelos seis fatores mencionados, com os itens e escala de classificação serão apresentados **pela área de Gestão de Treinamento e Desenvolvimento da DATAPREV** na reunião de alinhamento de capacitação, prevista no **subitem 1.1.1** para ciência e validação da **CONTRATADA**. Caso a **CONTRATADA**, para fins próprios, tenha a necessidade de mensurar outros fatores não previstos na avaliação padrão da **DATAPREV**, ela poderá utilizar o seu próprio formulário, porém este não será utilizado para aprovação da capacitação por parte da **DATAPREV**.

## 1.7. GARANTIA DA CAPACITAÇÃO

**1.7.1.** O resultado da capacitação será considerado **INSATISFATÓRIO** quando pelo menos uma das situações abaixo ocorrer:

- Média final da turma inferior a 7 (sete), excluindo-se o fator **Autoavaliação**.
- Média do fator **Ambiente** inferior a 7 (sete).
- Média do fator **Instrutoria** inferior a 7 (sete).
- Média de, pelo menos, dois fatores inferiores a 7 (sete), excluindo-se o fator **Autoavaliação**.

**1.7.2.** A **CONTRATADA** será obrigada a realizar, sem ônus para a **DATAPREV**, nova capacitação para todas as turmas em que ficar configurado resultado **INSATISFATÓRIO**, salvo se, por decisão do **Gestor Técnico do Contrato** e da **Área de Gestão de Treinamento e Desenvolvimento**

da **DATAPREV**, for adotada medida complementar que venha sanar o problema.

- 1.7.3. Em caso de nova capacitação, esta deverá acontecer segundo um novo calendário a ser definido pela **DATAPREV**, sendo automaticamente suspenso o calendário inicialmente planejado para as próximas turmas, caso haja, até que seja sanado o problema.

## 1.8. ENTREGA DOS MATERIAIS UTILIZADOS NA CAPACITAÇÃO

- 1.8.1. Após a conclusão da capacitação, mediante solicitação formal da **DATAPREV**, a **CONTRATADA** deverá fornecer cópia da apresentação utilizada em mídia eletrônica (CD, DVD ou PENDRIVE), em formatos padrão de mercado (PDF, DOC, PPT ou HTML).
- 1.8.2. A **DATAPREV** se reserva o direito de reproduzir trechos do material didático utilizado na capacitação, desde que registradas as devidas fontes, para realizar capacitações internas de seus empregados.

## 1.9. CERTIFICADOS E LISTA DE PRESENÇA

- 1.9.1. A **CONTRATADA** deverá disponibilizar, apenas para os participantes que obtiverem a frequência mínima de 75% (setenta e cinco por cento), os certificados de conclusão de curso, em meio eletrônico, ao final de cada turma.
- 1.9.2. A **CONTRATADA** deverá enviar **documento que comprove a frequência diária online e o(s) certificado(s)** digitais do(s) participante(s) que cumprirem, no mínimo, **75%** da carga horária programada.
- 1.9.2. A **CONTRATADA** deverá encaminhar à **DATAPREV** no prazo de até **05 (cinco) dias úteis** após solicitação, que pode ocorrer a qualquer momento, relatório que demonstre o nível de evolução e conclusão de atividades dos participantes.
- 1.9.3. Para fins de comprovação dos serviços prestados, visando o faturamento, a **CONTRATADA** deverá encaminhar para Área de Gestão de Treinamento e Desenvolvimento da **DATAPREV**, após o encerramento de cada turma, o documento de presença digitalizado, em **até 2 (dois) dias úteis**, e os certificados, em **até 5 (cinco) dias úteis**, a contar da data de encerramento de cada turma.

