



# Consulta Pública da solução OFD – Online Fraud Detection



## Sumário

Consulta Pública .....	2
Especificação Técnica .....	3
1. OBJETO .....	3
2. ESPECIFICAÇÃO DO OBJETO .....	3
3. NÍVEIS DE SERVIÇO .....	11
6. SELEÇÃO DO FORNECEDOR .....	16
8. GERENCIAMENTO CONTRATUAL .....	18

## Consulta Pública (complementar)

O SERPRO vem por meio desta realizar um complemento a consulta pública Número 1023/23, com o objetivo de esclarecer e conhecer os impactos, riscos e oportunidades com a inclusão do seguinte item na especificação:

“A solução deverá conter tantos módulos ou subsistemas quanto necessários, mas deve ser suportada e possuir atualizações de versão através de um único fabricante”

Desta forma, caso o item seja acrescido na especificação, perguntamos:

1. Há impacto técnico na solução ofertada? Qual(is)?
2. Há impacto nos níveis de serviço da solução ofertada? Qual(is)?
3. Há impacto comercial e/ou financeiro na solução ofertada? Qual(is)?

# Especificação Técnica

## 1. OBJETO

- 1.1. Contratação da Solução OFD (*Online Fraud Detection*) no modelo SaaS de computação em nuvem para detecção e prevenção de fraudes com objetivo de combater o abuso de contas da plataforma Acesso Gov.br, prioritariamente, e demais sistemas do Serpro, suportando seus canais web e mobile.

## 2. ESPECIFICAÇÃO DO OBJETO

- 2.1. Solução OFD (*Online Fraud Detection*) no modelo SaaS de computação em nuvem para detecção e prevenção de fraudes com objetivo de combater o abuso de contas da plataforma Acesso Gov.br, prioritariamente, e demais sistemas do Serpro, suportando seus canais web e mobile.
- 2.2. Para este processo de contratação, entende-se como processo de controle de acesso as seguintes operações com credenciais de acesso listadas abaixo:
- 2.2.1. Login por meio de usuário e senha, Certificado Digital, Certificado em Nuvem, Qrcode e Bancos credenciados;
- 2.2.2. Criação de conta com base em usuário e senha, Certificado Digital e Bancos credenciados;
- 2.2.3. Recuperação de conta com base em Email/Celular, reconhecimento facial e bancos credenciados;
- 2.2.4. A solução OFD deve atuar sobre o processo de controle de acesso no contexto das aplicações Serpro, não contemplando a atuação em provedor de identidade externo.
- 2.2.5. Para este processo de contratação, entende-se como requisição de detecção de fraude a ação de uma aplicação Serpro chamar o serviço contratado (SaaS), (aplicação essa que foi integrada ao serviço contratado o qual está coletando parâmetros de utilização da aplicação pelo usuário, de acordo com o funcionamento do serviço detalhado nesse requisito), com objetivo de obter a informação de nota de risco calculada por esse serviço (conforme seu funcionamento também definido nesse requisito), avaliando o potencial de fraude na utilização da aplicação e executando as ações pertinentes.
- 2.3. Para a solução, a quantidade a ser adquirida é definida conforme tabela abaixo e subitens:

ITEM	Descrição	Unidade	Quantidade	Localidade
1	Solução em Nuvem OFD (Online Fraud Detection)	Licença para usuários protegidos	159.286.385	Brasília

- 2.3.1. Para este documento a palavra conta será utilizada como identificador para conta de usuário protegida;
- 2.3.2. Para o item 1, licença por conta de usuário protegida, refere-se à forma de contratação da solução, sendo medida a partir do número de contas cujo processo de controle de acesso foi protegido pela solução OFD durante o mês aferido;
- 2.3.3. A quantidade apresentada na tabela do item 0 refere-se ao quantitativo máximo previsto de contas de acesso a serem protegidas;
- 2.3.4. As licenças serão utilizadas até o quantitativo máximo previsto na coluna "Quantidade" do quadro apresentado no item 0, sendo o número de licenças utilizadas aferido mensalmente;
- 2.3.5. Para efeito da contratação e medição dos valores a serem pagos, considera-se que uma conta, tem origem a partir do uso da conta durante o mês aferido, sendo contabilizado como apenas 1 (uma) licença independente de sua utilização ser registrada mais de 1(uma) vez

durante o mês. A utilização da conta pelo menos 1 (uma) vez no mês aferido já caracteriza a utilização de 1 (uma) licença;

- 2.3.6. A CONTRATADA deve demonstrar e permitir a monitoração contínua do uso das licenças de forma a permitir a aferição mensal por meio de relatório;
- 2.3.7. A entrega do relatório de consumo mensal de licenças deve ser realizada até o quinto dia útil do mês subsequente;
- 2.3.8. Somente serão pagos os quantitativos aferidos e validados pelo Serpro;
- 2.4. O objeto a ser contratado deve atender todos os itens deste documento e são obrigatórios;
- 2.5. A solução deve ser fornecida com todas as funcionalidades aqui especificadas, requisitos funcionais e não funcionais, operando de forma funcional, com todos os seus componentes, sem custo adicional para o Serpro;

## **2.6. Administração e requisitos de operação da solução**

- 2.6.1. A solução, uma vez configurada em uma aplicação, deve ter a opção de desativar e ativar a detecção de fraude sem a necessidade de alterações na aplicação;
- 2.6.2. A solução deve possuir interface de gerência web para acompanhamento e gestão de todo o funcionamento da solução, considerando seus requisitos funcionais e não funcionais;
  - 2.6.2.1. A solução deve possibilitar a realização de consultas com filtros na interface web de gerência da solução.
  - 2.6.2.2. A solução deve permitir o controle de acesso a suas funcionalidades na interface de gerência web através da segregação de perfis de acesso com a granularidade de funcionalidade. De forma a permitir as configurações de perfis para operação e também para gestão da solução:
    - 2.6.2.2.1. Caso a solução mantenha um cadastro de usuários, deve disponibilizar uma SDK/API para gestão (criação, edição e remoção) desse cadastro;
  - 2.6.2.3. A solução deve prover interface de gerência Web que suporte, no mínimo, os navegadores e versões: Mozilla Firefox 102.6.0 ESR, Google Chrome 114.0.5735.134 e Microsoft Edge 115.0.1901.183 e versões posteriores para todos os navegadores elencados;
  - 2.6.2.4. A solução deve prover, na sua interface de gerência web, o acompanhamento da disponibilidade da solução.

