FUNDAÇÃO BUTANTAN
Gestão é uma ciência

EDITAL N.º 090/2025

REQUISIÇÃO DE COMPRA: 3000657681
PROCESSO N° WS1994254294
MODALIDADE: ATO CONVOCATÓRIO
USO DE PLATAFORMA ELETRÔNICA ARIBA
TIPO: MENOR PREÇO
OBJETO DA SELEÇÃO: Solução de segurança da informação baseada em nuvem, de acesso seguro as aplicações, controle de acesso web que tenham recursos granulares, e garantam a segurança independentemente da localização dos usuários ou dispositivos, com os serviços de instalação/configuração, transferência de conhecimento, treinamento e suporte técnico (8x5).
Data e Hora – Evento Envelope: 10.03.2026 às 11:00 (Horário de Brasília)

Data e Hora - Evento de Simulação (Etapa de Lances): 10.03.2026 às 15:00 (Horário de Brasília)

Data e Hora - Evento de Negociação (Etapa de Lances): 11.03.2026 às 11:00 (Horário de Brasília)

QUESTIONAMENTO 2

1. **Quantidade de Aplicações –** Solicitamos esclarecimento sobre quantas aplicações deverão ser configuradas e disponibilizadas na solução ZTNA da plataforma SASE, considerando o ambiente atual e o escopo pretendido pelo Instituto Butantan

RESP FB: Em atendimento ao questionamento apresentado, esclarecemos que, conforme disposto no item 8.1.121 do edital, a solução a ser fornecida deverá possuir capacidade técnica para suportar, no mínimo, 10.000 (dez mil) aplicações, desta maneira o licitante deve considerar a configuração de 10 mil aplicações.

Tal requisito estabelece parâmetro objetivo de dimensionamento da solução, devendo a licitante comprovar que a plataforma ofertada atende integralmente à capacidade exigida

2. **Modelo de Proposta –** o portal Ariba não apresenta Anexos inseridos e/ou disponíveis para DOWNLOAD no ITEM 4.0 DA PLATAFORMA, (4.1 ANEXO II ; 4,2 ANEXO II.1 ; 4.3 PROPOSTA TÉCNICA).

Questiona-se: Previsão de disponibilização dos documentos para adequação da proposta.

RESP FB: Todas os anexos estão disponíveis no edital.

3. Referente ao Item 8.1.59 - Em atenção ao item 8.1.59, deste instrumento convocatório, que trata das capacidades de segurança de navegação e mecanismos de prevenção contra exploits, vimos, respeitosamente, solicitar esclarecimento quanto ao seu correto enquadramento técnico.

Considerando a descrição apresentada, especialmente no que se refere a funcionalidades como isolamento de navegação, inspeção de tráfego HTTPS, utilização de certificados digitais e mecanismos de proteção contra exploração de vulnerabilidades em aplicações de navegação, entendemos que o escopo do referido item está direcionado, precipuamente, à proteção das sessões de navegação web, contemplando a mitigação de ameaças oriundas da internet, o controle de acesso a conteúdo não autorizados e a proteção contra downloads potencialmente maliciosos. Está correto o nosso entendimento?

RESP FB: O item 8.1.59 integra o escopo dos itens 8.1.54 a 8.1.62 do edital, os quais tratam especificamente da capacidade da ferramenta de gerar alertas referentes aos eventos ali descritos.

Tais dispositivos estabelecem que, uma vez ocorridos os eventos no ambiente monitorado, a solução deverá ser capaz de gerar os respectivos alertas e encaminhá-los à CONTRATADA, conforme fluxo operacional previsto.

4. Referente Item 8.1.84 - Considerando os requisitos de segurança previstos no Termo de Referência, entendemos que, para assegurar a proteção adequada das comunicações corporativas, a inspeção do tráfego de voz (VoIP) deverá ser realizada obrigatoriamente por meio da plataforma SASE, não sendo admitido o simples bypass desse tráfego no stack de segurança.
Tal entendimento fundamenta-se nas melhores práticas de mercado e nos princípios de arquitetura Zero Trust, uma vez que a inspeção via SASE permite aplicação uniforme de políticas de segurança, prevenção de intrusões, mitigação de fraudes e ataques específicos a protocolos de sinalização (como SIP), além de garantir visibilidade, rastreabilidade e governança centralizada do tráfego de voz, sem comprometer desempenho ou qualidade do serviço quando devidamente dimensionado.
Dessa forma, questiona-se:
Está correto o entendimento de que a solução a ser contratada deverá contemplar inspeção ativa e mecanismos de proteção para o tráfego de voz dentro da arquitetura SASE?

