Anexo nº II/SEF/STI-GOVERNANÇA-DSI/2025

PROCESSO Nº 1190.01.0006603/2025-21

Item	Requisitos (para demonstração e/ou apresentação de documentação oficial)	Atende? (sim / sim parcialmente / não)	Observações
1	**Solução Security Service Edge (SSE)**		
1.1	**Características Gerais da Solução**		
1.1.1	A solução deve ser entregue em uma plataforma integrada do fabricante, permitindo a navegação entre as tecnologias por meio de console única. Considera-se composição a existência de gerenciamento segregado e a necessidade de login em solução de terceiros.		
1.1.2	A solução de SSE deve fornecer os seguintes recursos: • FWaaS (Firewall as a Service); • ZTNA (Zero Trust Network Access); • SWG (Secure Web Gateway); • RBI (Remote Browser Isolation); • CASB (Cloud Access Security Broker); • DLP (Data Loss Prevention);		
1.1.3	A solução deve ter ao menos um ponto de presença no Brasil;		
1.1.4	A solução deve permitir e estar licenciada para provisionamento em, no mínimo, 4 (quatro) pontos de presença (POP);		
1.1.5	Os 4 (quatro) pontos de presença incluídos na solução devem permitir a configuração de, no mínimo, 1 (um) endereço IP fixo para cada. Caso a solução exija licenciamento adicional, este deve ser entregue para todos os POPs;		

1.1.6	A solução deve possuir, além da redundância geográfica, a possibilidade da SEF/MG escolher em qual POP os logs serão armazenados para estar em compliance com legislações locais;		
1.1.7	O acesso à console de administração da solução SSE deve ser feito via navegador web e ter a possibilidade de se integrar com IdP para autenticação SSO dos usuários administrativos;		
1.1.8	A solução deve permitir a criação de políticas de acesso baseadas em contexto, como localização geográfica e horário;		
1.1.9	A solução deve garantir o acesso seguro à web, serviços em nuvem e aplicações privadas, independentemente da localização do usuário ou de onde essas aplicações estão hospedadas;		
1.1.10	A solução deve fornecer proteção contra ameaças à rede em tempo real, atuando sobre o tráfego originado no dispositivo do usuário com destino às aplicações e serviços de internet;		
1.1.11	A solução deve estar em conformidade com as regulamentações e padrões de segurança relevantes, como a Lei Geral de Proteção de Dados Pessoais (LGPD);		
1.1.12	A solução deve ser monitorada e gerenciada 24 (vinte e quatro) horas por dia, 07 (sete) dias por semanas, com disponibilidade mensal de 99.999% para todos os serviços;		
1.1.13	A comunicação entre agentes (clientes) e outras soluções de infraestrutura SSE devem sempre usar comunicação segura criptografada;		
1.1.14	A solução deve entregar tenant exclusivo e isolado, evitando que os dados possam ser acessados por outros tenants, mantendo o sigilo da informação, com acesso via internet e por conexão;		
1.1.15	O fabricante deve possuir ao menos uma das seguintes certificações de compliance SOC 2 Tipo 2, ISO 27001, ISO 27701 e ISO 27018.		

1.1.16	Para garantir segurança e agilidade na gestão da solução, todos os módulos de segurança (ZTNA, SWG, RBI e DLP) deverão ser do mesmo fabricante e possuir console única de gerenciamento, de forma que todas as configurações e monitoramento possam ser feitas de forma centralizada. Não será permitido integração com soluções de terceiros.		
1.1.17	Para um ecossistema de segurança robusto e unificado, visando proteger aplicações web, redes corporativas e acessos remotos, a solução deve possuir integração nativa com a solução de proteção de aplicação descrita no ITENS 1, 3 e 4. A integração deve ser através de uma console única ou via API.		
1.2	**Zero Trust Network Access**		
1.2.1	A solução deve atender a políticas de permissão e negação de acesso com base, no mínimo, nas seguintes condições condições: Postura do Dispositivo, Localização do Dispositivo/Usuário e Associação ao Grupo de Usuários;		
1.2.2	A solução deve possuir capacidade de analisar os acessos dos usuários remotos às aplicações na infraestrutura interna da Secretaria de Estado de Fazenda de Minas Gerais (SEF/MG);		
1.2.3	A solução deve possuir capacidade de controlar o acesso de usuários remotos a aplicações internas da SEF/MG, por meio da nuvem do fabricante, de modo que o usuário remoto tenha acesso apenas à aplicação especificada e não a um segmento de rede interna;		
1.2.4	A solução deve possuir, no mínimo, as seguintes funcionalidades: Antimalware, Sandboxing, controle de acesso URL;		
1.2.5	O ZTNA não deve ter acesso e nem ser atribuído a um segmento de rede interna como ocorre com a Virtual Private Network (VPN);		
1.2.6	A solução deve prover acesso a aplicações internas específicas, via browser, sem agente para usuários remotos com dispositivos não gerenciados;		

