

1. OBJETO

1.1. Avaliar via consulta pública o processo de contratação da Solução OFD (Online Fraud Detection) em nuvem para detecção, identificação, prevenção e combate a fraudes e abuso de contas para a plataforma Acesso Gov.br.

2. ESPECIFICAÇÃO DO OBJETO

2.1. Solução OFD (Online Fraud Detection) em nuvem para detecção, identificação, prevenção e combate a fraudes e abuso de contas para a plataforma Acesso Gov.br;

2.2. Para este processo, entende-se como processo de controle de acesso o processo de login e operação de credenciais de acesso listadas abaixo:

2.2.1. Login por meio de CPF e senha, Certificado Digital, Certificado em Nuvem, Qrcode e Bancos credenciados;

2.2.2. Criação de conta com base em CPF e senha, Certificado Digital e Bancos credenciados;

2.2.3. Recuperação de conta com base em Email/Celular, reconhecimento facial e bancos credenciados;

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	134.515.652	Brasília

2.3.1. Para o item 1, licença para usuários protegidos, refere-se a forma de contratação da solução em nuvem para prevenção, detecção e combate a fraudes e abuso de contas para contas de acesso da plataforma Acesso Gov.br, sendo medida a partir do número de usuários protegidos que utilizaram a solução durante o mês aferido;

2.3.2. A quantidade apresentada na tabela do item 2.2 refere-se ao quantitativo máximo previsto de contas de acesso a serem protegidas;

2.3.3. Para efeito da contratação e medição dos valores a serem pagos, considera-se que uma conta protegida, licença para usuários protegidos, tem origem a partir do uso da conta durante o mês aferido, sendo contabilizado como apenas 1 (uma) licença para usuário protegido independente de sua utilização ser registrada mais de 1 (uma) vez durante o mês. A utilização de pelo menos 1 (uma) vez no mês aferido já caracteriza 1 (uma) licença para usuário protegido;

2.3.4. O integrador ou o representante da solução no Brasil será responsável por realizar a conversão do modelo de comercialização do fabricante, caso o fabricante não possua modelo de comercialização conforme estabelecido neste termo, no modelo de contratação descrito no quadro apresentado no item 2.2 e subitens, os valores serão pagos conforme medição realizada a cada mês, onde serão identificados os volumes a serem pagos;

2.4. O objeto a ser contratado deve atender todos os itens deste documento e são obrigatórios;

2.5. Da operacionalização das licenças

2.5.1. As licenças serão utilizadas até o quantitativo máximo previsto na coluna “Quantidade” do quadro apresentado no item 2.2, sendo o número de licenças utilizadas aferido mensalmente;

2.5.2. A CONTRATADA deverá monitorar os quantitativos utilizados e indicar ao SERPRO os volumes consumidos durante o mês de aferição por meio de relatório;

2.5.3. A entrega do relatório deve ser realizada até o quinto dia útil do mês subsequente;

2.5.4. O SERPRO analisará as medições e relatórios recebidos e validará as informações com evidências identificadas internamente;

2.5.5. Somente serão pagos os quantitativos aferidos e validados pelo SERPRO;

2.5.6. Os itens serão entregues na localidade do SERPRO, na Regional Brasília;

2.5.7. As versões de licenças da solução devem ser as últimas disponíveis no mercado na data de entrega e durante a prestação dos serviços;

2.5.8. O idioma utilizado pela solução e da documentação técnica deve ser em português do Brasil ou em inglês;

2.5.9. A documentação técnica, composta por manuais de instalação, configuração e operação poderá ser em formato digital;

2.6. Tratamento dos dados

2.7. Para fins de clareza nas definições aqui apresentadas, a palavra dado será utilizada como definição para dados, metadados e informações;

2.8. 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, seja em trânsito ou em repouso, é definida como tratamento de dados;

2.8.1. 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, comportamentais, biométricos, os requisitos abaixo são obrigatórios:

2.8.1.1. Os dados devem ser definidos pelo SERPRO, não sendo permitido qualquer ação sobre demais dados que não tenham sido expressamente definidos;

2.8.1.2. Os dados devem ser protegidos por meio de criptografia, seja em trânsito ou em repouso, e as chaves criptográficas devem estar sob posse do SERPRO;

2.8.1.3. Os dados em forma não criptografada somente poderão sofrer tratamento de dados por representantes do SERPRO;

2.8.1.4. O tratamento dos dados somente poderá ocorrer para fins de identificação, criação de perfis de comportamento dos usuários da plataforma Acesso Gov.br com o objetivo de possibilitar a identificação de comportamentos que caracterizem possíveis fraudes ou abuso de conta e geração de notas de risco que serão fornecidas a plataforma Acesso Gov.br para tomada de decisão;