RESP FB: O item 8.1.84 integra o escopo dos itens 8.1.80 a 8.1.84 do edital, os quais tratam dos requisitos funcionais relacionados ao controle de banda.

Nesse contexto, faz-se necessário que a aplicação ofertada possua funcionalidade de controle de banda, permitindo a adequada gestão, limitação e priorização do tráfego, em conformidade com as diretrizes estabelecidas no edital.

5. **Referente ao Item 8.1.124:** Em atenção ao item 8.1.124, considerando os requisitos de auditoria, rastreabilidade e governança previstos no Termo de Referência, entendemos que a solução deverá contemplar retenção mínima de logs pelo período de 90 (noventa) dias, de forma nativa ou por meio de mecanismo complementar devidamente integrado.
Tal entendimento fundamenta-se em aspectos técnicos e de boas práticas amplamente adotadas no mercado, dentre os quais destacamos:

- A necessidade de manutenção de trilhas de auditoria suficientes para investigação de incidentes de segurança, cujo tempo médio de detecção (MTTD) pode ultrapassar semanas;
- A aderência a frameworks e normas de referência (como ISO/IEC 27001 e boas práticas de governança e continuidade), que recomendam retenção adequada de registros para fins de auditoria e resposta a incidentes;
- A garantia de rastreabilidade histórica para análises forenses, correlação de eventos e comprovação de conformidade regulatória;
- A mitigação de riscos associados a ameaças persistentes avançadas (APT), cujo ciclo de exploração pode ocorrer de forma silenciosa e prolongada.

Dessa forma, questiona-se:
Está correto o entendimento de que a solução a ser contratada deverá assegurar retenção mínima de logs por período não inferior a 90 (noventa) dias, garantindo integridade, disponibilidade e capacidade de consulta para fins de auditoria e investigação?

RESP FB: Conforme estabelecido no item 8.1.47 do edital, a solução deverá garantir a retenção de logs pelo período mínimo de 1 (um) mês de forma nativa

6. Após análise técnica sucinta do edital, nossos times técnicos identificaram alguns pontos que gostaríamos de submeter à apreciação dessa Comissão, especificamente em relação aos seguintes itens:

- 8.1.151 – Daily Bandwidth Quota (Quota Diária de Banda)
- 8.1.152 – Deve permitir controle de banda em MB para uso do WhatsApp Web
- 8.1.153 – O sistema deve bloquear ou restringir o acesso quando a quota diária for atingida

As soluções modernas de arquitetura SASE (Secure Access Service Edge), operam com mecanismos avançados de identificação de aplicações (App-ID), inspeção SSL/TLS e aplicação de políticas dinâmicas de controle de tráfego, dispensando o modelo tradicional de quota diária rígida por MB.

O conceito de Daily Bandwidth Quota é característico de arquiteturas legadas baseadas em proxy ou firewall perimetral, nas quais o controle era realizado por volume acumulado de tráfego diário.

Em ambientes corporativos modernos, esse modelo apresenta limitações relevantes:

•Interrupção abrupta de aplicações legítimas ao atingir limite diário.
•Impacto potencial na continuidade operacional.
•Necessidade de controle manual frequente.
• Complexidade administrativa sem ganho proporcional de segurança.

Arquiteturas SASE contemporâneas permitem:

• Classificação específica do WhatsApp Web como aplicação distinta.
• Controle granular de banda por meio de traffic shaping, com limitação de throughput (kbps/mbps), controle percentual ou priorização por política.
• Aplicação de políticas por usuário, grupo, perfil ou unidade organizacional.
• Monitoramento contínuo e geração de relatórios detalhados de consumo.

O objetivo de governança de banda pode ser plenamente atendido por meio de controle de banda configurável por aplicação, sem necessidade de bloqueio automático quando um volume diário for atingido.