1.2.7	O acesso sem agente deverá promover conexão segura ao portal da solução, o qual proverá controle de tráfego para as aplicações internet, SaaS e internas;		
1.2.8	A solução deve possibilitar a execução de políticas de segurança das seguintes formas: • Antes da conexão com a SEF/MG (verificação de compliance); • Após autenticação do usuário na estação; • Sob demanda da secretaria;		
1.2.9	A solução deve bloquear ou quarentenar usuários por perfis de acesso e grupo de ativos, quando esses não atenderem às políticas de segurança;		
1.2.10	A solução deve possuir mecanismos de checagem de conformidade do dispositivo remoto;		
1.2.11	A solução deve verificar, no mínimo, as seguintes informações no cliente remoto: Sistema Operacional, Processos Ativos, Antimalware e versão instalada;		
1.2.12	A solução deve assegurar que a conformidade seja mantida de maneira contínua durante a conexão, mudando o status para "Não compliance", caso seja detectada não conformidade;		
1.2.13	A solução deve prover a conexão entre a solução e a infraestrutura da SEF/MG, permitindo que os usuários remotos acessem as Aplicações/Serviços instalados na infraestrutura da secretaria;		
1.2.14	A solução deve prover a criação de conexões seguras para garantir a confidencialidade dos dados em trânsito entre a Solução e a infraestrutura da SEF/MG;		

1.2.15	A solução deve prover a configuração de um portal para acesso às aplicações internas sem a necessidade de agente instalado na máquina do usuário; • No caso de acesso sem o uso de agentes, o IdP (Identity Provider) deverá ser utilizado para validar a identidade do usuário antes de fornecer qualquer tipo de conectividade via Proxy Reverso, ou similar, com a aplicação Web privada;		
1.2.16	O portal para acesso às aplicações internas, sem a necessidade de um agente instalado na máquina do usuário, deve suportar a configuração de no mínimo: • Aplicações WEB (HTTP e HTTPS); • RDP; • SSH;		
1.2.17	A solução deve suportar a integração com aplicações SaaS e on-premises;		
1.2.18	A solução deve permitir a adição de aplicações web autogerenciadas, configurando-as como aplicações self-hosted;		
1.2.19	A solução deve oferecer integração com aplicações de infraestrutura, permitindo o controle de acesso a servidores SSH, bancos de dados e outros serviços não HTTP;		
1.2.20	A solução deve permitir a publicação segura de aplicações autogerenciadas na Internet, utilizando mecanismos de conexão segura entre o servidor de origem e a rede protegida;		
1.2.21	A solução deve possibilitar a aplicação de políticas de segurança específicas para cada aplicação;		
1.2.22	A solução deve permitir a configuração de páginas de login personalizadas para aplicações protegidas;		

1.2.23	A solução deve permitir a configuração de páginas de bloqueio personalizadas para acessos não autorizados;		
1.3	**Secure Web Gateway - SWG**		
1.3.1	A solução deve suportar a implementação de Secure Web Gateway (SWG) para controle e proteção do tráfego de internet;		
1.3.2	A solução deve ser responsável pela visibilidade e controle do tráfego por camada de aplicação de forma granular;		
1.3.3	A solução deve permitir a criação de listas customizadas para filtragem web, incluindo bloqueio e permissão por, no mínimo: • URL; • Categoria; • Domínio; • IP;		
1.3.4	A solução deve prover visibilidade e controle em tempo real de acesso a URLs, por meio de classificação baseada em categorias;		
1.3.5	A solução deve ser responsável pela visibilidade e controle do tráfego corporativo em direção ao Microsoft Office 365, em tempo real a partir de estações de trabalho com agente ou via RBI;		
1.3.6	A solução deve prevenir e restringir acesso a sites maliciosos;		
1.3.7	A solução deve prevenir contra download de artefatos maliciosos;		
1.3.8	A solução deve ser compatível com as plataformas Windows, MacOS, Linux, Android e IOS;		
1.3.9	A solução deve permitir aplicar ação de bloqueio para contas pessoais e corporativas do Microsoft Office 365 e demais aplicações SaaS;		