## **2.7. Segurança/Privacidade (LGPD)**

- 2.7.1. Para fins de clareza nas definições aqui apresentadas, a palavra dado será utilizada como definição para dados, metadados e informações;
- 2.7.2. Para fins de clareza nas definições apresentadas neste documento, entende-se que toda e qualquer forma de acesso ao dado, fazendo uso da definição apresentada no item 2.7.1, seja em trânsito ou em repouso, é definida como tratamento de dados;
- 2.7.3. Para todo e qualquer dado que seja necessário o tratamento de dados, onde aqui se incluem, mas não se limita, dos usuários, dos dispositivos dos usuários, de perfil comportamental, os requisitos abaixo são obrigatórios:
  - 2.7.3.1. Os dados coletados pela solução devem ser apresentados ao Serpro, de preferência diretamente na console de administração web.
    - 2.7.3.1.1. A solução deve permitir a customização da coleta de informações, possibilitando habilitar ou desabilitar a coleta de alguma informação.
    - 2.7.3.1.2. O tratamento de dados pessoais e pessoais sensíveis para um funcionamento com maior precisão da solução, deve ser analisado e aprovado pelo controlador das aplicações que utilizarem a solução.
    - 2.7.3.1.3. A solução deve prover meios para anonimização ou pseudonimização dos dados pessoais ou pessoais sensíveis sempre que necessário sua apresentação.

- 2.7.3.2. Os dados devem ser protegidos por meio de criptografia, seja em trânsito ou em repouso.
- 2.7.3.2.1. A solução deve garantir que o tráfego de dados seja feito de forma criptografada, atendendo minimamente a versão TLS 1.2;
- 2.7.3.2.2. O fornecedor deve apresentar as certificações SOC 2 type 2, ISO 27001, ISO 27701 e, mínimo, FIPS 140-2 nível 3, que demonstrem a aplicação das melhores práticas de segurança da informação na disponibilização do ambiente computacional em nuvem que hospede a solução, evidenciando os esforços para proteção e privacidade de dados sob sua custódia e governança (geração/guarda) de chaves criptográficas, na prestação dos serviços objeto deste edital.
- 2.7.3.3. O tratamento e apresentação de dados pela solução de forma não criptografada, só poderá ser feito no contexto de operação da solução e por/para usuário Serpro devidamente habilitado na solução, gerando assim a devida auditoria.
- 2.7.4. O tratamento dos dados somente poderá ocorrer para fins estabelecidos nesse processo e diretamente relacionados ao funcionamento de um OFD, limitando-se pura e exclusivamente ao atendimento da finalidade aqui estabelecida.
- 2.7.5. Todo e qualquer dado somente poderá sofrer tratamento de dados em território brasileiro, não sendo permitida a transferência internacional de dados.
- 2.7.6. A solução deve suportar o registro de log para todo e qualquer tratamento de dados em qualquer das operações no funcionamento da solução.

## **2.8. Garantias sobre a segurança da solução – SaaS**

- 2.8.1. A CONTRATADA deve garantir a disponibilidade, confidencialidade, autenticidade e integridade das informações e dos dados sob sua guarda.
- 2.8.2. A CONTRATADA deve prover mecanismo de acesso protegido aos dados, por meio de criptografia, garantindo que apenas aplicações e usuários autorizados tenham acesso.
- 2.8.3. Para a parte da solução instalada em ambiente SaaS, a solução deve atender às diretrizes de segurança da Lei Nº 13.709, de 14 de agosto de 2018, da Norma Complementar 14/IN01/DSIC/SCS/GSIPR de 13 de março de 2018, da ISO/IEC 27017 e da ISO/IEC 27018. Além disso, deve prover mapeamento e descrição de tabelas e campos do banco de dados da solução que contenham dados sensíveis de usuário ou da aplicação.
- 2.8.4. A CONTRATADA deve dispor de recursos e soluções técnicas que garantam a segurança da informação dos dados do Serpro, incluindo os seguintes itens:
  - 2.8.4.1. Solução de controle de tráfego de borda do tipo firewall (norte-sul, leste-oeste, e de aplicações de forma similar ou superior);
  - 2.8.4.2. Solução de prevenção e detecção de intrusão (IDS/IPS, de forma similar ou superior);
  - 2.8.4.3. Solução de gestão de logs;
  - 2.8.4.4. Solução de gestão integrada de pacotes de correção (patches).
- 2.8.5. A CONTRATADA deve garantir que possui mecanismos de proteção contra-ataques cibernéticos, inclusive em infraestruturas subcontratadas.
- 2.8.6. Durante a vigência do Contrato, a CONTRATADA deve estar aderente às certificações que podem ser exigidas pelo Serpro, relacionadas com a capacitação dos técnicos residentes, segurança da solução, entre outras, visando a qualidade da prestação do serviço contratado.
- 2.8.7. A CONTRATADA deve preservar os dados do Serpro contra acessos indevidos e informar imediatamente e formalmente ao Serpro qualquer tentativa, inclusive por meios judiciais, de acesso a estes dados.
- 2.8.8. Durante a vigência do contrato, quando solicitado pelo Serpro, a CONTRATADA deve demonstrar que possui procedimentos documentados e testados para resposta a incidentes, tanto no tratamento interno quanto nos contatos com cliente e mídia.

- 2.8.9.A CONTRATADA deve identificar e corrigir quaisquer problemas de segurança relacionados à prestação do serviço objeto dessa contratação, sem qualquer custo adicional para o Serpro.
- 2.8.10. A CONTRATADA deve certificar que todos dados e informações do Serpro, hospedados no ambiente provido pela solução serão destruídos, sem possibilidade de recuperação, em até 30 (trinta) dias corridos após a solicitação do Serpro, com exceção dos dados necessários para atender requisitos legais.
- 2.8.11. A propriedade dos dados e informações gerados pelo Serpro no ambiente provido pela solução, a qualquer momento, durante a vigência, término ou expiração do contrato, será exclusivamente do Serpro.
- 2.8.12. A CONTRATADA deve garantir o acesso do Serpro a relatórios elaborados por empresa de auditoria especializada independente, propostos pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados.

## **2.9. Auditoria da solução**

- 2.9.1. A solução deve possuir uma trilha de auditoria para registro das ações administrativas e de configurações em todas as suas funcionalidades.
  - 2.9.1.1. Esse registro de auditoria deve permitir rastrear quando, quais as ações foram executadas e por qual usuário foi executada, mesmo no cenário de interações entre sistemas;
  - 2.9.1.2. A solução deve possibilitar a exportação e envio de todos os registros de auditoria para fontes externas;
  - 2.9.1.3. A solução deve armazenar os registros por um período mínimo de 12(doze) meses;

## **2.10. Requisitos Não Funcionais da solução**

- 2.10.1. O idioma utilizado pela solução e da documentação técnica deve ser em português do Brasil ou em inglês;
- 2.10.2. A documentação técnica, composta por, no mínimo manuais, de integração, uso de SDK, configuração, operação e documentação de APIs.
  - 2.10.2.1. A documentação deve ser disponibilizada em formato digital;
  - 2.10.2.2. A documentação de APIs deve seguir a especificação do OpenAPI ou conter a completude dos aspectos necessários para a completa utilização da solução, tais como documentação de recursos, esquemas de dados, parâmetros de consulta e caminho, respostas e autenticação e segurança.
- 2.10.3. A versão da solução deve ser a última disponível no mercado na data de entrega e durante a prestação dos serviços;
- 2.10.4. O serviço deve ter capacidade de atender adequadamente o quantitativo previsto no quadro referente ao item 0 e subitens;
- 2.10.5. A Solução deve possuir suporte e capacidade de tratamento para IPv4 e IPv6;
- 2.10.6. O módulo de administração da solução, conforme item 2.6, deve permitir a integração com Login Único do Serpro com autenticação através de Federação SSO (Single Sign-On) compatível com ao menos um dos seguintes protocolos, em ordem de prioridade:
  - 2.10.6.1. OpenID Connect 1.0 com implementação de Authorization Code Flow. Caso a Solução necessite utilizar Client público, deve ser implementada a extensão "Proof Key for Code Exchange" (PKCE).
  - 2.10.6.2. SAML 2.0 com implementação de assinatura e criptografia do payload SAML.
- 2.10.7. A solução deve ser capaz de responder de forma síncrona a requisição de detecção de fraude com tempo máximo de 150ms em, pelo menos 97% das requisições.;
- 2.10.8. A solução deve ser capaz de atender no mínimo 6 mil requisições de detecção fraude por segundo;
- 2.11. **Integrações da solução**