## 1.10. OBRIGAÇÕES DA CONTRATADA

- 1.10.1. Em relação à prestação dos serviços de capacitação, a **CONTRATADA** deverá:

- Arcar com eventuais despesas de deslocamento, hospedagem e alimentação dos instrutores;
- Disponibilizar ao órgão responsável pela gestão de treinamento e desenvolvimento, anteriormente à liberação de acesso aos participantes, login de acesso temporário ao ambiente virtual de aprendizado (AVA), tendo em vista a realização de teste de desempenho e funcionalidades; validação técnica e pedagógica do material e conteúdo programático.
- Efetuar o cadastro, ativação e disponibilização de acesso dos participantes da DATAPREV ao Ambiente Virtual de Aprendizagem (AVA) pelo tempo e nas condições acordadas no **Plano de Capacitação ou pelo tempo de vigência do contrato**.
- Apurar a frequência diária online dos participantes.
- Providenciar a imediata correção das deficiências e/ou irregularidades que porventura venham a ser apontadas pela **CONTRATANTE**.
- Comparecer a reuniões de alinhamento sobre a capacitação nas dependências da **DATAPREV** ou remotamente, sempre que solicitada, tendo em vista a definição de procedimentos relativos à adequada entrega do serviço;
- Entregar documentação que comprove o atendimento da exigência do **subitem 1.3.1** deverá ser realizada com antecedência de até **15 (quinze) dias úteis** do início da realização da respectiva capacitação.
- Ministrar, na totalidade, o conteúdo programático contratado das capacitações;
- Emitir o certificado de conclusão dos cursos online em nome de cada participante que apresentar o percentual mínimo requerido de presença, e nota de avaliação final, quando for aplicável.;
- Encaminhar à **DATAPREV** os documentos comprobatórios de realização de cada turma (Lista de Presença e Certificados);
- Refazer as turmas que não forem bem avaliadas, de acordo com os critérios "**DA GARANTIA DA CAPACITAÇÃO**", em novo período a ser acordado com a **DATAPREV**.
- Realizar nova transmissão de reposição de aula, em data acordada com a DATAPREV, sempre que ocorrerem falhas técnicas na plataforma de transmissão que ocasionem prejuízo na entrega de conteúdo programático e no aprendizado. Neste caso, a ordem original de apresentação do conteúdo não deve ser alterada.

- 1.10.2. Em relação ao tratamento dos dados pessoais em treinamentos online síncronos ou assíncronos:

- A coleta de dados dos empregados se dará em observância aos termos da LGPD, estando as partes cientes de que a **DATAPREV** é controladora dos dados dos seus empregados, os quais devem ser utilizados estritamente para a finalidade do objeto contratual.
- É vedada a **CONTRATADA** o compartilhamento dos dados dos empregados da **DATAPREV** com terceiros ou empresas subcontratadas sem o prévio consentimento da **CONTRATANTE** a quem compete assegurar o consentimento ou esclarecimento quanto ao tratamento dos dados perante seus empregados.
- Fica ciente a **CONTRATADA** que o tratamento dos dados pessoais a que tiver acesso deve ocorrer em conformidade com a LGPD e nível de segurança adequados à classificação das informações que serão tratadas durante a execução do contrato.
- A **CONTRATADA** se compromete a utilizar os dados pessoais exclusivamente para a finalidade de inscrição, acompanhamento de progresso e certificação, quando aplicáveis. Nos casos em que o dado pessoal for um requisito para inscrição ou cadastro em ambientes virtuais de aprendizagem externos, a **CONTRATADA** fica obrigada a assinar Termo de Sigilo e Privacidade.
- É obrigação da **CONTRATADA** evidenciar para a **CONTRATANTE** o descarte seguro dos dados pessoais a que tiver acesso após a finalização do serviço objeto deste Termo de Referência.

## 1.11. OBRIGAÇÕES DA CONTRATANTE

- 1.11.1. Em relação à prestação dos serviços de capacitação, a **DATAPREV** deverá:

- Comunicar a **CONTRATADA**, no prazo **máximo de 5 (cinco) dias úteis** antes do início de cada capacitação, a relação de treinandos, para que sejam iniciados todos os preparativos necessários a adequada prestação do serviço, ressalvados os casos fortuitos e de força maior;
- Informar data, local e conteúdo, bem como informações para acesso ao curso online aos participantes envolvidos;
- Fiscalizar e acompanhar a prestação do serviço/objeto contratual, comunicando a **CONTRATADA** toda e qualquer deficiência e/ou irregularidade relacionada com a entrega do objeto, diligenciando nos casos que exigirem providências corretivas;
- Aferir a qualidade da capacitação por meio do **Formulário de Avaliação de Reação** e emitir o **Relatório Consolidado da Avaliação de Reação**, ao

final de cada turma.

