Termo de Referência
Serviço Testes de Penetração

Equipe Responsável	
Elaboração	
Divisão de Gestão de Insumos e Processos de Contratação de Infraestrutura de TIC **DGIC**	Lucio Antoniolo Netto 338.133
Aprovação Motivada *Considerando que o Termo de Referência elaborado se apresenta de forma conveniente e oportuna para atender a demanda exposta no **Estudo Técnico** 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.*	
Divisão de Planejamento de Infraestrutura de TIC **DIPL**	Carlos Wagner da Silva 346.241
Divisão de Detecção e Controle de Vulnerabilidade **DDCV**	Fernando Chagas de Almeida 349.712
Departamento de Gestão Técnica de Infraestrutura de TI **DEGI**	Sonia da Silva Pereira Garcia 286.800
Departamento de Planejamento e Serviços de Infraestrutura de TIC **DEPS**	Leandro Cianconi de Paiva Rodas 352.926
Departamento de Segurança Operacional **DESO**	Rogerio de Souza Braz do Canto Cyrillo 329.908
Superintendência de Planejamento e Gestão de TIC **SUTI**	Rodrigo Morgado da Silva 341.479
Superintendência de Operações **SUOP**	Bruno Manhaes de Souza 335.991

Sumário

1. OBJETO

1.1. Trata o presente processo da contratação de **empresa especializada para a prestação de serviços de testes de intrusão nas aplicações web disponibilizadas na Internet pela DATAPREV**, sob demanda, pelo período de **24 meses**.

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

ITEM	DESCRIÇÃO / PRODUTO	QUANTIDADE TOTAL	UNIDADE
1	**a)** Serviços de Testes de Intrusão para 12 aplicações disponibilizadas na Internet com entrega de relatórios.	12	Teste
	b) Serviços de Retestes de Intrusão para 12 aplicações disponibilizadas na Internet com entrega de relatórios.	12	Reteste

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

1.4. Permitida a formação de consórcio de empresas.

1.5. Os testes ou retestes serão realizados conforme a necessidade da **DATAPREV**, podendo ser realizados mais de um **teste** ou reteste ao mesmo tempo, caso esta seja a necessidade da empresa.

1.6. A especificação técnica do Serviço **Testes de Penetração** está contida **no ANEXO I – ESPECIFICAÇÃO TÉCNICA deste Termo de Referência**.

2. DOCUMENTAÇÃO OBRIGATÓRIA

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

2.1.1. No mínimo, 01 (um) atestado de capacidade técnica (declaração ou certidão), conforme **ANEXO III – MODELO DE ATESTADO OU DECLARAÇÃO DE CAPACIDADE TÉCNICA**, em papel timbrado e com identificação do emitente (nome

completo, e-mail e telefone de contato), em original ou cópia autenticada, emitido por empresa pública ou privada, comprovando o perfeito cumprimento das obrigações relativas ao fornecimento de **Serviço de Testes de Penetração**, com características técnicas e complexidade similares ao objeto especificado neste **Termo de Referência**, informando o período e o local da prestação dos serviços. Caso seja necessário, a **LICITANTE** vencedora poderá apresentar mais de um atestado, a fim de comprovar a capacidade nos serviços citados.

2.1.1.1 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;

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

3. PLANEJAMENTO

3.1. A **CONTRATADA** deverá se reunir com o **Gestor Técnico** do contrato, conforme descrito no **subitem 16.1** deste **Termo de Referência**, e com a Equipe Técnica responsável, 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:

3.1.1. Apresentar as características dos serviços, além de tratar das informações sobre o planejamento e cronograma da sua execução e esclarecer todos os questionamentos técnicos. A **DATAPREV** definirá, com o apoio da equipe técnica da **CONTRATADA** de que forma os serviços serão prestados. A **CONTRATADA** e a **DATAPREV**, em comum acordo, deverão fazer um planejamento das atividades.

3.2. 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.

3.3. A **CONTRATADA** deverá se reunir com o **Gestor Administrativo** do contrato, conforme descrito no **subitem 16.2** deste **Termo de Referência**, no Rio de Janeiro, em local a ser definido pela **DATAPREV**, 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.

Nesta reunião a **CONTRATADA** deverá:

3.3.1. Apresentar quem será o gestor do contrato por parte da **CONTRATADA** para tratar de questões comerciais e/ou contratuais.

4. TESTES E RETESTES DE PENETRAÇÃO

4.1. Durante a vigência contratual, a **CONTRATADA** deverá realizar 12 (doze) testes e 12 (doze) retestes, sob demanda, em aplicações conforme especificados no **ANEXO I – ESPECIFICAÇÃO TÉCNICA**.