2.8.2. Não é permitido o armazenamento de dados da plataforma Acesso Gov.br, bem como informações derivadas que tenham possibilidade mínima de reversibilidade e obtenção de dados pessoais ou pessoais sensíveis dos usuários da plataforma Acesso Gov.br sem autorização prévia do SERPRO;

2.8.2.1. Todo e qualquer dado somente poderá sofrer tratamento de dados em território brasileiro, não é permitido tratamento de dados da plataforma Acesso Gov.br fora da jurisdição brasileira;

2.9. Características Gerais da Solução

2.9.1. A solução deve coletar dados, identificar possíveis fraudes e abuso de contas e executar as ações definidas nas políticas definidas pelo SERPRO, bem como gerar as notas de risco

através de um conjunto de inteligência e políticas geradas pela solução a partir do processamento dos dados e comparações com padrões comportamentais e fornecer estas informações para a plataforma Acesso Gov.br para tomada de decisões com o objetivo de proteger o processo de controle de acesso;

2.9.2. A solução deverá coletar dados durante o processo de controle de acesso, conforme item 2.2, identificar padrões de comportamentos e perfil de utilização existente, realizar o cruzamento de informações mediante padrões, regras e inteligência da solução para determinação de nota de risco que indique grau de risco para potencial fraude ou abuso de conta e fornecer a informação para que a plataforma Acesso Gov.br possa executar ações com base na nota de risco fornecida;

2.9.2.1. A solução deve possuir um conjunto de regras que atenda ao objetivo de proteção contra fraudes e ameaças relacionadas ao processo de controle de acesso e que possa ser aplicada desde o início da operação;

2.9.2.2. A solução deve possuir tecnologia de aprendizado de máquina que, de forma automática, compreenda novos comportamentos de risco e atualize suas regras de negócio para utilização na proteção do processo de controle de acesso;

2.9.2.3. 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;

2.9.3. A solução deve possibilitar a customização de regras para atendimento de necessidades específicas definidas pelo SERPRO;

2.9.4. Não serão aceitas soluções que se encontrarem na situação de end-of-support ou end-of life, ou seja, com alguma previsão de descontinuidade de fornecimento, suporte ou vida;

2.9.5. O serviço deve ter capacidade e garantia de atendimento com base no quantitativo previsto no quadro referente ao item 2.2 e subitens;

2.9.6. A solução deve ser fornecida com todas as funcionalidades aqui especificadas, operando de forma funcional, com todos os seus componentes, sem custo adicional para o SERPRO;

2.9.7. A solução deve garantir que todas as requisições e tráfego de dados seja feita de forma criptografada, atendendo minimamente a versão TLS 1.2;

2.9.8. A solução, uma vez configurada, deve ter a opção de ser desativada e ativada sem a necessidade de alterações na plataforma Acesso Gov.br;

2.9.9. O tratamento de dados realizado pela solução deve ser compatível com as finalidades informadas no item 2.6 e subitens, limitando-se pura e exclusivamente ao atendimento dessas finalidades.

2.9.10. A solução deve disponibilizar relatórios gerenciais com informações sobre a identificação, análise, detecção e tomada de decisão relativo as ações executadas, possíveis fraudes e abuso de contas;

2.9.11. A solução deve abranger todo o serviço de inteligência para a proteção das contas de acesso da plataforma Acesso Gov.br, contemplando recursos tecnológicos e de pessoal para identificação de riscos e tratamento de fraudes, compreendendo novos comportamentos de risco, além de novos ataques digitais e, baseando-se nesta compreensão, criar novas regras e conhecimento para proteção das contas de acesso da plataforma Acesso Gov.br;

2.9.12. A solução deve atuar em todas as requisições executadas pelas contas de acesso da plataforma Acesso Gov.br, compreendendo o processo de controle de acesso, conforme item 2.2 e subitens;

2.9.13. A solução deve suportar os registros das operações do sistema e das ações de início e término de sessão durante a operação e gestão da solução em todas as interações com a plataforma Acesso Gov.br e usuários;

2.9.14. A solução deve possuir uma trilha de auditoria para que as alterações de configurações sejam mostradas quando necessário, informando quando foram executadas e por qual usuário, mesmo usuários de sistemas e interações entre sistemas;

2.10. Arquitetura e Implantação

2.10.1. A Solução em nuvem será entregue ao SERPRO como serviço gerenciado;

2.10.2. A Solução ofertada pela CONTRATADA deve possuir suporte e capacidade de tratamento para IPv4 e IPv6;

2.10.3. A Solução ofertada pela CONTRATADA 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:

2.10.3.1. OpenID Connect 1.0 com implementação de Authorization Code Flow. Caso a aplicação necessite utilizar Client público, deverá ser implementada a extensão "Proof Key for Code Exchange" (PKCE).