- 2.11.1. A solução deve disponibilizar API Rest para serem consumidas por outras aplicações externas independente da linguagem de programação utilizada;
- 2.11.1.1. O conjunto de APIs disponibilizadas deve apresentar as informações processadas e geradas pela solução de OFD considerando seu funcionamento, conforme requisitos definidos neste documento;
- 2.11.2. De forma desejável, a solução deve disponibilizar a opção de integração por Webhook (API callback).
- 2.12. Requisitos funcionais da solução**
- 2.12.1. A solução deve coletar dados durante o **processo de controle de acesso**, conforme item 2.2 e subitens, identificar padrões de comportamentos, características de dispositivo e perfil de utilização, realizar o cruzamento de informações mediante padrões, regras, inteligência artificial e aprendizado de máquina para determinação de nota de risco que indique potencial fraude ou abuso de conta, fornecendo a informação para que a aplicação integrada possa executar ações com base nessa nota de risco;
- 2.12.1.1. A solução deve permitir a marcação, por parte da equipe do Serpro, se determinado caso (nota de risco) é caracterizado ou não como fraude, de modo que a solução enriqueça as suas regras e utilize esse aprendizado no tratamento de futuros casos similares.
- 2.12.1.2. A solução deve atuar de forma transparente, sendo possível que o Serpro tenha pleno conhecimento e acesso a qualquer momento a todos os dados coletados, regras aplicadas, peso de cada regra e as métricas adotadas no cálculo da nota de risco.
- 2.12.2. A solução deve ter a capacidade de coletar e processar dados em larga escala.
- 2.12.3. A solução deve possuir um conjunto de regras que atenda ao objetivo de detecção e prevenção de fraudes relacionadas ao processo de controle de acesso e que possa ser aplicada desde o início da operação, sem a necessidade de aguardar que o processo de aprendizagem de máquina construa e agregue o conhecimento e informações necessárias para a identificação de fraudes e anomalias;
- 2.12.4. A solução deve possuir tecnologia de inteligência artificial com aprendizado de máquina que, de forma automática, compreenda novos comportamentos de risco e atualize suas regras de negócio com o objetivo de detecção e prevenção de fraudes relacionadas ao processo de controle de acesso;
- 2.12.5. A solução deve ser capaz de enriquecer suas regras a partir de bases de conhecimento construídas com dados e padrões de ameaças e fraudes já conhecidas;
- 2.12.6. A solução deve possibilitar a customização de regras para atendimento de necessidades específicas definidas pelo Serpro, possibilitando que esta customização também se dê a partir de qualquer dos parâmetros coletados, existentes e derivados.
- 2.12.7. A solução deve realizar identificação do dispositivo com emprego de técnicas combinadas que permitam realizar de forma inequívoca a identificação do dispositivo (Device Fingerprint).
- 2.12.7.1. O Device Fingerprint deve ser capaz de identificar novamente um mesmo dispositivo, mesmo em cenários em que cookies ou objetos locais sejam limpos.
- 2.12.8. A solução deve ter a capacidade de coletar e analisar informações para geração de biometria comportamental do usuário durante o processo de controle de acesso, considerando no mínimo as seguintes situações:
- 2.12.8.1. Colagem de informações em formulários;
- 2.12.8.2. Padrões de movimentação de mouse;
- 2.12.8.3. Padrões e ritmo de digitação;
- 2.12.8.4. No uso de dispositivos móveis a Inclinação, velocidade de swipe e pressão do toque;
- 2.12.8.5. Navegação anômala com base em conhecimento prévio da solução;
- 2.12.8.6. Padrões suspeitos com base em inteligência, como por exemplo acessos vindos de bots;
- 2.12.8.7. Tempo anormal na página;



- 2.12.8.8. Acessos de fuso horário incompatíveis com a origem;
- 2.12.8.9. Acessos fora do horário habitual do usuário com base em perfil comportamental;
- 2.12.8.10. Atividade identificadas como incomum usando um novo idioma no navegador;
- 2.12.8.11. Geolocalização ou cruzamento de antena ou IP;
- 2.12.9. Deve compreender e utilizar os padrões de biometria comportamental e de device *fingerprint*, para detectar o potencial de fraude do acesso que está sendo realizado pelo usuário, utilizando os itens abaixo descritos, mas não se limitando aos mesmos:
  - 2.12.9.1. Identificação de fraudadores conhecidos;
  - 2.12.9.2. Identificação de dispositivos conhecidos que são utilizados por fraudadores;
  - 2.12.9.3. Atividades identificadas como incomum usando um serviço de provedor de internet ou um serviço de hospedagem de conteúdo classificado como de alto risco;
  - 2.12.9.4. Acesso suspeito a múltiplas contas;
  - 2.12.9.5. Padrão de múltiplos acessos suspeitos para uma mesma conta;
  - 2.12.9.6. Acesso suspeito a uma conta de usuário com atributos diferentes daqueles normalmente vistos no dispositivo do usuário;
  - 2.12.9.7. Logins e demais ações realizadas para uma mesma conta de diferentes localizações geográficas dentro de um curto espaço de tempo, incluindo atividade incomum a partir de um novo país;
  - 2.12.9.8. Acesso identificado como suspeito a partir de um endereço IP classificado como de alto risco;
  - 2.12.9.9. Uso de um domínio de e-mail suspeito ou de origem duvidosa durante o processo de controle de acesso;
  - 2.12.9.10. Números de telefones identificados como suspeitos, em casos de acessos realizados por dispositivos móveis;
  - 2.12.9.11. Acesso a partir de um novo dispositivo desconhecido;
  - 2.12.9.12. Uso de uma conexão wireless insegura ou diferente do habitual;
- 2.12.10. Possuir a capacidade de avaliar, durante o processo de controle de acesso, e considerar no cálculo da nota de risco, no mínimo, os seguintes cenários suspeitos de ataques cibernéticos:
  - 2.12.10.1. Man-in-the-browser;
  - 2.12.10.2. Spoofing de IP;
  - 2.12.10.3. Spoofing de Geolocalização;
  - 2.12.10.4. Spoofing de identidade;
  - 2.12.10.5. Spoof de dispositivo;
  - 2.12.10.6. Account Take Over;
  - 2.12.10.7. Roubo de sessão;
  - 2.12.10.8. Acessos por Bots;
  - 2.12.10.9. Captura de credenciais, nas aplicações protegidas;
  - 2.12.10.10. Deve possuir mecanismos para identificar ataques por injeção de código no portal WEB que esteja integrado;
  - 2.12.10.11. Acesso remoto;
  - 2.12.10.12. Uso de proxy;
  - 2.12.10.13. Uso de VPN;
  - 2.12.10.14. Uso de Root/Jailbreak e hiders, em casos de acessos realizados por dispositivos móveis;
  - 2.12.10.15. Presença de overlay de tela;
  - 2.12.10.16. Acessos provenientes de ambiente virtual/emulado;
  - 2.12.10.17. Acessos provenientes de navegadores Tor ou similares;

