



MARINHA DO BRASIL
DIRETORIA DE COMUNICAÇÕES E TECNOLOGIA
DA INFORMAÇÃO DA MARINHA

APÊNDICE I - AO TERMO DE REFERÊNCIA

Nº Processo 63394.001006/2026-85

ESPECIFICAÇÕES TÉCNICAS

1 - OBJETIVO

Especificar tecnicamente a solução de Secure Web Gateway (Proxy) on-premises, suas subscrições de licenciamento, funcionalidades de segurança, gerenciamento centralizado, análise de conteúdo malicioso, atualização e suporte técnico, destinada à continuidade e modernização dos serviços de segurança de navegação da Rede de Comunicações Integrada da Marinha (RECIM).

1.1. Este Apêndice estabelece as características técnicas mínimas da solução. Os quantitativos e valores observarão o Termo de Referência, a pesquisa de preços e os respectivos mapas de formação de preços.

2 - ESCOPO E COMPOSIÇÃO DA SOLUÇÃO

2.1. A solução deverá ser fornecida na modalidade on-premises, integralmente implementada em ambiente virtualizado, com arquitetura distribuída e gerenciamento centralizado, preservando a interoperabilidade com a infraestrutura tecnológica atualmente existente na RECIM.

2.2. O licenciamento deverá contemplar capacidade para 40.000 (quarenta mil) usuários de internet, considerando média aproximada de 20.000 usuários simultâneos, e permitir a operação de, no mínimo, 30 (trinta) instâncias virtuais de proxy distribuídas geograficamente.

2.3. As instâncias poderão ser distribuídas em organizações e pontos de presença no território nacional e em localidades internacionais, incluindo Washington (EUA) e Londres (Inglaterra), devendo o gerenciamento centralizado ser realizado a partir da infraestrutura da Contratante no Rio de Janeiro.

2.4. A aplicação e a ativação das licenças na plataforma Skyhigh Secure Web Gateway On-Premises existente serão realizadas pela equipe técnica da Contratante, com apoio técnico remoto da Contratada quando necessário.

A administração da plataforma, a manutenção das políticas de segurança, a parametrização dos mecanismos de autenticação e a gestão das integrações existentes permanecerão sob responsabilidade da Contratante.

Não estão incluídos no objeto a implantação de nova plataforma, a migração integral de políticas para solução de outro fabricante ou a execução de projeto de reestruturação da infraestrutura da RECIM.

2.5. A contratação não deverá exigir aquisição adicional de ativos de hardware para habilitação das funcionalidades previstas neste Apêndice.

3 - ITENS DE SUBSCRIÇÃO

Grupo	Item	Descrição técnica mínima	Unidade	Qtd.
1	1	Subscrição de licenças para habilitação, implementação, uso e operação da solução de Secure Web Gateway (Proxy) on-premises, em no mínimo 30 instâncias virtuais, para atendimento a 40.000 usuários, incluindo gerenciamento centralizado, políticas, listas, autenticação, atualização e suporte técnico, pelo período de 12 meses.	UN	40.000
	2	Subscrição integrada para análise de conteúdo malicioso (antimalware) em tempo real, compatível com a solução Secure Web Gateway on-premises, com atualizações diárias da base de proteção e vigência de 12 meses, destinada aos mesmos 40.000 usuários.		

3.1. Os itens integram uma única solução tecnológica e deverão operar de forma conjunta e interoperável, sendo vedada composição que prejudique a gestão centralizada, a inspeção do tráfego ou a continuidade operacional.

4 - REQUISITOS FUNCIONAIS DO SECURE WEB GATEWAY

- Suportar operação como proxy explícito e, quando requerido pela arquitetura da Contratante, operação em modo transparente.
- Gerenciar tráfego HTTP, HTTPS e FTP, com aplicação de políticas por usuário, grupo, horário, endereço de origem, rede, localidade, aplicação, serviço, URL, domínio e categoria.
- Realizar inspeção de tráfego criptografado SSL/TLS, inclusive mediante emissão e utilização de certificados para inspeção HTTPS, de acordo com as políticas da Contratante.
- Permitir categorização de sítios e URLs com base mantida e atualizada pelo fabricante, incluindo mecanismo oficial para solicitação de categorização ou recategorização e possibilidade de categorização interna pela Contratante.
- Permitir filtragem por categoria e reputação de URL, com bloqueio de conteúdo malicioso, indesejado ou incompatível com as políticas institucionais.
- Permitir criação de políticas granulares e sequenciadas, com múltiplos critérios de decisão, listas de exceção e regras diferenciadas por contexto de acesso.
- Permitir importação e atualização automática de listas externas por HTTP, HTTPS, FTP ou SFTP, abrangendo, no mínimo, endereços IP, URLs, domínios, usuários, redes e faixas de endereços.
- Permitir utilização de cache de conteúdo, quando aplicável, de forma a contribuir para redução de latência e otimização do consumo de enlaces.
- Permitir exibição de páginas de bloqueio contendo informações sobre a requisição, o usuário e o dispositivo, conforme parametrização da Contratante.