4.2. Os **TESTES/RETESTES** serão executados em conformidade com as Ordens de Serviços (OS) a serem emitidas para sua execução, conforme modelo constante no **ANEXO V – MODELO DE ORDEM DE SERVIÇO**.

4.3. 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

videoconferência, com a finalidade de definir o escopo e planejamento da sua execução, além de serem discutidos e esclarecidos todos os questionamentos técnicos. A **DATAPREV** definirá, com o apoio da equipe técnica da **CONTRATADA**, de que forma os serviços deverão ser realizados. A **CONTRATADA** e a **DATAPREV**, de comum acordo, deverão fazer um planejamento prévio das atividades de execução dos serviços.

4.4. Após a realização desta primeira reunião, caso existam questionamentos direcionados à **DATAPREV** e/ou à **CONTRATADA**, será disponibilizado um prazo de até **5 (cinco) dias úteis**, contados a partir do dia seguinte à realização da reunião, para as respostas.

4.5. Como produto da reunião descrita no **subitem 4.3** deste Termo de Referência, a **CONTRATADA** deverá encaminhar, por meio eletrônico, em **5 (cinco) dias úteis** após a realização da reunião e esclarecimento de possíveis dúvidas remanescentes, o **PLANO DE EXECUÇÃO DOS SERVIÇOS**, o qual deverá conter de forma detalhada todas as fases do processo, cronograma de execução, prazo de realização, a infraestrutura necessária, detalhamento de todos os elementos que compõem o teste/reteste.

4.6. No prazo máximo de **5 (cinco) dias úteis**, a partir do recebimento formal do **PLANO DE EXECUÇÃO DOS SERVIÇOS**, a **DATAPREV** deverá se manifestar sobre sua aprovação. Caso seja necessário, será concedido à **CONTRATADA** um novo prazo de **5 (cinco) dias úteis** para eventuais ajustes e reapresentação da documentação reprovada. A versão definitiva do **PLANO DE EXECUÇÃO DOS SERVIÇOS** será a versão aprovada pela Equipe Técnica da **DATAPREV**.

4.7. Os testes/retestes deverão ser executados pela **CONTRATADA**, de acordo com planejamento realizado pela equipe da **DATAPREV** em conjunto com a equipe da **CONTRATADA**, obedecendo cronograma estabelecido no **plano de execução dos serviços**.

O início dos testes/retestes deverá ocorrer no **prazo máximo de até 5 (cinco) dias úteis** a partir do dia seguinte da aprovação da versão final do **PLANO DE EXECUÇÃO DOS SERVIÇOS** pela **DATAPREV**.

4.8. No prazo máximo de **5 (cinco) dias úteis após a comunicação formal da contratada sobre a conclusão do teste/reteste,** a **CONTRATADA** deverá entregar à **DATAPREV**, o **RELATÓRIO TESTE DE INVASÃO** referente ao teste/reteste realizado, contemplando no mínimo as informações descritas no **ANEXO I – ESPECIFICAÇÃO TÉCNICA**.

4.8.1. A **CONTRATADA** terá o prazo **máximo de 3 (três) dias úteis**, contados a partir do dia seguinte a entrega do **RELATÓRIO TESTE DE INVASÃO** para se reunir com o solicitante, presencialmente ou por meio de videoconferência, com a finalidade de apresentar de forma detalhada todo o conteúdo do **RELATÓRIO TESTE DE INVASÃO**, onde serão sanadas todas as dúvidas do corpo técnico da **DATAPREV.**

4.8.2. A **DATAPREV** terá o prazo de **30 (trinta) dias corridos**, contados a partir do dia seguinte à realização da reunião descrita no **subitem 4.8.1** para realizar validar o **RELATÓRIO TESTE DE INVASÃO.**

4.9. Após a **DATAPREV** finalizar a avaliação do **RELATÓRIO TESTE DE INVASÃO**, 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, e ser assinado por responsáveis da **CONTRATADA** e pelo Gestor Técnico da **DATAPREV**, conforme descrito no **item 16.1** deste **Termo de Referência**.

4.10. Somente o Gestor Técnico, descrito no **subitem 16.1** deste **Termo de Referência**, poderá oficializar, junto à **CONTRATADA**, as solicitações de OS.

4.11. Após a realização da reunião descrita no **subitem 4.8.1,** a **DATAPREV** irá trabalhar na remediação das vulnerabilidades e falhas apontadas no relatório descrito no **subitem 4.8**.

4.12. Concluída a remediação das vulnerabilidades, a **DATAPREV** poderá solicitar nova OS para que a **CONTRATADA** realize o reteste com a finalidade de verificar a remediação aplicada e apresentar o **RELATÓRIO FINAL DO TESTE DE INVASÃO**.