### **2.13. Formas de uso**

- 2.13.1. A solução precisa funcionar para proteção de canais web e mobile e a CONTRATADA deve garantir que sejam obtidos os mesmos resultados na análise de nota de risco com o uso de Javascript, em páginas web, e SDK, em dispositivos móveis:
  - 2.13.1.1. Funcionar em qualquer navegador compatível com Javascript, especificação EcmaScript versões 5 ou 6;
    - 2.13.1.1.1. O Javascript utilizado pela solução deve ser necessariamente minificado e ofuscado.
  - 2.13.1.2. Utilizar uma SDK para uso em dispositivos móveis;
    - 2.13.1.2.1. A SDK deve suportar, no mínimo, as plataformas e versões ANDROID 24 (Nougat 7.0), IOS 13, Flutter 3.7.\* e Ionic 6, e versões posteriores para todas as plataformas elencadas.
- 2.13.2. A solução deve possibilitar seu funcionamento sem a necessidade de instalação de agentes nos clientes, sem comprometer qualquer funcionalidade prevista neste documento;
- 2.13.3. A solução deve permitir a integração sem exigir alterações que requeiram mudanças arquiteturais à aplicação usuária.
- 2.13.4. A solução deve executar sua função de forma transparente ao usuário final da aplicação usuária, não requisitando nenhuma atuação do mesmo;

### **2.14. Acompanhamento na utilização da solução (dashboards, relatórios)**

- 2.14.1. A solução deve gerar relatórios gerenciais na interface de gerência Web para qualquer das informações geradas e processadas pela solução, em tempo real. Os relatórios devem permitir no mínimo a análise dos scores gerados, o detalhamento do cálculo da nota de riscos inclusive com as informações coletadas e utilizadas.
  - 2.14.1.1. A solução deve possibilitar a realização de filtros e customizações de saída nos relatórios gerados.
    - 2.14.1.1.1. A solução deve suportar a emissão de relatórios com filtros de intervalo de tempo sobre os dados: diários, semanais, mensais e anuais;
    - 2.14.1.1.2. A geração dos relatórios deve permitir a apresentação de informações de forma detalhada e também de forma sumarizada (por exemplo: totalização de determinada informação).
  - 2.14.1.2. A solução deve suportar a emissão de relatórios gerados no formato PDF e formato CSV ou JSON;
- 2.14.2. A solução deve disponibilizar a visualização de Dashboard na interface de gerência web para qualquer das informações geradas e processadas pela solução, em tempo real.
  - 2.14.2.1. A solução deve permitir a customização dos dashboards permitindo filtros, gráficos e Drill-downs.
- 2.14.3. A solução deve ter recursos que permitam a monitoração em tempo real da solução considerando todo o funcionamento da análise da nota de risco, bem como o desempenho e a disponibilidade da mesma. Com isso ajudando as equipes de segurança a tomar medidas corretivas quando necessário.
  - 2.14.3.1. O monitoramento deve permitir no mínimo a avaliação do volume de requisição de detecção de fraude sendo solicitadas na linha do tempo, o comportamento de aplicação das regras no cálculo de scores e os alertas gerados.

### **2.15. Geração de Alertas pela solução**

- 2.15.1. A solução deve possibilitar a visualização de alertas por meio da interface de gerência Web;

- 2.15.2. A solução deve permitir a configuração de alertas, de forma independente ao da geração da nota de risco, conforme item 2.12.1, com base em diferentes critérios relacionados ao objetivo do OFD no processo de controle de acesso, permitindo uma ação do Serpro de forma imediata e adequada para lidar com as possíveis fraudes. Um exemplo da geração desses alertas, seria em casos de grande volume de notas baixas em determinado aspecto do cálculo da nota de risco.
- 2.15.2.1. A solução deve suportar a entrega desses alertas, no mínimo, em canais como e-mail, mensagem instantânea e Webhooks.

### 3. NÍVEIS DE SERVIÇO

#### 3.1. Garantia, Suporte e Atualização

- 3.1.1. O objeto especificado e seus componentes terão garantia de 12 (doze) meses, prorrogáveis por até o limite de 60 (sessenta) meses, contados a partir da data do recebimento definitivo;
- 3.1.2. O Serpro não terá nenhum ônus adicional com manutenção, operação, atualização, suporte, necessidade de ampliação do parque computacional e garantia de hardware e software que compõem a solução da CONTRATADA;
- 3.1.3. Os custos relativos aos serviços de suporte e atualização dos serviços prestados pela CONTRATADA são de total responsabilidade da mesma;
- 3.1.4. A CONTRATADA responsabilizar-se-á pelas ações executadas ou recomendadas por analistas e consultores de seu quadro, assim como pelos efeitos delas advindos na execução das atividades previstas neste contrato ou no uso dos acessos, privilégios ou informações obtidas em função das atividades por esta executada;
- 3.1.5. Comunicar, por escrito, ao Serpro, sempre que constatar condições inadequadas de funcionamento ou má utilização a que estejam submetidos os serviços objeto deste contrato, fazendo constar a causa de inadequação e a ação devida para a correção;
- 3.1.6. A CONTRATADA deve manter, durante a vigência do suporte e atualização, a correta integração entre os elementos que compõe a solução, nas mesmas condições de desempenho e confiabilidade que apresentavam no momento de emissão do Termo de Recebimento Definitivo;
- 3.1.7. O suporte e atualização contemplará atendimento técnico quanto à configuração e solução de problemas envolvendo a Solução e seus componentes;
- 3.1.8. O serviço de atualização deve incluir correções ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades;
- 3.1.9. A cada nova evolução, atualização, melhorias da Solução e recursos que a compõem, a CONTRATADA deve apresentar as novas funcionalidades e disponibilizá-las o Serpro, que analisará sua adesão e o impacto no modelo de negócio implementado, não havendo nenhum ônus adicional pela adesão;
- 3.1.10. Nas intervenções corretivas na Solução, em que haja risco de indisponibilidade total ou parcial, o Serpro deve ser previamente notificado para que se proceda a aprovação e o agendamento da operação em horário conveniente o Serpro e seus clientes;
- 3.1.11. É de inteira responsabilidade da CONTRATADA a entrega dos serviços contratados;
- 3.1.12. A garantia contemplará atendimento técnico quanto à configuração e solução de problemas envolvendo o produto fornecido, bem como a atualização de novos recursos na solução contratada;
- 3.1.13. As funções definidas para a solução neste documento devem ser mantidas em operação ininterrupta durante 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;
- 3.1.14. O serviço de atualização deve incluir correções ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades da solução contratada;
- 3.1.15. Durante o prazo de validade do contrato da solução, a CONTRATADA deve assegurar ao Serpro a prestação de serviços técnicos complementares relativos ao adequado funcionamento da solução, consideradas as suas especificações;
- 3.1.16. Caso a solução seja descontinuada na linha de comercialização do fabricante, durante o prazo de vigência contratual, a CONTRATADA deve manter a prestação de serviços, bem como dos serviços técnicos complementares relativos ao adequado funcionamento da solução, consideradas as suas especificações, sem quaisquer ônus adicionais.
- 3.1.17. A CONTRATADA deve comunicar quaisquer vulnerabilidades encontradas na solução e ainda não solucionadas, bem como o prazo para disponibilização de rotina ou versão que