Importante destacar que o bloqueio ou restrição automática por quota diária não representa prática recomendada nas arquiteturas SASE modernas, cujo modelo prioriza controle inteligente, priorização de tráfego e qualidade de serviço, mantendo equilíbrio entre segurança e continuidade operacional.

Nosso Pedido

Dessa forma, solicitamos que o atendimento aos itens 8.1.151, 8.1.152 e 8.1.153 possa ser considerado através da funcionalidade:

“Deve permitir controle de banda para uso do WhatsApp Web.”

Tal abordagem atende tecnicamente ao objetivo do edital, com maior aderência às melhores práticas atuais de mercado em segurança baseada em nuvem.

RESP FB: Sim, consideramos que os itens 8.1.151, 8.1.152 e 8.1.153, com a abordagem atual de controle de banda por aplicação, atendem aos requisitos estabelecidos.

7. Item 8.1.10 Utilização de proxy explícito via arquivos PAC (Proxy Auto-Configuration), neste caso com funcionalidades limitadas a acesso Web HTTP, HTTPS e FTP;

Entendemos que a utilização de arquivos PAC (Proxy Auto-Configuration) está diretamente relacionada à funcionalidade de Secure Web Gateway (SWG), cuja aplicação se dá, primordialmente, sobre tráfego Web, notadamente os protocolos HTTP e HTTPS.

Considerando que o protocolo FTP possui uso cada vez mais restrito e que, tecnicamente, o modelo de proxy explícito via PAC é amplamente aplicado ao controle de tráfego Web (HTTP/HTTPS), entendemos que o atendimento do requisito por meio do suporte a proxy explícito via PAC para acessos HTTP e HTTPS é suficiente para caracterizar conformidade com o item. Está correto o entendimento?

RESP FB: Está correto o entendimento.

Item 8.1.17 Deve ser possível definir a localização do usuário baseado em IP e País de Origem;

Esclarecemos que a solução permite o controle de acesso à console de gerenciamento com base em endereços IP previamente definidos.

Entretanto, a restrição direta por "país de origem", baseada exclusivamente em geolocalização, não é realizada de forma nativa como critério isolado. Entendemos que o atendimento ao requisito pode ser viabilizado por meio da definição de regras de acesso baseadas nos blocos de endereçamento IP oficialmente atribuídos ao país desejado, restringindo, assim, o acesso aos intervalos de IP correspondentes àquela localidade.

Dessa forma, entendemos que o requisito será considerado atendido mediante a implementação de restrições baseadas em faixas de IP associadas ao país pretendido. Está correto o entendimento?

RESP FB: Considerar que o item 8.1.17 está ligado a item 8.1.16 esta correto o entendimento, seguindo que a definição da regra seja configurada pelo licitante.

Item 8.1.18 O portal de administração da plataforma deve suportar a adição de usuários. Na configuração de senha do novo usuário deve ser possível as seguintes opções para criação da senha: Senha definida pelo próprio usuário, senha definida pelo administrador da solução e senha autogerada pela própria plataforma

Esclarecemos que a solução suporta a modalidade de senha definida pelo próprio usuário, em conformidade com boas práticas de segurança e governança de acesso.

Entendemos que a obrigatoriedade de disponibilização simultânea das três modalidades de definição de senha não impacta diretamente a operacionalização do console de gerenciamento, tampouco compromete os controles de segurança, considerando que o requisito pode ser plenamente atendido por meio da política de autenticação adotada (inclusive com integração a provedor de identidade, quando aplicável).

Adicionalmente, a exigência cumulativa das três modalidades pode restringir a competitividade do certame, ao limitar a participação de soluções consolidadas no mercado que adotam modelo distinto de gestão de credenciais.

Dessa forma, entendemos que o atendimento a uma das modalidades de definição de senha, especialmente a opção de senha definida pelo próprio usuário, será considerado suficiente para fins de conformidade com o item 8.1.18. Está correto o entendimento?

RESP FB: Está correto o entendimento

8. Item 8.1.36 Fedora;

Observamos que a distribuição Linux Fedora possui perfil predominantemente voltado a desenvolvimento e ambientes de testes, não sendo amplamente adotada em ambientes corporativos de produção.