4.12.1. A realização de retestes seguirá o disposto nos **subitens 4.2 a 4.10**.

4.13. Os testes/retestes deverão ser realizados por pelo menos um profissional especializado, possuindo, pelo menos, 2 (duas) das certificações listadas a seguir, sendo no mínimo, básica/intermediária e 1 (uma) avançada, para desempenhar as atividades propostas para os serviços contratados:

Certificações Básicas / Intermediárias:

- CEH – *Certified Ethical Hacker*
- CPT - IACRB *Certified Penetration Tester*
- CPTE - *Certified Penetration Testing Engineer - Mile2*
- eWPTX v2 - *Elearn Security Web Penetration Tester Extreme v2*
- *CompTIA Pentest+*
- DCPT - *Desec Certified Penetration Tester*

Certificações Avançadas:

- LPT - *EC-Council Licensed Penetration Tester Master*
- CEPT - *Certified Expert Penetration Tester*
- GXPN - *Exploit Researcher and Advanced Penetration Tester*
- OSCP - *Offensice Security Certified Professional*
- OSWE - *Offensive Security Web Expert*
- CPENT- *Certified Penetration Testing Professional*
- C|EH *Practical*

4.13.1. A(s) certificação(ões) exigida(s) no **subitem 4.13**. deve(m) estar válida(s) durante o período de prestação dos serviços.

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

Cada solicitação de serviço 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).**

4.15. 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.

4.16. 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**.

Os casos em que a execução dos serviços ocorrera fora do horário comercial, para testes/retestes de aplicações específicas, serão informados previamente pela equipe da **DATAPREV** na reunião definida no **subitem 4.3** deste **Termo de Referência**.

4.17. As fases dos **TESTES/RETESTES** deverão obedecer aos seguintes prazos:

- **Planejamento (16 dias úteis)**
    - Reunião para definição do escopo de planejamento. (3 dias úteis a partir da abertura da ordem de serviço);
    - Envio de questionamentos e respostas. (5 dias úteis a partir da reunião);
    - Encaminhamento pela **CONTRATADA** do Plano de Execução dos Serviços. (5 dias úteis a partir da reunião);
    - Avaliação da Dataprev para o Plano de Execução dos Serviços. (5 dias úteis a partir do envio do Plano de Execução dos Serviços);
    - Eventuais ajustes na documentação. (3 dias úteis a partir da avaliação da **DATAPREV**).

- **Testes e Retestes de Penetração (estimativa de até 53 dias úteis)**
    - Descoberta e enumeração de serviços. (5 dias úteis - **CONTRATADA**);
    - Ataque. (10 dias úteis - **CONTRATADA**);
    - Elaboração do Relatório Teste de Invasão. (5 dias úteis - **CONTRATADA**);

- Reunião com a Dataprev para apresentação do relatório Teste de Invasão. (3 dias úteis - **CONTRATADA** e **DATAPREV**);
- Dataprev aplica as recomendações para remediar ou assume os riscos (em até 30 dias corridos - **DATAPREV**);
- Reavaliação, novo teste pós remediação (Reteste). (5 dias úteis a partir da correção e emissão de nova ordem de serviço pela **DATAPREV** - **CONTRATADA**);
- Elaboração do Relatório Final do Teste de Invasão. (3 dias úteis - **CONTRATADA**).

5. CONDIÇÕES GERAIS PARA PRESTAÇÃO DOS SERVIÇOS DE GARANTIA DOS TESTES E RETESTES

5.1. A **CONTRATADA** deverá garantir que as aplicações testadas não sejam impactadas. Caso venha ocorrer algum dano após a execução dos testes/retestes, a **CONTRATADA** deverá fornecer informações que auxiliem na solução de problemas que possam ocorrer como resultado dos testes/retestes de penetração.

5.2. A garantia dos serviços contratados deverá considerar o período mínimo de **3 (três) meses** a partir da data de sua execução, por aplicação testada.

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

5.4. A modalidade de atendimento deverá ser em regime 8x5 (8 horas por dia x 5 dias da semana), de segunda a sexta (9:00 às 18:00 horas), excluindo os feriados nacionais.

6. RELATÓRIOS

6.1. Durante todo o período de prestação dos serviços a **CONTRATADA** deverá apresentar, mensalmente, um arquivo contendo o **RELATÓRIO TESTE DE INVASÃO**, conforme descrito no item **4.8**. O relatório deverá conter as informações indicadas no **item 16** do **ANEXO I** deste **Termo de Referência**.

6.2. Durante todo o período de prestação dos serviços, 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 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 16** 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).

