



Consulta pública eletrônica ao
mercado para subsidiar futura
contratação de subscrição da
solução de Proteção
Automatizada de Apps Mobile



1.Objeto

1.1. Consulta pública eletrônica ao mercado para subsidiar futura contratação de subscrição da solução de Proteção Automatizada de Apps Mobile em tempo de execução, incluindo atualização e manutenção, pelo período de 24 (vinte e quatro) meses

2. Especificação do Objeto

2.1. Contratação de subscrição da solução de Proteção Automatizada de Apps Mobile em tempo de execução, incluindo atualização e manutenção, conforme tabela a abaixo:

Item	Descrição	Métrica	Quantidade
1	Subscrição da solução de Proteção Automatizada de Apps Mobile	Unidade	1

2.1.1 Contratação sob demanda de subscrição da solução de Proteção Automatizada de Apps Mobile em tempo de execução, incluindo atualização e manutenção, conforme tabela a abaixo:

Item	Descrição	Métrica	Quantidade
2	Subscrição da solução de Proteção Automatizada de Apps Mobile	Unidade	2

2.2. Requisitos Funcionais

2.2.1 As funcionalidades mínimas e obrigatórias a serem atendidas pela solução de proteção automatizada de apps mobile deve atender aos requisitos abaixo especificados.

2.2.1.1 A solução deve ser capaz de realizar o monitoramento online, em tempo real, gerando dados e produzindo informações sobre comportamentos suspeitos de tentativa de violação do aplicativo, no qual foram incorporadas as funcionalidades de segurança.

2.2.2 A solução deve garantir que o processo de adição de proteções ocorra diretamente nos binários (APKS, AABs, PAs), e que o código original do aplicativo permanece intacto e inalterado.

2.2.3 A solução deve ser 100% compatível e interoperável com qualquer linguagem ou framework de programação utilizado pelos apps mobile, sem limitações ou impacto no funcionamento das proteções.

2.2.4 A solução deve implementar as proteções dentro dos apps mobile (Android ou iOS) sem nenhuma dependência de SDKs (Software Development Kits), codificação manual ou esforços de desenvolvimento, compilando as proteções selecionadas de forma automatizada.

2.2.5 A solução deve ser SaaS (Software as a Service), sendo sua operação, execução e tratamento de dados em território nacional, respeitando as melhores práticas o SOC 2 Type e ISO 9001.

2.2.6 A solução deve permitir a partir da mesma interface unificada a geração de builds (compilações), definição de templates de segurança, assinatura dos apps, gestão de acesso e permissões, criação de equipes de trabalho (Produção, Homologação, etc.), consulta do histórico dos builds gerados com as proteções e auditoria das proteções e controles de segurança implementados.

2.2.7 A solução deve fornecer para os usuários da plataforma a capacidade de habilitar ou desabilitar as proteções/controles de segurança de maneira fácil e intuitiva, sem requerer qualquer tipo de codificação manual ou desenvolvimento.

2.2.8 A solução deve implementar a ofuscação de código, proporcionando dificuldades extras na interpretação da sequência de comandos a serem executadas, na adição de código fictício, na troca de nomes de variáveis, métodos e classes, entre outras práticas. (Code-Obfuscation)

2.2.9 A solução deve implementar a encriptação de classes, criptografando o código binário das classes em aplicativos Android e iOS. (Class Encryption)

2.2.10 A solução deve implementar a encriptação de dados, criptografando os arquivos de configuração do aplicativo. (Data Encryption)

2.2.11 A solução deve implementar a encriptação de strings, criptografando todos os conteúdos que representam informações do tipo sequência de caracteres textuais. (String Encryption)

2.2.12 A solução deve implementar proteção contra rooted e jailbroken, detectando se o sistema operacional do dispositivo móvel prevê as restrições de segurança padrão do fornecedor do dispositivo.

2.2.12.1 A solução deve implementar um fluxo de testes para certificar se os aplicativos desenvolvidos para Android e iOS permitem acesso de usuário administrador (Root Detection).