solucione a falha detectada. Nos casos em que a vulnerabilidade permitir validações incorretas e/ou paralisação do ambiente, a CONTRATADA deve implementar medida de contorno para o restabelecimento do ambiente à condição operacional. A medida de contorno poderá permanecer ativa dentro de um prazo máximo de 30(trinta) dias.

### 3.2. Do Nível de Disponibilidade, Severidade e Sancionamentos

3.2.1. A garantia de disponibilidade operacional da solução deve ser realizada conforme critérios abaixo:

- 3.2.1.1. Os atendimentos aos chamados devem ser prestados 24 (vinte e quatro) horas por dia, e 7 (sete) dias por semana (à exceção dos chamados de severidade 4);
- 3.2.1.2. Os chamados de severidade 4 – Baixa devem ser prestados 9 (nove) horas por dia, das 8 às 17 horas, de segunda-feira a sexta-feira, excluindo os feriados;
- 3.2.1.3. O atendimento aos chamados para o exercício da garantia deve obedecer à seguinte classificação quanto ao nível de severidade, conforme Tabela:

Severidade	Descrição	Tempo de Atendimento	Tempo de solução	Penalidades
1 – Crítica	Chamados referentes a situações de emergências ou problema crítico, caracterizados pela existência de ambiente paralisado, casos de situações inesperadas e falsos positivos, marcação de fraudes como falsas ou verdadeiras que impactem um grande volume de usuários ou quando não estiver executando as funções especificadas	No máximo 1 (Uma) horas após a abertura do chamado	No máximo 2 (Duas) horas após o início do atendimento do chamado	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,15% (zero vírgula quinze por cento) do valor contratual, por hora ou fração de hora de atraso
2 – Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho	No máximo 2 (Duas) horas após a abertura do chamado	No máximo 8 (Oito) horas após o início do atendimento do chamado	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,1% (zero vírgula um por cento) do valor contratual, por hora ou fração de hora de atraso
3 – Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente, casos de troca de informações sobre fraudes e ataques para ajuste das políticas de detecção da solução	No máximo 4 (Quatro) horas após a abertura do chamado	No máximo 24 (vinte e quatro) horas após o início do atendimento do chamado	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,075% (zero vírgula zero setenta e cinco por cento) do valor contratual, por hora ou fração de hora de atraso
4 – Baixa	Chamados com objetivo de sanar dúvidas quanto ao uso ou à implementação da	No máximo 24 (vinte e quatro) horas após a abertura do	No máximo 72 (setenta e duas) horas após o início do atendimento do chamado	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,05% (zero vírgula zero cinco por

	solução, esclarecimentos da documentação, sugestões, solicitação de desenvolvimento de melhorias. Impacto mínimo para os usuários	chamado		cento) do valor contratual, por hora ou fração de hora de atraso
--	---	---------	--	---

- 3.2.1.4. Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento;
- 3.2.1.5. Durante o período de garantia, a CONTRATADA deve fornecer informações sobre as correções a serem aplicadas ou a própria correção;
- 3.2.1.6. Deve fornecer orientações para diagnóstico de problemas e ajuda na interpretação de trilhas, dumps e logs;
- 3.2.1.7. Nos casos de problemas não documentados, os registros enviados pelo Serpro (tais como: traces, dumps e logs) devem ser encaminhadas aos laboratórios do responsável técnico, a fim de que sejam fornecidas as devidas correções;
- 3.2.1.8. Deve possuir suporte técnico para toda a Solução, durante o período de vigência da garantia, assegurando prazo de atendimento;
- 3.2.1.9. A Disponibilidade Mensal do Serviço (DMS), para a solução e seus componentes, conforme especificações contidas neste documento deve ser de 99,9% (noventa e nove vírgula nove por cento);
- 3.2.1.10. A Disponibilidade Mensal do Serviço apurada será calculado pela seguinte fórmula:
- 3.2.1.10.1.  $DMS (\%) = (1 - (\text{Tempo Total de Interrupção Mensal} / \text{Tempo Total Mensal})) \times 100$ ;
- 3.2.1.11. Dever ser entendido como "Tempo Total de Interrupção Mensal" a soma de todos os tempos (em minutos) entre a(s) formalização do(s) registro(s) do(s) chamado(s) e a completa solução do(s) problema(s) com o respectivo fechamento entre o Serpro e a CONTRATADA, desde que não seja constatada responsabilidade do Serpro. O Serpro fará a formalização do registro de chamado nas seguintes situações:
- 3.2.1.11.1. A impossibilidade de direcionamento de tráfego das aplicações para a solução em nuvem da CONTRATADA, causados por problemas da CONTRATADA;
- 3.2.1.11.2. A impossibilidade de tratamento das requisições das aplicações causados por problemas da CONTRATADA;
- 3.2.1.11.3. A indisponibilidade das ferramentas de visibilidade e administração do serviço;
- 3.2.1.11.4. O não atendimento a qualquer um dos indicadores técnicos descritos neste documento;
- 3.2.1.12. Dever ser entendido como "Tempo Total Mensal" do serviço:
- 3.2.1.12.1. A quantidade de dias da prestação do serviço, expresso em minutos, considerando-se o mês comercial nos meses da ativação e da desativação do serviço;
- 3.2.1.12.2. A quantidade em minutos aferida para o mês corrente para os demais meses;
- 3.2.1.13. Ocorrências que se repitam em um período de menos de 03 (três) horas serão consideradas problemas intermitentes, sendo considerado o tempo decorrido entre a primeira e a última ocorrência para efeito de cálculo do tempo de interrupção;
- 3.2.1.14. Não serão computadas no cálculo do DMS, 2 (duas) interrupções anuais do serviço, agendadas, em comum acordo, com antecedência mínima de 15 (quinze) dias corridos, ou outro período concedido pela Serpro, sendo de no máximo 4 (quatro) horas de duração;
- 3.2.1.15. Falhas na infraestrutura sob responsabilidade da Serpro, que comprometam a disponibilidade do Serviço contratado, não acarretarão ônus à CONTRATADA;
- 3.2.1.16. O não atingimento dos requisitos dos itens 2.10.7 ou 2.10.8 será entendido como indisponibilidade do serviço;

### **3.3. Local de entrega e prestação dos serviços**

3.3.1. Regional Brasília/DF, SGAN, Av. L2 Norte Quadra 601 – Módulo G – Brasília, Distrito Federal, CEP: 70830-900, Telefone Geral: (61) 2021-9000, Inscrição Estadual: 07334743/002-94, Inscrição Municipal: 07334743/002-94, e CNPJ: 33.683.111/0002-80.