2.10.3.2. SAML 2.0 com implementação de assinatura e criptografia do payload SAML.

2.10.4. Caso a solução mantenha uma base com informações de usuários, deve disponibilizar uma SDK/API para gestão (criação, edição e remoção) dessas contas de usuários;

2.10.4.1. A solução deve atuar no modelo Sempre Ativo (Always-On), mas também possibilitar que o tratamento das requisições seja desativado quando necessário;

2.10.5. A CONTRATADA deve ser capaz de disponibilizar o serviço de adaptação e implementação na fase de configuração inicial para garantir a configuração adequada da solução em um ambiente de produção, sem causar nenhum tipo de impacto a plataforma Acesso Gov.br;

2.10.6. A CONTRATADA deve possibilitar a comunicação em português por meio de recursos que garantam a segurança na comunicação com os especialistas da CONTRATADA durante as interações necessárias com as equipes do SERPRO;

2.10.7. A solução deve possuir uma plataforma centralizada de análise de informações coletadas durante as requisições com inteligência para identificação e tratamento de ameaças digitais para a prevenção, identificação e tratamento de fraudes e abuso de contas e ações nocivas contra as contas de acesso da plataforma Acesso Gov.br;

2.10.8. As informações que serão analisadas pela plataforma centralizada serão coletadas por meio de análise das requisições, através de Javascript ou SDK;

2.10.8.1. O Javascript utilizado pela solução deve ser necessariamente ofuscado.

2.10.9. A solução deve realizar a obtenção de informações, device fingerprint, através do uso de Javascript, análise conjunta das requisições e SDK nos dispositivos móveis, bem como nos computadores pessoais, quando os mesmos forem utilizados:

2.10.9.1. O SERPRO não utilizará obrigatoriamente bibliotecas SDK nos dispositivos móveis, nesta situação, a CONTRATADA deve garantir que sejam obtidos os mesmos resultados com o uso de Javascript e análise conjunta das requisições, excetuando características únicas obtidas a partir do uso de SDK;

2.10.10. A solução deve fornecer uma biblioteca (SDK) compatível com as plataformas utilizadas pelo SERPRO;

2.10.11. A solução deve prover biblioteca que suporte pelo menos as plataformas ANDROID e IOS, nas versões com suporte vigente pelos respectivos fabricantes;

2.10.12. As bibliotecas SDK e Javascript e SDK terão suas configurações customizadas para o SERPRO e devem estar disponíveis e atualizados de forma incremental;

2.10.13. A solução deve prover biblioteca que possibilite ser embarcada nos aplicativos desenvolvidos pelo SERPRO;

2.10.14. A solução deve possibilitar seu funcionamento sem a necessidade de instalação de agentes nos clientes, sem comprometer qualquer funcionalidade prevista neste documento;

2.10.15. A solução deve possuir arquitetura que possibilite a integração com a plataforma Acesso Gov.br sem exigir alterações que requeiram mudanças arquiteturais nas aplicações;

2.10.16. A solução deve ser capaz de responder com tempo máximo de 150ms;

2.11. Características Técnicas da Solução

2.11.1. A solução deve ser capaz de identificar fraudes e comportamentos suspeitos e tratá-los nos seguintes cenários e situações durante as requisições e operação do processo de controle de acesso da plataforma Acesso Gov.br:

2.11.1.1. Detecção de risco e fraudes nos canais web e mobile;

2.11.1.2. Detecção de risco e fraudes em qualquer navegador compatível com Javascript;

2.11.1.3. Deve possibilitar a utilização de uma SDK para aplicação em dispositivos móveis;

2.11.2. A solução deve fornecer informações em tempo real sobre qualquer transação realizada durante o processo de controle de acesso da plataforma Acesso Gov.br;

2.11.3. A solução deve prover mecanismos, técnicas e bases de informações e utilizá-las desde o início de sua 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;

2.11.4. A solução deve possibilitar a integração por meio de API com as aplicações do SERPRO independente da linguagem de programação, possibilitando a customização de funcionalidades para a API;

2.11.5. A solução deve garantir o monitoramento de transações suspeitas, maliciosas ou fraudulentas e retornar informações que possibilitam a plataforma Acesso Gov.br tomar decisões com base nas notas de risco informadas e demais informações que se façam necessárias;

2.11.6. A solução deve garantir a atualização constante de bases de assinatura e heurísticas relacionadas às ações maliciosas e fraudes;

2.11.7. A solução deve executar sua função de forma transparente ao usuário final, não requisitando nenhuma atuação do mesmo para sua operação;

2.11.8. A solução deve possuir pelo menos as seguintes tecnologias para monitoração e proteção dos navegadores dos dispositivos que acessam a plataforma Acesso Gov.br, detectando anomalias e enviando eventos/logs para análise e mitigação de risco:

2.11.8.1. Possuir tecnologia de identificação de navegador por similaridade, com intuito de fornecer insumos ao motor de análise e mitigação de risco, permitindo assim a análise do comportamento dos usuários e seus navegadores comuns;