1.3.10	A solução deve permitir a criação de regras para acesso à plataforma do Office 365 Corporativo;		
1.3.11	A solução deve oferecer políticas para inspecionar tráfego DNS, de rede, HTTP e de saída, permitindo o bloqueio de domínios e endereços IP maliciosos;		
1.3.12	A solução deve realizar inspeção de SSL/TLS em 100% do tráfego Web, sem limites de volume de transações ou percentual inspecionado, em protocolos TLS 1.2 e superior;		
1.3.13	A solução deve permitir a criação de regras granulares de exceção à inspeção SSL/TLS, com base nas categorias de URL, hosts e domínios de destino, usuário, grupo, ou tipo de browsers;		

1.3.14	A solução deve permitir a configuração de políticas de isolamento de navegador, garantindo que o tráfego seja renderizado em um navegador isolado para proteger contra ameaças da web, possuindo os seguintes requisitos: • Implementar a funcionalidade RBI de forma transparente aos usuários, sem necessidade de alteração de configurações no navegador e sem necessidade de instalação de plugins, além de não provocar impacto significativo no desempenho do site/experiência do usuário do site acessado; • Possibilitar a configuração de forma seletiva (site, domínio, web app), para acessar sites relacionados a novos domínios ou ainda potencialmente maliciosos, de forma isolada e restrita, protegendo o dispositivo do usuário de possíveis ameaças; • Ser compatível com os principais navegadores de mercado como, por exemplo: Google Chrome, Safari, Firefox e Microsoft Edge; • Efetuar a identificação precisa de usuários por meio dos agentes da solução. Para os casos de tráfego associado a usuários em equipamentos sem agente na rede corporativa, a solução deve possibilitar alternativas de rastreabilidade, como a integração com Microsoft AD e Entra ID via SAML;		
1.3.15	A solução deve permitir a aplicação de políticas baseadas na identidade do usuário, utilizando seletores de identidade para filtrar o tráfego de saída;		
1.3.16	A solução deve fornecer logs detalhados e recursos de monitoramento para análise e auditoria;		
1.3.17	A solução deve oferecer autenticação integrada para assegurar que apenas usuários autorizados acessem a internet;		

1.3.18	A solução deve fornecer relatórios detalhados sobre o uso da web e incidentes de segurança;		
1.3.19	A solução deve suportar a análise e controle de tráfego de aplicativos em tempo real;		
1.3.20	A solução deve permitir a configuração de políticas baseadas em identidade do usuário e grupos;		
1.3.21	A solução deve permitir a inspeção de tráfego de aplicações SaaS, fornecendo controle sobre uso de ferramentas não autorizadas;		
1.3.22	A solução deve permitir o controle de acesso a categorias não autorizadas, que imponham risco à segurança, como Botnets, Domain Generation Algorithms (DGA), Command & Control, Sites Maliciosos e Phishing e a sites restritos, como Pornografia, Drogas, Atividades Criminais e Apostas;		
1.3.23	A solução deve possibilitar o bloqueio dinâmico de domínios recém-criados ou suspeitos;		
1.3.24	A solução deve permitir a segmentação de tráfego por perfil de risco para definir níveis diferenciados de acesso e proteção;		
1.4	**Cloud Access Security Broker (CASB)**		
1.4.1	A solução deve possuir funcionalidades de SSPM (SaaS Security Posture Management – Gerenciamento de postura de segurança SaaS) com a finalidade de identificar, monitorar de forma contínua, categorizar automaticamente aplicações de nuvem em uso (Gerenciadas ou não-gerenciadas), considerando múltiplos critérios de segurança, como postura e compliance;		

