ANEXO I

PROVA DE CONCEITO (PoC)

ITEM	ÍTENS OBRIGATÓRIOS CARACTERÍSTICAS FUNCIONAIS DA SOLUÇÃO	ATENDE	NÃO ATENDE
1	**INFRAESTRUTURA**		
1.1	Hospedagem em nuvem (cloud) com mínimo de 4TB de armazenamento inicial.		
1.2	Compatibilidade e integração com ambiente cPanel ou solução equivalente		
1.3	Painel administrativo baseado em cPanel ou equivalente, com acesso pleno para a equipe de TI		
1.4	Solução de Webmail com suporte à customização gráfica completa do front-end		
1.5	Gateway de e-mail ou tecnologia equivalente, com inspeção do tráfego de saída, análise de reputação, verificação antivírus, detecção e bloqueio de phishing e inspeção de conteúdo.		
1.6	Demonstrar, por meio de painel, console, diagrama de arquitetura, documentação técnica, relatório de auditoria ou outro meio técnico idôneo, os mecanismos de alta disponibilidade, redundância e failover da solução, contemplando os componentes críticos necessários à operação do serviço, incluindo DNS autoritativo, SMTP, serviços de acesso às caixas postais por IMAP e POP3, Webmail, Mail Gateway, serviços de autenticação, bancos de dados, armazenamento de e-mails e metadados, componentes de segurança e conectividade. A demonstração deverá evidenciar os mecanismos de contingência destinados a preservar a continuidade dos serviços em caso de falha de servidor, dispositivo ou nó de armazenamento, banco de dados, conectividade, fornecimento de energia elétrica ou indisponibilidade total do ambiente principal de hospedagem, demonstrando que a arquitetura não possui ponto único de falha capaz de provocar a interrupção integral dos serviços de correio eletrônico. A LICITANTE deverá, ainda, comprovar que o Datacenter indicado para hospedagem da solução atende ao padrão mínimo Tier III ou superior, conforme classificação do Uptime Institute, ou padrão técnico equivalente, mediante apresentação de certificação, documentação técnica do Datacenter, relatório de auditoria, declaração formal do operador da infraestrutura acompanhada dos respectivos elementos técnicos comprobatórios, ou outro documento técnico idôneo que possibilite à Comissão verificar objetivamente o atendimento do requisito. Quando apresentada certificação Tier, deverá ser possível identificar o Datacenter a que se refere, sua localização e a classificação obtida.		
1.7	Configuração e manutenção de SPF, DKIM e DMARC.		
1.8	Separação lógica ou física entre a camada de aplicação		

	(Webmail) e a camada de armazenamento.		
1.9	Suporte aos protocolos IMAP, POP3 e SMTP com criptografia TLS e sincronização via ActiveSync ou equivalente		
1.10	Abertura de chamados para suporte técnico de forma on-line, através de ambiente WEB (site) e telefone		
1.11	Armazenamento de alta performance para groupware (ex: SQL para calendário/tarefas)		
2	**FUNCIONALIDADES DO WEBMAIL**	**ATENDE**	**NÃO ATENDE**
2.1	Funcionalidades básicas (envio/recebimento, interface acessível via navegador, HTML, pesquisa por: remetente, assunto, conteúdo e data, visualização de anexos)		
2.2	Organização de mensagens (pastas personalizadas, marcadores, arquivamento, ordenação, filtros automáticos)		
2.3	Anexos (envio, download, visualização de PDFs/imagens/docs)		
2.4	Contatos e Agenda (catálogo, grupos, importação/exportação CSV/vCard, agenda de compromissos, convites)		
2.5	Encaminhamento e Respostas (automático, assinatura personalizada, confirmação de leitura)		
2.6	Segurança (acesso HTTPS, autenticação com políticas de senha, MFA, filtros anti-spam/phishing, bloqueio de remetentes, logs)		
2.7	Configurações do Usuário (reset/troca de senha self-service, idioma/fuso horário, layout/tema)		
2.8	Integração com Outros Clientes (compatibilidade IMAP/SMTP, uso simultâneo com Outlook/Thunderbird/apps móveis)		
2.9	Calendário corporativo integrado com suporte ao padrão iCal/RFC 5545 e compartilhamento		
2.10	Lista de Endereços Global (GAL) unificada, com sincronização automática com periodicidade mínima de 6 horas e máxima de 12 horas		
2.11	Controle de Spam Personalizado (Whitelist, Blacklist, ajuste de sensibilidade via web)		
2.12	Regras de Filtragem e Respostas Automáticas (Sieve/ManageSieve)		

2.13	Indicador de utilização de armazenamento: A interface do Webmail deverá disponibilizar ao usuário indicador visual e informativo da utilização da capacidade de armazenamento de sua caixa postal, permitindo visualizar o espaço utilizado e o espaço disponível em relação à cota atribuída à conta. O indicador terá caráter exclusivamente informativo, não permitindo ao usuário alterar a cota ou a capacidade de armazenamento definida para sua caixa postal.		
3.	**FUNCIONALIDADES DO CPANEL OU EQUIVALENTE**	**ATENDE**	**NÃO ATENDE**
3.1	E-mail Corporativo (gerenciamento completo de contas, webmail integrado, filtros, cotas, autenticação, recuperação de e-mails excluídos)		
3.2	Filtros de SPAM e regras personalizadas, o administrador poderá marcar mensagens como SPAM, criar listas de bloqueio e regras de encaminhamento;		
3.3	Suporte a IMAP, POP3 e SMTP;		
3.4	Gerenciamento de Arquivos (File Manager, upload/download, compressão)		
3.5	Gerenciamento de cotas de email por usuário		
3.6	Recuperação de emails excluídos, restore por usuário, restore por período		
3.7	Segurança (Certificados SSL/TLS), proteção contra força bruta/Hotlink, anti-spam/malware/phishing, firewall)		
3.8	bloqueio de IPs		
3.9	proteção contra força bruta/Hotlink		
3.10	Backup e Restauração (full semanal, incremental diário, armazenamento distinto, retenção 90 dias, restauração seletiva/total)		
3.11	Configurações e Monitoramento (uso de recursos, logs, tarefas agendadas, bloqueio remoto/reset de senha admin)		
3.12	Aplicações e Automação (instalador de apps/CMS, suporte APIs/scripts)		
3.13	Gerenciamento de Usuários (criação/admin de contas, limites/permissões)		
3.14	Relatórios (estatísticas de acesso/uso/e-mail, auditoria, políticas de retenção)		
4.	**SEGURANÇA GERAL**	**ATENDE**	**NÃO ATENDE**
4.1	Web Application Firewall (WAF), sistemas anti-malware/spam/phishing com atualizações automáticas e quarentena		

4.2	Autenticação multifator (MFA) para usuários e administradores, permitindo à CONTRATANTE definir, por política de segurança, quais usuários, grupos ou contas deverão utilizar MFA obrigatoriamente		
4.3	Logs de auditoria no painel de administração (acessos, alterações, movimentação de mensagens)		
4.4	Monitoramento contínuo com alertas de segurança, anti-spoofing, proteção contra ransomware, análise comportamental		