## 2 TABELA DE PRAZOS

Ação	Responsável	Prazo Máximo	Referência para o Prazo
<b>ABERTURA</b>			
Solicitação Formal da reunião	DATAPREV	Quando necessário	Após a Assinatura do Contrato
Reunião de alinhamento da Capacitação	DATAPREV CONTRATADA	5 (cinco) dias úteis	Após a solicitação Formal da Dataprev
Início da primeira turma de treinamento	CONTRATADA	45 (quarenta e cinco) dias corridos	Após validação do Plano de Capacitação
<b>PLANO DE CAPACITAÇÃO</b>			
Envio do Plano de Capacitação	CONTRATADA	10 (dez) dias úteis	Reunião de alinhamento da Capacitação
Aprovação do Plano de Capacitação	DATAPREV	05 (cinco) dias úteis	Recebimento do Plano de Capacitação
Implementação de ajustes no Plano de Capacitação (se necessário)	CONTRATADA	03 (três) dias úteis	Retorno sobre Aprovação/Desaprovação do Plano de Capacitação
Aprovação da Versão Definitiva do Plano de Capacitação	DATAPREV	05 (cinco) dias úteis	Recebimento de versão ajustada do Plano de Capacitação
<b>ACESSO AO CURSO</b>			
Envio da Relação de Treinandos	DATAPREV	05 (cinco) dias úteis	Antes da Data acordada para a Capacitação
Envio de todos os dados de acesso ao curso	CONTRATADA	10 (dez) dias corridos	Dias que antecedem a data da capacitação
<b>TEMPO DE ATENDIMENTO (CANAIS)</b>			
Atendimento a Canal de solicitação dos empregados participantes dos cursos	CONTRATADA	48 (quarenta e oito) horas úteis	Do registro da Solicitação
<b>INSTRUTORIA</b>			
Envio dos dados do Instrutor	CONTRATADA	15 (quinze) dias úteis	Antes da Data acordada para a Capacitação
<b>MATERIAL DIDÁTICO</b>			
Disponibilização do Material Didático	CONTRATADA	10 (dez) dias úteis	Antes da Data acordada para a Capacitação
Validação do Material Didático	DATAPREV	05 (cinco) dias úteis	Após o recebimento do Material Didático
Disponibilização do Material Didático ajustado	CONTRATADA	05 (cinco) dias úteis	Após validação da Dataprev
<b>RELATÓRIO DE ACOMPANHAMENTO DOS ALUNOS</b>			
Envio de relatório que demonstre o nível de evolução	CONTRATADA	05 (cinco) dias úteis	Após a solicitação formal da Dataprev
<b>NOVA CAPACITAÇÃO</b>			
Realização de Nova Capacitação (Se resultado insatisfatório)	CONTRATADA	A definir	Segundo um novo calendário a ser definido pela DATAPREV
<b>DOCUMENTOS APÓS CAPACITAÇÃO</b>			
Envio de Documento de Presença Digitalizado	CONTRATADA	02 (dois) dias úteis	Após data de encerramento de cada turma
Envio de Certificado de Conclusão de Curso	CONTRATADA	05 (cinco) dias úteis	Após data de encerramento de cada turma

## 3 AVALIAÇÃO DE REAÇÃO

### Treinamento Online ao Vivo (síncrono)

#### PROGRAMA E METODOLOGIA

*O significado e a importância do tema do curso foram compreendidos e abordados adequadamente*

*Os tempos destinados à apresentação e exploração dos conteúdos de cada tópico foram suficientes*

*De uma maneira geral os objetivos do curso foram alcançados*

#### INSTRUTORIA

*O instrutor apresentou o tema de forma objetiva, organizada, segura e fluente*

*O instrutor esclareceu adequadamente as questões e dúvidas dos participantes*

#### AMBIENTE

*As aulas ao vivo, foram transmitidas com qualidade de áudio e vídeo*

*A interação online com o instrutor ocorreu de forma satisfatória*

*Foi possível interagir com os demais participantes durante o curso*

*Os recursos utilizados permitiram a execução adequada de atividades práticas ou colaborativas*

#### MATERIAL

*A qualidade do material disponibilizado respondeu às necessidades apoiando o meu aprendizado*

*O material didático era claro e adequado*

*Os exercícios de fixação/ avaliação se relacionaram adequadamente com o conteúdo apresentado*