1.4.2	A solução deve permitir o bloqueio de aplicações não gerenciadas, para classificação da reputação, contemplando parâmetros, tais como: • Categoria da aplicação; • Configurações inseguras; • Duplo fator de autenticação (MFA) habilitado; • Mecanismos de criptografia; • Score de risco; • Shadow IT (Uso de software não autorizado);		
1.4.3	A solução deve permitir a configuração de quais aplicações SaaS devem ter a inspeção do túnel TLS ativada;		
1.4.4	A solução deve possuir relatório com métricas de utilização dos usuários, atividades e volume de tráfego;		
1.4.5	A solução deve identificar o uso de aplicações não autorizadas e com risco elevado, além de visualização dos usuários que estão utilizando essas aplicações, permitindo ações de mitigação, tais como: • Auditoria; • Cancelar compartilhamento para todos; • Cancelar compartilhamento para usuários externos; • Cancelar compartilhamento para usuários Internos; • Quarentena		
1.4.6	A solução deve prover mecanismos de chamada a sistemas externos por meio de APIs Rest, para automação de processos de notificação, alertas e controle de acesso;		
1.4.7	A solução deve possuir técnicas de monitoração quanto à exposição de dados na internet, identificando ameaças e permitindo criar políticas de segurança automatizadas;		

1.4.8	A solução deve possuir suporte as principais aplicações SaaS hospedadas em infraestrutura de nuvem pública como Azure, AWS e Google, permitindo o registro e monitoramento de todas as atividades do usuário;		
1.4.9	A solução deve possuir alertas de malicious insiders (acesso suspeito de dados), como, por exemplo, alta quantidade de download em curto espaço de tempo;		
1.4.10	A solução deve possuir análise de comportamento de usuários automática para detecção de utilização anômala e comportamento suspeito;		
1.4.11	A solução deve possuir controle de políticas de acesso customizadas para controle de Bring Your Own Device (BYOD) e dispositivos corporativos;		
1.4.12	A solução deve permitir controlar download e upload de arquivos;		
1.4.13	A solução deve permitir criar políticas que revoguem o acesso à determinada aplicação terceira;		
1.4.14	A solução deve permitir monitorar todas as atividades de usuários pré-selecionados;		
1.4.15	A solução deve detectar anomalias e identificar padrões indicativos de atividade maliciosa;		
1.4.16	A solução deve proteger: • contra malwares; • contra sequestro de conta ou sessão;		
1.4.17	A solução deve oferecer controle de acesso granular contextual ou por políticas, com base em variedade de fatores, tais como, dispositivo, localização e atividade;		
1.4.18	A solução deve executar ações de análise de comportamento da entidade do usuário (UEBA), visando a detecção de ameaças internas e contas comprometidas;		
1.5	**Data Loss Prevention**		

1.5.1	A solução deve suportar a inspeção e análise avançada de tráfego para identificar padrões de exfiltração de dados;		
1.5.2	A solução deve suportar a integração com APIs para controle de dados em aplicações de terceiros;		
1.5.3	A solução deve suportar a prevenção de compartilhamento não autorizado de dados entre ambientes de nuvem distintos;		
1.5.4	A solução deve suportar políticas de DLP para identificação de padrões como expressões regulares, OCR e fingerprinting de documentos;		
1.5.5	A solução deve suportar a análise de tráfego HTTP e HTTPS para detecção de dados sensíveis em tempo real;		
1.5.6	A solução deve permitir a configuração de ações automáticas para bloqueio e alerta;		
1.5.7	A solução deve permitir a aplicação de políticas de DLP com base no perfil do usuário, grupo ou área de negócio;		
1.5.8	A solução deve oferecer relatórios detalhados sobre incidentes de DLP, fornecendo visibilidade completa das violações e ações tomadas;		
1.5.9	A solução deve permitir a configuração de listas de permitidos e bloqueados para controle de informações confidenciais compartilhadas;		
1.5.10	A solução deve possibilitar a análise de padrões de transferência de dados para detectar atividades anômalas e suspeitas;		
1.5.11	A solução deve oferecer a capacidade de aplicar políticas granulares para diferentes tipos de dados;		
1.5.12	A solução deve suportar a conformidade com regulamentações como GDPR, LGPD e outras normas de proteção de dados;		
1.5.13	A solução deve permitir auditoria e rastreamento de eventos de DLP para investigações forenses e conformidade regulatória;		