2.11.8.2. Deve capturar e compreender padrões para geração de biometria comportamental, detectando se o acesso está sendo realizado pelo usuário legítimo ou não, utilizando os itens abaixo descritos, mas não se limitando aos mesmos:

2.11.8.2.1. Padrões de movimentação de mouse;

2.11.8.2.2. Padrões de digitação;

2.11.8.2.3. No uso de dispositivos móveis:

2.11.8.2.4. Inclinação, velocidade de swipe, pressão do toque;

- 2.11.8.3. Deve detectar mecanismos de colagem de informações nos formulários presentes no portal WEB em que o Javascript esteja integrado e executando;
- 2.11.9. A solução deve ter a capacidade de detectar as seguintes situações para a coleta de informações para identificação de anomalias e possíveis fraudes e abuso de contas durante o processo de controle de acesso:
- 2.11.9.1. Navegação anômala com base em conhecimento prévio da solução;
 - 2.11.9.2. Padrões suspeitos com base em inteligência;
 - 2.11.9.3. Acesso remoto;
 - 2.11.9.4. Uso de proxy;
 - 2.11.9.5. Uso de VPN;
 - 2.11.9.6. Spoof de dispositivo;
 - 2.11.9.7. Identificação de fraudadores conhecidos;
 - 2.11.9.8. Tempo anormal na página.
 - 2.11.9.9. Uso de Root/Jailbreak e hiders;
 - 2.11.9.10. Geolocalização ou cruzamento de antena ou IP;
 - 2.11.9.11. Análise de dados de gps, evitando fake gps;
 - 2.11.9.12. Verificação de overlay de tela;
 - 2.11.9.13. 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;
 - 2.11.9.14. Acessos de fuso horário incompatíveis com a origem;
 - 2.11.9.15. Acessos fora do horário habitual do usuário com base em perfil comportamental;
 - 2.11.9.16. Atividades identificadas como incomum usando um serviço de hospedagem classificado como de alto risco;
 - 2.11.9.17. Atividade identificadas como incomum usando um novo idioma no navegador;
 - 2.11.9.18. Acesso suspeito a múltiplas contas;
 - 2.11.9.19. Acesso de um dispositivo suspeito usando atributos falsificados;
 - 2.11.9.20. Identificação de dispositivos conhecidos que são utilizados por fraudadores;
 - 2.11.9.21. Acesso identificado como suspeito a partir de um endereço IP classificado como de alto risco;
 - 2.11.9.22. Atividade em uma conta bloqueada;
 - 2.11.9.23. Identificar quando estiver operando em ambiente virtual/emulado;
 - 2.11.9.24. Acesso a partir de um novo dispositivo desconhecido;
 - 2.11.9.25. Uso de um domínio de e-mail suspeito ou de origem duvidosa durante o processo de controle de acesso;
 - 2.11.9.26. Padrão de múltiplos acessos suspeitos;
 - 2.11.9.27. Login a partir de uma conexão wireless inseguros;
 - 2.11.9.28. Acesso suspeito a uma conta de usuário com atributos diferentes daqueles normalmente vistos no dispositivo do usuário;
 - 2.11.9.29. Atividade de um dispositivo suspeito usando navegador Tor ou similares;
 - 2.11.9.30. Números de telefones identificados como suspeitos;

2.11.10. Possuir a capacidade de detecção de anomalias na navegação web, no processo de controle de acesso, para detecção e prevenção contra, no mínimo, os seguintes ataques cibernéticos:

2.11.10.1. Man-in-the-browser;

2.11.10.2. Phishing;

2.11.10.3. Captura de identidade;

2.11.10.4. Bots;

2.11.10.5. Captura de credenciais;

2.11.10.6. Deve possuir mecanismos para identificar ataques por injeção de código no portal WEB que esteja integrado;

2.11.11. Detecção de fraudes através da correlação de eventos;

2.11.12. Capacidade de mapear tentativas fraudulentas do usuário;

2.11.13. A solução deve ter a capacidade de executar a análise de logs e registros de auditoria para identificar e tratar ações suspeitas executadas na aplicação;

2.11.14. A solução deve permitir que sejam identificados padrões de comportamento com o passar do tempo e ajudar o SERPRO na identificação de anomalias e refinamento das políticas e estratégias para proteção contra fraudes;

2.12. Monitoração, Eventos, Logs e Relatórios

2.12.1. A solução deve possibilitar a geração de relatórios detalhados após o tratamento das requisições e apresentar visualizações gráficas;

2.12.2. A solução deve possibilitar a visualização de eventos de alerta por meio da interface de gerência Web;

2.12.3. A solução deve possibilitar a geração dos relatórios com o conteúdo listado, bem como sua apresentação no dashboard da solução com no mínimo os conteúdos abaixo listados:

2.12.3.1. Distribuição de violações de segurança;

2.12.3.2. Identificação de possíveis fraudes que ocorram;

2.12.4. A solução deve fornecer relatórios pós-incidentes:

2.12.4.1. Sumarização dos eventos ocorridos com identificação dos riscos identificados e respectivas informações que evidenciam os registros, bem como seu tratamento;

2.12.4.2. Eventos de auditoria;

2.12.5. A solução deve possibilitar o armazenamento de logs de auditoria e alertas;

2.12.6. A solução deve possibilitar a exportação e envio de todos os logs e registros de auditoria para fontes externas;

2.12.7. A solução deve ser possibilitar a integração com mínimo as seguintes soluções de SIEM:

2.12.7.1. Microfocus Arcsight;

2.12.7.2. QRadar IBM;

2.12.7.3. Splunk;

2.12.7.4. Kibana;

2.12.7.5. McAfee Enterprise Security Manager;

2.12.8. A solução deve gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos os seus componentes;

2.12.9. A solução deve gerar, no mínimo, o registro dos seguintes eventos:

2.12.9.1. Login;

2.12.9.2. Acesso com dispositivo suspeito;

2.12.9.3. Acesso com dispositivo fraudador;

2.12.9.4. Alertas com base na criticidade a partir da monitoração da própria solução;

2.12.10. A solução deve permitir a configuração de alertas para detecção de ameaças ou fraudes relacionadas ao processo de controle de acesso.

2.12.10.1. Esses alertas devem permitir no mínimo canais como e-mail, SMS, soluções de mensagem instantânea.

2.13. Interface de Gerência Web

2.13.1. A solução deve possuir interface web para acompanhamento de todas as ações executadas pela solução durante o processo de controle de acesso em sua operação de coleta, detecção, prevenção e atuação contra possíveis fraudes e abuso de contas para o processo de controle de acesso da plataforma Acesso Gov.br;

2.13.2. A solução deve possibilitar a segregação de funções no acesso a operação e gestão da solução;

2.13.3. A solução deve prover interface de gerência Web que forneça acesso a todos os serviços disponíveis, visualização dos eventos e tratamento aplicado;

2.13.4. A solução deve possuir um Dashboard que faça sumarização dos eventos em execução em tempo real;

2.13.5. A solução deve mostrar informações sobre o tratamento das informações e ações executadas, mesmo que as ações sejam relacionadas ao encaminhamento ou fornecimento de informações a outros sistemas externos;

2.13.6. A solução deve prover interface de gerência Web que suporte no mínimo os navegadores os Mozilla Firefox, Google Chrome, Microsoft Edge;

2.13.7. A solução deve possuir dashboard com gráficos estatísticos da disponibilidade do serviço;

2.13.8. A solução deve prover gerenciamento capaz de gerar relatórios gráficos para análise de tráfego sendo tratado, notas de risco geradas e suas respectivas origens, análise de fraudes e relatórios de resumo.

2.13.9. A solução deve possibilitar a exportação de relatórios nos seguintes formatos:

2.13.9.1. HTML ou XML;

2.13.9.2. PDF;

2.13.9.3. CSV;

2.13.9.4. JSON;

2.13.10. A solução deve prover gerenciamento capaz de gerar relatórios diários, semanais, mensais e anuais;

2.13.11. A interface de gerência Web deve possibilitar, no mínimo, a apresentação das seguintes informações para o SERPRO:

2.13.11.1. Análise de ambiente, relativo aos dispositivos utilizados pelos usuários, mostrando dados consolidados em tempo real ou por filtro de tempo definido na plataforma, sobre o seguinte:

2.13.11.1.1. Acessos registrados;

2.13.11.1.2. Acessos de dispositivos sem risco;

2.13.11.1.3. Acessos de dispositivos suspeitos;

- 2.13.11.1.4. Dispositivos únicos acessados;
- 2.13.11.1.5. Dispositivos registrados;
- 2.13.11.1.6. Navegadores mais utilizados e dispositivos que sejam virtualizados/emulados;
- 2.13.11.1.7. Análise de recebimento de eventos maliciosos;
- 2.13.11.1.8. Análise de ocorrências de fraudes;
- 2.13.11.1.9. Análise de incidentes gerais;
- 2.13.11.1.10. Análise detalhando por incidente;
- 2.13.11.2. Análise de transações e acessos, com filtro por período definido na plataforma, mostrando os seguintes dados:
 - 2.13.11.2.1. Total de transações/acessos sem risco;
 - 2.13.11.2.2. Total de transações/acessos com risco;
 - 2.13.11.2.3. Proporção de notas de risco;
 - 2.13.11.2.4. Lista do detalhamento de cada transação/acesso (id da transação, usuário, sessão, razão do risco, data de tratamento e nota de risco numérica);
 - 2.13.11.2.5. A solução deve possibilitar a apresentação das razões para as notas de riscos e devem ser apresentadas por categorias de riscos, descrevendo o fato motivador do risco;
 - 2.13.11.2.6. A solução deve possibilitar a realização de consultas, buscas e filtros no ambiente web a partir de características como modelo do dispositivo, IP de acesso, faixa temporal e faixa de valores dos indicadores e métricas gerados no processo;
- 2.14. Entrega e recebimento definitivo
 - 2.14.1. Regional Brasília: SGAN Av. L2 Norte, Quadra 601 Módulo "G", Brasília/DF - CEP: 70.836-900; CNPJ: 33.683.111/0002-80; Inscrição Estadual: 07334743/002-94; Inscrição Municipal: 07334743/002-94;
 - 2.14.2. O serviço deverá ser disponibilizado e ativado em até 30 (trinta) dias corridos do início da vigência do contrato.
 - 2.14.3. Entende-se por cumprimento do prazo de entrega o recebimento do serviço conforme especificados neste instrumento, sua instalação e execução dos serviços no SERPRO;
- 2.15. Consulta ao mercado
 - 2.15.1. Solicitamos especificar e detalhar a arquitetura da solução e aplicabilidade em outras plataformas ou modelos de implementação.