7. USO DA LÍNGUA PORTUGUESA

7.1. Em todas as atividades 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**.

7.2. A abertura, o acompanhamento e o atendimento das ocorrências deverão ser feitos em língua portuguesa.

8. SIGILO E INVIOLABILIDADE

8.1. 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.

8.2. A **CONTRATADA** deverá prestar esclarecimentos à **DATAPREV** sobre eventuais atos ou fatos noticiados que se refiram à mesma.

9. SANÇÕES ADMINISTRATIVAS

9.1. Será aplicada multa pelo descumprimento dos prazos relacionados no **item 3 – 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.

9.2. Será aplicada multa de 1% (um por cento) ao dia, até o limite máximo de 20% (vinte por cento) do valor do respectivo Serviço, pelo atraso, causado pela **CONTRATADA**, na **conclusão dos testes e retestes de penetração**, conforme descritos no **item 4** deste **Termo de Referência**. O descumprimento de cada prazo implicará em uma nova multa, aplicadas cumulativamente conforme o caso.

9.3. Será aplicada multa pelo atraso, causado pela **CONTRATADA**, no fornecimento das informações sobre os canais de atendimento, conforme descrito nos **subitens 4.14** 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.

9.4. 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 **pelo inadimplemento contratual relacionado às situações não previstas nos subitens anteriores.**

9.5. 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.

9.6. Caso o valor total pago mensalmente pela **DATAPREV** para os serviços 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.

9.7. 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.

10. AVALIAÇÃO DO FORNECEDOR

10.1. 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.

10.2. 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.

10.3. 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)

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

11. OBRIGAÇÕES DA CONTRATADA

11.1. 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 pelo menos um profissional certificado pelo fabricante para realizar os serviços, em conformidade com o exigido no **item 4.13** 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.

11.2. O vínculo jurídico-legal do(s) profissional(ais) citado(s) no(s) **subitens 11.1** 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

11.3. Durante a vigência contratual, caso a **CONTRATADA** queira apresentar um novo profissional com a certificação para atender à exigência descrita nos **subitens 11.1**deste

Termo de Referência, deverá entregar a documentação descrita no **subitem 11.2** deste **Termo de Referência**.

11.4. Caso a **CONTRATADA** descumpra o estabelecido nos **subitens 11.1 à 10.3** 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.

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

12. OBRIGAÇÕES DA CONTRATANTE

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

13. FATURAMENTO

13.1. Serviços de testes e retestes: mediante o envio pela **DATAPREV** do Relatório de Medição do serviço prestado pela **CONTRATADA**. Se dará de acordo com o fechamento das Ordens de Serviços concluídas no período.

13.2. 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).

14. PAGAMENTO

14.1. 15 (quinze) dias após recebimento da fatura pela **DATAPREV.**

15. VIGÊNCIA CONTRATUAL

15.1. A vigência contratual será de **24 (vinte e quatro) meses.**

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

16. GESTÃO CONTRATUAL

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

16.2. **Gestão Administrativa** – Divisão de Gestão Administrativa de Contratos de TIC – DGFT.

16.2.1. **Fiscais** – Empregados relacionados no "Grupo DGFT".

17. 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 – MODELO DE ORDEM DE SERVIÇO

ANEXO I – ESPECIFICAÇÃO TÉCNICA

1. Os testes deverão ser realizados em 12 aplicações disponibilizadas na Internet que serão definidas pela Dataprev durante o período contratual que será de 24 meses.

1.1. As aplicações que serão alvo dos testes ficam hospedadas nos *Data Centers* da Dataprev (RJ, SP e DF).

1.2. As 12 aplicações pertencem ao ambiente de produção e homologação.

1.3. Não haverá testes em aplicações *Mobile* e *Wireless*.

1.4. Não haverá testes em API's (*Application Programming Interface*).

1.5. Não haverá análise de código fonte das aplicações.

1.6. Os objetivos dos testes serão o de testar e aperfeiçoar os controles de segurança implementados e aumentar o grau de maturidade da equipe de segurança para ações de *Pentest* na infraestrutura da Dataprev, de acordo com as lições aprendidas com os resultados dos testes.

1.7. Os seguintes normativos são seguidos pela Dataprev para fins de conformidade:

1.7.1. ISO 27001;

1.7.2. LGPD (Lei nº 13.709, de 14 de agosto de 2018);

1.7.3. POSIC da Dataprev;

1.7.4. Normas complementares do CTIR.GOV.

2. Os testes deverão ser realizados em horário comercial.

2.1. Aplicações para as quais os testes não possam ser executados em horário comercial, a Dataprev indicará no escopo dos testes o horário de execução.