1.5.14	A solução deve suportar a exportação e compartilhamento de logs de DLP para ferramentas de análise e correlação de eventos de segurança;		
1.6	**Monitoramento de Logs**		
1.6.1	A solução deve oferecer alertas automáticos para anomalias de segurança e tentativas de acesso não autorizadas.		
1.6.2	A solução deve suportar logs detalhados para integração com ferramentas externas.		
1.6.3	A solução deve permitir armazenamento seguro dos logs em conformidade com regulamentações como LGPD e GDPR.		
1.6.4	A solução deve suportar auditoria detalhada de eventos de acesso, incluindo logs de autenticação e ações executadas.		
1.6.5	A solução deve permitir exportação automatizada de logs para plataformas SIEM;		
1.6.6	A solução deve suportar retenção de logs por períodos configuráveis para conformidade regulatória;		
1.6.7	A solução deve permitir segmentação de logs por usuário, dispositivo e aplicação acessada;		
1.6.8	A solução deve suportar registros de tentativas de acesso bloqueadas e motivos da rejeição;		
1.6.9	A solução deve oferecer APIs para acesso aos logs e eventos de monitoramento;		
1.7	**Gerenciamento de Políticas**		
1.7.1	A solução deve suportar a criação e gestão centralizada de políticas de acesso.		
1.7.2	A solução deve permitir a definição de políticas com base em identidade, localização e postura do dispositivo.		
1.7.3	A solução deve oferecer mecanismo de atualização dinâmica de políticas com base em inteligência de ameaças.		

1.7.5	A solução deve possibilitar a configuração de ações específicas (permitir, bloquear, bypass, autenticação de serviço) dentro das políticas de acesso.		
1.7.6	A solução deve suportar a definição de regras de inclusão, exclusão e requisitos dentro das políticas, permitindo o controle granular sobre quem pode acessar quais recursos.		
1.7.7	A solução deve permitir a utilização de seletores variados, como identidade do usuário, grupos, endereços IP, países e métodos de autenticação, para a construção de políticas robustas.		
1.7.8	A solução deve fornecer mecanismos para evitar configurações incorretas comuns, como a inclusão inadvertida de todos os usuários em uma política.		
1.7.9	A solução deve oferecer suporte a políticas de acesso extensíveis, permitindo chamadas a qualquer API durante a avaliação de uma política.		
1.7.10	A solução deve permitir a aplicação de políticas de acesso baseadas em contexto e com privilégios mínimos para cada recurso, reduzindo a superfície de ataque e eliminando movimentos laterais.		
1.7.11	A solução deve possibilitar a autenticação de usuários terceirizados (como prestadores de serviços) com opções sem cliente, provedores de identidade, dentre outros métodos.		
1.7.12	Deve fornecer ferramentas para monitoramento e validação contínuos das políticas de acesso implementadas, garantindo conformidade e segurança contínuas.		
1.7.13	Deve permitir a aplicação do princípio do menor privilégio, garantindo que os usuários tenham apenas o acesso necessário para desempenhar suas funções.		
1.8	**Consultas e Relatórios**		
1.8.1	A solução deve possuir opção para gerar relatórios a partir dos dados monitorados;		

1.8.2	A solução deve possibilitar a visualização dos eventos contextualizados e ocorridos no passado (base histórica), possibilitando investigação dos incidentes e suas causas raízes;		
1.8.3	A solução deve disponibilizar todo o ciclo de execução de processos suspeitos, com a opção de visualizar os dados relevantes à análise dos incidentes, com a opção de filtros de buscas;		
1.8.4	A solução deve demonstrar na forma de linha do tempo todos os passos da execução das atividades consideradas suspeitas;		
1.8.5	A solução deve monitorar a experiência do usuário quanto a latência e disponibilidade das aplicações que interagem com a infraestrutura da SEF/MG;		

Documento assinado eletronicamente por **Daniel de Oliveira Rezende**, **Servidor Público**, em 23/07/2025, às 17:30, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Rogério Zupo Braga**, **Superintendente**, em 28/07/2025, às 10:57, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **118803604** e o código CRC **4D42D228**.