3. NÍVEIS DE SERVIÇO E SANCIONAMENTOS

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. 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;
- 3.1.3. 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;

3.1.4. O serviço de atualização deve incluir correções ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades da solução licenciada;

3.1.5. A cada nova versão ou atualizações da solução, a CONTRATADA deve apresentar as novas funcionalidades para o SERPRO que analisará a adesão de novas funcionalidades, não haverá nenhum ônus adicional pela adesão das novas funcionalidades;

3.1.6. Durante o prazo de validade técnica da versão das licenças da solução, a CONTRATADA deve assegurar ao SERPRO a prestação de serviços técnicos complementares relativos ao adequado funcionamento da solução licenciada, consideradas as suas especificações;

3.1.7. Caso a solução licenciada 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.

3.1.8. Nas intervenções corretivas, 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 ao SERPRO;

3.1.9. A CONTRATADA deverá comunicar quaisquer vulnerabilidades encontradas na solução instalada no SERPRO 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 deverá 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 dias.

3.2. Do Nível de Disponibilidade e Sancionamentos

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

3.2.1.1. A Disponibilidade Mensal do Serviço (DMS), para a solução e seus componentes, conforme especificações contidas neste documento deve ser de 99,99% (noventa e nove vírgula noventa e nove por cento);

3.2.1.2. A Disponibilidade Mensal do Serviço apurada será calculado pela seguinte fórmula:

3.2.1.2.1. $DMS (\%) = (1 - (\text{Tempo Total de Interrupção Mensal} / \text{Tempo Total Mensal})) \times 100$;

3.2.1.3. 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 a SERPRO e a CONTRATADA, desde que não seja constatada responsabilidade do SERPRO. A SERPRO fará a formalização do registro de chamado nas seguintes situações:

3.2.1.3.1. A impossibilidade de direcionamento de tráfego do Acesso Gov.br para a solução em nuvem da CONTRATADA, causados por problemas da CONTRATADA;

3.2.1.3.2. A impossibilidade de tratamento das requisições do acesso Gov.br causados por problemas da CONTRATADA;

3.2.1.3.3. A indisponibilidade das ferramentas de visibilidade e administração do serviço;

3.2.1.3.4. O não atendimento a qualquer um dos indicadores técnicos descritos neste documento;

3.2.1.4. Deve ser entendido como “Tempo Total Mensal” do serviço:

3.2.1.4.1. 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;

3.2.1.4.2. A quantidade em minutos aferida para o mês corrente para os demais meses;

3.2.1.5. 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;

3.2.1.6. 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;

3.2.1.7. Falhas na infraestrutura sob responsabilidade da SERPRO, que comprometam a disponibilidade do Serviço contratado, não acarretarão ônus à CONTRATADA;

3.2.1.8. A CONTRATADA deve garantir o tratamento e vazão de no mínimo 99,99% (noventa e nove vírgula noventa e nove por cento) das requisições direcionadas a solução da CONTRATADA. O não atendimento a este item será entendido como indisponibilidade do serviço;

3.2.1.9. O exercício da garantia para retorno da condição operacional da solução deve ser realizado conforme critérios abaixo:

3.2.1.10. 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);

3.2.1.11. O atendimento aos chamados para o exercício da garantia deve obedecer à seguinte classificação quanto ao nível de severidade, conforme Tabela:

Severidade	Descrição	Tipo	Tempo de Atendimento	Tempo de solução	Penalidades
1 – Crítica	Chamados referentes a situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado	Remoto	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	Remoto	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, incluindo os casos em que haja necessidade de substituição de componentes	Remoto	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 do produto	Remoto	No máximo 24 (vinte e quatro) horas após a abertura do chamado	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 cento) do valor contratual, por hora ou fração de hora de atraso

3.2.1.12. Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento;