3. Os profissionais da CONTRATADA que efetuarão os testes não ficarão nas dependências da Dataprev.

3.1. A Dataprev não fornecerá infraestrutura (software/hardware) para a execução dos testes.

4. A Dataprev poderá solicitar o acompanhamento dos testes. Neste caso, os testes serão agendados e acompanhados pelo Microsoft Teams.

5. Deverão ser realizados testes de caixa preta, cinza e branca.

5.1. A princípio será considerado o teste de caixa preta no qual não serão disponibilizadas informações prévias sobre os alvos. No entanto, dependendo da evolução dos testes, a Dataprev poderá solicitar testes de caixa cinza e/ou branca com o fornecimento de informações.

5.2. Uma vez que o teste resulte na invasão de uma aplicação/servidor, será solicitado pela Dataprev que os testes continuem com o intuito de saber se, a partir deste ponto, é possível invadir outras aplicações, servidores e a rede interna.

6. Os testes deverão ser realizados em serviços que estão disponibilizados na Internet.

7. Os testes realizados não devem causar danos aos sistemas e serviços da Dataprev.

8. Quaisquer atividades que possam comprometer ou prejudicar algum ambiente ou ativo deverá ser imediatamente reportada, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos.

9. Não será permitida a execução de testes de Negação de Serviço (DoS).

10. Antes das execuções dos testes, a Dataprev deverá ser comunicada do início das atividades.

11. A CONTRATADA deverá manter o sigilo de todas as informações em relação aos testes e ambiente computacional da Dataprev.

12. Os alvos, premissas e condições para a realização dos testes serão definidos através de Ordem de Serviço (OS).

13. Todas as fases dos testes serão supervisionadas pela Dataprev.

14. Após remediação das vulnerabilidades encontradas por parte da Dataprev, a CONTRATADA deverá refazer os testes (reteste) com intuito de validar a remediação.

14.1. A Dataprev informará à CONTRATADA sobre a aplicação da remediação e emitirá Ordem de Serviço (OS) para o reteste.

15. Para cada teste a ser realizado, a CONTRATADA deverá:

15.1. Apresentar, explicar e discutir com a equipe da Dataprev o plano de testes.

15.2. Explicar todos os passos tomados para atingir os resultados esperados.

15.3. Tirar todas as dúvidas que possam surgir durante os testes.

15.4. Confeccionar os relatórios dos testes.

15.5. Entregar os relatórios dos testes para a equipe de Segurança Operacional da Dataprev.

16. Para cada teste realizado deverá ser emitido um relatório contendo, no mínimo, os itens abaixo:

16.1. Dados do escopo escolhido.

16.2. Planejamento das etapas dos testes realizados.

16.3. Tipos de testes e ataques realizados.

16.4. Informações coletadas durante os testes.

16.5. Métodos, ferramentas e comandos utilizados para a coleta de informações e execução dos testes.

16.6. Vulnerabilidades encontradas e não exploradas.

16.7. Vulnerabilidades encontradas e exploradas.

16.8. Proposta de solução técnica para as vulnerabilidades exploradas.

16.9. Proposta de solução técnica para as vulnerabilidades não exploradas.

16.10. Data e hora dos testes.

16.11. Tempo de duração da execução dos testes.

16.12. Ameaças encontradas.

16.13. Contramedidas para mitigar as ameaças encontradas.

16.14. Riscos levantados ao ambiente computacional.

16.15. A descrição das vulnerabilidades encontradas (nome, descrição, nível de risco e CVE).

16.16. Se houve obtenção de acesso e possível escalada de privilégios.

16.17. Se houve acesso a informações sigilosas.

16.18. Metodologia dos ataques.

16.19. Metodologia de análise de vulnerabilidades.

16.20. Controles de segurança necessários para correção das vulnerabilidades.

16.21. Apresentação das evidências apuradas.

16.22. Evidências dos sucessos dos ataques.

16.23. Portas e serviços em execução.

16.24. Serviços ativos e vulneráveis.

16.25. Configurações feitas nas aplicações sem observância de boas práticas em segurança da informação.

16.26. Uso indevido de sistema de arquivos e arquivos temporários.

16.27. Se houve evasão de informações por identificação de configurações default.

16.28. Identificação de tratamento indevido para entrada de dados.

16.29. Problemas relacionados à má configuração dos serviços.

16.30. Padrões internacionais utilizados (item 18).

16.31. Testes realizados com base na publicação OWASP TESTING GUIDE 3.0 (item 19).

17. Os Testes em aplicações *Web* deverão contemplar no mínimo, mas não se limitando aos tipos de ataques a seguir:

17.1. *Cross Site Scripting* (XSS).

17.2. *Cross Site Request Forgery* (CSRF).