- Permitir que o usuário finalize sua sessão ativa de forma controlada, sem depender exclusivamente do tempo de inatividade ou expiração automática.

5 - AUTENTICAÇÃO E CONTROLE DE ACESSO

- Integrar-se aos mecanismos de autenticação existentes na Marinha do Brasil, preservando a confidencialidade e a integridade das credenciais durante o trânsito entre proxy e serviço de autenticação.
- Possuir compatibilidade com LDAPS e mecanismos de autenticação do tipo Digest, quando aplicáveis ao ambiente da Contratante.
- Permitir autenticação por janela de navegador (popup) ou por página HTTPS redirecionada automaticamente.
- Correlacionar usuários com localização, perfil de acesso, grupo organizacional e contexto da conexão.
- Permitir políticas de restrição de acesso por localidade definida no serviço de autenticação.
- Permitir controle de duplicidade de uso de credenciais, com possibilidade de criação de exceções e definição de quantidade permitida de dispositivos por usuário ou perfil.

6 - PROTEÇÃO CONTRA CONTEÚDO MALICIOSO

- Realizar análise de conteúdo malicioso em tempo real no tráfego processado pela solução.
- Possuir base de proteção contra malware e ameaças com atualização diária ou em periodicidade menor disponibilizada pelo fabricante.
- Detectar e bloquear ameaças conhecidas e, quando suportado pela solução, ameaças sem assinatura com base em mecanismos de reputação, heurística ou análise comportamental.
- Operar de forma integrada ao mecanismo de inspeção SSL/TLS e às políticas do Secure Web Gateway, sem necessidade de console independente para a aplicação das regras de segurança.

7 - GERENCIAMENTO CENTRALIZADO E ALTA DISPONIBILIDADE

- Disponibilizar console centralizado para administração unificada das instâncias de proxy, políticas, objetos, listas, parâmetros de autenticação, eventos e relatórios.
- Permitir inclusão de novas instâncias virtuais de proxy no gerenciamento centralizado durante a vigência da solução.
- Permitir replicação e distribuição de políticas de forma centralizada, com rastreabilidade das alterações administrativas.
- Suportar arquitetura de alta disponibilidade, redundância e failover compatíveis com a implantação distribuída da RECIM.
- Permitir operação e manutenção sem dependência de um único ponto de gerenciamento local nas unidades remotas.

8 - LOGS, AUDITORIA E INTEGRAÇÃO COM SIEM

- Gerar registros de acesso e eventos de segurança suficientes para auditoria, correlação e investigação de incidentes.
- Permitir concentração de logs em servidor ou componente central definido pela Contratante.
- Manter logs localmente em cada instância de proxy por período mínimo de 10 (dez) dias, com mecanismo de rotação, gerenciamento e expurgo controlado.
- Permitir integração com a solução de SIEM da Marinha do Brasil por mecanismos seguros, incluindo HTTPS e/ou SFTP, conforme arquitetura definida pela Contratante.

- Disponibilizar mecanismos de pesquisa, consulta e geração de relatórios por usuário, URL, categoria, período, política aplicada, decisão de bloqueio/liberação e demais atributos disponíveis.

9 - REQUISITOS DE DESEMPENHO E CAPACIDADE

- A solução deverá ser dimensionada para 40.000 usuários cadastrados e média aproximada de 20.000 acessos simultâneos, sem degradação incompatível com o uso institucional.
- O processamento de regras, inspeção de conteúdo e inspeção SSL/TLS deverá ocorrer com capacidade compatível com os picos de consumo da RECIIM e com margem para expansão durante a vigência.
- A arquitetura deverá permitir expansão horizontal mediante adição de instâncias virtuais, sem perda do gerenciamento centralizado.
- A solução deverá permitir monitoramento da utilização dos recursos e disponibilizar informações suficientes para diagnóstico de filas, gargalos, indisponibilidades e degradações de desempenho.