2.2.13 A solução deve implementar proteção contra repackaging, evitando o uso do código original do aplicativo alterado e empacotado em uma outra aplicação. (Anti-Repackaging)

2.2.14 A solução deve implementar proteção contra tampering, evitando modificações no aplicativo mesmo quando em execução. (Anti-Tampering)

2.2.15 A solução deve prover proteção contra a clonagem de aplicativos, detectando modificações na estrutura, nas permissões e nos metadados do aplicativo. Essa proteção deve garantir que os aplicativos clonados não funcionem, evitando acesso não autorizado, distribuição de malware e roubo de dados. (Anti-cloning)

2.2.16 A solução deve implementar proteção contra hooking, prevenindo a alteração do comportamento de aplicações por meio da inserção de instruções em tempo de execução. (Anti-Hooking)

2.2.17 A solução deve implementar proteção contra emulador, bloqueando a execução do aplicativo em emuladores do sistema operacional. (Anti-Emulator)

2.2.18 A solução deve implementar proteção contra debug, bloqueando a execução do aplicativo em modo de depuração. (Anti-Debbuging)

2.2.19 A solução deve implementar proteção contra pinning, limitando as cadeias de autoridades certificadoras válidas para a aplicação. (Anti-Pinning)

2.2.20 A solução deve implementar proteção UI, validando se a interface gráfica, do sistema operacional do dispositivo, está protegida por senha. (Anti-Screen Reader)

2.2.21 A solução deve garantir que o processo de proteção onere minimamente o desempenho da aplicação protegida, não sendo perceptível ao usuário.

2.2.22 A solução deve possibilitar a incorporação com ferramentas de integração contínua, permitindo que o sistema possa ser executado utilizando processos de integração contínua, Gitlab CI/CD.

2.2.23 A solução deve permitir encriptação de código nativo.

2.2.24 A solução deve implementar proteção para vulnerabilidades do Open Web Application Security Project (OWASP), tais como: injeção de SQL, uploads mal-intencionados, injeção de comando do sistema operacional (SO).

2.2.25 A solução deve garantir proteção contra explorações de vulnerabilidades de dia zero

2.2.26 A solução deve ter capacidade de integração com ferramentas de SOC e SIEM (tais como Arcsight ESM e Elastic Search) utilizadas pelo SERPRO.

2.2.27 A solução deve implementar funcionalidade de detecção de “falsos positivos”, com índice de assertividade superior a 95%.

2.2.28 A solução deverá ser implantada, como parte do aplicativo que protege, podendo ser executada em qualquer ambiente onde o aplicativo protegido esteja em produção, inclusive em nuvem.

2.2.29 A solução deve implementar criptografia de caixa branca, visando estabelecer um mecanismo de proteção contra a descoberta de chave criptográfica. (White-Box Cryptography)

2.2.30 A solução deve implementar proteção contra Keylogger, evitando o monitoramento indesejado do dispositivo protegido e, conseqüentemente, a captura de informações pessoais do usuário. (Anti-Keylogger)

2.3. Requisitos Não Funcionais.

2.3.1 - A solução deverá ter seus itens validados e homologados, após a declaração do vencedor no processo licitatório;

2.3.2 - Faz-se necessário após o término da licitação, homologação do vencedor que haja o repasse do conhecimento do uso da ferramenta;

2.3.3 - O contrato deverá ser de 24 meses prorrogáveis até 60 meses;

2.3.4 - A plataforma deve estar disponível para novas configurações 24/7;

2.3.5 - O prestador deve entregar suporte remoto 8/5, oito horas por dia, cinco dias por semana.

2.4. Prazo de entrega:

2.4.1. As licenças de software referente a contratação devem ser entregues em até 15 (quinze) dias corridos a partir da data de início da vigência contratual.

2.5. Local de entrega e prestação dos serviços:

2.5.1. Regional Brasília

Endereço: SGAN AV. L2 Norte Quadra 601 Módulo G

Brasília/DF - CEP 70.836-900

Inscrição Estadual: 07334743/002-94

CNPJ: 33.683.111/0002-80.

2.6. Recebimento definitivo

2.6.1. O prazo para Recebimento Definitivo por parte do Serpro é de 10 (dez) dias corridos a partir da data do recebimento dos documentos fiscais.

2.6.2 O Recebimento Definitivo somente será emitido após comprovação por meio de documentação do fabricante dos softwares enviados pela Contratada ou a confirmação no site do fabricante:

3. Níveis de Serviço e Sancionamentos

3.1. A contratada deverá prestar suporte técnico inerente a contratação de subscrição da solução de Proteção Automatizada de Apps Mobile para apoio nas atualizações de software, atendimento técnico especializada para solução de problemas e para resolução de dúvidas, com os seguintes requisitos:

3.1.1. Para os chamados de severidade 1 - Crítica e 2 – Alta o atendimento remoto ocorrerá 24 (vinte e quatro) horas por dia durante 7 (sete) dias na semana, inclusive feriados.

3.1.2. Para os chamados de severidade 3 - Média e 4 -Baixa o atendimento remoto ocorrerá em dias úteis, exceto feriados nacionais, das 08:00 (oito) horas às 18:00 (dezoito) horas.