#### ESTRUTURA DO CURSO

*A forma de apresentação foi adequada ao conteúdo*

*A carga horária diária sugerida para o curso foi adequada ao volume e a complexidade do conteúdo*

*A metodologia permitiu interação e/ou colaboração online entre participantes*

#### AUTOAVALIAÇÃO

*Realização das atividades propostas*

*Aumento do conhecimento sobre o assunto*

*Os conhecimentos adquiridos ou atualizados foram suficientes para cumprir os objetivos propostos*

*Possibilidade de aplicação do conhecimento no cotidiano de trabalho*

*Respostas às minhas expectativas*

# PLANO DE CAPACITAÇÃO

## <Assunto>

<Empresa/instituição responsável>

### Registro de Revisões

Versão	Data	Notas de Revisão	Responsável

\* A cada nova turma a ser aplicada, a contratada deve submeter nova versão do Plano de Capacitação, adicionando as novas informações.

## Sumário

### 1. Capacitação

- 1.1.1 Informações Gerais
- 1.1.2 Disciplina 1
- 1.1.3 Objetivo/Resultados Esperados
- 1.1.4 Instrutoria / Tutoria
- 1.1.5 Modalidade:
- 1.1.6 Público Alvo
- 1.1.7 Pré-requisitos
- 1.1.8 Conteúdo Programático

### 2. Disciplina 2

- 1.1.9 Objetivo
- 1.1.10 Instrutoria / Tutoria
- 1.1.11 Modalidade:
- 1.1.12 Público Alvo
- 1.1.13 Pré-requisitos
- 1.1.14 Conteúdo Programático

.....

### 3. Disciplina N

- 1.1.15 Objetivo
- 1.1.16 Instrutoria / Tutoria
- 1.1.17 Modalidade:
- 1.1.18 Público Alvo
- 1.1.19 Pré-requisitos
- 1.1.20 Conteúdo Programático

### 4. Local de Realização

### 5. Requisitos Tecnológicos

### 6. Cronograma de Execução

### 7. Considerações Finais

## 1- Capacitação

### 1.1 Informações gerais

<Informar as disciplinas de capacitação, a quantidade de turmas, quantidade de treinandos, carga horária. Apresentar quadro geral com as informações>

Disciplina	Carga horária	Instrutor	Período de Realização
<nome>			

### 1.2 Disciplina 1

#### 1.2.1 Objetivo/ Resultados Esperados

<Informar o objetivo da capacitação para cada uma das disciplinas do curso>

#### 1.2.2 Instrutoria / Tutoria

< Informar o nome do(s) instrutor(es), apresentar mini curriculum>

#### 1.2.3 Público Alvo

< Informar qual o perfil de profissional adequado para realizar o curso>

#### 1.2.4 Pré-requisitos :

<Informar os pré-requisitos para o curso detalhando quais são necessários e aqueles que são apenas desejáveis>

#### 1.2.5 Plano de Aula e Conteúdo Programático

<Aqui deverá ser detalhado o conteúdo programático por dia de curso.

Dia 1

Horário	Tópico Geral	Detalhamento
	BREAK	
	ALMOÇO	
	BREAK	

Dia 2

Horário	Tópico Geral	Detalhamento
	BREAK	
	ALMOÇO	
	BREAK	

## 2- Local de Realização dos Treinamentos

< Informar o local físico da capacitação quando presencial, informando o endereço completo do local do curso. Para capacitações em EAD, neste tópico deverá constar informações sobre acesso ao ambiente virtual de aprendizagem (AVA) ou plataforma interativa de web conferência>

## 3- Requisitos Tecnológicos

<Os requisitos tecnológicos necessários para o pleno funcionamento da infraestrutura de cada disciplina da capacitação como, por exemplo, a capacidade das máquinas, memória RAM, softwares adicionais que precisam estar instalados.>

## 4- Cronograma de Execução

<Aqui deverá ser apresentado o cronograma detalhado do(s) curso(s), conforme prazos estabelecidos no Termo de Referência, devendo ser elencadas atividades relacionadas a preparação e entrega do material didático, preparação da infraestrutura física e computacional do curso, instrutoria e demais informações pertinentes. >