### **3.4. Chamados, Registro e Início de Prazos**

3.4.1. O atendimento aos chamados deve obedecer à tabela de classificação quanto ao nível de severidade, conforme Tabela apresentada no item 3.2.1.3;

3.4.2. O chamado será registrado na CONTRATADA, recebendo uma identificação para acompanhamento, controle e histórico;

3.4.3. O chamado fechado sem anuência do Serpro ou sem que o problema ou solicitação tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas;

3.4.4. Deve ser disponibilizado canal de atendimento e chamado técnico, disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de sítio na Internet e canal telefônico gratuito, independente da região do Brasil de origem da ligação;

3.4.5. Atendimento a chamados

3.4.5.1. Para todos os efeitos da contratação em espécie, vigoram os seguintes conceitos:

3.4.5.1.1. Suporte Técnico de Primeiro Nível: equipe treinada para atender diretamente os usuários em demandas referentes a diagnóstico e tratamento de problemas, configuração e administração do ambiente e esclarecimento de dúvidas em geral;

3.4.5.1.2. Suporte Técnico de Segundo Nível: equipe multidisciplinar treinada, certificada e com grande experiência em ambientes críticos e complexos, que exigem alta disponibilidade;

3.4.5.1.3. Suporte Técnico de Terceiro Nível: escalonamento obrigatório ao fabricante, devido à necessidade de retaguarda nas tecnologias suportadas;

3.4.5.2. A CONTRATADA deve prover acesso para suporte técnico de 2º e 3º níveis no suporte a solução, sem ônus adicional para Serpro;

3.4.5.3. O serviço de suporte técnico deve ser prestado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e sem número limite de chamados, para toda a solução contratada, por técnicos devidamente habilitados e sem qualquer ônus adicional;

3.4.5.4. Para o suporte a chamados a CONTRATADA deve disponibilizar, sempre que solicitado pelo Serpro, profissionais com capacidade técnica para analisar, mitigar e soluções questões relativas à contratação.

3.4.5.5. A CONTRATADA concederá ao Serpro suporte integral durante todo o período do contrato com atendimento 24 horas por dia e 7 dias por semana e sem número limite de chamados, a contar da data de instalação, contra qualquer defeito que a solução venha a apresentar;

3.4.5.6. O suporte técnico será acionado em caso de quaisquer indisponibilidades da Plataforma CONTRATADA, devendo haver o atendimento conforme Tabela apresentada no item 3.2.1.3

3.4.5.7. As informações referentes aos chamados efetuados pelo Serpro deverão, logo que registradas, estar disponíveis para consultas no ambiente de portal help desk disponibilizado pela CONTRATADA, pelo período de vigência do contrato, contado a partir da data de fechamento do chamado;

3.4.5.8. O atendimento aos chamados deve ser realizado em conformidade com os itens estabelecidos neste Termo e devem conter no mínimo as seguintes informações:

3.4.5.8.1. Número de acionamento;

3.4.5.8.2. Descrição da ocorrência;

3.4.5.8.3. Localidade;

3.4.5.8.4. Severidade;



- 3.4.5.8.5. Nome do responsável do Serpro pela abertura do chamado;
- 3.4.5.8.6. Data e hora de abertura do chamado;
- 3.4.5.8.7. Data e hora do início do atendimento;
- 3.4.5.8.8. Tipo do atendimento;
- 3.4.5.8.9. Data e hora de encerramento;
- 3.4.5.8.10. Descrição da resolução adotada;
- 3.4.5.9. O Portal de help desk deve permitir a realização de consultas e impressão de relatórios, individualizados ou cumulativos, por número do chamado, status, data/período de abertura, unidade responsável pela abertura, técnico encarregado do atendimento e chamados com falhas de atendimento;
- 3.4.5.10. Ao receber uma solicitação de abertura de chamado, o atendente deve registrar as informações relativas ao mesmo (responsável pela abertura, descrição do problema, etc) e fornecer o número que lhe foi atribuído;
- 3.4.5.11. Ao receber uma ligação para um chamado já aberto, o atendente deve solicitar o número que lhe foi atribuído por ocasião da abertura, registrar as novas informações passadas e transmiti-las ao técnico responsável pelo acompanhamento e resolução;
- 3.4.5.12. Quando as informações e solicitações passadas exigirem uma nova interlocução com o Serpro, de forma análoga aos procedimentos de abertura, o técnico responsável pelo acompanhamento e resolução do chamado deve entrar em contato com o responsável pela abertura em prazo inferior ao prazo definido como tempo de solução apresentado na Tabela do item 3.2.1.3, visando solucionar o chamado dentro do tempo de solução estabelecido para o nível de criticidade do chamado;
- 3.4.5.13. Quando solucionados, os chamados deverão ser fechados pelo responsável pelo atendimento, de comum acordo com o Serpro, não sendo admitido, em nenhuma hipótese, o fechamento de chamados sem o consentimento do responsável pela abertura.

#### **3.4.6. Canais de Atendimento**

- 3.4.6.1. Atendimento por meio site da Internet, através de portal para abertura de chamados, e de canal telefônico gratuito 0800 ou tarifação reversa, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;
- 3.4.6.2. A CONTRATADA deve fornecer suporte técnico no Brasil, obrigatoriamente em língua portuguesa, falada no Brasil para prestar atendimento e resolver todos os problemas relacionados às possíveis falhas ou interrupções de funcionamento da solução proposta, sempre que solicitado pelo Serpro;
- 3.4.6.3. A CONTRATADA deve disponibilizar por meio da Internet uma aplicação WEB para registro dos chamados de suporte técnico através de login e senha fornecida para os usuários autorizados do Serpro. De modo a assegurar alta disponibilidade do canal de suporte técnico para o Sistema fornecido, o registro de chamados deve estar disponível em regime de 24x7x365 (vinte e quatro horas por dia durante todos os dias do ano, inclusive sábados, domingos e feriados);
- 3.4.6.4. Cada pessoa cadastrada no sistema como usuário deve receber identificação e senha que permitam acesso seguro tanto ao sistema, como ao recurso de abertura de chamadas de suporte técnico, de maneira a evitar que pessoas não autorizadas possam acionar o serviço;

#### **3.4.7. Entrega Mensal de Relatórios**

- 3.4.7.1. Mensalmente deve ser entregue relatório constando os acionamentos técnicos abertos, em andamento e encerrados no período do exercício da garantia;
- 3.4.7.2. O relatório deve conter no mínimo as seguintes informações: número de acionamento, descrição da ocorrência, localidade, severidade, nome do responsável do Serpro pela abertura do chamado, data e hora de abertura do chamado, data e hora do início do



atendimento, tipo do atendimento, data e hora de encerramento e descrição da resolução adotada;