3.2.1.13. Durante o período de garantia, a CONTRATADA deve fornecer informações sobre as correções a serem aplicadas ou a própria correção;

3.2.1.14. Deve fornecer orientações para diagnóstico de problemas e ajuda na interpretação de trilhas, dumps e logs;

3.2.1.15. 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;

3.2.2. Deve possuir suporte técnico para as licenças, durante o período de vigência da garantia, assegurando prazo de atendimento; Chamados, Registro e Início de Prazos

3.2.2.1. O atendimento aos chamados deve obedecer à tabela de classificação quanto ao nível de severidade;

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

3.2.2.3. Um chamado fechado sem anuência do SERPRO ou sem que o problema 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;

3.2.3. Atendimento a chamados

3.2.3.1. A CONTRATADA deve prover todas as correções e atualizações necessárias durante a vigência do contrato;

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

3.2.3.3. O SERPRO poderá efetuar um número ilimitado de chamados para suporte técnico, durante a vigência do contrato, para suprir suas necessidades com relação aos produtos de segurança.

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

3.2.3.4.1. 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;

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

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

3.2.4. Canais de Atendimento

3.2.4.1. 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;

3.2.4.2. A CONTRATADA deverá 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;

3.2.4.3. A CONTRATADA deverá 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);

3.2.4.4. Cada pessoa cadastrada no sistema como usuário deverá 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;

3.3. Chamados, Registro e Início de Prazos

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

3.3.1.1. Número de acionamento;

3.3.1.2. Descrição da ocorrência;

3.3.1.3. Localidade;

3.3.1.4. Severidade;

3.3.1.5. Nome do responsável do SERPRO pela abertura do chamado;

3.3.1.6. Data e hora de abertura do chamado;

3.3.1.7. Data e hora do início do atendimento;

3.3.1.8. Tipo do atendimento;

3.3.1.9. Data e hora de encerramento;

3.3.1.10. Descrição da resolução adotada;

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

3.3.3. 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;

3.3.4. Entrega Mensal de Relatórios

3.3.4.1. Mensalmente deve ser entregue relatório constando os acionamentos técnicos abertos, em andamento e encerrados no período do exercício da garantia;

3.3.4.2. 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;

3.3.4.3. O relatório deve ser entregue mesmo quando não houver chamados no período;

3.3.4.4. A entrega do relatório deve ser realizada até o quinto dia útil do mês subsequente;

3.3.4.5. 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. ESPECIFICAÇÃO DE VALORES E FORMAS DE PAGAMENTO

4.1. O pagamento será efetuado, mensalmente, no 1º (primeiro) dia útil, após o 30º (trigésimo) dia corrido da data do recebimento definitivo dos serviços prestados ao SERPRO, indicados nas respectivas notas fiscais e/ou entregues no Protocolo Geral do SERPRO ou através do endereço eletrônico a ser informado pelo Gestor do Contrato;

4.2. O prazo para emissão do Termo de Recebimento Definitivo por parte do SERPRO, será de 5 (cinco) dias úteis, a partir do recebimento da Nota fiscal, condicionado à apresentação do relatório mensal de serviços, pela CONTRATADA;

4.3. No primeiro mês de faturamento, o valor deverá ser rateado à base de 1/30 (um trinta avos) do valor da contraprestação mensal, por dia, considerando-se o mês de 30 dias.

4.4. Nos meses subsequentes, os serviços serão cobrados com base no período de 1 a 30 do mês da efetiva execução dos serviços.

4.5. No último mês de vigência do contrato o valor deverá ser rateado à base de 1/30 (um trinta avos) do valor da contraprestação mensal, por dia, considerando-se o mês de 30 dias.

4.6. Consulta ao mercado

4.6.1. Solicitamos especificar e detalhar o modelo de comercialização da sua solução, bem como a forma de precificação.

5. SELEÇÃO DO FORNECEDOR

5.1. Documentação Técnica do Fabricante:

5.2. 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;

5.3. Apresentar Atestado de Capacidade Técnica comprovante a implantação e uso da solução em 03 (três) clientes;

5.4. Avaliação de Amostra

5.4.1. 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;

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

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

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

5.4.5. O prazo de avaliação de amostra poderá ser prorrogado a critério do SERPRO;

5.4.6. 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;

5.4.7. 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;

5.4.8. Esta etapa será executada por prepostos do SERPRO em conjunto com os prepostos das LICITANTES no ITEM específico da aquisição;

5.4.9. Os testes de bancada, nas etapas da avaliação de amostra, serão realizados nas dependências do SERPRO, endereço descrito no subitem a seguir:

5.4.10. 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;

5.4.11. 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;

5.4.12. Ao fim de cada dia de testes de bancada, nas etapas da avaliação de amostra, deverá ser emitida, assinada e distribuída Ata de Atividades e Ocorrências a todos os presentes até o próximo dia;