TURMA/ DISCIPLINA < INFORMAR NOME>	DATA
ENTREGA DO MATERIAL DIDÁTICO PARA VALIDAÇÃO	
VALIDAÇÃO DO MATERIAL	
ENTREGA DA DOCUMENTAÇÃO DO INSTRUTOR	
CONFIRMAÇÃO DO LOCAL DE REALIZAÇÃO	
REALIZAÇÃO DA AULA TESTE (QUANDO APLICÁVEL)	
AJUSTES NO MATERIAL PÓS-VALIDAÇÃO	
ENTREGA DO MATERIAL VALIDADO	
EXECUÇÃO DA TURMA	
ENTREGA DO RELATÓRIO DE FREQUÊNCIA	
DISPONIBILIZAÇÃO DOS CERTIFICADOS	

TURMA/ DISCIPLINA < INFORMAR NOME>	DATA
ENTREGA DO MATERIAL DIDÁTICO PARA VALIDAÇÃO	
VALIDAÇÃO DO MATERIAL	
ENTREGA DA DOCUMENTAÇÃO DO INSTRUTOR	
CONFIRMAÇÃO DO LOCAL DE REALIZAÇÃO	
REALIZAÇÃO DA AULA TESTE (QUANDO APLICÁVEL)	
AJUSTES NO MATERIAL PÓS-VALIDAÇÃO	
ENTREGA DO MATERIAL VALIDADO	
EXECUÇÃO DA TURMA	
ENTREGA DO RELATÓRIO DE FREQUÊNCIA	
DISPONIBILIZAÇÃO DOS CERTIFICADOS	

## 5- Cronograma do Projeto/Implantação/Instalação

<Anexar macro cronograma acordado com a Dataprev ou destacar marcos relacionados à testes, homologação, aceite, instalação/entrada em produção.>

## 6- Considerações Finais

<Incluir informações relacionadas a itens que precisam de maior detalhamento ou informações específicas da capacitação que não foram contempladas em outros itens....>

Empresa/instituição responsável	
< cargo>	< assinatura>
< cargo>	< assinatura>
Dataprev	
<cargo e função>	<assinatura>
<cargo e função>	<assinatura>

ANEXO VI – MODELO DE CADERNO DE TESTE

Introdução

1.1. Propósito

1.2. Definições, Acrônimos e Abreviações

Sigla	Significado

1.3. Referências

Como referências estão sendo utilizados os seguintes documentos, além das informações definidas nas reuniões de após o Kick-off:

Documento	Descrição

2. Plano de Testes

2.1. Responsáveis pelas equipes



Responsável	Empresa

## 2.2. Ambiente

### 2.2.1. Produção

Hostname	Sistema Operacional	Aplicação

### 2.2.2. Homologação

Hostname	Sistema Operacional	Aplicação

## 3. Plano de Testes

### 3.1. Testes administrativos e operacionais

#### 3.1.1. Acessar o ambiente como Administrator

#### 3.1.2.

## 4. Aceitação

Um Caso de Teste é considerado aceito quando todos os seus passos e pontos de verificação (PV) são cumpridos conforme previstos.

Assinatura do profissional do CONTRATANTE:

---

**\* Este documento se torna válido a partir da assinatura de todos os signatários indicados. Estando automaticamente invalidadas assinaturas posteriores realizadas por usuários não indicados.**