17.3. Injeção de Código.

17.4. *Remote File Inclusion Attack*.

17.5. Referência Direta a Objetos.

17.6. Vazamento de Informações, onde deve ser verificada a exposição inadvertida de informações na aplicação.

17.7. Ataques baseados em Gerenciamento de Sessões.

17.8. Deverão ser analisadas, pelo menos, as vulnerabilidades dos últimos dois relatórios OWASP Top 10.

17.9. Ataques customizados baseados na arquitetura das aplicações.

17.10. SQL *Injection*.

17.11. *Directory Transversal*.

17.12. *Buffer Overflow*.

17.13. *Remote Code Inclusion*.

17.14. *File Disclosure*.

17.15. Sequestro de Conexões.

17.16. *Brute Force Login*.

17.17. Descoberta de Credenciais.

17.18. *Eavesdropping*.

17.19. Escalonamento de privilégios.

17.20. *Defacement*.

17.21. PHP *Injection*.

17.22. *Command Injection*.

17.23. *Script Injection*.

17.24. *Misconfiguration*.

17.25. *Server Side Includes* (SSI) *Injection*.

17.26. *Information Leakage*.

17.27. *Zero day attacks*.

17.28. Comprometimento do acesso remoto.

17.29. Encobrimento de rastros da invasão.

17.30. Vírus, *Worms* e Cavalos de Tróia.

17.31. Problemas com o SNMP.

17.32. *Cookie Injection*.

17.33. *Cookie Poisoning*.

17.34. *Forceful Browsing*.

17.35. Violações do protocolo HTTP.

17.36. HTTP *Parameter Pollution*.

17.37. HTTP *Hidden Field Manipulation*.

17.38. HTTP *Request Smuggling*.

17.39. HTTP *Response Splitting*.

17.40. HTTP *Verb Tampering*.

17.41. *Web Scraping.*

17.42. *Web Service XML Attack.*

18. Para a realização dos testes, deverão ser observadas as orientações e técnicas emanadas pelos seguintes padrões internacionais abaixo:

18.1. OSSTMM 3 (The Open Source Security Testing Methodology Manual).

18.2. ISSAF/PTF (Information Systems Security Assessment Framework).

18.3. NIST Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment).

18.4. NIST Special Publication 800-42 (Guideline on Network Security Testing).

19. Para a realização dos testes, deverão ser observados e aplicados, os seguintes testes baseados na publicação OWASP TESTING GUIDE 3.0 (*The Open Web Application Security Project*):

19.1. Para testes de **coleta de informações**, aplicar padrão: OWASP-IG-001, OWASP-IG-002, OWASP-IG-003, OWASP-IG-004, OWASP-IG-005 e OWASP-IG-006.

19.2. Para testes de **gerenciamento de configuração**, aplicar padrão: OWASP-CM-001, OWASP-CM-002, OWASP-CM-003, OWASP-CM-004, OWASP-CM-005, OWASP-CM-006, OWASP-CM-007, OWASP-CM-008.

19.3. Para testes de **autenticação**, aplicar padrão: OWASP-AT-001, OWASP-AT-002, OWASP-AT-003, OWASP-AT-004, OWASP-AT-005, OWASP-AT-006, OWASP-AT-007, OWASP-AT-008, OWASP-AT-009 e OWASP-AT-010.

19.4. Para testes de **gerenciamento de sessão**, aplicar padrão: OWASP-SM-001, OWASP-SM-002, OWASP-SM-003, OWASP-SM-004, OWASP-SM-005.

19.5. Para testes de **autorização**, aplicar padrão: OWASP-AZ-001, OWASP-AZ-002 e OWASP-AZ-003.

19.6. Para testes de **negócio lógico**, aplicar padrão: OWASP-BL-001.

19.7. Para testes de **validação de dados**, aplicar padrão: OWASP-DV-001; OWASP-DV-002, OWASP-DV-003, OWASP-DV-004, OWASP-DV-005, OWASP-DV-006, OWASP-DV-007, OWASP-DV-008, OWASP-DV-009, OWASP-DV-010, OWASP-DV-011, OWASP-DV-012, OWASP-DV-013, OWASP-DV-014, OWASP-DV-015 e OWASP-DV-016.

19.8. Para testes de **serviços web**, aplicar padrão: OWASP-WS-001, OWASP-WS-002, OWASP-WS-003, OWASP-WS-004, OWASP-WS-005, OWASP-WS-006 e OWASP-WS-007.