3.2. O atendimento aos chamados deverá obedecer às seguintes classificações quanto ao nível de severidade:

Severidade	Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução ou de contorno	Penalidades
1 – Crítica	Chamados referentes à situação de emergência ou problemas críticos, caracterizados pela existência de sistema paralisado;	Remoto	No máximo 1 (uma) hora após a abertura do chamado.	No máximo 4 (quatro) horas após o início do atendimento.	O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à Contratada de 1% (um por cento) do valor total mensal dos serviços, 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) hora após a abertura do chamado.	No máximo 6 (seis) horas após o início do atendimento.	O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à Contratada de 0,8% (zero vírgula oito por cento) do valor total mensal dos serviços, 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.	Remoto	No máximo 2 (duas) horas após a abertura do chamado	No máximo 12 (doze) horas após o início do atendimento.	O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à Contratada de 0,6% (zero vírgula seis por cento) do valor total mensal dos serviços, por hora ou fração de hora de atraso.
	Chamados com objetivo de apoio na	Remoto	No máximo 4 (quatro) horas após a	Conforme agendamento	

	atualização de software(s)		abertura do chamado		
4 – Baixa	Chamados com objetivo de sanar dúvidas quanto ao uso ou à implementação do produto	Remoto	No máximo 4 (quatro) horas após a abertura do chamado	No máximo 24 (vinte e quatro) horas após o início do atendimento.	O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à Contratada de 0,4% (zero vírgula quatro por cento) do valor total mensal dos serviços, por hora ou de hora fração de atraso.

3.3. Entende-se por suporte técnico

3.3.1. Ações que visem assegurar os padrões de qualidade, segurança, durabilidade e desempenho do software.

3.3.2. Direito de atualização dos softwares que englobando o fornecimento novas versões, releases e patches de segurança;

3.3.2.1. A atualização deve incluir correções dos produtos ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidade dos produtos;

3.3.3. Configurar e solucionar problemas envolvendo os produtos ofertados;

3.3.4. Informar sobre as correções a serem aplicadas ou a própria correção;

3.3.5. Orientar para diagnósticos de problemas e ajuda na interpretação de traces, dumps e logs;

3.3.6. No caso de problemas não documentados, os registros enviados pelo Serpro (tais como traces, dumps e logs) devem ser encaminhados aos laboratórios do responsável técnico, a fim de que sejam fornecidas as devidas correções;

3.3.7. Apresentar as novas funcionalidades, sem ônus adicional para o Serpro, a cada nova versão instalada;

3.3.8. Caso o software fornecido seja descontinuado na linha de comercialização do fabricante, manter as condições da presente contratação ou providenciar a substituição por outro produto disponível que execute as mesmas funcionalidades, sem ônus adicionais para o Serpro.

3.4. Do Atendimento do Chamados

3.4.1. Os atendimentos para os chamados deverão ser efetuados por especialistas devidamente habilitados, que trabalharão o tempo que for necessário para a solução do problema, sem ônus adicional para o Serpro e sem prejuízo para os demais prazos.

3.4.2. O atendimento não poderá ser interrompido até o completo restabelecimento do software envolvido, mesmo que se estenda em períodos noturnos e dias não úteis, observando os níveis de severidade.

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

3.5. Dos Canais de atendimento

3.5.1. O atendimento e os chamados técnicos deverão ser realizados por meio de canal telefônico gratuito 0800 ou tarifação reversa ou local, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e/ou site na Internet;

3.6. Do Monitoramento do Atendimento dos Chamados

3.6.1. Todos os chamados serão controlados por sistema de informação da Contratada.

3.6.2. O fechamento do chamado poderá se dar, quer pela aplicação de correção ao produto ou pela aplicação de solução de contorno que possibilite a operação do sistema.

3.6.3. A disponibilização de medida corretiva definitiva poderá, a critério da Contratada, vir a ser incorporada em futuras versões do software.

3.6.4. Antes do fechamento de cada chamado, a Contratada consultará o Serpro para validar o fechamento do chamado.

3.6.5. 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.

3.6.6. A Contratada manterá cadastro das pessoas indicadas pelo Serpro que poderão efetuar abertura e autorizar fechamento de chamados.

3.7. Da Entrega dos Relatórios

3.7.1. A Contratada deverá enviar relatório constando os acionamentos técnicos abertos, em andamento e encerrados no mês imediatamente anterior, por localidade, com no mínimo as seguintes informações: número do contrato, período de referência, número de acionamento, descrição da ocorrência, severidade, nome do responsável do Serpro pela abertura do chamado, data e hora de abertura do chamado, data e hora do início do atendimento, data e hora do início de atendimento local, se for o caso, data e hora de encerramento ou contorno e descrição da resolução adotada. O relatório deverá ser entregue mesmo quando não houver chamados no período.