Documento assinado eletronicamente por **Felipe Queto de Souza Pinto, Gerente, Substituto(a)**, em 03/12/2025, às 17:03, conforme horário oficial de Brasília, com fundamento no [Decreto nº 8.539, de 8 de outubro de 2015](#) e no [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Natalia Barbosa Ramos, Gerente**, em 04/12/2025, às 11:45, conforme horário oficial de Brasília, com fundamento no [Decreto nº 8.539, de 8 de outubro de 2015](#) e no [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Carlos Alberto Torres Quintanilha Neto, Gerente**, em 04/12/2025, às 11:47, conforme horário oficial de Brasília, com fundamento no [Decreto nº 8.539, de 8 de outubro de 2015](#) e no [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Bruno Manhaes de Souza, Superintendente**, em 04/12/2025, às 11:55, conforme horário oficial de Brasília, com fundamento no [Decreto nº 8.539, de 8 de outubro de 2015](#) e no [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Marcelo Andre Ferreira Silva, Gerente Executivo**, em 04/12/2025, às 12:02, conforme horário oficial de Brasília, com fundamento no [Decreto nº 8.539, de 8 de outubro de 2015](#) e no [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Raquel Goncalves Caldeira Brant Losekann, Gerente**, em 04/12/2025, às 16:09, conforme horário oficial de Brasília, com fundamento no [Decreto nº 8.539, de 8 de outubro de 2015](#) e no [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Leandro Cianconi de Paiva Rodas, Superintendente**, em 04/12/2025, às 16:37, conforme horário oficial de Brasília, com fundamento no [Decreto nº 8.539, de 8 de outubro de 2015](#) e no [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Carlos Wagner da Silva, Gerente Executivo**, em 04/12/2025, às 16:42, conforme horário oficial de Brasília, com fundamento no [Decreto nº 8.539, de 8 de outubro de 2015](#) e no [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Sonia da Silva Pereira Garcia, Gerente Executivo**, em 08/12/2025, às 09:45, conforme horário oficial de Brasília, com fundamento no [Decreto nº 8.539, de 8 de outubro de 2015](#) e no [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site [https://dataprev.sei.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://dataprev.sei.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0191056** e o código CRC **BF6B447E**.

Referência: Processo nº 44129.009517/2025-50

SEI nº 0191056



**ANEXO VII**

**PREGÃO ELETRÔNICO Nº 91065/2025**

**PROCESSO Nº 44129.009517/2025-50**

**DECLARAÇÃO DE PREFERÊNCIA DE CONTRATAÇÃO**

**(IDENTIFICAÇÃO DA LICITAÇÃO)**

**(IDENTIFICAÇÃO COMPLETA DO REPRESENTANTE DA LICITANTE)**, como representante devidamente constituído de **(IDENTIFICAÇÃO COMPLETA DA LICITANTE OU DO CONSÓRCIO)** doravante denominado **(LICITANTE/CONSÓRCIO)**, para fins do disposto no item **(COMPLETAR)** do Edital **(COMPLETAR COM IDENTIFICAÇÃO DO EDITAL)**, declara, sob as penas da Lei, em especial o Art. 299 do Código Penal Brasileiro, que:

Possuo a Certificação de Tecnologia desenvolvida no País, nos termos da Lei nº 8.248, de 23 de outubro de 1991 e dos Decretos nº 5.906, de 26 de setembro de 2006, ou pelo Decreto nº 10.521, de 15 de outubro de 2020;

Possuo a Certificação de Processo Produtivo Básico, nos termos da Lei nº 8.248, de 23 de outubro de 1991 e dos Decretos nº 5.906, de 26 de setembro de 2006, ou pelo Decreto nº 10.521, de 15 de outubro de 2020;

Ainda, declara, que está plenamente ciente do teor e da extensão desta Declaração e que detém plenos poderes e informações para firmá-la.

\_\_\_\_\_, em \_\_\_\_ de \_\_\_\_\_ de \_\_\_\_\_

\_\_\_\_\_  
(NOME COMPLETO)

CPF:

RG:

<b>ANEXO VIII – MODELO DE DECLARAÇÃO DE NÃO OCORRÊNCIA DO REGISTRO DE OPORTUNIDADE</b>
--

À

EMPRESA DE TECNOLOGIA E INFORMAÇÕES DA PREVIDÊNCIA – DATAPREV S.A.

Ref.: Pregão nº 91065/2025

**Objeto: Aquisição de Solução de Firewalls de Rede com garantia pelo período de 60 (sessenta) meses, para instalação nos Data Centers da Dataprev, incluindo prestação dos serviços de capacitação e orientação técnica a serem utilizadas sob demanda.**

Prezados Senhores,

O (LICITANTE), (qualificação), por meio de seu representante legal, **DECLARA**, que para a apresentação de proposta ao referido Edital, **NÃO** houve ocorrência do “Registro de Oportunidade”, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública, conforme disposto no Art. 2º, inciso IV, da Resolução CGPAR nº 29, de 5 de abril de 2022.

**Local e data**

---

**Assinatura e carimbo do emissor**

**(com nº de matrícula ou do CPF)**

**telefone de contato e e-mail**

**Observação: este documento deve ser emitido em papel timbrado que identifique o emissor.**