20. Os testes deverão obedecer às seguintes fases:

20.1. Planejamento.

20.2. Descoberta.

20.3. Ataque.

20.4. Relatório Teste de Invasão.

20.5. Reunião com a Dataprev para apresentação do relatório Teste de Invasão.

20.6. Dataprev aplica as recomendações para remediar os riscos.

20.7. Reavaliação, novo teste pós remediação.

20.8. Relatório Final do Teste de Invasão.

21. Planejamento

21.1. Deverá ser realizada com a Dataprev reunião para planejamento para execução dos serviços.

21.2. Todas as premissas, processos, atividades descritas e aprovadas na Ordem de Serviço (OS), inclusive os cronogramas serão detalhados e apresentados na fase de planejamento.

21.3. Informações sobre o ambiente corporativo, utilizando-se das técnicas caixa-preta, caixa-cinza e caixa-branca (podendo ser utilizadas mais de uma, conforme definição do escopo).

22. Descoberta

22.1. Deverão ser utilizadas ferramentas de análise de vulnerabilidade comerciais, gratuitas e técnicas manuais de análise de vulnerabilidade. As ferramentas deverão ser apresentadas à Dataprev para ciência e aprovação, antes de sua efetiva utilização, assim como a metodologia para a análise manual de vulnerabilidades.

22.2. A ferramenta de análise de vulnerabilidades não deve ser baseada na necessidade de instalação prévia de agentes no ambiente corporativo da Dataprev.

22.3. O processo de varredura não deve causar impacto no ambiente da Dataprev.

23. Ataque

23.1. Nesta fase todos os testes e ataques descritos nos itens 17, 18, 19 e seus subitens deverão ser executados.

23.2. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo deverá ser imediatamente reportada, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos.

23.3. Deverão ser realizados testes de vulnerabilidades e invasões nas aplicações *web*, as quais serão informadas através de Ordem de Serviço (OS) junto com as demais informações sobre o escopo para a execução das atividades.

24. Relatório Teste de Invasão

24.1. Deverá ser elaborado e entregue à Dataprev após a fase de ataque, o relatório "RELATÓRIO TESTE DE INVASÃO" para cada teste que será realizado, contemplando no mínimo as informações descritas no item 16 e seus subitens.

25. Reunião para apresentação do relatório Teste de Invasão

25.1. Será realizada reunião conduzida pela Contratada, onde será apresentado de forma detalhada todo o conteúdo do "Relatório Teste de Invasão", onde serão sanadas todas as dúvidas do corpo técnico da Dataprev.

26. Reavaliação, novo teste (reteste) pós remediação

26.1. A Dataprev, após receber o Relatório de Teste de Invasão e sua devida apresentação (reunião) e recomendações, optará por aplicar as recomendações, remediar os riscos ou mesmo assumi-los. Após essa etapa, caso a Dataprev opte por aplicar as recomendações, a CONTRATADA deverá refazer os testes de invasão (reteste) e emitir novo relatório (Relatório Final do Teste de Invasão) apontando a remediação ou não das vulnerabilidades. Os respectivos prazos para essas etapas se encontram definidos no Termo de Referência.

ANEXO II – PLANILHA DE FORMAÇÃO DE PREÇOS

ITEM	DESCRIÇÃO	QUANTIDADE (A)	UNIDADE	PRODUTOS / SERVIÇOS	
				VALOR UNITÁRIO (B)	SUBTOTAL A x B
1	a) Serviços de Testes de Intrusão para 12 aplicações disponibilizadas na Internet com entrega de relatórios.	12	un.	R$ -	R$ -
	b) Serviços de Retestes de Intrusão para 12 aplicações disponibilizadas na Internet com entrega de relatórios.	12	un.	R$ -	R$ -
				TOTAL	**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) _____, _____("prestou serviços de testes de penetração") 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 n° 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/2021
PROCESSO Nº

TERMO DE SIGILO E PRIVACIDADE VINCULADO AOS CONTRATOS

Cláusula Primeira - OBJETO

Constitui objeto deste Termo o estabelecimento de condições especificas 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 n° 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 á 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 especificas e/ou tomada de decisão.

2.1.6 Informação de acesso restrito

Aquelas que estão submetidas temporariamente á restrição de acesso público.

2.1.7 Informação sigilosa

Aquelas que estão submetidas á 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 n° 5.172/196);
   b) Sigilo bancário (Art. 1^0 da Lc n° 105/2001);
   c) Sigilo Comercial (§2° do art. 155 da Lei n° 6.404/1976);
   d) Sigilo Empresarial (Art. 169 da Lei n° 11.101/2005); e
   e) Sigilo Contábil (Art. 1.190 e 1.191 da Lei n° 5.869/1973).