5.4.13. 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;

5.4.14. 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;

5.4.15. Entre os técnicos indicados apenas 1 (um) técnico poderá acompanhar os testes de avaliação de amostra;

5.4.16. 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;

5.4.17. As indicações devem ser realizadas com, no mínimo, 2 (dois) dias úteis de antecedência e apenas serão permitidos questionamentos diretos aos técnicos do SERPRO;

5.4.18. 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;

5.4.19. 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;

5.4.20. A critério do SERPRO os testes de bancada, nas etapas da avaliação de amostra, poderão ser reiniciados após atualização de versão;

5.4.21. Os testes deverão ser realizados no horário compreendido entre 09:00 e 17:00 de segunda-feira a sexta-feira;

5.4.22. A avaliação de amostra da Solução ofertada deverá ser instalada sem nenhum custo para o SERPRO;

5.4.23. A licitante que for reprovada na avaliação de amostra não terá direito a qualquer indenização;

5.4.24. Será emitido um relatório descrevendo os exames realizados e contendo a aprovação ou não da avaliação de amostra;

5.4.25. Somente após todos os testes de bancada, nas etapas da avaliação de amostra, será emitido o parecer técnico aprovando ou não a amostra apresentada;

5.4.26.. A documentação, bem como os manuais necessários para a homologação, deverá estar disponível para os representantes do SERPRO;

6. REPASSE DE CONHECIMENTO

6.1. A CONTRATADA deve prover o repasse de conhecimento dos profissionais do SERPRO para configuração e operação da Solução;

6.2. A CONTRATADA deve repassar o conhecimento sem ônus adicional para o SERPRO, incluindo todo o material didático necessário;

6.3. O material de aula deverá abordar conteúdo teórico e prático, e deverá ser submetido ao SERPRO para aprovação antes da realização da capacitação;

- 6.4. Após a assinatura do contrato, a CONTRATADA deverá realizar o repasse do conhecimento da Solução, que poderá ocorrer em paralelo a fase de instalação;
- 6.5. A CONTRATADA deve repassar o conhecimento através de profissionais habilitados e credenciados pelos fabricantes ou empresa credenciada para tal finalidade;
- 6.6. Deverá ser apresentado com até 10 dias de antecedência do repasse de conhecimento a declaração que os profissionais são habilitados para ministrar o curso;
- 6.7. Deve ser entregue pela CONTRATADA, até 10 dias antes do início do repasse de conhecimento a ementa.
- 6.8. A ementa deve estar no idioma português, e conter nome, objetivo, conteúdo programático e carga horária que será aprovada pelo SERPRO e todo o material didático.
- 6.9. A CONTRATADA deve providenciar o repasse de conhecimento para 02 (duas) turmas, com capacidade para 10 (dez) participantes cada, abordando toda solução contratada envolvendo teoria e prática, em datas a serem negociadas entre o SERPRO e a CONTRATADA e deve ser aplicado de forma on-line e síncrona;
- 6.10. A carga horária mínima para cada turma deve ser de 24 (vinte e quatro) horas;
- 6.11. O repasse de conhecimento deve ser prestado em local externo ao SERPRO de responsabilidade da CONTRATADA.
- 6.12. A CONTRATADA deve disponibilizar toda infraestrutura necessária ao repasse de conhecimento (sendo aceita máquinas virtuais, desde que na mesma versão do software fornecida ao SERPRO);
- 6.13. O repasse de conhecimento deve abordar: operação básica e avançada da Solução, customização e gestão de fluxos, com conteúdo teórico e prático com seguinte conteúdo mínimo:
- 6.14. Instruções de manuseio e operação, incluindo resolução de problemas;
- 6.15. Ao final do repasse de conhecimento, o SERPRO, por meio do formulário especificado pelo SERPRO, fará a avaliação do repasse ministrado para emissão de termo de aceite, a qual a CONTRATADA deve obter a média de 70% de conceitos “bom e/ou ótimo”.
- 6.16. Caso não atinja o conceito mencionado na subcláusula anterior, o SERPRO encaminhará um relatório a CONTRATADA informando o que deve ser adequado para a realização de um novo repasse.
- 6.17. A CONTRATADA deve encaminhar ao SERPRO as alterações para análise e aprovação;
- 6.18. Se aprovado, o prazo do novo repasse de conhecimento deve ser acordado com a equipe do SERPRO.
- 6.19. Após cada repasse a CONTRATADA deve ser emitido certificado para cada participantes de acordo com a carga horária.
- 6.20. O certificado deve conter as seguintes informações: nome completo do participante, nome do repasse de conhecimento, período de realização, carga horária e conteúdo programático.
- 6.21. 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.
- 6.22. O prazo de vigência do contrato é de 12 (doze) meses, podendo ser prorrogado mediante assinatura de Termo Aditivo, limitada sua duração a 60 (sessenta) meses.