3.7.2. A entrega do relatório mensal será condição necessária para o Serpro realizar o recebimento definitivo, para fins de pagamento dos serviços executados.

4. Especificação de Valores e Formas de Pagamento

4.1. O pagamento será efetuado em parcela única no 1º (primeiro) dia útil após o 30º (trigésimo) dia corrido da data do recebimento definitivo das subscrições indicadas nos respectivos documentos fiscais entregues no protocolo geral do SERPRO ou por meio do endereço eletrônico a ser informado pelo gestor do contrato.

4.2. No preço estão inclusos todos os impostos, taxas, tributos, seguro, encargos sociais, mão de obra, serviços de instalação e configuração, manuais, gastos com deslocamento, estadia e alimentação dos profissionais se for o caso, e demais despesas decorrentes da prestação do serviço, quando couber.

5. Seleção do Fornecedor

5.1. A contratação será realizada na Modalidade de Pregão Eletrônico conforme disposto no Art. 32, inciso IV, da Lei nº 13.303/2016 c/c os procedimentos do Pregão definidos na Lei nº 14.133/2021.

5.2. Será considerada vencedora do processo licitatório a empresa que apresentar proposta com o menor preço por item.

5.3. Apresentar Atestado de Capacidade Técnica de acordo com Cláusula editalícia padrão do SERPRO.

6. Da Resposta a Consulta Pública

6.1 As empresas interessadas devem responder à Consulta Pública, por meio do endereço eletrônico: cp.ecnti@serpro.gov.br.

6.2 As empresas interessadas devem responder à consulta pública com as seguintes informações:

6.2.1 Anexo "A" - Planilha de requisitos

6.2.1.1 A planilha de requisitos preenchida, conforme orientações abaixo:

6.2.1.1.1 "N" = requisito "Nativo".

6.2.1.1.2 "NP" = requisito "Necessita de Parametrização".

6.2.1.1.3 "C" = requisito "Customizado".

6.2.1.1.4 "NA" = requisito "Não Atende".

6.2.1.1.4.1 Se não atende, como poderia atender? Indique customizações necessárias e de baixa complexidade para ser atendido plenamente - a empresa se compromete a implementá-lo na totalidade até a implantação da solução

6.2.2. Da Plataforma.

6.2.2.1. Nome da solução ofertada.

6.2.2.2. Site WEB do fabricante da solução (www).

6.2.3. Proposta comercial

6.2.3.1. A proposta comercial deve conter no mínimo:

6.2.3.1.1. descrição do objeto, valor unitário e total dos serviços;

6.2.3.1.2. Cadastro Nacional de Pessoa Jurídica - CNPJ;

6.2.3.1.3. endereços físico e eletrônico e telefone de contato;

6.2.3.1.4. data de emissão; e

6.2.3.1.5. nome completo e identificação do responsável.

6.2.3.2. A proposta deve considerar todas e quaisquer despesas com recursos humanos, bem como os demais encargos trabalhistas, previdenciários, fiscais e comerciais, materiais, inclusive de consumo, taxas, inclusive de administração, emolumentos, prêmios de seguro, despesas e obrigações financeiras de qualquer natureza e outras despesas diretas ou indiretas, enfim, todos os componentes de custo dos serviços, inclusive lucro, necessários ao perfeito cumprimento do serviço.

7. Da Transparência

7.1. Todos os documentos e informações relacionados ao processo de contratação do Serpro e desta consulta pública estão disponíveis no site:

<https://www.transparencia.serpro.gov.br/acesso-a-informacao/licitacoes-e-contratos>

7.2. Para este processo foi observado a política de integridade de acordo com art. 32, inc. V, da Lei nº 13.303/2016, Programa Corporativo de Integridade do SERPRO - PCINT (TR - 138/2022) e a Cartilha de Integridade do Processo de Aquisições e Contratações.

7.2.1. Para conhecimento das regras de conduta no relacionamento entre fornecedores e empregados do SERPRO, acesse a Cartilha de Integridade do Processo de Aquisições e Contratações, disponível no link:

https://www.transparencia.serpro.gov.br/acesso-a-informacao/licitacoes-e-contratos/documentos/Cartilha_paq_verso_final_diagramada.pdf

7.3. Ressaltamos que o Serpro não concede ou autoriza nenhum tipo de registro de oportunidade em seus processos de contratação.