III. Hipóteses de sigilo decorrentes de processos e procedimentos:
   a) Sigilo de inquérito policial (Art. 20 da Lei n° 3.689/1941);
   b) Segredo de justiça no processo civil (Art. 155 da Lei n° 5.869/1973); e
   c) Segredo de justiça no processo penal (§6° do art. 201 da Lei n° 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

§1° 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.

§2° 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.

§3° 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

§1° 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

§1° **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 deste Termo.

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

§3° **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.

§4° **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.

§5° **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.

§6° **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

§1° 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 n° 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD).

§2° Necessidades de coleta de consentimento para outras finalidades deverão ser identificadas e correr sob responsabilidade da **PARTE REVELADORA.**

§3° São escopo de tratamento somente os dados pessoais indispensáveis para a execução do objetivo contratual, e conforme bases legais pré-estabelecidas e acordadas, cabendo à **PARTE RECEPTORA** observar estritamente a finalidade a que se destinam os dados

pessoais a que venha a ter conhecimento

§4° À PARTE RECEPTORA é vedada qualquer forma de compartilhamento de dados pessoais com terceiros fora do âmbito do contrato.

§5° 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**

§6°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

§1° 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.

§2° 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 Politica de Segurança da Informação e Comunicações - POSIC e o Código de Ética e Integridade, disponiveis 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 irretratável, 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 de 2021.

EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DA PREVIDÊNCIA - DATAPREV	PARTE RECEPTORA

ANEXO V – MODELO DE ORDEM DE SERVIÇO

ORDEM DE SERVIÇO Nº XXX/202X

ABERTURA

1. DADOS DO CONTRATO

CONTRATO Nº		**PEDIDO DE COMPRAS Nº**		
CONTRATADA		**GESTOR TÉCNICO**		
OBJETO		**VIGÊNCIA**		
DESCRIÇÃO	**QUANTIDADE**	**UNIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**

2. REGISTRO DA ABERTURA DA ORDEM DE SERVIÇO - OS

Nº DO CHAMADO	DATA DO CHAMADO	RESPONSÁVEL DATAPREV ABERTURA DA OS / MATRÍCULA	ÓRGÃO

3. DEFINIÇÃO DE ESCOPO DA ORDEM DE SERVIÇO - OS

DATA DA REUNIÃO	RESPONSÁVEL DATAPREV	RESPONSÁVEL CONTRATADA

DESCRIÇÃO
SERVIÇO A SER ENTREGUE COM A DEVIDA DOCUMENTAÇÃO COMPROBATÓRIA

4. PLANEJAMENTO DA EXECUÇÃO DA ORDEM DE SERVIÇO-OS

DATA DE ENVIO CRONOGRAMA E TOTAL DE HORAS ESTIMADOS	CRONOGRAMA ESTIMADO		Nº TOTAL DE HORAS ESTIMADO	
	DATA DE INÍCIO	DATA DE CONCLUSÃO	NÍVEL 1	NÍVEL 2

5. APROVAÇÃO DO PLANEJAMENTO DA ORDEM DE SERVIÇO-OS

ASSINATURA / CARIMBO RESPONSÁVEL CONTRATADA	ASSINATURA / CARIMBO GESTOR TÉCNICO DATAPREV	DATA DA APROVAÇÃO DATAPREV

ANEXO V – MODELO DE ORDEM DE SERVIÇO

ORDEM DE SERVIÇO Nº XXX/202X
ACEITE

1. DADOS DO CONTRATO

CONTRATO Nº	**PEDIDO DE COMPRAS Nº**
CONTRATADA	**GESTOR TÉCNICO**
OBJETO	**VIGÊNCIA**

QUANTIDADE	UNIDADE	NÍVEL DO SERVIÇO	VALOR UNITÁRIO	VALOR TOTAL

2. EXECUÇÃO DA ORDEM DE SERVIÇO - OS

DATA DE INÍCIO EFETIVO	DATA DE CONCLUSÃO EFETIVA	TOTAL DE HORAS REALIZADA	
		NÍVEL 1	NÍVEL 2

DESCRIÇÃO / JUSTIFICATIVA

3. ENTREGA / VALIDAÇÃO DO SERVIÇO EXECUTADO

ASSINATURA/CARIMBO RESPONSÁVEL CONTRATADA	ASSINATURA / MATRÍCULA RESPONSÁVEL DATAPREV

4. ACEITE DA ORDEM DE SERVIÇO - OS

DATA DO ACEITE	ASSINATURA / MATRÍCULA RESPONSÁVEL DATAPREV

OBSERVAÇÃO: OS NÍVEIS DE SERVIÇO EXIGIDOS ESTÃO DESCRITOS NO ITEM ORIENTAÇÃO TÉCNICA DO TERMO DE REFERÊNCIA.