banco da amazônia

GESEC – Gerência Executiva de Segurança Corporativa
COSCI – Coordenadoria de Segurança Cibernética

NOTA TÉCNICA GESEC/COSCI Nº 019/2025 Data: 05/11/2025

ASSUNTO: ANÁLISE TECNICA DA SOLUÇÃO DE DRP DA EMPRESA DFENSE SECURITY - PE 90022/2025

De acordo:

05/11/2025

X 

Eduardo da Costa Dias Junior
Gerente Executivo Interino - GESEC
Assinado por: 7177

Senhor Pregoeiro,

I – INTRODUÇÃO

O objetivo desta Nota Técnica é levarmos ao seu conhecimento nossos esclarecimentos acerca da Prova de Conceito (PoC) da solução de Proteção contra Riscos Digitais (DRP) apresentada no dia 30/10/2025 pela empresa DFENSE Security – inscrita no CNPJ sob o nº 29.559.799/0001-32, em conformidade com o Edital do Pregão Eletrônico nº 90022/2025 e seu Anexo I-C – Prova de Conceito.

II – ANÁLISE TÉCNICA DA GESEC/COSCI

1. CONTEXTO

A PoC foi realizada em 30/10/2025, das 09h às 10h30, por videoconferência na plataforma Microsoft Teams do Banco da Amazônia, com compartilhamento de tela pela licitante, em conformidade com os requisitos metodológicos estabelecidos no Anexo I-C – Prova de Conceito, e teve por objetivo comprovar, na prática, o atendimento às funcionalidades e condições de operação da solução de DRP, tomando como referência a planilha de atendimento ponto a ponto enviada pela licitante e o respectivo conjunto de requisitos funcionais da solução.

2. METODOLOGIA

Durante a sessão, a empresa DFENSE Security:

- Compartilhou uma planilha com o mapeamento de cada requisito da PoC aos recursos da solução (plataforma Vider, do fabricante Zenuex), seguindo a mesma numeração dos itens do Anexo I-C – Prova de Conceito (ex.: 2.7.x).

- Configurou o monitoramento utilizando os ativos previstos no edital (domínios, marca e identidade visual do Banco da Amazônia), em linha com o item 2.2 do Anexo I-C – Prova de Conceito.

- Demonstrou ao vivo a ocorrência de eventos reais relacionados ao Banco da Amazônia (menções, documentos, vídeos, repositórios de código, credenciais, etc.) e, quando não havia incidente real no período da PoC (ex.: defacement de página do Banco), utilizou eventos de demonstração para comprovar a capacidade técnica da solução.

Durante toda a apresentação, a área técnica pôde interromper, questionar e pedir detalhamento – o que foi prontamente atendido pela equipe da licitante.

3. AVALIAÇÃO TÉCNICA

Abaixo, um resumo consolidado dos principais grupos de requisitos da PoC seguidos de sua avaliação técnica:

1. **Monitoramento de marca, páginas e anúncios falsos**
    - Foram demonstradas detecções de:
        - Páginas e conteúdos utilizando o nome e a marca do Banco da Amazônia em sites de terceiros.
        - Anúncios em redes sociais com menções ao Banco.
    - A solução apresentou o conteúdo capturado (URL, texto, imagem, datas, severidade e links originais), permitindo análise de fraude e uso indevido da marca.
    - **Avaliação técnica:** requisitos atendidos – monitoramento de marca com boa visibilidade operacional.
2. **Defacement e typosquatting / domínios e certificados suspeitos**
    - Defacement: por se tratar de um tipo de incidente eventual, não houve caso real envolvendo o Banco da Amazônia no período da PoC; a funcionalidade foi demonstrada em ambiente de demonstração da Zenuex, mostrando como o sistema identifica alteração maliciosa de conteúdo (“hackeado por…”) em página monitorada.
    - Typosquatting / domínios suspeitos: foram apresentados eventos reais de domínios semelhantes ao nome do Banco, com variações na grafia, incluindo detalhes técnicos do domínio e certificado (código de resposta HTTP, código-fonte da página, certificado, tecnologias utilizadas, requisições de rede, etc.).
    - **Avaliação técnica:** requisitos atendidos – funcionalidade existente e demonstrada; no caso de defacement, a validação foi feita por simulação controlada, o que é aceitável dada a natureza do requisito.

3. **Monitoramento de credenciais vazadas (corporativas e de clientes)**

    - A solução demonstrou:

        - Coleta de credenciais expostas (combo lists e infostealers), com distinção entre eventos históricos e recentes.

        - Visualização de usuários, parte da senha (no caso de contas de cliente) e senha em texto aberto nos casos de contas corporativas, com possibilidade de exportação estruturada (CSV) contendo, inclusive, o campo de senha descriptografada.

        - Capacidade de recuperar o pacote completo gerado por malware (pasta com arquivos de sistema, senhas de navegadores, cookies de sessão, etc.), o que permite investigação aprofundada de incidentes.

    - **Avaliação técnica:** requisitos atendidos – monitoramento de credenciais vazadas com nível de detalhamento adequado para resposta a incidentes e gestão de risco de credenciais.

4. **Cartões e BINs, chaves de código, tokens e arquivos críticos (Git, repositórios, parceiros)**

    - BINs de cartões: como não havia caso real com BIN do Banco no período da PoC, foi utilizado um grupo de mensageria controlado para demonstrar a detecção de BIN e a geração de alerta.