A solução ofertada não contempla suporte específico ao Fedora. Considerando o contexto de uso corporativo e visando ampliar a competitividade do certame, entendemos que a compatibilidade com essa distribuição possa ser tratada como característica desejável, e não obrigatória, desde que sejam atendidas as demais distribuições Linux com ampla adoção e suporte corporativo.

Está correto o entendimento?

RESP FB: Está correto o entendimento

9. Item 8.1.38 CentOS;

Verificamos que o sistema operacional CentOS Linux teve seu ciclo de vida encerrado (End of Life – EOL) pelo fabricante em 2024, conforme comunicado oficial da Red Hat.

Considerando que se trata de uma distribuição descontinuada, sem atualizações regulares de segurança e suporte oficial do mantenedor, entendemos que a exigência de compatibilidade com sistemas operacionais fora do ciclo de suporte do fabricante pode representar risco operacional e de segurança.

Dessa forma, entendemos que o agente único deva ser compatível com sistemas operacionais que estejam em ciclo ativo de suporte pelo respectivo fabricante, não sendo obrigatório o atendimento específico ao CentOS descontinuado. Está correto o entendimento?

RESP FB: Está correto o entendimento

10. Item 8.1.39 MacOS 10.10 e superiores;

Observamos que o requisito estabelece suporte a versões do macOS a partir da 10.10. Entretanto, diversas versões compreendidas nesse intervalo já se encontram fora do ciclo de suporte (End of Life – EOL) pelo fabricante, não recebendo mais atualizações de segurança ou correções oficiais.

Nossa solução oferece suporte a versões do macOS a partir da versão 14, contemplando exclusivamente sistemas operacionais que estejam em ciclo ativo de suporte pelo fabricante, em conformidade com boas práticas de segurança da informação e gestão de vulnerabilidades.

Dessa forma, entendemos que o agente único deva ser compatível apenas com sistemas operacionais que possuam suporte ativo do respectivo fabricante, não sendo obrigatória a compatibilidade com versões já descontinuadas. Está correto o entendimento?

RESP FB: Está correto o entendimento

11. Item 8.1.40 IOS 9 e superiores;

O requisito estabelece suporte a versões do iOS a partir da versão 9. Contudo, diversas versões compreendidas nesse intervalo já se encontram fora do ciclo de vida (End of Life – EOL) definido pelo fabricante, não recebendo atualizações de segurança ou suporte oficial.

Nossa solução oferece suporte a versões do iOS a partir da versão 15.1, contemplando exclusivamente sistemas operacionais que estejam em ciclo ativo de suporte pelo fabricante, em conformidade com boas práticas de segurança da informação e gestão de vulnerabilidades.

Dessa forma, entendemos que o agente único deva ser compatível apenas com sistemas operacionais que possuam suporte ativo do respectivo fabricante, não sendo obrigatória a compatibilidade com versões já descontinuadas. Está correto o entendimento?

RESP FB: Está correto o entendimento

12. Item 8.1.41 Android 8 e superiores;

O requisito estabelece suporte a versões do Android a partir da versão 8. Contudo, diversas versões compreendidas nesse intervalo já se encontram fora do ciclo de vida (End of Life – EOL) definido pelo fabricante e pelo ecossistema de suporte, não recebendo atualizações regulares de segurança.

Nossa solução oferece suporte a versões do Android a partir da versão 13, contemplando exclusivamente sistemas operacionais que estejam em ciclo ativo de suporte, em conformidade com boas práticas de segurança da informação, gestão de vulnerabilidades e

recomendações de fabricantes.

Dessa forma, entendemos que o agente único deva ser compatível apenas com sistemas operacionais que possuam suporte ativo pelo respectivo fabricante, não sendo obrigatória a compatibilidade com versões já descontinuadas. Está correto o entendimento?

RESP FB: Está correto o entendimento

13. Item 8.1.65 Deve ser capaz de bloquear versões antigas de TLS para certas aplicações, usuários e grupos;

Considerando que versões antigas do protocolo TLS apresentam vulnerabilidades amplamente conhecidas e representam risco à segurança da informação, entendemos que tais versões devem ser bloqueadas por padrão, como medida de proteção abrangente ao ambiente.