10 - LICENCIAMENTO, ATUALIZAÇÃO E SUPORTE TÉCNICO

- As licenças deverão ser novas, originais, oficiais do fabricante e válidas por, no mínimo, 12 (doze) meses, contados da ativação aceita pela Contratante.
- O licenciamento deverá assegurar, durante toda a vigência, o direito de uso das funcionalidades contratadas, atualizações de software e bases de proteção, correções de segurança e acesso ao suporte oficial.
- O suporte deverá estar disponível em regime 24x7 (24 horas por dia, 7 dias por semana), diretamente pela Contratada ou por canal oficial autorizado do fabricante.
- Os chamados deverão gerar protocolo rastreável e permitir acompanhamento até a solução ou encaminhamento técnico adequado.
- A Contratada deverá manter capacidade de suporte e manutenção durante toda a vigência contratual e deverá assegurar escalonamento ao fabricante quando necessário.
- Os profissionais responsáveis pelo suporte deverão possuir capacitação compatível com os produtos contratados e acesso aos recursos oficiais de diagnóstico e atualização.
- A qualificação técnica dos profissionais responsáveis pelo suporte constitui obrigação da Contratada ou do canal oficial autorizado do fabricante e não implica a realização de cursos, treinamentos ou serviços formais de transferência de conhecimento à equipe da Contratante.
- O fornecimento de documentação técnica oficial e as orientações relacionadas à ativação, atualização, renovação e utilização das funcionalidades contratadas permanecem compreendidos nas obrigações de licenciamento e suporte, sem pagamento autônomo.
- O suporte técnico deverá ser prestado por profissionais com conhecimentos e experiência compatíveis com a solução contratada, diretamente pela Contratada ou por meio de canal oficial autorizado do fabricante, com acesso aos recursos necessários ao diagnóstico, tratamento e escalonamento de ocorrências, observados os níveis de serviço estabelecidos no Termo de Referência.
- O dimensionamento da equipe técnica será de responsabilidade da Contratada, não sendo exigido quantitativo mínimo fixo de profissionais, formação acadêmica específica ou certificação profissional individual, sem prejuízo da obrigação de assegurar a continuidade e a qualidade do suporte técnico durante toda a vigência contratual.

11 - SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

- A solução deverá observar a Política de Segurança da Informação da Contratante e as demais normas internas aplicáveis.
- A Contratada deverá preservar a confidencialidade, integridade, disponibilidade e autenticidade das informações às quais tiver acesso durante a execução do objeto.
- A Contratada deverá manter sigilo sobre dados, configurações, endereçamentos, credenciais, registros de acesso, políticas e demais informações relacionadas à infraestrutura da RECI.
- A solução e a prestação dos serviços deverão observar a Lei nº 13.709/2018 (LGPD), a Lei nº 12.965/2014 (Marco Civil da Internet) e, quando aplicável, as boas práticas da ABNT NBR ISO/IEC 27002.
- Deverá existir procedimento para comunicação de incidentes de segurança relacionados à solução, com notificação tempestiva à Contratante e fornecimento das evidências necessárias à apuração.

12 - ENTREGA, ATIVAÇÃO E ACEITAÇÃO

- A entrega das licenças deverá ocorrer por meio oficial do fabricante, mediante portal, chave, entitlement, grant, arquivo de licença ou mecanismo equivalente que permita comprovar o direito de uso e a vigência contratada.
- A Contratada deverá fornecer documentação suficiente para comprovação da originalidade, validade, quantidade e vinculação das subscrições ao ambiente da Contratante.
- A aceitação ficará condicionada à ativação das licenças, à validação das funcionalidades contratadas, à integração com o gerenciamento centralizado e à confirmação da cobertura de suporte.
- Quando solicitado, deverão ser realizados testes de integração, autenticação, aplicação de políticas, inspeção SSL/TLS, geração de logs, integração com SIEM e análise antimalware antes do recebimento definitivo.
- Não serão aceitos licenciamentos temporários, de avaliação, educacionais ou de natureza diversa daquela prevista para uso corporativo em produção.

13 - DISPOSIÇÕES FINAIS

13.1. A solução ofertada deverá ser plenamente compatível com a arquitetura de proxy já utilizada pela Marinha do Brasil, preservando as integrações existentes, a gestão centralizada, a continuidade operacional e a possibilidade de expansão da infraestrutura sem aquisição adicional obrigatória de hardware.

13.2. Eventual indicação de part number ou código comercial nos documentos de proposta deverá corresponder à subscrição oficial do fabricante para o escopo contratado. No mapa comparativo de preços foi identificado o part number MVWECE-AA-AA em uma das propostas comerciais, devendo a Contratada comprovar a correspondência do código efetivamente ofertado com todas as funcionalidades e condições deste Apêndice.

13.3. Qualquer substituição de código comercial, versão ou modalidade de licenciamento somente poderá ser aceita se oficialmente reconhecida pelo fabricante, preservar integralmente as funcionalidades, capacidade, vigência e suporte previstos e for previamente aprovada pela Contratante.

ALLAN RODRIGO DE SOUZA BRAGA
Capitão de Corveta (T)
Integrante Técnico

JONATAS DE CASTRO OLIVEIRA PASSOS
Primeiro-Tenente (EN)
Integrante Técnico