    - Repositórios de código / Git: foram mostrados eventos reais envolvendo:

        - Repositórios públicos contendo referências ao Banco da Amazônia (nome, domínios, identidade visual, simuladores e páginas de eventos).

        - Extração do trecho de código relevante, com possibilidade de baixar o arquivo original, mesmo que o repositório venha a ser tornado privado posteriormente.

    - A solução permite monitorar termos específicos, nomes de projetos, dependências vulneráveis, etc., inclusive em repositórios de parceiros (monitoramento de supply chain).

    - **Avaliação técnica:** requisitos atendidos – a solução oferece visibilidade compatível com as necessidades de DRP e de segurança de desenvolvimento / terceiros.

5. **Documentos vazados e classificação; OCR, similaridade de logotipo e imagens**

    - Foram demonstradas coletas de documentos e apresentações públicos que mencionam o Banco da Amazônia (ex.: apresentações em Slideshare, Scribd, documentos técnicos), com extração de texto e metadados.

    - A solução realizou:

        - OCR em imagens, capturando menções textuais ao Banco em prints e publicações.

        - Similaridade de logotipo, detectando uso da marca em imagens em diferentes contextos.

    - Um caso concreto apresentado foi uma palestra antiga do próprio Banco, identificada pela ferramenta, usada como exemplo para discussão de ajuste de sensibilidade (falso positivo x interesse do Banco).

    - **Avaliação técnica:** requisitos atendidos – funcionalidades presentes e operacionais; sensibilidade é ajustável em conjunto com o fabricante e com a empresa DFENSE Security, para equilibrar abrangência e volume de falsos positivos.

6. **Tracking pixel / monitoramento de integridade de páginas**

    - Foi explicada a forma de uso do tracking pixel, cuja implementação depende da inserção de tag nos portais/aplicações do Banco.

    - Embora não haja tag hoje nos portais do Banco, foi demonstrado o fluxo de geração da tag e ativação da regra, assim como a lógica de detecção de alterações/registros irregulares de scripts.

    - **Avaliação técnica:** requisitos atendidos – capacidade disponível, sujeita à futura implantação técnica pelo Banco.

7. **Uso de Inteligência Artificial, triagem e redução de falsos positivos**

    - A plataforma utiliza IA:

        - Na extração de entidades a partir de linguagem natural (não apenas regex).

        - Na triagem de eventos x alertas, priorizando casos mais relevantes.

- Na análise estatística de combos duplicados x credenciais novas, reduzindo ruído (ex.: bilhões de linhas processadas com deduplicação).

- Na geração de relatórios analíticos (PDF) com interpretação automática dos dados e indicadores.

- Foi demonstrada também a interface conversacional para consultas e investigações (assistente interno da plataforma).

- **Avaliação técnica:** requisitos atendidos – aderentes ao uso de IA na triagem/exclusão de falsos positivos, com potencial para reduzir carga operacional da equipe de segurança.

8. Histórico, trilhas de auditoria, filtros, exportações e APIs

- A PoC demonstrou:

  - Linha do tempo (log) de cada evento, com registro de criação, alteração de status, atribuições, marcação como falso positivo e anotações.

  - Filtros personalizados por categoria, origem, entidade, caso de uso, severidade, status, intervalo de datas, eventos históricos x novos, etc.

  - Exportação em CSV e geração de relatórios PDF customizáveis, com possibilidade de templates e agendamento recorrente.

  - Disponibilidade de API documentada (Swagger) para consulta de eventos, integração com ServiceNow, mensageria e outros sistemas – inclusive via webhooks (Teams, e-mail, etc.), o que atende ao requisito de integração com ferramentas já utilizadas pelo Banco.

- **Avaliação técnica:** requisitos atendidos – funcionalidades atendem ao que foi previsto no Anexo I-C – Prova de Conceito para armazenamento de evidências, trilha de auditoria, relatórios e integração.

4. OBSERVAÇÕES

- Não foram identificadas falhas ou lacunas funcionais na solução apresentada, em relação aos requisitos da PoC descritos no Anexo I-C – Prova de Conceito.

- Alguns requisitos que dependem de incidentes reais no ambiente do Banco (como defacement de página ou exposição de BINs próprios) foram validados por meio de demonstração controlada, o que é compatível com a natureza da PoC.

- A solução oferece recursos adicionais que podem ser explorados na fase de implantação, tais como:
    - Monitoramento de risco em fornecedores e parceiros (supply chain);
    - Integração com Teams / ServiceNow para notificação automática de eventos de severidade alta/crítica;
    - Ajuste fino da sensibilidade de detecção de imagens e logotipo, em conjunto com o time da empresa DFENSE Security e do fabricante, para reduzir falsos positivos sem perda de cobertura.

III – CONCLUSÃO

À luz do que foi apresentado na sessão de 30/10/2025 e considerando os requisitos definidos no Anexo I-C – Prova de Conceito e no item 11.1 do Edital, a área técnica de Segurança Cibernética do Banco da Amazônia conclui que a solução de DRP ofertada pela empresa DFENSE Security atendeu, de forma satisfatória, aos requisitos funcionais e operacionais avaliados na Prova de Conceito.

Dessa forma, manifestamo-nos pela APROVAÇÃO da Prova de Conceito, nos termos do Edital, de modo a permitir a continuidade do certame, em especial a aceitação da proposta da licitante pelo Pregoeiro e o prosseguimento para a fase de habilitação, conforme item 11.3 do Edital.

05/11/2025

X 

Deivison Pinheiro Franco
Coordenador - GESEC/COSCI
Assinado por: 6862