Nossa solução realiza o bloqueio integral de conexões que utilizem versões obsoletas de TLS, aplicando essa política de forma global ao tráfego. Adicionalmente, quando tecnicamente necessário, é possível configurar exceções específicas relacionadas à inspeção (por exemplo, definição de destinos que não serão decriptografados), mantendo-se, ainda assim, os controles de segurança aplicáveis.

Dessa forma, entendemos que o atendimento ao requisito se dá por meio do bloqueio global de versões antigas de TLS, por representar abordagem mais segura e alinhada às boas práticas de mercado, ainda que não segmentado especificamente por aplicação, usuário ou grupo. Está correto o entendimento?

RESP FB: Considerando que no ambiente da CONTRATADA existem exceções que precisam ser atendidas, a solução deverá contemplar integralmente o atendimento ao item 8.1.65.

Itens 8.1.151 Daily Bandwidth Quota (Quota Diária de Banda)

8.1.152 Deve permitir definição de limite diário em MB para uso do WhatsApp Web.

8.1.153. O sistema deve bloquear ou restringir o acesso quando a quota diária for atingida.

A solução permite a definição de limites de utilização de banda para aplicações específicas, incluindo o WhatsApp Web, por meio de políticas de controle de tráfego baseadas em percentual da banda total disponível ou em valores absolutos de throughput (expressos em Mbps ou Gbps).

Esclarecemos que o controle de banda é aplicável aos acessos realizados por meio de integração via túneis IPSEC/GRE, não sendo suportado para tráfego direcionado por agente único.

Dessa forma, entendemos que o requisito é atendido por meio da limitação de banda por aplicação e consequente restrição de tráfego quando atingidos os parâmetros configurados, ainda que a métrica adotada seja baseada em throughput e não especificamente em volume acumulado diário em MB, e restrita ao modo de encaminhamento via túnel. Está correto o entendimento?

RESP FB: Sim, consideramos que os itens 8.1.151, 8.1.152 e 8.1.153, com a abordagem atual de controle de banda por aplicação, atendem aos requisitos estabelecidos.

14. Itens 8.1.79 A solução deve suportar controle de banda;

8.1.80 Deve ser possível aplicar o controle de banda para as seguintes classes de aplicações:

8.1.81 Navegação em Geral;

8.1.82 Streaming;

8.1.83 File Sharing;

A solução permite a definição de políticas de controle de banda aplicáveis a categorias específicas de aplicações, incluindo Navegação em Geral, Streaming e File Sharing, por meio de limitação baseada em percentual da banda total disponível ou em valores absolutos de throughput (expressos em Mbps ou Gbps).

Esclarecemos que o controle de banda é suportado para tráfego encaminhado por meio de integração via túneis IPSEC/GRE, não sendo aplicável ao tráfego direcionado por agente único.

Dessa forma, entendemos que o requisito é atendido por meio da implementação de políticas de limitação de banda por categoria de aplicação, ainda que restrito ao modo de encaminhamento via túnel. Está correto o entendimento?

RESP FB: Os itens 8.1.79 a 8.1.83 do edital deverão ser atendidos pela solução, independentemente do método utilizado para sua implementação.

15. O item 6.9 do Edital estabelece que a etapa de lances terá duração de 15 (quinze) minutos. O item 6.12, por sua vez, prevê prorrogação automática de 5 (cinco) minutos sempre que um lance for registrado nos últimos 2 (dois) minutos do prazo. Solicita-se esclarecer se há limite máximo de prorrogações sucessivas ou se a sessão pode ser prorrogada indefinidamente enquanto houver lances nos últimos 2 minutos de cada período.
RESP FB: **Não existe limite de prorrogação.**

16. Considerando que a prorrogação é automática e sucessiva, confirma-se que os 15 minutos previstos no item 6.9 representam apenas o prazo mínimo de duração da etapa, podendo a sessão se estender por período superior caso as condições de prorrogação sejam atingidas?
RESP FB: Correto.

17. A prorrogação automática se aplica a qualquer lance registrado nos últimos 2 minutos, independentemente do valor ou da redução mínima exigida de 2%? Ou seja, um lance válido nos últimos 2 minutos é suficiente para acionar a prorrogação?
RESP FB: Correto entre partes, qualquer lance válido aciona a prorrogação, já que o sistema não deixará ocorrer nenhuma redução abaixo da redução mínima já citada no edital.