- 3.4.7.3. O relatório deve ser entregue mesmo quando não houver chamados no período;
- 3.4.7.4. A entrega do relatório deve ser realizada até o quinto dia útil do mês subsequente;
- 3.4.7.5. A entrega dos relatórios mensais será condição necessária para o Serpro realizar o ateste da nota fiscal e/ou fatura, para fins de pagamento dos serviços executados;

**4. Item reservado para ações futuras**

**5. Item reservado para ações futuras**

## **6. SELEÇÃO DO FORNECEDOR**

6.1. A contratação será na Modalidade de Pregão na forma eletrônica, conforme disposto no Art. 32, inciso IV, da Lei nº 13.303/2016 c/c Lei nº 10.520/2002.;

6.2. Será considerada vencedora do processo licitatório a LICITANTE que apresentar a proposta com o menor valor global.;

**6.3. Documentação Técnica do Fabricante:**

6.3.1. A LICITANTE com a proposta de menor preço, deve apresentar no prazo estipulado pelo pregoeiro, documentação técnica do fabricante da solução comprovando o atendimento a todos os requisitos contidos na Especificação do objeto a ser contratado;

6.3.2. A LICITANTE deve fornecer uma planilha ponto-a-ponto indicando documento e página onde consta o cumprimento de cada um dos requisitos das especificações técnicas;

6.3.3. Não serão aceitas referências a futuros releases ou versões de produtos para comprovar a existência ou aderência a qualquer quesito desta especificação;

6.3.4. Cada documento apresentado deve descrever claramente a referência ao modelo apresentado na proposta, não sendo válidas referências genéricas;

6.3.5. Será aceita Carta do Fabricante, como comprovação de atendimento de requisitos técnicos e de compatibilidade especificados neste Edital, apenas para os itens que não constarem na documentação da maioria dos fabricantes ou que não puderem ser mensurados;

6.3.6. Caso a documentação apresentada, deixe de comprovar o atendimento de qualquer item da especificação técnica, a proposta será desclassificada, não passando para a etapa seguinte de testes das funcionalidades especificadas;

6.3.7. Todas as configurações descritas e que serão homologadas, além de estarem identificadas, garante não só à LICITANTE VENCEDORA, como seus concorrentes mensurar esses resultados, pois trata-se de SERVIÇO COMUM, onde todos oferecem as mesmas condições descritas para uso;

**6.4. Avaliação de Amostra**

6.4.1. Ao licitante classificado em primeiro lugar, o CONTRATANTE exigirá avaliação de amostra, que consiste na comprovação de funcionalidades descritas nas especificações do objeto deste Edital;

6.4.2. Após o aceite da documentação comprobatória, a LICITANTE vencedora deve disponibilizar todos os recursos necessários para a realização de avaliação de amostra;

6.4.3. A CONTRATADA deve disponibilizar um ambiente operacional que possibilite a realização dos testes de amostra, conforme o especificado no item 6.4.9.

6.4.4. A entrega da Solução e licenças necessárias à avaliação de amostra deve ocorrer em até 10 (dez) dias corridos contados a partir da solicitação formal do Serpro;

6.4.5. O prazo de execução da avaliação de amostra será de 20 (vinte) dias corridos a contar da entrega;

6.4.6. O prazo de avaliação de amostra poderá ser prorrogado a critério do Serpro;

6.4.7. A aceitação final da proposta da LICITANTE VENCEDORA somente será realizada após a aprovação em testes de bancada, na avaliação de amostra, descritas nesta seção;

- 6.4.8. Esta etapa caberá à LICITANTE VENCEDORA, para todos os itens e subitens especificados para a avaliação de amostra, comprovar na prática, por meio dos testes de bancada, nas etapas da avaliação de amostra, das características e funcionalidades exigidas
- 6.4.9. Será absolutamente imprescindível para os testes de bancada, a comprovação dos seguintes itens: 2.6.1; 2.6.2; 2.6.2.1; 2.6.2.2; 2.6.2.2.1; 2.6.2.3; 2.6.2.4; 2.9.1; 2.9.1.1; 2.9.1.2; 2.9.1.3; 2.12.1.1; 2.12.6; 2.12.8; 2.12.8.1; 2.12.8.8; 2.12.9; 2.12.9.4; 2.12.9.5; 2.12.9.6; 2.12.10; 2.12.10.10; 2.12.10.14; 2.12.10.15; 2.14; 2.14.1; 2.14.1.1; 2.14.1.1.1; 2.14.1.1.2; 2.14.1.2; 2.14.2; 2.14.2.1; 2.14.3; 2.14.3.1; 2.15.1; 2.15.2; e 2.15.2.1
- 6.4.10. Esta etapa será executada por prepostos do Serpro em conjunto com os prepostos das LICITANTES no ITEM específico da aquisição;
- 6.4.11. Os testes de bancada, nas etapas da avaliação de amostra, serão realizados nas dependências do Serpro, endereço descrito no subitem a seguir:
- 6.4.11.1. Regional Brasília/DF, SGAN, Av. L2 Norte Quadra 601 – Módulo G – Brasília, Distrito Federal, CEP: 70830-900, Telefone Geral: (61) 2021-9000, Inscrição Estadual: 07334743/002-94, Inscrição Municipal: 07334743/002-94, e CNPJ: 33.683.111/0002-80;
- 6.4.12. Todos os testes de bancada, nas etapas da avaliação de amostra, e relacionamento dos técnicos da LICITANTE com o Serpro devem ser efetuados no idioma português;
- 6.4.13. Ao fim de cada dia de testes de bancada, nas etapas da avaliação de amostra, deve ser emitida, assinada e distribuída Ata de Atividades e Ocorrências a todos os presentes até o próximo dia;
- 6.4.14. Se um subitem referente às especificações for considerado não atendido, não sendo corrigidos nos prazos estabelecidos, a proposta, em avaliação de amostra, será totalmente desclassificada;
- 6.4.15. Cada LICITANTE poderá indicar previamente os nomes de, no máximo, 02 (dois) técnicos nas etapas da avaliação de amostra. Esses técnicos deverão ser representantes legais da LICITANTE, comprovado por meio de documentação de vínculo contratual ou procuração;
- 6.4.16. Entre os técnicos indicados apenas 1 (um) técnico poderá acompanhar os testes de avaliação de amostra;
- 6.4.17. A critério da LICITANTE de melhor oferta, as etapas da avaliação de amostra poderão ser executadas com apoio de no máximo um técnico do fabricante;
- 6.4.18. As indicações devem ser realizadas com, no mínimo, 2 (dois) dias úteis de antecedência e apenas serão permitidos questionamentos diretos aos técnicos do Serpro;
- 6.4.19. No caso de ausência, em qualquer dos períodos durante a realização dos testes de bancada, nas etapas da avaliação de amostra, dos técnicos indicados pelas demais empresas concorrentes do pregão, não serão aceitos quaisquer questionamentos sobre sua realização;
- 6.4.20. Durante a realização dos testes de bancada, nas etapas da avaliação de amostra, serão permitidas somente 02 (duas) atualizações de software e sistema operacional da Solução sob avaliação, visando a correção ou adaptação para atendimento aos requisitos do edital. Essas atualizações poderão corrigir mais de um item simultaneamente;
- 6.4.21. A critério do Serpro os testes de bancada, nas etapas da avaliação de amostra, poderão ser reiniciados após atualização de versão;
- 6.4.22. Os testes deverão ser realizados no horário compreendido entre 09:00 e 17:00 de segunda-feira a sexta-feira;
- 6.4.23. A avaliação de amostra da Solução ofertada deve ser instalada sem nenhum custo para o Serpro;
- 6.4.24. A licitante que for reprovada na avaliação de amostra não terá direito a qualquer indenização;
- 6.4.25. Será emitido um relatório descrevendo os exames realizados e contendo a aprovação ou não da avaliação de amostra;

- 6.4.26. Somente após todos os testes de bancada, nas etapas da avaliação de amostra, será emitido o parecer técnico aprovando ou não a amostra apresentada;
- 6.4.27. A documentação, bem como os manuais necessários para a homologação, deve estar disponível para os representantes do Serpro;

## **7. Item reservado para ações futuras**

## **8. GERENCIAMENTO CONTRATUAL**

- 8.1. O prazo de vigência do presente contrato é de 12 (doze) meses, contados a partir de \_\_/\_\_/\_\_, podendo ser prorrogado mediante assinatura de Termo Aditivo que indique a respectiva provisão orçamentária, limitada sua duração a 60 (sessenta) meses;

### **8.2. Obrigações da contratada**

- 8.2.1. A CONTRATADA deve executar atividades com diversos níveis de complexidade, de modo a garantir a adequada execução da solução, compreendendo funções de desenvolvimento, atividades relacionadas ao serviço de detecção e tratamento de fraudes, avaliações de falsos positivos, tuning de regras e avaliação dos comportamentos da solução, apoio estratégico na arquitetura dos projetos, instalação, definição de arquitetura de produção, integração com sistemas complementares à Solução, definição da segurança dos ambientes da Solução e configuração do ambiente da Solução.

### **8.3. Repasse de Conhecimento**

- 8.3.1. A CONTRATADA deve prover o repasse de conhecimento para os profissionais da CONTRATANTE para configuração, operação e gestão da solução e seus componentes;
- 8.3.2. A CONTRATADA deve repassar o conhecimento sem ônus adicional para a CONTRATADA, incluindo todo o material didático necessário;
- 8.3.3. O material de aula deve abordar conteúdo teórico e prático, e deve ser submetido a CONTRATADA para aprovação antes da realização do repasse;
- 8.3.4. O material didático referente ao repasse de conhecimento e gravações em vídeo do repasse deverão ser apresentados em língua portuguesa do Brasil;
- 8.3.5. O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE;
- 8.3.6. A CONTRATADA será responsável por fornecer todo o material didático necessário para a realização do repasse de conhecimento;
- 8.3.7. Após a assinatura do contrato, a CONTRATADA deve realizar o repasse do conhecimento da Plataforma e seus componentes;
- 8.3.8. A CONTRATADA deve repassar o conhecimento através de profissionais habilitados e credenciados pelos fabricantes ou empresa credenciada para tal finalidade;
- 8.3.9. Deverá ser apresentado com até 10(dez) dias de antecedência do repasse de conhecimento a declaração que os profissionais são habilitados para ministrar o curso;
- 8.3.10. Deve ser entregue pela CONTRATADA, até 10(dez) dias antes do início do repasse de conhecimento a ementa;
- 8.3.11. A ementa deve estar no idioma português, e conter nome, objetivo, conteúdo programático e carga horária que será aprovada pela CONTRATANTE e todo o material didático;
- 8.3.12. A CONTRATADA deve providenciar o repasse de conhecimento para 2 (duas) turmas em Brasília, com capacidade para 15 (quinze) participantes cada, abordando toda solução

contratada envolvendo teoria e prática, em datas a serem negociadas entre a CONTRATANTE e a CONTRATADA.

- 8.3.13. A carga horária mínima para cada turma deve ser de 40 (quarenta) horas;
- 8.3.14. O repasse de conhecimento poderá ser realizado na modalidade online de forma síncrona e será de responsabilidade da CONTRATADA;
- 8.3.15. A CONTRATADA deve disponibilizar toda infraestrutura necessária ao repasse de conhecimento;
- 8.3.16. O repasse de conhecimento deve abordar conteúdos relativos à operação básica e avançada de todas as soluções, ferramentas e recursos que compõem a solução;
- 8.3.17. Todo o conteúdo relativo à gestão e operação básica e avançada da solução e seus componentes deve abranger teoria e prática:
  - 8.3.17.1. Todas as funções relativas à operação e gestão da solução e seus componentes deve abranger abordagem *hands on* (realização prática das atividades) por meio de laboratórios, estudos de caso e execução prática de operação e gestão;
- 8.3.18. Ao final do repasse de conhecimento, funcionários definidos pela CONTRATANTE devem obrigatoriamente estar aptos a gerir e operar a Plataforma e seus componentes, efetuando gestão, operação e configuração avançada das funcionalidades do(s) console(s);
- 8.3.19. O repasse de conhecimento deve ser gravado para fins de disseminação junto ao corpo técnico do CONTRATANTE;
- 8.3.20. Ao final do repasse de conhecimento, a CONTRATANTE, por meio do formulário especificado pela CONTRATANTE, fará a avaliação do repasse ministrado para emissão de termo de aceite, a qual a CONTRATADA deve obter a média de 70% (setenta por cento) de conceitos "bom e/ou ótimo";
- 8.3.21. Caso não atinja o conceito mencionado na subcláusula anterior, a CONTRATANTE encaminhará um relatório a CONTRATADA informando o que deve ser adequado para a realização de um novo repasse;
- 8.3.22. A CONTRATADA deve encaminhar a CONTRATANTE as alterações para análise e aprovação;
- 8.3.23. Se aprovado, o prazo do novo repasse de conhecimento deve ser acordado com a equipe da CONTRATANTE;
- 8.3.24. Após cada repasse a CONTRATADA deve ser emitido certificado para cada participante de acordo com a carga horária;
- 8.3.25. O certificado deve conter as seguintes informações: nome completo do participante, nome do repasse de conhecimento, período de realização, carga horária e conteúdo programático;
- 8.3.26. O(s) certificado(s) deverá(ão) ser(ão) encaminhado(s) ao responsável da Universidade Corporativa do Serpro na localidade onde ocorreu o repasse de conhecimento;
- 8.3.27. Deverá ser disponibilizado material didático impresso e em formato eletrônico, sem custo adicional para o CONTRATANTE, devendo ainda estar em língua portuguesa (Brasil);
- 8.3.28. Deverão ser fornecidos manuais de gestão, operação e configuração de todas as ferramentas, soluções e recursos que compõem a solução contratada necessários à completa operacionalização dos recursos exigidos nesta especificação, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês).