ESTUDO TÉCNICO PRELIMINAR

ETP

Projeto: **Cibersegurança + adequação à LGPD**

Sumário

GLOSSÁRIO

Termo	Definição
ETP	Estudo Técnico Preliminar; documento que avalia a viabilidade e os requisitos para a contratação de serviços na administração pública.
LGPD	Lei Geral de Proteção de Dados (Lei n.º 13.709/2018); legislação brasileira que regula o tratamento de dados pessoais.
Cibersegurança	Conjunto de práticas e tecnologias que visam proteger sistemas, redes e informações contra ataques cibernéticos.
Painel de Prevenção de Phishing	Ferramenta que detecta e bloqueia tentativas de phishing, minimizando o risco de comprometimento de credenciais e dados sensíveis.
Simulação de Ataques DDoS	Processo de simulação de ataques de negação de serviço distribuído (DDoS) para avaliar a resiliência da infraestrutura.
Testes de Invasão	Avaliações periódicas realizadas para identificar vulnerabilidades em sistemas e aplicações.
Compliance	Conformidade com leis e regulamentos, nesse caso, com a LGPD; um conjunto de práticas e procedimentos que garantem que uma organização atenda a requisitos legais.
Vulnerabilidade	Falha ou fraqueza em um sistema que pode ser explorada por atacantes.
Incident Response	Resposta a incidentes; conjunto de ações a serem realizadas quando ocorre um incidente de segurança, como um ataque cibernético.
SLA	Acordo de Nível de Serviço; um contrato que

Termo	Definição
	define o nível esperado de serviços a serem prestados e as métricas para medir essa performance.
Certificação CISSP	Certified Information Systems Security Professional; certificação reconhecida internacionalmente que valida conhecimentos em segurança da informação.
Inteligência Artificial (IA)	Uso de algoritmos e sistemas para simulação de inteligência humana, podendo prever e analisar comportamentos de segurança.
Monitoramento de Vulnerabilidades	Processo contínuo de identificação e avaliação de vulnerabilidades na infraestrutura de TIC.
Nível de Maturidade em Governança de TIC	Avaliação do desenvolvimento e implementação de práticas de governança de TI em uma organização.
Análise de Risco	Processo de identificação e avaliação de riscos que podem afetar a segurança da informação e a conformidade com a LGPD.
Gestão de Consentimento	Processos para gerenciar o consentimento dos titulares dos dados, assegurando que suas escolhas sejam respeitadas conforme a LGPD.
Treinamento em Segurança Cibernética	Programa de capacitação para colaboradores sobre práticas de segurança e uso adequado de plataformas de segurança.
Relatório de Impacto à Proteção de Dados (DPIA)	Documento que avalia os riscos associados ao tratamento de dados pessoais e estabelece medidas para mitigá-los.
Gerenciamento de Riscos	Práticas para identificar, avaliar e priorizar riscos, seguidas por ações coordenadas para minimizá-los ou controlá-los.
Princípio da	Princípio da administração pública que busca a

Termo	Definição
Economicidade	eficiência e utilização racional dos recursos públicos.
Gestão de Crises	Conjunto de práticas e procedimentos para gerenciar incidentes críticos e minimizar suas consequências.
Disaster Recovery	Estratégias e processos para garantir a recuperação de sistemas críticos após um incidente grave ou desastre.
Acordo de Nível de Serviço (SLA)	Estabelecimento de parâmetros de qualidade e eficiência que devem ser cumpridos por um prestador de serviços.
Ferramenta de ITSM	Software que ajuda a gerenciar e fornecer serviços de TI, utilizando práticas de gerenciamento de serviços.
Diretiva de Segurança da Informação	Conjunto de políticas que definem a abordagem de uma organização em relação à segurança da informação.
Inventário de Ativos	Registro de todos os ativos de informação dentro de uma organização, essencial para a gestão de segurança.
Testes Automatizados (BAS)	Simulações automatizadas que testam a eficácia dos controles de segurança, revelando quaisquer brechas e vulnerabilidades.
Auditorias de Segurança	Avaliações realizadas para verificar a adequação e a eficácia dos processos e controles de segurança implementados.
Conformidade com Normas ISO	Alinhamento com as normas da Organização Internacional de Normalização (ISO) relativas à segurança da informação (ISO/IEC 27001).
Plano Diretor de Tecnologia da	Documento que estabelece as diretrizes para a gestão dos serviços e recursos de TI dentro da

Termo	Definição
Informação (PDTI)	administração pública.
Indicadores de Desempenho Senhor	Métricas que ajudam a avaliar a eficácia e eficiência dos serviços prestados e da segurança implementada.
Capacitação Técnico-Operacional	Treinamento e desenvolvimento da equipe para assegurar que possam implementar e gerenciar os processos de segurança e conformidade de maneira eficaz.
Proteção de Dados Pessoais	Conjunto de práticas técnicas e administrativas que protegem informações pessoais contra acesso não autorizado e tratamento inadequado.
Termo de Compromisso	Acordo que define responsabilidades e obrigações de um profissional designado para atuar em um projeto ou serviço.
Trabalhos de Conformidade	Processos de verificação e adaptação às exigências da legislação e normas aplicáveis.
Análise Comparativa de Custos	Estudo que compara as opções de contratação disponíveis e seus respectivos custos e benefícios.
Registro de Preços	Sistema que permite que a administração pública registre preços para futuras contratações, visando eficiência e economia.

1. INFORMAÇÕES BÁSICAS

Introdução

1.1. O presente Estudo Técnico Preliminar (ETP) tem por objetivo analisar a viabilidade e os requisitos para a contratação e implementação de solução integrada com gerenciamento de vulnerabilidades de forma continua, com painel de prevenção de phishing, simulação de ataques DDoS, testes de invasão, monitoramento de vulnerabilidades, relatórios, plataforma de compliance LGPD com suporte técnico especializado e apoio a resposta a incidentes, destinada a promover a adequação à Lei Geral de Proteção de Dados (LGPD), em conformidade com as melhores práticas de segurança cibernética. Esta solução deverá contar com o suporte de uma equipe técnica qualificada, responsável pela implantação, execução, manutenção e monitoramento contínuo do projeto.

1.2. O presente estudo foi impulsionado pela crescente complexidade dos sistemas de informação, aumento das ameaças cibernéticas e a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) impõe a necessidade de uma gestão robusta de segurança e da privacidade dos dados.

1.3. A seleção do recurso mais adequado será cuidadosamente planejada para atender às necessidades específicas da Administração Pública Municipal, visando aprimorar o serviço público com maior eficiência e segurança nos órgãos da administração municipal, tanto os da administração direta quanto os da administração indireta. Esta iniciativa contribuirá para a adoção de melhores práticas e para o cumprimento das normas e regulamentos na execução das atividades e na prestação de serviços à população.

1.4. A análise realizada neste estudo abrangerá todos os requisitos, alternativas, resultados pretendidos e demais características relevantes do recurso em questão. O objetivo é fornecer informações completas e detalhadas que possibilitem a análise da solução mais adequada, levando em consideração as necessidades da Administração Pública Municipal, por meio da CODEMAR.

1.5. Ao final deste estudo, será emitido um parecer conclusivo sobre a viabilidade da solução escolhida, auxiliando na decisão do modelo de contratação com maior probabilidade de alcançar os resultados desejados, com base nos princípios da economicidade, transparência e eficiência, garantindo o uso otimizado dos recursos públicos e a satisfação da população.

2. DESCRIÇÃO DA NECESSIDADE

2.1. A CODEMAR – Companhia de Desenvolvimento de Maricá/RJ, visando

fortalecer a segurança cibernética e garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD) Municipal, identifica a imprescindibilidade da contratação de uma solução integrada de cibersegurança e adequação à LGPD e compliance. Esta necessidade surge da crescente complexidade do cenário de ameaças digitais e da responsabilidade em proteger os dados pessoais sob sua guarda, em alinhamento com o PDTIC, o PETI municipal e as melhores práticas de mercado.

Da necessidade de serviços de TIC e cenário atual

2.2. Em meio a um cenário tecnológico em constante evolução, o Município de Maricá, com uma estrutura administrativa composta por 38 (trinta e oito) Secretarias, 6 (seis) Órgãos de Assessoramento e Controle, 5 (cinco) Autarquias, 2 (duas) Sociedade de Economia Mista[1] e aproximadamente 8.000 (oito mil) servidores e empregados públicos, identificou uma necessidade de uma solução voltada a cibersegurança, LGPD e compliance, com intuito de aumentar a proteção dos dados e serviços executados na administração pública direta e indireta da municipalidade.

2.3. O atual ambiente tecnológico do município demanda medidas robustas de segurança cibernética. A CODEMAR, através do Decreto nº 049, de 14 de março de 2025, vem atuando em um contexto de transformação digital, com crescentes interações online e processamento de dados sensíveis, em que necessita proteger suas informações e infraestrutura contra ameaças cada vez mais sofisticadas. A dependência da tecnologia implica em maior exposição a riscos cibernéticos, como ataques de ransomware, phishing e vazamento de dados. A contratação desta solução se torna crucial para mitigar esses riscos e garantir a continuidade dos serviços da municipalidade.

Da motivação e contextualização

2.4. A motivação para esta contratação reside na necessidade premente de proteger os ativos digitais da administração pública direta e indireta e garantir a conformidade com a LGPD (Lei n.º 13.709/2018) no município, evitando sanções e prejuízos à imagem da instituição. A crescente quantidade de dados pessoais processados pela Administração Municipal exige uma postura proativa em relação à segurança da informação, alinhada às diretrizes da Política Nacional de Cibersegurança e da Estratégia Nacional de Segurança Cibernética. Adicionalmente, a conformidade com a LGPD não apenas protege os direitos dos titulares dos dados, mas também fortalece a confiança do público na CODEMAR e

[1] De acordo com a Lei Complementar nº 398, de 12 de dezembro de 2024.

na Prefeitura de Maricá. A contratação se alinha diretamente com os objetivos estratégicos Municipais, contribuindo para a eficiência operacional, a segurança da informação e a conformidade legal, conforme previsto no PPA 2022-2025 (Lei n.º 3.536/2024), no PETI 2022-2025, no PDTI, no Manual de LGPD de Maricá e na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

Adequação à LGPD

2.5. A solução permitirá o mapeamento detalhado dos processos de tratamento de dados, facilitando a identificação de não conformidades com a LGPD. Isso possibilitará a implementação de medidas corretivas eficazes, garantindo que a organização esteja em conformidade com a legislação. Estudos indicam que 60% das empresas que não se adequam à LGPD enfrentam sanções financeiras severas, o que destaca a urgência dessa adequação.

Avaliação de Riscos e Impactos

2.6. Combinando a plataforma de compliance com serviços de análise de vulnerabilidades, a administração municipal terá acesso a informações precisas e atualizadas sobre riscos de segurança e seus impactos. Isso permitirá identificar vulnerabilidades potenciais, capacitando a tomada de decisões mais assertivas e eficientes. A avaliação contínua dos riscos é fundamental, visto que 85% das violações de dados são causadas por falhas conhecidas que poderiam ser mitigadas.

Monitoramento e Auditoria

2.7. A solução proporcionará um acompanhamento contínuo da eficácia das medidas de segurança e conformidade, com geração regular de relatórios e alertas. Isso permitirá à organização identificar rapidamente e corrigir não conformidades, promovendo uma cultura de responsabilidade e transparência em relação à segurança da informação.

Fortalecimento da Segurança Cibernética

2.8. A análise e o gerenciamento contínuo das vulnerabilidades permitirão identificar e corrigir falhas nos sistemas, protegendo os dados pessoais contra-ataques cibernéticos. Em um cenário onde 43% dos ataques cibernéticos visam pequenas empresas, fortalecer a segurança cibernética é crucial para garantir a proteção dos ativos da organização.

Redução dos Custos

2.9. Investir em prevenção é sempre mais econômico do que lidar com as

consequências de incidentes de segurança. Com a prevenção de incidentes de segurança e o cumprimento a LGPD se evitam perdas financeiras e custos com ações judiciais e sanções administrativas devido a possíveis incidente e não cumprimento das leis.

Melhora da Imagem Institucional

2.10. Ao demonstrar compromisso com a segurança da informação e a proteção dos dados pessoais, a organização poderá melhorar sua imagem perante clientes, parceiros e a sociedade em geral. A reputação sólida é um ativo valioso.

Aumento da Eficiência nos Processos

2.11. Por fim, a implementação dessa solução resultará em processos mais eficientes e eficazes no tratamento de dados pessoais. A automação das avaliações e monitoramentos permitirá que as equipes se concentrem em atividades estratégicas, aumentando a produtividade geral da organização.

3. ALINHAMENTO DA SOLUÇÃO COM O PLANEJAMENTO DA COMPANHIA

3.1. A adoção de solução tecnológica de serviços especializados em Análise e Gerenciamento Contínuo de Vulnerabilidades Técnicas e Aplicações Web, com Plataforma de Compliance abrangente para adequação à LGPD, está intrinsecamente alinhada com o planejamento estratégico da CODEMAR, tendo como objetivo final o atendimento e a satisfação das necessidades da administração municipal, mas também com as diretrizes estabelecidas no Plano Diretor de Tecnologia da Informação (PDTI) e no Manual de LGPD de Maricá.

Alinhamento com o PDTI

3.2. O Plano Diretor de Tecnologia da Informação (PDTI)[2] de Maricá estabelece um conjunto de diretrizes para a gestão dos serviços e recursos de TI, visando a modernização e a segurança das informações. A solução proposta contribui para os seguintes aspectos do PDTI:

3.2.1. O PDTI enfatiza a importância de garantir a segurança dos dados e a proteção das informações sensíveis. A análise contínua de vulnerabilidades e o gerenciamento de aplicações web são fundamentais para atender a essa demanda, mitigando riscos e fortalecendo a segurança cibernética;

3.2.2. Estabelece a necessidade de uma governança eficaz nas atividades de

[2] PDTI - PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO (tecnologia.marica.rj.gov.br)

tecnologia. A implementação da plataforma de compliance não só atende às exigências da LGPD, mas também promove uma gestão transparente e responsável dos dados pessoais;

3.2.3. Ainda, a solução está alinhada com as iniciativas do PDTI que visam ampliar o controle sobre os dados e garantir a conformidade com normas e regulamentos, contribuindo para uma administração pública mais eficiente e segura.

Alinhamento com o Manual de LGPD

3.3. O decreto municipal nº 840 de 05 de abril de 2022[3] da Prefeitura de Maricá foi criado para regulamentar a aplicação da Lei Geral de Proteção de Dados no município, estabelecendo diretrizes claras sobre o tratamento de dados pessoais. A solução proposta está em conformidade com os seguintes pontos do manual:

3.3.1. O Manual de LGPD[4] da Prefeitura de Maricá orienta sobre a necessidade de revisar processos relacionados ao tratamento de dados pessoais. A análise contínua das vulnerabilidades nas aplicações web garantirá que os dados sejam tratados com segurança e em conformidade com a legislação vigente;

3.3.2. Além disso, destaca a importância da capacitação dos usuários sobre os riscos associados ao tratamento inadequado dos dados. A solução incluirá programas de treinamento que visam educar os colaboradores sobre as melhores práticas em segurança da informação e conformidade com a LGPD;

3.3.3. E prevê um plano para gerenciamento de incidentes relacionados à segurança dos dados. A solução proposta permitirá um monitoramento eficaz e resposta rápida a possíveis incidentes, assegurando que as obrigações legais sejam cumpridas.

Alinhamento com o Plano Plurianual (PPA)

3.4. A solução está prevista no Plano Plurianual (PPA) para o quadriênio 2022-2025 (Lei nº 3.536/2024 - Revisão do PPA), no programa destinado às despesas com ações de tecnologia. Isso demonstra o compromisso da administração pública com a modernização da gestão e a segurança da informação, reservando recursos para iniciativas como esta.

Alinhamento com o Planejamento Estratégico de TI (PET)

3.5. O Planejamento Estratégico de TI (PET)[5] de Maricá, que visa atender as

[3] Decreto nº 840, de 05 de abril de 2022
[4] Manual de LGPD (marica.rj.gov.br)
[5] PET - PORTAL DA TECNOLOGIA DA INFORMAÇÃO (marica.rj.gov.br)

necessidades da prefeitura, prevê, em seu Eixo OE2.4, a ação de garantir a disponibilidade da estrutura tecnológica para preservar a continuidade dos serviços das demais organizações públicas. Esta iniciativa tem como meta manter os ativos de infraestrutura disponíveis 24x7, com um percentual de disponibilidade de 95% para o ano de 2025. A implementação da solução integrada com gerenciamento de Vulnerabilidades de forma contínua, com Painel de Prevenção de Phishing, Simulação de Ataques DDoS, Testes de Invasão, Monitoramento de Vulnerabilidades, Relatórios, Plataforma de Compliance LGPD com Suporte Técnico Especializado e apoio a resposta a Incidentes contribui diretamente para o alcance desta meta, pois:

3.5.1. Ao identificar e mitigar vulnerabilidades, a solução diminui a probabilidade de incidentes de segurança que poderiam comprometer a disponibilidade dos serviços.

3.5.2. A adequação à LGPD, promovida pela plataforma de compliance, evita sanções e interrupções nas operações decorrentes de não conformidade com a legislação.

3.5.3. A análise contínua de vulnerabilidades e a gestão de aplicações web protegem os ativos de TI contra ameaças cibernéticas, garantindo a integridade e a confidencialidade dos dados e sistemas.

4. DOS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

4.1. O presente estudo técnico preliminar tem como objetivo analisar a melhor solução para que o Município, por meio da CODEMAR, atenda às suas necessidades de negócio, buscando alinhamento aos objetivos estratégicos de modernização da gestão pública, adequação às legislações vigentes, fortalecimento da segurança da informação e melhoria da prestação de serviços aos cidadãos. Este alinhamento está em consonância com as diretrizes da Lei Geral de Proteção de Dados e as melhores práticas de governança de TI no setor público.

4.2. O escopo deste estudo tem como objetivo atender as exigências da LGPD e fortalecer a sua segurança cibernética de possíveis ataques, visando sempre a conformidade com a LGPD, proteção contra ameaças cibernéticas, otimizando a gestão de riscos, fortalecendo a imagem do órgão público através do suporte técnico especializado, e garantindo a continuidade dos serviços públicos.

4.3. A solução apresentada nesse Estudo Técnico Preliminar, deverá atender aos seguintes requisitos:

Requisitos de negócio

4.4. A adequação à Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que regula as atividades de tratamento de dados pessoais, que também altera os artigos 7º e 16º do Marco Civil da Internet e estabelece um novo marco legal para o tratamento de dados pessoais no Brasil, impactando diretamente a forma como as organizações coletam, utilizam, armazenam e compartilham informações, é fundamental pois a lei também estabelece direitos, obrigações e sanções rigorosas para o descumprimento, incluindo multas de até 2% do faturamento, limitadas a R$ 50 milhões, além de outras penalidades como a suspensão ou proibição do exercício de atividades relacionadas ao tratamento de dados.

4.5. A legislação se fundamenta em diversos valores, como o respeito à privacidade; à autodeterminação informativa; à liberdade de expressão, de informação, comunicação e de opinião, à inviolabilidade da intimidade, da honra e da imagem; ao desenvolvimento econômico e tecnológico e a inovação; à livre iniciativa, livre concorrência e defesa do consumidor e aos direitos humanos de liberdade e dignidade das pessoas.

4.6. A LGPD cria um conjunto de novos conceitos jurídicos, estabelece as condições nas quais os dados pessoais podem ser tratados, define um conjunto de direitos para os titulares dos dados, gera obrigações específicas para os controladores dos dados e cria uma série de procedimentos e normas para que haja maior cuidado com o tratamento de dados pessoais e compartilhamento com terceiros.

4.7. Nesse contexto, a análise e o gerenciamento contínuo de vulnerabilidades em sistemas e aplicações web tornam-se essenciais para identificar e mitigar riscos que possam comprometer a segurança dos dados pessoais sob a responsabilidade da instituição, além de garantir a conformidade da infraestrutura de TIC. A implementação de uma plataforma de compliance abrangente, por sua vez, permitirá o monitoramento e a gestão das atividades de tratamento de dados, garantindo a conformidade com a LGPD e outras regulamentações aplicáveis.

4.8. A conformidade da infraestrutura de TIC diz respeito à garantia do cumprimento de requisitos de qualidade, estabelecidos pelos padrões técnicos sobre as tecnologias de infraestrutura homologadas pela administração municipal. Pode abranger diversos aspectos, como garantir o desempenho, segurança, disponibilidade e suporte aos ativos da infraestrutura de TIC.

4.9. O serviço de análise e gerenciamento contínuo de vulnerabilidades, integrado a uma plataforma de compliance e LGPD, é de extrema importância e

traz uma série de benefícios significativos.

4.10. A análise de viabilidade deverá considerar como a solução a ser implementada atenderá aos objetivos estratégicos da administração municipal, modernizando a gestão pública, garantindo a adequação às legislações vigentes, fortalecendo a segurança da informação e melhorando a prestação de serviços aos cidadãos. Além disso, deverá avaliar a capacidade da solução em promover a Gestão Contínua de Vulnerabilidades e de Exposição a Ameaças, de forma proativa e recorrente, por meio da identificação, avaliação, categorização, priorização, tratamento e análise crítica de vulnerabilidades e riscos de segurança de ativos corporativos de TIC, gerenciamento e análise de exposição a ameaças e da superfície de ataque interna e externa. A solução deverá ser capaz de realizar Testes de Segurança Automatizados (BAS), planejamento, execução, análise e relatório de testes automatizados continuados de segurança com ferramenta de simulação de brechas e ataques.

4.11. A plataforma deverá ser capaz de mapear os processos de tratamento de dados, identificar não conformidades com a LGPD e auxiliar na implementação de medidas corretivas.

4.12. Deverá realizar uma análise completa e detalhada das vulnerabilidades técnicas nos sistemas, aplicações e infraestrutura do órgão, incluindo testes de penetração e varreduras de segurança.

4.13. A solução deverá oferecer funcionalidades para centralizar as informações sobre os riscos de segurança, permitindo assim a gestão eficiente e o acompanhamento das ações de mitigação.

4.14. A solução deverá gerar relatórios detalhados sobre as vulnerabilidades encontradas, riscos associados e as recomendações para possíveis correções, onde o poder das decisões informadas sejam tomadas pelo órgão público.

4.15. Deverá realizar o monitoramento contínuo dos sistemas e aplicações, com alertas em tempo real sobre novas vulnerabilidades e ameaças.

4.16. A administração municipal deverá ter acesso a uma equipe de suporte técnico especializado, para auxiliar na implementação das medidas de segurança e na resolução de problemas.

4.17. A solução deverá ser escalável para acompanhar o crescimento das demandas da administração pública e o aumento da complexidade dos sistemas e aplicações, além de possuir interface intuitiva e fácil de usar;

4.18. O local de prestação dos serviços será nas dependências da CODEMAR e da Prefeitura de Maricá, devendo abranger todo o município, inclusive os órgãos da administração direta e indireta.

Requisitos de tecnologia

4.19. A realização de uma Prova de Conceito (“proof of concept” – “PoC”) deverá ser obrigatória para validar a eficácia da solução escolhida, conforme Apêndice A deste estudo.

4.20. Além disso, a solução deverá obrigatoriamente atender aos seguintes itens:

Solução de Gerenciamento de Vulnerabilidades

4.21. A solução de segurança cibernética deverá ser capaz de realizar monitoramento ativo para abranger até 20 endereços IP públicos, 8475 endpoints e 398 Nomes de domínio totalmente qualificados Externos e internos (FQDNs) simultaneamente. Essa capacidade permitirá que toda a infraestrutura de TIC Municipal seja analisada de forma contínua, proporcionando uma visão completa e detalhada do ambiente digital. A solução deverá realizar escaneamentos periódicos e automatizados, buscando identificar não apenas vulnerabilidades conhecidas, mas também possíveis falhas de configuração que possam representar riscos à segurança.

4.22. O processo de análise de vulnerabilidades deverá ser complementado pela utilização de Inteligência Artificial (IA). Onde a IA permitirá uma análise preditiva, capaz de identificar padrões anormais e possíveis brechas de segurança antes mesmo que se tornem uma ameaça real. Além disso, a IA deverá contribuir para a priorização das vulnerabilidades encontradas, classificando-as de acordo com a criticidade baseada no padrão CVSS (Common Vulnerability Scoring System), de forma a facilitar a tomada de decisões rápidas e assertivas pela equipe de segurança da informação.

4.23. Entre as funcionalidades oferecidas, a solução deverá também ter a capacidade de detectar vulnerabilidades Zero-Day, ou seja, falhas ainda não divulgadas publicamente e que podem ser exploradas por atacantes antes que correções sejam disponibilizadas. Essa detecção em tempo real é essencial para manter um alto nível de proteção, especialmente em ambientes onde a segurança da informação é crítica.

4.24. Os testes de intrusão, também conhecidos como Pentests, são uma peça-chave na estratégia de segurança proposta. A solução deverá de forma automatizada realizar testes de penetração utilizando ferramentas modernas e

eficientes. Os testes devem ser conduzidos em três diferentes modalidades:

4.24.1. Black-box: onde o executor do teste não possui qualquer conhecimento prévio sobre a infraestrutura ou sistemas da organização, simulando um ataque externo real.

4.24.2. Gray-box: onde o teste é realizado com informações limitadas, proporcionando uma visão equilibrada entre o desconhecimento completo e o acesso total ao ambiente.

4.24.3. White-box: onde o executor do teste tem pleno acesso a informações detalhadas sobre o ambiente tecnológico e a arquitetura da rede, permitindo uma análise profunda e minuciosa.

4.24.4. A solução deverá integrar um painel de prevenção de Phishing, onde será possível criar campanhas específicas para treinar e conscientizar os usuários finais sobre os riscos do Phishing. Essas campanhas permitirão o envio automatizado de e-mails simulados de Phishing, monitorando em tempo real a quantidade de e-mails disparados, o número de cliques realizados e, consequentemente, quantos usuários foram "capturados" pela tentativa de Phishing. O painel administrativo oferecerá funcionalidades para edição, reenvio de campanhas e geração de relatórios detalhados, proporcionando insights valiosos para reforçar políticas de segurança e promover treinamentos mais eficazes.

4.25. Os testes de intrusão deverão incluir simulações de diferentes tipos de ataques cibernéticos, como SQL Injection, Cross-Site Scripting (XSS), ataques de negação de serviço (DDoS), tentativas de força bruta e testes de phishing. Essas simulações permitem avaliar a robustez das defesas do sistema, identificar possíveis pontos fracos e sugerir soluções específicas para cada tipo de vulnerabilidade detectada.

4.26. Gerenciamento e análise da exposição a ameaças e da superfície de ataque (interna e externa).

4.27. Utilização de ferramenta especializada para:

4.27.1. Gerenciamento de vulnerabilidades.

4.27.2. Varredura e avaliação de vulnerabilidades e configuração segura.

4.27.3. Análise e priorização de risco cibernético.

Painel de Prevenção de Phishing

4.28. O módulo de prevenção de phishing será um componente fundamental da

solução, devendo oferecer uma plataforma completa para a criação e gerenciamento de campanhas de conscientização de segurança. Através do painel administrativo, o usuário administrador deverá conseguir configurar campanhas simuladas de phishing, enviando e-mails personalizados para grupos específicos de colaboradores.

4.29. Dessa forma a interface do painel deverá permitir:

4.29.1. O administrador poderá criar campanhas de prevenção, definir o modelo de e-mail e o público-alvo.

4.29.2. Acompanhar o envio dos e-mails e o progresso da campanha, como quantidade de e-mails enviados, cliques nos links suspeitos e identificação dos usuários que caíram na simulação.

4.29.3. A solução deverá gerar relatórios abrangentes, exibindo métricas como taxa de cliques, percentual de usuários suscetíveis ao phishing e insights para aprimoramento das práticas de segurança.

4.29.4. Caso necessário, deverá ser possível reenviar campanhas para reforçar o treinamento dos usuários que demonstraram vulnerabilidades.

Simulação de Ataques DDoS

4.30. O módulo de simulação de ataques DDoS (Distributed Denial of Service) deverá oferecer uma abordagem prática para testar a resiliência da infraestrutura da organização. Com uma interface intuitiva, o painel permite:

4.31. O administrador poderá definir o tipo de ataque DDoS, o volume de requisições e o alvo específico (IP ou URL).

4.32. Acompanhar métricas como o número de solicitações por segundo, latência de resposta e taxa de erro durante o ataque simulado.

4.33. O painel deverá também exibir gráficos detalhados sobre o tempo de resposta e o impacto na disponibilidade do sistema, permitindo identificar gargalos e possíveis melhorias na infraestrutura.

Testes de Invasão e Segurança

4.34. A solução deverá incluir uma variedade de testes de invasão (Pentest) para identificar vulnerabilidades e fortalecer a segurança do ambiente digital. Entre os testes disponíveis, destacar-se-ão:

4.35. Avaliação da segurança a partir da rede interna da organização, simulando

um ataque de um colaborador mal-intencionado ou de uma máquina comprometida.

4.36. Simulação de ataques vindos de fora da organização, avaliando a robustez de firewalls, sistemas de detecção de intrusão (IDS) e a exposição de serviços públicos.

4.37. Verificação da segurança de sites e sistemas web, utilizando técnicas como injeção de SQL, Cross-Site Scripting (XSS) e análise de vulnerabilidades em APIs.

Monitoramento e Análise de Vulnerabilidades

4.38. O sistema de monitoramento contínuo deverá utilizar ferramentas avançadas de análise para detectar vulnerabilidades conhecidas e novos vetores de ataque. As principais funcionalidades incluirão:

4.38.1. Varredura automatizada em sistemas, servidores e dispositivos conectados à rede, identificando falhas de configuração, softwares desatualizados e possíveis pontos de entrada para invasores.

4.38.2. Integração com sistemas de coleta de logs, permitindo identificar padrões anômalos e atividades suspeitas em tempo real.

4.38.3. Utilização de bases de dados atualizadas sobre ameaças conhecidas, aplicando correlações entre eventos monitorados e possíveis ataques.

4.38.4. Realização de varreduras automatizadas completas em ativos internos e externos.

4.38.5. Varreduras autenticadas e não autenticadas.

4.38.6. Compatibilidade mínima com o protocolo SCAP (Security Content Automation Protocol).

Monitoramento de Vazamento de Dados

4.39. Realizar o monitoramento, análise e busca inteligente por dados vazados ou expostos, incluindo o monitoramento deles na DarkWeb.

Relatórios e Indicadores de Desempenho

4.40. A solução deverá oferecer uma ampla variedade de relatórios gerenciais e técnicos, fornecendo insights valiosos para a tomada de decisão:

4.40.1. Com uma linguagem acessível, ideal para apresentações a gestores, destacando os principais riscos e as ações tomadas para mitigar vulnerabilidades.

4.40.2. Detalhamento das vulnerabilidades encontradas, incluindo evidências, métodos utilizados nos testes e sugestões práticas para correção.

4.40.3. A solução deverá permitir o usuário configurar o painel de controle, escolhendo os indicadores mais relevantes para o seu ambiente.

Camada de Segurança, Autenticidade e Validade Jurídica

4.41. Possuir mecanismo de armazenamento e coleta de documentos digitais auditáveis com validade jurídica, baseada em blockchain.

4.42. Assegurar a autenticidade de documentos digitais.

4.43. Gerar relatórios técnicos com informações registradas, com validade jurídica conforme o artigo 369 do CPC/2015.

4.44. Possuir método de autenticação robusto com chave física USB única (Chave de Hardware) para acesso à interface de gerenciamento, além de usuário e senha.

4.45. Possuir modulo para identificar e mitigar domínios semelhantes que possam ser usados em ataques de phishing

Testes de Segurança Automatizados (BAS)

4.46. Implementação de testes de segurança automatizados para simular ataques e validar a eficácia dos controles de segurança.

Processo de Testes Automatizados

4.47. Planejamento, execução, análise e geração de relatórios de testes automatizados contínuos de segurança.

4.48. Utilização de ferramenta de simulação de brechas e ataques (Breach and Attack Simulation - BAS).

Capacidades da Ferramenta BAS

4.49. Realização de baterias de testes de simulação de ataques com base em bibliotecas atualizadas de ameaças e exploits.

4.50. Execução imediata ou agendada.

4.51. Abrangência:

4.51.1. Infiltração de rede e aplicações web (ator malicioso externo para ativo-alvo interno).

4.51.2. Endpoint (comprometimento e exfiltração em ativo-alvo interno, estação de trabalho ou servidor, com cobertura mínima do sistema operacional Microsoft Windows).

Bases de Conhecimento de Segurança

4.52. A solução deverá ter integração as seguintes bases de conhecimento de segurança:

4.52.1. NIST National Vulnerability Database (NVD).

4.52.2. MITRE Common Vulnerabilities and Exposures (CVE).

4.52.3. NIST Official Common Platform Enumeration (CPE).

4.52.4. MITRE Common Weakness Enumeration (CWE).

4.52.5. OWASP Top 10.

4.52.6. CIS Benchmarks.

Abrangência dos Ativos de TIC

4.53. A solução deve abranger uma ampla gama de ativos de TIC, incluindo:

4.53.1. Dispositivos de usuário final (estações de trabalho, notebooks, dispositivos móveis e periféricos).

4.53.2. Dispositivos de rede.

4.53.3. Dispositivos inteligentes conectados à rede (IoT).

4.53.4. Servidores.

4.53.5. Contêineres.

4.53.6. Sistemas operacionais.

4.53.7. Serviços e aplicações em rede.

4.53.8. Ativos e postura de segurança em nuvem.

Plataforma de Compliance e adequação à LGPD

4.54. A Plataforma de Compliance para Adequação a Lei de Proteção de Dados (LGPD) deverá auxiliar a CODEMAR e a Prefeitura no processo de conformidade, oferecendo as seguintes funcionalidades:

Mapeamento dos Processos de Tratamento de Dados

4.55. Identificação detalhada dos dados coletados, incluindo natureza, finalidade e base legal.

4.56. Mapeamento do fluxo dos dados, desde a coleta até o descarte, incluindo as etapas de armazenamento, processamento e compartilhamento.

4.57. Identificação dos responsáveis pelo tratamento dos dados, tanto internos quanto externos ao órgão público.

4.58. Documentação completa dos processos de tratamento de dados, incluindo políticas, procedimentos e controles de segurança.

Avaliação dos Riscos de Segurança

4.59. Análise e identificação dos riscos de incidentes de segurança e vazamento de dados, considerando as vulnerabilidades técnicas e administrativas.

4.60. Avaliação do impacto potencial dos riscos identificados, tanto para o órgão público, quanto para os titulares dos dados.

4.61. Implementação de medidas de segurança preventivas e corretivas para mitigar os riscos identificados.

4.62. Monitoramento contínuo dos riscos e das medidas de segurança implementadas.

4.63. Identificação e sugestão de medidas para mitigar ameaças.

4.64. Plataforma integrada para reportar e gerenciar incidentes de segurança.

4.65. Sistema de IA automatização de tarefas e otimização contínua do programa de privacidade.

Gerenciamento dos Direitos dos Titulares dos Dados

4.66. Canais de comunicação claros e acessíveis para receber e responder às solicitações dos titulares dos dados.

4.67. Procedimentos eficientes para atender às solicitações dos titulares, incluindo acesso, retificação, exclusão, portabilidade e oposição ao tratamento dos dados.

4.68. Prazo máximo de resposta para as solicitações dos titulares, conforme estabelecido pela LGPD.

4.69. Documentação das solicitações dos titulares e das respostas fornecidas.

4.70. Ferramenta integrada para gerenciar o consentimento dos titulares.

Monitoramento da Conformidade

4.71. Acompanhamento contínuo do cumprimento das normas da LGPD, incluindo a realização de auditorias internas e externas.

4.72. Identificação de não conformidade e implementação de medidas corretivas para as falhas identificadas.

4.73. Identificação de pontos fracos e geração automática de atividades de melhoria.

Manutenção de registros e evidencias da conformidade com a LGPD

4.74. Atualização contínua das políticas e procedimentos de segurança para acompanhar as mudanças na legislação e nas melhores práticas.

4.75. Criação automatizada de políticas de privacidade e termos de uso.

4.76. Subsídios para Diagnósticos de Maturidade e Melhoria da Governança de TIC.

4.77. Coleta de dados e informações sobre os processos de tratamento de dados para subsidiar o diagnóstico de maturidade da governança de TIC.

4.78. Identificação de oportunidades de melhoria na governança de TIC, com base nos resultados do diagnóstico e nas melhores práticas.

4.79. Proposição de ações de melhoria para fortalecer a governança de TIC e garantir a conformidade com a LGPD.

4.80. Integração da plataforma de compliance com o Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) e o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC).

Relatórios e Solução de Business Analytics e Business Intelligence

4.81. Visualização de dados consolidada e acessível, incluindo monitoramento, análise de métricas e tomada de decisões baseada em dados.

4.82. Integração da plataforma de compliance com solução de Business Analytics e BI para o setor público.

4.83. Disponibilização de dashboards personalizáveis para análise de dados e suporte à decisão, incluindo informações sobre o cumprimento da LGPD.

4.84. Utilização de dados e informações da plataforma de compliance para gerar insights e relatórios sobre a proteção de dados no órgão público.

4.85. Geração rápida de relatórios personalizados:

4.85.1. Relatório de Conformidade;

4.85.2. Relatório Gerencial;

4.85.3. Relatório de Impacto;

4.85.4. RoPA;

4.85.5. Prestação de contas;

4.85.6. Relatório de Medidas de Segurança;

4.85.7. Relatório de Ameaças;

4.85.8. Relatório de Treinamento;

4.85.9. Relatório de Legítimo Interesse;

4.85.10. Relatório de Consentimentos;

4.85.11. Relatório de Auditoria;

Demais serviços e funcionalidades

4.86. Gestão de Terceiros: Cadastro e avaliação de fornecedores.

4.87. Diagnóstico de Maturidade: Avaliação do nível de maturidade da empresa.

4.88. Banner de Cookies: Ferramenta para implementar banners de cookies.

4.89. Central de Privacidade: Um portal de comunicação que centraliza e facilita o atendimento das demandas

4.90. Personalização e Identidade Visual: Recurso para customizar a área do cliente.

4.91. DPO as a Service: DPO substituto, com a realização de reuniões mensais de acompanhamento, participação em comitê de privacidade, priorização em questionários de due diligence, apoio na criação de plano de ação, treinamentos exclusivos e personalizados.

4.92. Mapeamento de Processos Guiado: Realização do mapeamento de processos para garantir a conformidade.

4.93. Enquadramento Legal: Análise e enquadramento legal dos processos de tratamento de dados.

4.94. Comprovação para Clientes e Fornecedores: Ferramentas para comprovar a adequação à LGPD.

4.95. Resposta ao Titular de Dados: Apoio na resposta às solicitações dos titulares de dados.

Requisitos de implantação e capacitação

4.96. Como preparação para a implantação dos serviços, a contratada deverá realizar um levantamento e avaliação detalhada do ambiente de Tecnologia da Informação e Comunicação (TIC), incluindo um diagnostico abrangente da situação da cibersegurança. A implantação será gerenciada como um projeto, com acompanhamento de um preposto técnico especialista em TIC.

4.97. Dada a amplitude e complexidade dos serviços, a equipe técnica diretamente envolvida na gestão, operações de cibersegurança e execução das atividades será capacitada. O treinamento abrangerá os principais componentes das soluções, proporcionando uma visão geral e aprofundada do sistema.

Levantamento e avaliação inicial da infraestrutura e dos ativos de TIC

4.98. Para complementar o diagnóstico e avaliação inicial da situação e maturidade, será necessário realizar um levantamento abrangente para mapear de forma precisa e detalhada a superfície de ataque da CODEMAR e da Prefeitura, bem como de suas unidades descentralizadas. Este trabalho deverá ser complementado através do apoio de entrevistas técnico-gerenciais.

4.99. É fundamental que a análise considere a necessidade de um levantamento e avaliação detalhada do ambiente de TIC e da cibersegurança da administração municipal. Isso inclui Levantamento e descoberta de ativos de Hardware e software, arquitetura geral de infraestrutura de TIC, estrutura física de data center, salas de dados e processos existentes, bem como a avaliação de sua criticidade e vulnerabilidade. A análise deve também levar em conta a necessidade de integração da solução com a infraestrutura existente, bem como a identificação de possíveis impactos na operação da organização.

Requisitos de suporte e manutenção

4.100. Para garantir a eficácia contínua da solução de cibersegurança e adequação à LGPD, é fundamental estabelecer requisitos claros de suporte e manutenção. Esses requisitos devem abranger desde a disponibilidade de suporte técnico especializado até a garantia de atualizações regulares de segurança.

Suporte Técnico Especializado para cibersegurança

4.101. A solução deve oferecer suporte técnico especializado disponível 24 horas por dia, 7 dias por semana, para atender a incidentes de segurança críticos.

4.102. Deve haver múltiplos canais de comunicação para o suporte, como telefone, e-mail e chat online, para facilitar o acesso rápido e eficiente.

4.103. O tempo de resposta para solicitações de suporte deve ser mínimo, garantindo que problemas sejam resolvidos rapidamente para minimizar o impacto nos serviços.

Suporte Técnico Especializado para Adequação à LGPD

4.104. A solução deve oferecer suporte especializado disponível em horário comercial (das 08:00h às 18:00h), para atender a incidentes de críticos ou não críticos correlacionados a adequação à LGPD e a plataforma de compliance.

4.105. Deve haver múltiplos canais de comunicação para o suporte, como telefone, e-mail e chat online, para facilitar o acesso rápido e eficiente.

4.106. O tempo de resposta para solicitações de suporte deve ser mínimo, garantindo que problemas sejam resolvidos rapidamente para minimizar o impacto nos serviços.

Atualizações de Segurança e Manutenção Preventiva

4.107. A solução deve receber atualizações regulares de segurança para garantir que ela permaneça eficaz contra novas ameaças cibernéticas.

4.108. A manutenção preventiva deve ser realizada periodicamente para garantir a integridade dos sistemas e evitar falhas inesperadas.

4.109. A equipe técnica da CODEMAR deve ser notificada sobre atualizações disponíveis e suas implicações, permitindo um planejamento adequado para a implementação, além de prestar suporte na implementação de atualizações e patches regulares de segurança.

4.110. Apoiar na criação de ambiente de homologação para testes antes da implementação de atualizações.

Apoio a resposta a Incidentes

4.111. Deve ser criado um plano bem estruturado para responder a incidentes de segurança e vazamento de dados, garantindo que as medidas de proteção sejam acionadas no tempo correto.

4.112. A solução deve incluir a capacidade de mobilizar uma equipe especializada em resposta a incidentes para lidar com situações críticas.

4.113. A documentação técnica e de usuário atualizada e acessível.

Acordo de Nível de Serviço – SLA

4.114. O objetivo do SLA é estabelecer os critérios e níveis de serviços para o atendimento de suporte e abertura de chamados relacionados à solução a ser contratada, bem como o desempenho técnico do sistema para garantir sua estabilidade e confiabilidade.

Tempo para Resolução do Problema – TRP, dividido em três categorias de problemas, conforme o impacto:

- **Alto:** Solução em até 2 horas.
- **Médio:** Solução em até 6 horas.
- **Baixo:** Solução em até 24 horas.
- **Meta por mês:** ≥95%

Tempo de Disponibilidade Mensal - TDM

4.115. Além da qualidade do atendimento, é fundamental monitorar o desempenho técnico do sistema para garantir sua estabilidade e confiabilidade. Para isso, utiliza-se a métrica de Uptime do Sistema (Disponibilidade), em que a **meta é de ≥99.8% por mês**.

4.116. Ferramentas e técnicas de controle deverão ser utilizadas para o monitoramento contínuo dos serviços

4.117. Também deverá ser estabelecido um processo de revisão periódica do SLA para garantir que ele permaneça adequado às necessidades do órgão contratante e do fornecedor, ajustando-se conforme mudanças no ambiente de TIC ou nas expectativas da Contratante.

Requisitos da segurança da Informação e privacidade

4.118. A solução deve ser capaz de realizar baterias de testes de simulação de ataques baseados em bibliotecas atualizadas de ameaças e exploits, com

execução imediata ou agendamentos, abrangendo infiltração de rede e aplicações web, ambos com o fluxo de ator malicioso externo para ativo-alvo interno; e endpoint, com comprometimento e exfiltração em ativo-alvo interno.

4.119. A solução de tecnologia deverá contemplar os seguintes aspectos de segurança da informação e privacidade, alinhados com as melhores práticas e normas técnicas:

4.119.1. Controle de Segurança: Implementação de controles de segurança baseados nas normas ISO/IEC 27001 e 27002, que abrangem desde a gestão de riscos e políticas de segurança até os controles técnicos e físicos.

4.119.2. Criptografia de Dados: Apoio na implementação de criptografia de dados em repouso e em trânsito.

4.119.3. Autenticação Multifator: Apoio na implementação de autenticação multifator (MFA) para acesso aos sistemas, como forma de aumentar a segurança e proteger contra acessos não autorizados.

4.119.4. Registro e Monitoramento de Logs: Apoio na implementação de registro e monitoramento de logs de acesso e atividades, permitindo a identificação de possíveis incidentes de segurança e o rastreamento de ações realizadas no sistema.

4.119.5. Testes de Penetração e Análises de Vulnerabilidade: Realização de realização de testes de penetração e análises de vulnerabilidade periódicos.

4.119.6. Plano de Resposta a Incidente: Apoio na implementação de um plano de resposta a incidentes de segurança da informação, que defina os procedimentos a serem seguidos em caso de ocorrência de incidentes.

4.119.7. Política de Backup e Recuperação de Dados: Apoio na implementação de uma política de backup e recuperação de dados, que garanta a disponibilidade das informações em caso de falhas, perdas ou desastres.

Treinamento e Capacitação

4.120. Treinamento para Equipes: A solução deve incluir programa de treinamento inicial para administradores, usuários finais e para as equipes técnicas da organização, garantindo que elas estejam capacitadas para operar e manter a solução de forma eficaz.

4.121. Atualizações Técnicas: O fornecedor deve oferecer atualizações técnicas e workshops periódicos para garantir que as equipes estejam atualizadas sobre as

melhores práticas e novas funcionalidades.

4.122. Deverá ser disponibilizado documentação e tutoriais passo a passo atualizados para utilização e operação das plataformas, bem como sobre as boas práticas da Segurança de Informação e da LGPD.

4.123. Treinamento para Representantes: Ensina a manusear a plataforma e formalizar as documentações e nomeações de Encarregado de Dados da organização.

4.124. Treinamento para Líderes de Departamento: Aborda o papel dos líderes na adequação à LGPD e como utilizar as ferramentas da plataforma.

4.125. Treinamento para a Diretoria: Explica a importância da adequação da empresa à LGPD.

4.126. Treinamento Específico para Uso da ferramenta integrada de DPO e DAI: Capacitação para aproveitar ao máximo as funcionalidades avançadas de IA e gestão estratégica.

Requisitos legais

4.127. Para garantir a conformidade com as leis e regulamentações aplicáveis, a solução de cibersegurança, compliance e adequação à LGPD deve atender aos seguintes requisitos legais:

4.127.1. Lei Federal nº 13.303/2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.

4.127.2. Instrução Normativa SLTI/MP nº 01/2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras.

4.127.3. Instrução Normativa SGD/ME nº 94/2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação – TIC.

4.127.4. Nota técnica SGE nº 01/2015 da Coordenadoria de Auditorias Temáticas e Operacionais/Secretaria Geral de Controle Externo (CTO/SGE) na área de Tecnologia da Informação do TCE-RJ.

4.127.5. Nota técnica TCE-RJ nº 06/2023, sobre o procedimento de planejamento para aquisição de bens e serviços de Tecnologia da Informação (TI).

4.127.6. Nota técnica TCE-RJ nº 08/2024, sobre orientação aos jurisdicionados do TCE-RJ acerca da definição de níveis mínimos de serviço nas contratações de TI.

4.127.7. Lei Federal nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD).

4.127.8. Lei Federal nº 12.846/2013, chamada de Lei anticorrupção.

4.127.9. Decreto Municipal nº 937, de 18 de novembro de 2022, regulamenta o Sistema de Registro de Preços - SRP no âmbito da Administração Direta e Indireta do Poder Executivo do Município de Maricá.

4.127.10. Planejamento Estratégico de TI (PETI) 2022-2025[6]

4.128. A solução deve estar alinhada com as diretrizes da Política Nacional de Cibersegurança[7], que visa promover a segurança cibernética no Brasil. Isso inclui a adoção de medidas para prevenir, detectar, tratar e responder a ameaças cibernéticas.

4.129. A solução deve ser implementada sob um modelo de governança que promova a coordenação e a análise conjunta dos desafios cibernéticos, conforme estabelecido pela Estratégia Nacional de Segurança Cibernética.

4.130. A solução deve promover a educação e a conscientização sobre cibersegurança, conforme proposto em projeto de lei[8] que visam incrementar a resiliência das organizações públicas e privadas a incidentes cibernéticos.

Requisitos temporais

4.131. A contratação do serviço continuado deverá ter prazo de vigência inicial de 12 (doze) meses, podendo ser prorrogado por período igual.

4.132. A solução deverá estar completamente disponibilizada, instalada, configurada e operacional em até 45 (quarenta e cinco) dias corridos, contados a partir da data do recebimento da Ordem de Início dos Serviços, de acordo com a quantidade.

4.133. Em caso de necessidade, a Contratada poderá solicitar prorrogação do

[6] https://tecnologia.marica.rj.gov.br/wp-content/uploads/2021/11/PET.pdf
[7] https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf
[8] https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2389487&filename=PL+428%2F2024

prazo constante no parágrafo anterior à Contratante.

4.134. O suporte em caso de renovação contratual, por meio de termo aditivo, deverá ser prestado de forma automática, ou seja, não deverá sofrer interrupção. Caso ocorra interrupção dos serviços sem justificativa deferida pela fiscalização, o atraso será contado em dias a partir do momento da interrupção.

4.135. Na contagem dos prazos estabelecidos neste ETP, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

4.136. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos (ou horas corridas, quando definido em horas).

4.137. Os esclarecimentos solicitados pela fiscalização do contrato deverão ser prestados imediatamente pela Contratada, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 6 (seis) horas úteis.

4.138. Não será computado o tempo de atraso quando este estiver sido ocasionado pelo Contratante ou por fatos supervenientes que independam de ações da Contratada, desde que devidamente justificado e aceito pela Contratante.

4.139. Não são considerados casos ou fatos supervenientes as situações externas que poderiam ter sido contornadas ou mitigadas por ações de logísticas preventivas ou reativas da Contratada.

Requisitos sociais, ambientais e culturais

4.140. Os sistemas e manuais das soluções ser disponibilizados em idioma português do Brasil, admitindo-se no idioma inglês quando não houver em idioma português do Brasil.

4.141. A pretensa contratação deverá seguir, quando aplicável, ao disposto no programa A3P (Agenda Ambiental na Administração Pública) do Ministério do Meio Ambiente, que insere critérios socioambientais nas atividades dos órgãos públicos dos poderes executivo, legislativo e judiciário, das esferas federal, estadual e municipal.

4.142. Quanto aos requisitos sociais, os profissionais da Contratada, quando nas dependências do Contratante, deverão apresentar-se vestidos de forma adequada ao ambiente de trabalho, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional da Contratante.

4.143. Os profissionais também deverão respeitar todos os servidores, funcionários

e colaboradores em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo.

5. LEVANTAMENTO DE MERCADO

5.1. O levantamento de mercado visa identificar e analisar as soluções disponíveis para atender à necessidade da Administração Pública Municipal por meio da CODEMAR de uma solução integrada de cibersegurança e adequação à LGPD, conforme as diretrizes da IN 94/2022 SGD/ME e da Lei n.º 13.303/2016. Este levantamento considerou necessidades similares em outros órgãos públicos, alternativas de mercado, softwares disponíveis (Portaria STI/MP n.º 46/2016), políticas e padrões de governo, necessidades de adequação do ambiente da Contratante e diferentes modelos de prestação de serviço.

Identificação das soluções

5.2. Foram identificadas as seguintes soluções que potencialmente atendem às necessidades da CODEMAR:

5.3. **Solução A:** Solução integrada com gerenciamento de Vulnerabilidades de forma contínua, com Painel de Prevenção de Phishing, Simulação de Ataques DDoS, Testes de Invasão, Monitoramento de Vulnerabilidades, Relatórios, Plataforma de Compliance LGPD com Suporte Técnico Especializado e apoio a resposta a Incidentes.

5.4. **Solução B:** Combinação de diferentes ferramentas e serviços de diferentes fornecedores, integrando soluções open source e comerciais para compor a solução completa.

5.5. **Solução C:** Desenvolvimento interno de uma plataforma customizada para atender às necessidades específicas da CODEMAR.

Análise comparativa das soluções

5.6. A análise comparativa considerou os seguintes critérios: funcionalidades, performance, escalabilidade, segurança, usabilidade, suporte técnico, custo, conformidade com a LGPD, e integração com a infraestrutura de TIC existente.

Solução A:

5.7. Vantagens: Implantação rápida, facilidade de uso, suporte técnico completo, atualizações constantes.

5.8. Desvantagens: Custo potencialmente mais elevado a longo prazo, menor flexibilidade de customização.

Solução B:

5.9. Vantagens: Maior flexibilidade, potencial para menor custo a curto prazo. Desvantagens: Maior complexidade de integração, necessidade de expertise interna, potenciais gaps de segurança e suporte.

Solução C:

5.10. Vantagens: Total customização, potencial para maior controle.

5.11. Desvantagens: Alto custo de desenvolvimento e manutenção, longo prazo de implantação, necessidade de equipe especializada.

Descrição dos cenários de cada solução

5.12. Cenário Solução A: Contratação de um fornecedor único para a solução completa, com SLA e suporte técnico garantidos.

5.13. Cenário Solução B: Contratação de diferentes fornecedores para as diversas ferramentas e serviços, com integração e gerenciamento pela equipe interna da CODEMAR.

5.14. Cenário Solução C: Alocação de recursos internos para o desenvolvimento e manutenção da solução, com potencial contratação de consultores especializados.

Registro de soluções consideradas inviáveis

5.15. A Solução C (desenvolvimento interno) foi considerada inviável devido ao alto custo, longo prazo de implantação e necessidade de equipe especializada, o que não se alinha com a realidade da administração pública municipal. Esta solução representaria um risco elevado para o projeto, com potencial para atrasos, custos excessivos e dificuldades de manutenção a longo prazo. A equipe de planejamento da contratação, priorizando a eficiência, a segurança e a conformidade, optou por descartar esta alternativa.

5.16. As soluções A e B foram analisadas em conformidade com a Lei Federal n.º 13.303/2016, a Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, as Notas Técnicas do TCE-RJ, a LGPD, a Lei Anticorrupção, o Decreto Municipal n.º 937/2022 e o PETI 2022-2025, considerando os padrões de governança e segurança da informação. A contratação da solução escolhida visa fortalecer a segurança cibernética da administração pública municipal, por meio da CODEMAR, garantir a adequação à LGPD e otimizar os processos de gestão de dados, contribuindo para a melhoria dos serviços prestados e para o aumento da eficiência operacional.

ANÁLISE DE CONFORMIDADE DAS SOLUÇÕES				
Requisito	**Solução**	**Sim**	**Não**	**Não se Aplica**
A SOLUÇÃO ENCONTRA-SE IMPLANTADA EM OUTRO ÓRGÃO OU ENTIDADE DA ADMINISTRAÇÃO PÚBLICA?	Solução A	X		
	Solução B	X		
	Solução C		X	
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução A		X	
	Solução B		X	
	Solução C		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução A		X	
	Solução B	X		
	Solução C	X		
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, e PWG?	Solução A			X
	Solução B			X
	Solução C			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução A			X
	Solução B			X
	Solução C			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução A			X
	Solução B			X
	Solução C			X

5.17. Após realizar uma análise comparativa abrangente das soluções disponíveis, chegou-se à escolha da "SOLUÇÃO A" em virtude dos seguintes benefícios:

5.17.1. **Expertise e Especialização:** A contratação de empresas especializadas em governança de TIC e segurança cibernética oferece acesso a expertise e conhecimento técnico de alto nível, o que garante a implementação de soluções de segurança mais eficazes e alinhadas com as melhores práticas do mercado. Essa expertise é fundamental para proteger os dados da administração pública municipal contra as ameaças cibernéticas em constante evolução, bem como para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD).

5.17.2. **Tecnologia Avançada:** As empresas especializadas em segurança e governança de TIC mantêm-se na vanguarda da inovação, investindo constantemente em pesquisa e desenvolvimento de novas tecnologias e soluções. Essa prática garante que a administração pública municipal tenha acesso às ferramentas mais avançadas e eficazes para a proteção de dados dos cidadãos e a gestão eficiente dos recursos municipais.

5.17.3. **Atualização Contínua:** Essas empresas investem continuamente em pesquisa e desenvolvimento, adaptando seus serviços e soluções para garantir que a administração pública municipal esteja sempre protegida contra os ataques cibernéticos mais recentes e que seus processos de governança de TIC sejam eficientes e eficazes.

5.17.4. **Foco no Core Business e Transformação Digital:** Ao terceirizar os serviços de segurança cibernética e governança de TIC, a equipe interna de TIC da administração pública municipal poderá redirecionar seus esforços para atividades mais estratégicas e que agregam maior valor ao órgão, além de eliminar a obrigatoriedade de gastos com estrutura, capacitação e admissão de profissionais especializados em segurança e governança, proporcionando uma redução significativa de custos a longo prazo.

5.17.5. **Escalabilidade e Flexibilidade:** A contratação de serviços especializados oferece à gestão pública benefícios como escalabilidade e flexibilidade. A escalabilidade permite ajustar os serviços conforme as demandas variam, enquanto a flexibilidade possibilita personalizações para atender a exigências específicas, como novas tecnologias ou normas regulatórias. Combinando esses aspectos, a administração pública municipal, por meio da CODEMAR, avança na governança de TIC, fortalece a proteção de dados sensíveis e garante a continuidade dos serviços à população de maneira mais eficiente.

5.17.6. **Conformidade Integrada:** A solução proposta proporciona uma abordagem abrangente e integrada para o cumprimento de diversas regulamentações de segurança e governança, simplificando o processo de adequação da administração pública municipal, por meio da CODEMAR, às normas como a Lei Geral de Proteção de Dados Pessoais (LGPD) e a Lei de Acesso à Informação.

5.17.7. **Gestão de Riscos Abrangente:** A plataforma oferece uma visão abrangente dos riscos de segurança e governança, permitindo que a administração pública municipal, por meio da CODEMAR, identifique, avalie e mitigue ameaças de forma mais eficiente em toda a sua estrutura.

5.17.8. **Melhoria Contínua dos Processos:** A expertise em governança de TIC oferece à administração pública municipal a oportunidade de otimizar e automatizar seus processos internos, resultando em um aumento significativo da eficiência operacional.

5.18. Diante do cenário atual, a contratação de solução integrada com gerenciamento de Vulnerabilidades de forma contínua, com Painel de Prevenção de Phishing, Simulação de Ataques DDoS, Testes de Invasão, Monitoramento de Vulnerabilidades, Relatórios, Plataforma de Compliance LGPD com Suporte Técnico Especializado e apoio a resposta a Incidentes para adequação a LGPD e aumento da Segurança Cibernética, é a alternativa mais adequada para a administração pública municipal, pois ela garante a melhor solução técnica, operacional e econômica visando a proteção de dados, a conformidade com as leis

e a eficiência operacional.

5.19. A adoção dessa solução integrada representa um passo importante para a administração pública municipal, que não apenas fortalece sua postura de segurança cibernética, mas também estabelece uma base sólida e eficiente a conformidade contínua com a Lei Geral de Proteção de Dados (LGPD) e outras regulamentações relevantes.

5.20. Após análise criteriosa, considerando a qualidade dos serviços, a produtividade, o nível de maturidade, a complexidade de gestão do contrato e o alinhamento com as necessidades da Contratante, conclui-se que a Solução A (Solução integrada com gerenciamento de Vulnerabilidades de forma contínua, com Painel de Prevenção de Phishing, Simulação de Ataques DDoS, Testes de Invasão, Monitoramento de Vulnerabilidades, Relatórios, Plataforma de Compliance LGPD com Suporte Técnico Especializado e apoio a resposta a Incidentes para adequação a LGPD e aumento da Segurança Cibernética) é a mais adequada para o contexto atual. Essa opção oferece atendimento eficiente, conformidade com as necessidades da Contratante e uma relação custo-benefício favorável ao longo do ciclo de vida da solução, permitindo uma gestão eficiente dos recursos e previsibilidade orçamentária, além de incentivar a melhoria contínua da qualidade dos serviços. Portanto, considerando os fatores analisados, a Solução A é a opção mais vantajosa para Adequação a LGPD e aumento da Segurança Cibernética.

6. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

6.1. Para dimensionar adequadamente a contratação da solução de gerenciamento de vulnerabilidades, compliance e adequação à LGPD, foi elaborado um modelo de **memória de cálculo** que considera as melhores práticas de dimensionamento de soluções de TIC e governança. Esse modelo leva em conta não apenas o número estimado de usuários, mas também outros fatores relevantes, como a complexidade do ambiente, o volume de dados e processos, e o nível de maturidade da organização em governança de TIC.

Item	Elementos do Ambiente	Resposta/QTD Mínima Estimada
1	Data Center	2
2	Switches Gerenciáveis	215
3	Switches Não Gerenciáveis	-
4	Access Points	50
5	IP públicos	20
6	Servidores Windows	51

7	Servidores Linux	97
8	Roteadores	0
9	Estações de Trabalho (notebooks e desktops)	8327
10	Câmeras e Dispositivos de Controle de Acesso	2240 - Patrimonial + Urbanas
11	Aplicações Web/Portais	56
12	Ambiente de Virtualização	1
13	Controladoras Wi-Fi	2
14	Instâncias de Bancos de Dados	20
15	Central Telefônica	0
16	Firewall	1
17	Contas de e-mail	629
18	Storages	1
19	Relógios Eletrônicos de Ponto	0
20	Solução de Backup	1
21	Usuários no AD	6150
22	Grupos no AD	708
23	Prédios Remotos	258
24	Impressoras	379
25	Ferramenta de Monitoramento de Rede	2 Zabbix e Observium
26	Ferramenta de ITSM	0
27	Videowall	2
28	FQDNs Domínios Internos	278
29	FQDNs Domínios Externos	120
30	VPN Usuários	408
31	VPN Site-to-Site	1
32	Endereços FTP	0

Número Aproximado de Ativos e Usuários

6.2. O primeiro passo para estimar a demanda é determinar o número de ativos e usuários que serão diretamente ou indiretamente atendidos pela solução. Consideram-se tanto os ativos de TIC quanto os usuários que dependem da infraestrutura de TIC que será protegida e aprimorada.

6.2.1. Total de Estações de Trabalho: 8327.

6.2.2. Total de Servidores: 148 (51 Windows + 97 Linux).

6.2.3. Total de Usuários no AD: 6.150.

6.2.4. Total de Contas de E-mail: 629.

6.3. Esses números indicam uma estrutura administrativa complexa e

diversificada, justificando a necessidade de uma plataforma de cibersegurança robusta e adequação à LGPD.

Volumetria de Dados

6.4. Estimativa em 20 TB (Terabytes) do volume de dados a serem gerenciados, esta estimativa parece razoável considerando o tamanho da organização. Conforme a LGPD, será crucial implementar medidas técnicas e organizacionais para proteger informações pessoais e dados sensíveis, incluindo criptografia, controle de acesso, e políticas de retenção e exclusão de dados.

Complexidade da Infraestrutura de TI

6.5. Para avaliar a complexidade da infraestrutura de Tecnologia da Informação e Comunicação (TIC) da administração pública municipal,, e assim dimensionar adequadamente a solução integrada, foi utilizada uma escala de 1 a 5, onde:

1 ⟶ Representa um ambiente de TIC muito simples
2 ⟶ Representa um ambiente simples.
3 ⟶ Representa um ambiente de complexidade média.
4 ⟶ Representa um ambiente complexo.
5 ⟶ Representa um ambiente de alta complexidade.

6.6. Essa escala considera fatores como o número de sistemas, a diversidade de tecnologias, a integração entre os sistemas, a quantidade de dispositivos e a criticidade dos serviços suportados pela infraestrutura de TIC.

6.7. Com base nessa escala, a infraestrutura de TIC da administração pública municipal foi classificada como complexa (4). Essa classificação é coerente com a estrutura organizacional apresentada, que inclui um número significativo de secretarias e órgãos, com uma variedade de sistemas e serviços que dependem da TIC. A implementação da solução, portanto, deverá levar em conta os desafios de integração e adaptação a essa infraestrutura complexa.

6.8. Nível de Maturidade em Governança de TIC

6.9. Para avaliar o nível de maturidade da administração pública municipal em relação à Governança de Tecnologia da Informação e Comunicação (TIC), foi utilizada uma escala de 1 a 5 baseada no modelo ITIL (Information Technology Infrastructure Library), que é um conjunto de melhores práticas para gerenciamento de serviços de TI reconhecido internacionalmente. Os níveis de maturidade, de acordo com a ITIL, são:

1 ⟶ Inicial: Processos de TI são imprevisíveis, pouco controlados e reativos.
2 ⟶ Repetível: Processos básicos de TI são estabelecidos, mas a gestão ainda é reativa.
3 ⟶ Definido: Processos de TI são documentados, padronizados e proativos.

4 ⟶ Gerenciado: Processos de TI são medidos e controlados, com foco na melhoria contínua.
5 ⟶ Otimizado: Foco na otimização contínua dos processos de TI, com base em dados e análise.

6.10. Essa escala permite identificar o estágio atual da administração pública municipal e direcionar os esforços de melhoria em governança de TIC.

6.11. Com base na escala, foi classificada no nível Repetível (2) em Governança de TIC. Isso indica que, embora alguns processos básicos de TIC já estejam estabelecidos, ainda há um caminho considerável a percorrer para atingir níveis mais altos de maturidade, como a padronização, a medição e a otimização dos processos. A implementação da solução contribuirá para essa evolução.

Estimativa da Demanda por Bens e Serviços

6.12. Com base nos dados apresentados, a estimativa da demanda inclui:

ITEM	CATSER	DESCRIÇÃO	UNIDADE DE MEDIDA	QTD MÍNIMA	QTD MÁXIMA
1	27340	Plataforma de Segurança Cibernética (por Ativo, 12 meses): Licença de uso de plataforma de segurança cibernética, cobrindo ativos (endpoints e FQDNs), incluindo: • Gerenciamento contínuo de vulnerabilidades (descoberta, avaliação, priorização, relatórios). • Painel de prevenção de phishing. • Simulação de ataques DDoS. • Testes de invasão (pentest) automatizados. • Monitoramento contínuo de vulnerabilidades e ameaças. • Relatórios de diagnóstico, recomendações e planos de ação. Cobertura Mínima: 8.873 ativos, sendo a soma de 8.475 endpoints (estações de trabalho e servidores) e 398 FQDNs (278 internos + 120 externos).	Ativo (Endpoint / FQDN)	8.873	10.000
2	27260	Serviços Gerenciados de Segurança e Resposta a Incidentes (12 meses): Serviços especializados contínuos de: • Suporte técnico especializado para a plataforma (Item 1). • Consultoria em segurança cibernética.	Mês	12	12

		• Análise e investigação aprofundada de vulnerabilidades e ameaças. • Planejamento e apoio à execução de testes de invasão (pentest) realizados por meio da plataforma ou por outros meios, conforme necessidade. • Monitoramento proativo de alertas, ameaças e indicadores de comprometimento. • Relatórios gerenciais e executivos periódicos.			
3	27260	Serviços de Compliance e Adequação à LGPD (12 meses): Serviços especializados e contínuos para garantir a conformidade com a LGPD, incluindo: • Mapeamento e gestão de dados pessoais. • Gestão de consentimento. • Atendimento a requisições de titulares. • Elaboração e acompanhamento de Relatórios de Impacto à Proteção de Dados (DPIA/RIPD). • Apoio à gestão de incidentes de segurança da informação com foco em dados pessoais. • Desenvolvimento e manutenção de políticas e procedimentos de privacidade. • Consultoria especializada em LGPD. • Acompanhamento de mudanças na legislação e melhores práticas. • Inclui: Implementação de metodologia/processos, treinamento básico (até 8 horas) e suporte técnico durante o período.	Mês	12	12
4	27022	Treinamento em Segurança Cibernética e Uso da Plataforma (por turma): Treinamento técnico e prático para a equipe da CONTRATANTE, abordando: • Conceitos fundamentais de segurança cibernética. • Melhores práticas de segurança e hardening. • Uso completo da Plataforma de Segurança Cibernética (Item 1).	Turma	10	15

		• Interpretação de relatórios e aplicação de recomendações. • Procedimentos de resposta a incidentes. • Carga horária: Mínimo de 20 horas. • Formato: Híbrido (presencial e/ou online), com material didático completo. • Turmas: Até 10 participantes por turma.			

6.13. Essa estimativa visa garantir a cobertura adequada dos ativos de TIC e a conformidade com as regulamentações aplicáveis, além de promover a segurança cibernética contínua.

7. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

7.1. O custo anual estimado da contratação é R$ XXX (xxx), conforme mapa de pesquisa de preços anexo.

8. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

8.1. A solução atenderá a demanda crescente por segurança cibernética e conformidade legal, em linha com as diretrizes do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), Plano Estratégico de Tecnologia da Informação (PETI) e a Instrução Normativa SGD/ME n.º 94/2022.

8.2. A solução proposta visa mitigar esses riscos, melhorando a segurança da informação e a eficiência operacional da Administração Pública Municipal, por meio da CODEMAR.

8.3. A solução escolhida contempla a CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA IMPLEMENTAÇÃO DE SOLUÇÃO INTEGRADA COM GERENCIAMENTO DE VULNERABILIDADES DE FORMA CONTINUA, COM PAINEL DE PREVENÇÃO DE PHISHING, SIMULAÇÃO DE ATAQUES DDOS, TESTES DE INVASÃO, MONITORAMENTO DE VULNERABILIDADES, RELATÓRIOS, PLATAFORMA DE COMPLIANCE LGPD, COM SUPORTE TÉCNICO ESPECIALIZADO E APOIO A RESPOSTA À INCIDENTES, DESTINADA A PROMOVER A ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD), EM CONFORMIDADE COM AS MELHORES PRÁTICAS DE SEGURANÇA CIBERNÉTICA, conforme especificações técnicas, quantidades e demais condições previstas neste estudo.

8.4. Por todo o exposto, trata-se de serviços essenciais de natureza continuada SEM dedicação exclusiva de mão de obra.

A solução integrada de cibersegurança contemplará:

8.5. **Solução de Gerenciamento de Vulnerabilidades:** Capacidade de abranger simultaneamente no mínimo 20 endereços IP públicos, 8.475 endpoints e 398 FQDNs (internos e externos), garantindo a identificação e mitigação de vulnerabilidades em toda a infraestrutura de TIC.

8.6. **Painel de Prevenção de Phishing:** Sistema para detectar e bloquear tentativas de phishing, reduzindo o risco de comprometimento de credenciais e dados sensíveis.

8.7. **Simulação de Ataques DDoS:** Ferramenta para simular ataques de negação de serviço distribuído (DDoS), permitindo a avaliação da resiliência da infraestrutura e o planejamento de ações de resposta.

8.8. **Testes de Invasão e Segurança (Pentests):** Avaliações periódicas para identificar vulnerabilidades de segurança em sistemas e aplicações, permitindo a correção de falhas antes que sejam exploradas por atacantes.

8.9. **Monitoramento e Análise de Vulnerabilidades:** Monitoramento contínuo da infraestrutura de TIC, proporcionando alertas em tempo real sobre novas vulnerabilidades e potenciais ameaças.

8.10. **Relatórios e Indicadores de Desempenho:** Geração de relatórios periódicos e indicadores de desempenho, permitindo a avaliação da eficácia das medidas de segurança implementadas.

A plataforma de compliance e adequação à LGPD contemplará:

8.10.1. **Dashboard e Indicadores:** Ferramenta de visualização de dados que apresenta informações de forma consolidada e acessível, facilitando o monitoramento do desempenho, a identificação de tendências, a análise de métricas e a tomada de decisões embasadas nos dados apresentados.

8.10.2. **Atendimento a Titulares de Dados:** Canal de comunicação para atender as demandas dos titulares de dados.

8.10.3. **Banner de Cookies:** Ferramenta para implementar banners de cookies conforme as diretrizes da ANPD.

8.10.4. **Geração de Políticas e Termos:** Criação automatizada de políticas de privacidade e termos de uso.

8.10.5. **Marketplace de Soluções para LGPD:** Plataforma para encontrar soluções e serviços relacionados à LGPD.

8.10.6. **Gestão de Terceiros:** Ferramenta para cadastrar e avaliar fornecedores quanto à conformidade com a LGPD.

8.10.7. **Diagnóstico de Maturidade:** Avaliação do nível de maturidade da empresa em relação à LGPD.

8.10.8. **Sugestão de Ameaças:** Identificação e sugestão de medidas para mitigar ameaças à privacidade dos dados.

8.10.9. **Gestão de Processos e Riscos:** Mapeamento de processos e avaliação de riscos para garantir a conformidade.

8.10.10. **Gestão de Consentimento:** Ferramenta para gerenciar o consentimento dos titulares de dados.

8.10.11. **Gestão de Incidentes:** Plataforma para reportar e gerenciar incidentes de segurança.

8.10.12. **Central da Privacidade:** Portal de comunicação para atender as demandas referentes à LGPD.

8.10.13. **Relatórios:** Geração de relatórios em poucos cliques (RIPD, ROPA, LIA, Gerenciais).

8.10.14. **Centralização e Visão Unificada:** Painel consolidado para gerenciar a conformidade de múltiplas empresas.

8.10.15. **Personalização e Identidade Visual:** Recurso para customizar a área do cliente e relatórios.

8.10.16. **Diagnósticos Avançados e Melhoria Contínua:** Identificação de pontos fracos e geração automática de atividades de melhoria.

8.10.17. **Relatórios Simplificados:** Geração rápida e fácil de relatórios de conformidade personalizados.

8.10.18. **Inteligência Artificial (DAI):** Sistema de IA para automatização inteligente de tarefas e otimização contínua do programa de privacidade.

8.11. Suporte técnico especializado para cibersegurança e adequação à LGPD: Suporte técnico especializado para auxiliar na implementação, operação e manutenção da solução, garantindo o seu funcionamento adequado.

8.12. Resposta à incidentes: Plano e procedimentos para resposta rápida e eficaz a incidentes de segurança, minimizando os impactos negativos e garantindo a continuidade dos serviços.

Justificativa técnica da escolha da solução

8.13. A proposta é baseada em uma solução integrada que proporciona uma visão holística da segurança da informação e da conformidade com a LGPD. A integração dos diferentes módulos (gerenciamento de vulnerabilidades, prevenção de phishing, simulação de ataques DDoS, testes de invasão, monitoramento e análise de vulnerabilidades e plataforma de compliance com apoio a resposta a incidentes) permite uma gestão mais eficiente e eficaz dos riscos. A escolha por uma solução integrada se justifica pela necessidade de automatização, monitoramento em tempo real e relatórios consolidados, crucial para a administração pública de grande porte. A solução atenderá às necessidades específicas da administração pública municipal, por meio da CODEMAR, abrangendo o volume de ativos (endpoints, IPs e FQDNs) e garantindo a conformidade com as normas técnicas e legais aplicáveis, incluindo a Lei n.º 13.303/2016 e a Instrução Normativa SGD/ME n.º 94/2022. A utilização de ferramentas e metodologias de segurança de última geração, testadas e validadas pelo mercado, assegurará a eficácia da solução, promovendo:

8.14. Proteção aprimorada contra ameaças cibernéticas: A solução permitirá que a administração pública municipal, por meio da CODEMAR se proteja de forma mais eficaz contra as ameaças cibernéticas em constante evolução, como ransomware, DDoS e outros ataques sofisticados.

8.15. Conformidade com a LGPD: A adequação à Lei Geral de Proteção de Dados (LGPD) garantirá que a administração pública municipal esteja em conformidade com a legislação e evite sanções por descumprimento.

8.16. Melhoria na gestão de riscos: A plataforma integrada de governança de TIC permitirá que a administração pública municipal, por meio da CODEMAR, tenha uma visão holística dos riscos de segurança e governança, facilitando a identificação, avaliação e mitigação de ameaças.

8.17. Aumento da eficiência operacional: A solução contribuirá para a otimização e a automatização de processos internos, aumentando a eficiência operacional da administração pública municipal.

8.18. Melhoria na qualidade dos serviços: A contratação permitirá que a administração pública municipal, por meio da CODEMAR, ofereça serviços de maior qualidade aos cidadãos, de forma mais segura, confiável e eficiente.

8.19. Redução de custos: A solução proposta é escalável e permite que a administração pública municipal ajuste os custos aos seus recursos, evitando gastos desnecessários.

Justificativa econômica da escolha da solução

8.20. Embora a solução integrada possa apresentar um custo total de propriedade (TCO) elevado a longo prazo, a prevenção de incidentes de segurança e a conformidade com a LGPD resultam em economia a longo prazo. O custo da não conformidade com a LGPD (multas, ações judiciais e danos à reputação) é significativamente maior do que o investimento em uma solução preventiva como a proposta. A solução permite a redução de custos com:

8.20.1. **Incidentes de segurança:** A prevenção e a resposta eficaz a incidentes reduzem perdas financeiras e danos à reputação.

8.20.2. **Auditoria e consultoria externa:** A solução integrada minimiza a necessidade de contratação de consultoria especializada para gestão de vulnerabilidades e conformidade com a LGPD.

8.20.3. **Horas de trabalho:** A automatização dos processos de monitoramento e análise de vulnerabilidades libera recursos humanos para outras atividades estratégicas.

8.20.4. **Multas e sanções:** A conformidade com a LGPD evita o pagamento de multas significativas.

8.21. A análise custo-benefício demonstra que a adoção da solução integrada é mais econômica e eficaz do que a abordagem fragmentada ou a ausência de uma estratégia de cibersegurança robusta. A solução proposta apresenta um ótimo custo-benefício ao considerar os riscos e os custos associados a não adoção de medidas adequadas de segurança e conformidade legal. A licitação será conduzida consoante a Lei n.º 13.303/2016 e demais normativas aplicáveis, assegurando a transparência e a melhor relação custo-benefício.

Conclusão

8.22. Diante das considerações acima, a solução se apresenta como a alternativa mais adequada para a administração pública municipal de Maricá. Esta solução não apenas atende às necessidades atuais da gestão, mas também se alinha com os princípios de eficiência, transparência e responsabilidade fiscal, fundamentais em um contexto de gestão pública. A solução permite que a administração pública forneça seus serviços à população de maneira mais segura e em conformidade com as leis, de forma mais eficaz e garantindo a modernização contínua dos serviços prestados.

9. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

9.1. A contratação será efetuada por Lote Único, em virtude de considerações

técnicas, administrativas e econômicas. A preservação do objeto como um único conjunto indivisível é fundamental para assegurar a qualidade e a eficiência na gestão do serviço.

9.2. Conforme definição estabelecida pelo art. 2º, inciso VII da IN n.º 94/2022, a solução de TIC é "conjunto de bens e/ou serviços que apoiam processos de negócio mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações". No entendimento da equipe de planejamento da contratação, a solução de TIC em questão engloba todos os elementos (bens e serviços de TIC) que se integram para o alcance dos resultados pretendidos, referindo-se a cada lote.

9.3. A adjudicação do objeto da pretensa contratação à empresas distintas, além de aumentar seu custo administrativo, abre margem para que as empresas deixem de prestar o serviço contratado, alegando que a falha de um serviço sob sua responsabilidade foi causada por falha de componente sob responsabilidade de outra contratada. De modo a impedir que esse cenário se torne realidade, é fundamental que os itens que compõem o objeto da contratação sejam adjudicados a uma única licitante.

9.4. A unificação em um único contrato e com uma mesma contratada proporciona uma clara economia para a administração, devido à redução de custos resultante do compartilhamento de recursos humanos, tecnológicos, gerenciais, operacionais e logísticos.

9.5. Além disso, a alocação de recursos públicos será mais eficiente com a gestão de um contrato único, uma vez que demanda menos recursos do que seria necessário para o controle de vários ajustes. Assim, a unicidade contratual se apresenta como uma vantagem econômica para a administração municipal.

9.6. A contratação em lote de um único fornecedor resultará em um maior volume de serviços, o que refletirá em preços unitários e totais mais baixos, proporcionando, assim, uma economia significativa para a Contratante.

9.7. Sob o aspecto econômico, é evidente que o parcelamento proporcionará inquestionável prejuízo no que concerne ao ganho de escala, visto que impossibilitaria o compartilhamento de custos.

9.8. O próprio TCU já teve a oportunidade de se manifestar no sentido de que a licitação por lote único seria mais eficiente para a administração municipal, conforme descrito no Acórdão nº 3.140/2006 - "*(...) Cabe considerar, porém, que o modelo para a contratação parcelada adotado nesse parecer utilizou uma excessiva pulverização dos serviços. Para cada um de cinco prédios, previram-se*

vários contratos (ar condicionado, instalações elétricas e eletrônicas, instalações hidrossanitárias, civil). Esta exagerada divisão de objeto pode maximizar a influência de fatores que contribuem para tornar mais dispendiosa a contratação (...) embora as estimativas numéricas não mostrem consistência, não há nos autos nenhuma evidência no sentido oposto de que o parcelamento seria mais vantajoso para a Administração. Ao contrário, os indícios são coincidentes em considerar a licitação global mais econômica" (Acórdão nº3140/2006 do TCU).

9.9. A não divisão do objeto simplifica a execução dos serviços e a sua fiscalização, resultando em uma entrega de serviços e produtos com um grau de objetividade elevado. Isso permite a implementação e auditoria eficaz do SLA contratado. Por outro lado, a separação por itens poderia encarecer a contratação e comprometer a potencial economia de escala, dificultando a execução adequada do objeto e a definição de padrões, além de complicar a fiscalização do contrato.

9.10. Assim, nas hipóteses de licitação com diversidade de serviços e produtos, o entendimento dos Tribunais de Contas tem sido o de que o parcelamento ou não do objeto da licitação deve ser auferido sempre no caso concreto, perquirindo-se essencialmente acerca da viabilidade técnica e econômica do parcelamento e da divisibilidade do objeto.

9.11. O TCU, no Acórdão nº 732/2008, se pronunciou ainda da seguinte forma: "*(...) a questão da viabilidade do fracionamento deve ser decidida com base em cada caso, pois cada obra tem as suas especificidades, devendo o gestor decidir analisando qual a solução mais adequada no caso concreto (...)*".

9.12. O Professor Jorge Ulisses Jacoby Fernandes, no Parecer nº 2086/00, elaborado no Processo nº 194/2000 do TCDF, assim descreve o seu entendimento sobre o assunto — *"Desse modo, a regra do parcelamento deve ser coordenada com o requisito que a própria lei definiu: só se pode falar em parcelamento quando há viabilidade técnica para sua adoção. Não se imagina, quando o objeto é fisicamente único, como um automóvel, que o administrador esteja vinculado a parcelar o objeto. Nesse sentido, um exame atento dos tipos de objeto licitados pela Administração Pública evidencia que embora sejam divisíveis, há interesse técnico na manutenção da unicidade, da licitação ou do item da mesma. Não é, pois, a simples divisibilidade, mas a viabilidade técnica que dirige o processo decisório"*.

9.13. Observa-se que, na aplicação dessa norma, a avaliação sob o aspecto técnico precede a avaliação econômica, conforme a disposição dos requisitos apresentados em seu conteúdo. Essa abordagem jurídica se alinha à lógica prática. Caso um objeto divisível seja mais vantajoso sob o aspecto econômico, mas apresente inviabilidade técnica para ser licitado de forma separada, a avaliação

econômica perde a sua relevância. Para exemplificar, considere o caso de um automóvel: se as peças isoladamente custassem menos, ainda assim seria recomendável não dividir a contratação. Isso se deve ao fato de que, sob a perspectiva técnica, é a visão do conjunto que determina a garantia do fabricante, assegurando que as partes se integrem de forma orgânica e harmônica. Por essa razão, o bom administrador deve, primeiramente, avaliar se o objeto é divisível. Caso afirmativo, o próximo passo será analisar a conveniência técnica de licitá-lo como um todo ou em partes.

9.14. A concentração de atos por único prestador assegura maior efetividade e qualidade aos serviços prestados garantindo que ativos sejam compatíveis, fator de extrema relevância para a administração pública que opera diversos sistemas. Há ainda inegável ganho sob a ótica da interação entre as diversas etapas contratuais: fornecimento, cumprimento de cronogramas, observância de prazos, fiscalização e gestão do contrato, todos concentrados em uma única empresa.

9.15. O mesmo se aplicaria a um possível prejuízo na qualidade da prestação do serviço, caso ocorra um conflito entre prestadores diferentes, incluindo na manutenção, quanto à identificação e à solução do problema. Não se pode descartar a possibilidade de que um prestador tente transferir a responsabilidade para o outro, o que poderia atrasar ou até inviabilizar a resolução da falha técnica.

9.16. A rigor, o agrupamento de vários itens em um mesmo lote não compromete a competitividade do certame, desde que haja diversas empresas no mercado com condições e aptidão para cotar todos os itens. É importante considerar a modalidade adotada, na qual os recursos de tecnologia da informação e comunicação desempenham um papel fundamental ao aproximar pessoas e encurtar distâncias. Isso resulta em uma ampliação significativa da competitividade, gerando inúmeras repercussões positivas no processo de licitação pública. Entre essas repercussões, destaca-se a maior probabilidade de a Administração Pública firmar contratos mais vantajosos, uma vez que recebe um número maior de propostas, o que, por sua vez, beneficia a eficiência nos contratos administrativos.

9.17. Por fim, esclarecemos que todos os dispositivos previstos na Lei Federal nº 13.303/2016, bem como as definições relacionadas ao processo de contratação, Garantia foram analisados sob a ótica dos princípios da isonomia e da competitividade. Esses princípios não visam a exclusão de qualquer participante, uma vez que a seleção da proposta mais vantajosa para a Administração Pública ocorre de forma natural. Para assegurar a execução do contrato e o pleno cumprimento do objeto, apenas estabeleceram-se requisitos mínimos.

10. OPÇÃO PELO SISTEMA DE REGISTRO DE PREÇOS

10.1. A equipe de planejamento da contratação sugere a realização de procedimento licitatório utilizando o Sistema de Registro de Preços para a contratação pretendida pelo fato de que a execução do referido objeto aplicar-se-á de forma parcelada, bem como pela impossibilidade de definir previamente o quantitativo total a ser utilizado pela estrutura da administração pública, por conta das necessidades de equipamentos de TIC que surgirão no decorrer da execução do objeto, de acordo com o art. 66 da Lei Federal nº 13.303/2016 c/c art. 3º, incisos I, III e IV, do Decreto Municipal nº 937[9], de 18 de novembro de 2022.

10.2. O órgão gerenciador da possível Ata de Registro de Preços a ser firmada mediante a realização do procedimento licitatório é a Companhia de Desenvolvimento de Maricá S/A - CODEMAR.

10.3. Serão participantes do Registro de Preços, os seguintes órgãos:

- Companhia Maricá Alimentos S/A - BIOTEC
- Companhia de Saneamento de Maricá S/A - SANEMAR
- Companhia de Desenvolvimento de Maricá S/A - CODEMAR, concentrando o restante de toda a estrutura da administração municipal.

11. DO PROCEDIMENTO LICITATÓRIO

11.1. A modalidade de licitação adotada deverá ser a de PREGÃO ELETRÔNICO, conforme disposto no art. 32, IV da Lei 13.303/2016.

11.2. O modo de disputa deverá ser o ABERTO, conforme disposto no art. 52 da Lei Federal nº 13.303/2016.

12. CRITÉRIOS DE QUALIFICAÇÃO TÉCNICA

12.1. A qualificação técnica será demonstrada por meio da comprovação de aptidão para o desempenho de atividades pertinentes e compatíveis com o objeto desta licitação, abrangendo tanto a capacidade técnico-profissional quanto a capacidade técnico-operacional da licitante.

Da capacidade técnico-profissional

12.2. Deverá ser apresentado junto com a documentação de habilitação, comprovação de no mínimo, três das seguintes certificações, distribuídas entre os profissionais da equipe (não é necessário que um único profissional possua todas): CISSP, GSEC, CompTIA Security+, Auditor Líder ISO 27001, Auditor Líder ISO

[9] DECRETO Nº 937 DE 18 DE NOVEMBRO DE 2022.

22301, CompTIA CySA+, CISA (ambas as certificações), OSCP com comprovação de vínculo: CTPS, contrato social, contrato de prestação de serviços ou declaração de contratação futura (com anuência do profissional).

12.3. Designação de um profissional com certificação CEH (Certified Ethical Hacker) para a execução dos serviços de Pentest. Comprovação de vínculo: CTPS, contrato social, contrato de prestação de serviços ou declaração de contratação futura (com anuência do profissional). Termo de Compromisso: Termo assinado pelo representante legal da empresa e pelo profissional, garantindo sua alocação para os serviços.

12.4. Deverá possuir funcionário com certificação ITIL Foundation ou certificação compatível ou superior compatível, para comprovar sua capacidade técnica. O documento comprobatório deve ser enviado junto com a documentação de habilitação.

12.5. Será admitida a comprovação da aptidão técnico-profissional por meio de certidões ou atestados de serviços similares em complexidade tecnológica e operacional, equivalentes ou superiores.

12.6. A empresa licitante poderá apresentar mais de um atestado para fins de composição e comprovação da qualificação técnico-profissional. Os atestados devem possibilitar determinar de forma inequívoca o período de execução dos serviços.

12.7. A Contratante reserva-se no direito de executar diligências para verificar e validar as informações prestadas no(s) atestado(s) de capacidade técnico-profissional fornecido(s) pelo vencedor do certame. Também poderão ser requeridos cópia do(s) contrato(s), nota(s) fiscal(is) ou qualquer outro documento que comprove, inequivocamente, a veracidade do(s) atestado(s).

12.8. O documento apresentado pela licitante para comprovação de sua qualificação técnica, além de possuir informações técnicas e profissionais suficientes para qualificar o escopo realizado, deverá conter dados que possibilitem à Contratante, por intermédio de seu Pregoeiro, caso julgue necessário, confirmar sua veracidade junto ao cedente emissor.

Da capacidade técnico-operacional

12.9. Deverá ser apresentado registro ou inscrição da empresa em qualquer entidade profissional competente. O documento comprobatório deve ser enviado junto com a documentação de habilitação.

12.10. Deverá ser apresentado atestado(s) comprovando a capacidade da licitante para fornecer, implantar, treinar, dar suporte e garantir o funcionamento de uma solução completa de segurança cibernética, incluindo monitoramento de vulnerabilidades, testes de intrusão, assistência na correção de falhas e elaboração de relatórios.

12.11. Deverá ser apresentado atestado(s) comprovando a capacidade da licitante para fornecer, implantar, treinar, dar suporte e garantir o funcionamento de uma solução de LGPD e Compliance.

12.12. Deverá ser apresentado atestado(s) comprovando a capacidade da licitante para fornecer e implantar a LGPD.

12.13. A capacidade técnico-operacional das licitantes deverá ser comprovada por meio da apresentação de Atestado(s) de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, que comprove ter a licitante cumprido, de forma satisfatória, a execução de serviço compatível ao objeto ou com complexidade superior ao especificado neste instrumento, com clara menção de execução bem-sucedida, quanto ao cumprimento de prazos, especificações e qualidade. A documentação apresentada deverá conter informações que permitam contatar a empresa atestante, para fins de aferição, bem como quantitativos e descrições que permitam avaliar a compatibilidade consideradas as parcelas de maior relevância.

12.14. A presente exigência de qualificação técnico-operacional da licitante se dá em razão da natureza da prestação do serviço a ser contratado, sendo também necessária e não excessiva, onde será imprescindível da empresa licitante aptidão técnica, operacional e financeira, para manter tal prestação de serviço essencial a municipalidade, prevalecendo, assim, a supremacia do interesse público.

12.15. Quanto ao valor significativo, sugere-se como referência o percentual mínimo de 4% do valor global. Na capacitação técnico-profissional não haverá exigência de comprovação de quantitativos mínimos, enquanto que na capacitação técnico-operacional, os quantitativos a exigir deverão ser limitados a, no máximo, 50% das quantidades previstas nos itens que compõem o Lote Único, com base na jurisprudência do TCU (a título exemplificativo: Acórdãos nº 1.284/03, 2.088/04, 2.215/08, 1432/2010-Plenário e 1851/2015–Plenário) e decisões anteriores desta Corte (processos TCE-RJ nº 277.821- 4/15 e 105.640-9/16, por exemplo)".

12.16. Considerando a quantidade total estimada dos serviços nos atestados citados no item anterior, o licitante deverá comprovar que tenha executado Contrato(s) com um mínimo de 47,75% dos valores licitados, configurando a

parcela de maior relevância do serviço licitado, conforme Súmula nº 263 do TCU, c/c - Constituição Federal, art. 37º, inciso XXI, sendo:

Item	Item (Parcela de maior relevância)	Quant. mínimo a ser comprovado	Porcentagem mínima exigida
A	Licença de uso de plataforma de segurança cibernética, cobrindo ativos (endpoints e FQDNs), incluindo: * Gerenciamento contínuo de vulnerabilidades (descoberta, avaliação, priorização, relatórios). * Painel de prevenção de phishing. * Simulação de ataques DDoS. * Testes de invasão (pentest) automatizados. * Monitoramento contínuo de vulnerabilidades e ameaças. * Relatórios de diagnóstico, recomendações e planos de ação.	4.237 Endpoints	47,75%

Justificativa técnica das qualificantes mínimas do lote único

12.17. Os requisitos de qualificação técnica são definidos considerando os requisitos de vulto econômico (valor correspondente a, no mínimo, 4% do valor estimado do orçamento total) e/ou considerando requisitos técnicos essenciais para a plena execução do objeto da contratação, assim como pela segurança contratual.

12.18. Item A – trata-se de serviço correspondente a **44%** do orçamento total estimado do objeto da contratação, que exigirá da futura contratada a comprovação de expertise técnica na prestação de serviços de LICENÇA DE USO DE PLATAFORMA DE SEGURANÇA CIBERNÉTICA, considerando seus requisitos técnicos específicos constantes deste instrumento.

12.19. Será admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados, de forma concomitante, dos serviços executados.

12.20. O(s) atestado(s) de capacidade técnica deverão se referir a serviços prestados no âmbito de sua atividade econômica principal e/ou secundária especificadas no Contrato Social registrado na junta comercial competente ou no cadastro de pessoas Jurídicas da Receita Federal do Brasil – RFB. (Acórdão TCU nº 8364/2012 - 2ª Câmara).

13. PARTICIPAÇÃO DE EMPRESAS EM CONSÓRCIO

13.1. Deverá ser permitida a participação de pessoas jurídicas organizadas em consórcio constituído, conforme as regras previstas na legislação vigente.

14. POSSIBILIDADE DE SUBCONTRATAÇÃO

14.1. Deverá ser vedada a cessão ou transferência parcial ou total do objeto da pretensa contratação.

14.2. A Contratada poderá subcontratar os serviços até o limite de 30% (trinta por cento) do valor do contrato, referente os serviços relativos aos itens 2 e 4, mediante comunicação expressa à Contratante e concordância desta, através de instrumento próprio.

14.3. A Subcontratada será solidariamente responsável com a Contratada por todas as obrigações legais e contratuais decorrentes do objeto do contrato, nos limites da subcontratação, inclusive as de natureza trabalhista e previdenciária.

15. GARANTIA CONTRATUAL

15.1. A prestação da garantia deverá ser de 5% (cinco por cento) do valor do contrato nos termos do art. 70 da Lei Federal nº 13.303/2016.

15.2. A validade da garantia deverá estar em consonância com o prazo de vigência contratual.

15.3. No caso de alteração do valor do contrato ou prorrogação de sua vigência, a garantia será readequada ou renovada nas mesmas condições e parâmetros, mantido o percentual sobre o valor atualizado do contrato.

16. NÍVEIS MÍNIMOS DE SERVIÇOS EXIGIDOS – NMSE

16.1. Os níveis mínimos de serviços exigidos são indicadores mensuráveis estabelecidos pela Contratante para aferir objetivamente os resultados pretendidos com a contratação, de acordo com as orientações contidas na nota técnica TCE-RJ nº 08/2024, que orienta os jurisdicionados do TCE-RJ acerca da definição de níveis mínimos de serviço nas contratações de TI.

16.2. São considerados para a pretensa contratação os seguintes indicadores:

Indicador TPR - Tempo para Resolução do Problema

1	**Descrição/Objetivo do Indicador**	1. O Tempo para Resolução do Problema (TPR) refere-se ao tempo total decorrido desde a abertura do chamado pela Contratante até a resolução efetiva do problema ou incidente relatado. Este indicador visa garantir que a Contratada atenda os prazos estipulados no Acordo de Nível de Serviço (SLA) e que os problemas sejam resolvidos de forma eficiente, minimizando impactos nas operações da Contratante. 2. O TPR será dividido em três categorias de problemas, conforme o impacto: alto, médio e baixo. O cálculo do TPR levará em consideração o tempo de atendimento e o tempo para a resolução final do problema, incluindo quaisquer intervenções on-site, quando aplicável. 3. O tempo será medido em horas ou dias úteis, conforme a urgência do problema e os prazos estabelecidos no SLA. 4. O tempo para resolução será considerado em sua totalidade, incluindo períodos de espera justificados e não justificados para a conclusão do atendimento.
2	**Meta**	95% dos chamados resolvidos dentro dos prazos acordados no SLA, conforme a categoria do problema (alto, médio ou baixo impacto).
3	**Periodicidade**	Apuração mensal, sempre considerando o mês de competência da medição dos serviços.
4	**Método de Medição (Fórmula)**	O indicador TPR deve ser calculado da seguinte forma: **TPR** = (CR / CA) x 100 **TPR** - Tempo para Resolução do Problema **CR** - Total de chamados resolvidos dentro do prazo **CA** - Total de chamados abertos O valor final será arredondado para o inteiro mais próximo, conforme metodologia definida pela Resolução nº 886/66 IBGE.

<table>
<tr>
<td>5</td>
<td>Glosa</td>
<td>A glosa para o TPR será aplicada sobre o valor mensal total dos serviços prestados pela Contratada referente aos itens 2 e/ou 3, limitada a 10% por item, caso a meta não seja atingida.

Tabela - Nível de glosa para descumprimento do indicador TPR.
<table>
<tr><th>Demandas executadas dentro do prazo</th><th>Desconto sobre o valor mensal da fatura</th></tr>
<tr><td>≥ 95%</td><td>0%</td></tr>
<tr><td>94%</td><td>3,00%</td></tr>
<tr><td>93%</td><td>5,00%</td></tr>
<tr><td>92%</td><td>7,00%</td></tr>
<tr><td>91%</td><td>9,00%</td></tr>
<tr><td>≤ 90%</td><td>10,00%</td></tr>
</table>
</td>
</tr>
<tr>
<td>6</td>
<td>Sanção</td>
<td>As sanções serão aplicadas conforme previsão no Termo de Referência.</td>
</tr>
<tr>
<td>7</td>
<td>Exemplos</td>
<td>Exemplo 01: Não atingir a meta com Glosa
1º passo: Obter os dados necessários:
• Fatura mensal dos serviços gerenciados de segurança e resposta à incidentes = R$ 500.000,00; e/ou
• Fatura mensal dos serviços de compliance e adequação à LGPD = R$ 400.000,00
Totalização de chamados registrados e atendidos no mês de referência:
Total de chamados (CA): 100
Total de chamados resolvidos dentro do prazo (CR): 93
Total de chamados fora do prazo (CFP): 7

2º passo: Calcular o TPR e arredondar para o número inteiro mais próximo.
TPR = (CR / CA) x 100
TPR = (93 / 100) x 100 = 93%

3º passo: Calcular o valor da glosa considerando o não atingimento da meta para o item 2, a título de exemplo:
• Valor dos serviços gerenciados de segurança e resposta à incidentes = R$ 500.000,00
• Glosa = R$ 500.000,00 * 5,00%
• Glosa = R$ 25.000,00</td>
</tr>
</table>

Indicador TDM - Tempo de Disponibilidade Mensal

<table>
<tr><td>1</td><td>Descrição/Objetivo do Indicador</td><td>Percentual de tempo, durante o período do mês de operação, em que a plataforma de segurança cibernética venha a permanecer em condições normais de funcionamento.</td></tr>
<tr><td>2</td><td>Meta</td><td>Disponibilidade mínima mensal: ≥99.8%</td></tr>
<tr><td>3</td><td>Periodicidade</td><td>Apuração mensal, sempre considerando o mês de competência da medição dos serviços.</td></tr>
<tr><td>4</td><td>Método de Medição (Fórmula)</td><td>TDM = [(To – Ti) / To] x 100, onde:
TDM = Índice de Tempo de Disponibilidade Mensal do Serviço.
To = Tempo total mensal (total de dias da prestação do serviço vezes 1440 minutos).
Ti = Somatório dos tempos de inoperância durante o período de operação em um mês (em minutos).

O valor final será arredondado para o inteiro mais próximo, conforme metodologia definida pela Resolução nº 886/66 IBGE.</td></tr>
<tr><td>5</td><td>Glosa</td><td>A glosa para o TDM será aplicada sobre o valor mensal total dos serviços prestados pela Contratada referente ao item de licença de uso da plataforma de segurança cibernética, limitada a 10%, caso a meta não seja atingida.

Tabela - Nível de glosa para descumprimento do indicador TDM.
<table>
<tr><th>Demandas executadas dentro do prazo</th><th>Desconto sobre o valor mensal do serviço</th></tr>
<tr><td>≥ 99.8%</td><td>0%</td></tr>
<tr><td>99.7% a 99.2%</td><td>3,00%</td></tr>
<tr><td>99.1% a 98.6%</td><td>5,00%</td></tr>
<tr><td>98.5% a 98.0%</td><td>7,00%</td></tr>
<tr><td>97.9% a 97.5%</td><td>9,00%</td></tr>
<tr><td>≤ 97%</td><td>10,00%</td></tr>
</table>
A glosa deverá ser retratada nos relatórios de prestação dos serviços junto ao faturamento apresentado mensalmente.</td></tr>
<tr><td>6</td><td>Sanção</td><td>As sanções serão aplicadas conforme previsão no Termo de Referência.</td></tr>
</table>

7	**Exemplos**	***Exemplo 01: Não atingir a meta com Glosa*** 1º passo: Obter os dados necessários: • Fatura mensal dos serviços de licença de uso = R$ 500.000,00 • Totalização de tempos de inoperância no mês de referência (em minutos): 240min 2º passo: Calcular o ***TDM*** e arredondar para o número inteiro mais próximo. • **TDM = [(To – Ti)/To] * 100** • **To** = 30dias x 1440min. (24hrs) = 43.200 • **Ti** = 240min. (tempo de inoperância) • **TDM** = ((43.200 – 240) / 43.200) x 100 = 99,4% 3º passo: Calcular o valor da glosa Valor do serviço = R$ 500.000,00 Glosa = R$ 500.000,00 * 3,00% Glosa = R$ 15.000,00

17. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

17.1. A contratação da Solução trará diversos benefícios para a administração pública de Maricá, conforme elencado abaixo:

17.2. Redução de riscos de segurança: Diminuição da exposição a ataques cibernéticos e vulnerabilidades.

17.3. Conformidade com a LGPD: Adequação dos processos de tratamento de dados aos requisitos da lei.

17.4. Melhoria da gestão de vulnerabilidades: Identificação e tratamento mais eficientes de vulnerabilidades.

17.5. Fortalecimento da postura de segurança: Aumento da proteção dos ativos de informação da Prefeitura.

18. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

18.1. A contratação da Solução, embora seja um passo crucial para a modernização da infraestrutura de TIC da administração pública de Maricá, demanda a contratação correlata e interdependente de serviços de infraestrutura de TIC para garantir a sua plena funcionalidade e a integração eficiente dos equipamentos ao ambiente tecnológico da administração pública.

18.2. Serviços de infraestrutura de TIC essenciais para sustentar a execução do contrato de locação:

a. **Conectividade e internet:** É fundamental a contratação de serviços de internet com alta disponibilidade, velocidade e segurança adequados para suportar o acesso aos sistemas da Prefeitura e à internet. A estabilidade e a qualidade da conexão são imprescindíveis para o bom desempenho das atividades administrativas e a prestação de serviços à população.

b. **Suporte técnico especializado:** A complexidade da infraestrutura de TIC exige a contratação de serviços de suporte técnico especializado para auxiliar na configuração, instalação e resolução de problemas relacionados aos equipamentosde TIC e à sua integração com os sistemas existentes. O suporte técnico deve atuar de forma preventiva e corretiva, garantindo a continuidade das operações e a rápida resolução de incidentes.

c. **Gerenciamento de rede:** A contratação de serviços de gerenciamento de rede é crucial para garantir a estabilidade, segurança e o bom desempenho da infraestrutura de TIC. O gerenciamento de rede inclui o monitoramento do tráfego de dados, a configuração de switches e roteadores, a gestão de acessos e a implementação de políticas de segurança.

18.3. A ausência ou a deficiência em qualquer um desses serviços de infraestrutura de TIC poderá comprometer a boa execução dos serviços propostos neste estudo, impactando negativamente a produtividade dos servidores e colaboradores, a qualidade dos serviços prestados à população e a segurança das informações da administração pública municipal.

18.4. Portanto, a prestação desses serviços complementares e interdependentes é imprescindível para o sucesso da implementação da Solução A e a obtenção de todos os benefícios esperados com a pretensa contratação.

19. PROVIDÊNCIAS A SEREM ADOTADAS

19.1. Visando garantir a fluidez e a celeridade do processo de contratação, todas as providências administrativas prévias à celebração do contrato já foram cuidadosamente adotadas, estando a CODEMAR plenamente preparada para a imediata implementação da solução.

19.2. **Fiscalização:** A CODEMAR dispõe de equipes capacitadas para a fiscalização da prestação dos serviços, garantindo o acompanhamento e a qualidade da execução do contrato.

19.3. **Gestão contratual:** A gestão contratual será conduzida pela CODEMAR, que possui equipe estruturada e expertise em gestão de contratos, assegurando o cumprimento de todas as cláusulas e obrigações estabelecidas.

19.4. **Adequação do ambiente:** A memória de cálculo foi elaborada considerando as necessidades específicas da administração pública municipal, em que o ambiente já se encontra plenamente adequado para a execução dos serviços, sem a necessidade de adaptações ou investimentos adicionais.

19.5. Por se tratar de contratação pelo Sistema de Registro de Preços, o cronograma de entrega dos itens deverá seguir a necessidade da administração pública municipal, em que definirão as quantidades a serem solicitadas.

19.6. Dessa forma, a contratação poderá ser efetivada sem a necessidade de providências adicionais, assegurando a pronta disponibilização da solução e a plena continuidade das atividades da administração pública.

20. CONCLUSÃO

20.1. A contratação de serviços de Tecnologia da Informação e Comunicação (TIC) pela CODEMAR é um processo complexo e essencial para a modernização e eficiência das obrigações institucionais da empresa, conforme Decreto nº 049, de 14 de março de 2025. Este estudo técnico preliminar destacou a importância de uma abordagem estratégica e bem planejada para a seleção e gestão desses serviços.

20.2. Os principais pontos abordados incluem a necessidade de transparência e conformidade com as normas legais, a importância de uma análise criteriosa das necessidades específicas da administração pública de Maricá, e a avaliação rigorosa das soluções de mercado identificadas.

20.3. Recomenda-se que a CODEMAR adote um modelo de contratação que priorize a qualidade e a inovação, ao mesmo tempo em que assegure a eficiência dos recursos públicos. A utilização de contratos flexíveis e a realização de monitoramentos periódicos são estratégias que podem contribuir para a melhoria contínua dos serviços de TIC contratados.

20.4. Em suma, a contratação de serviços de TIC deve ser vista como uma oportunidade para a CODEMAR aprimorar seus processos e desenvolver um padrão cada vez maior de excelência na prestação de serviços.

20.5. A adoção de boas práticas e a busca constante por aperfeiçoamento são elementos chave para alcançar esses objetivos, principalmente se aliada às boas

práticas e ao uso adequado da legislação correlata, sobretudo no que se refere aos serviços que envolvam inovação tecnológica.

21. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

21.1. O presente Estudo Técnico Preliminar (ETP) considerou a necessidade de contratação do objeto, os requisitos técnicos, legais, ambientais e os do próprio negócio, o mercado em que o objeto se encontra inserido, bem como todos os demais requisitos necessários para a caracterização e quantificação da demanda identificada, bem como o processo de escolha da solução que melhor se adequa à Administração Pública de Maricá nesta oportunidade. Foram considerados ainda os requisitos ambientais e os aspectos legais.

21.2. Desta forma, entende-se ser **VIÁVEL** a contratação em comento, e visando dar início à implementação do objeto aqui delineado, recomenda-se a elaboração de Termo de Referência com base no presente estudo e o encaminhamento para o setor competente para o prosseguimento do feito.

Maricá, 14 de abril de 2025.

INTEGRANTE REQUISITANTE/ TÉCNICO	**INTEGRANTE ADMINISTRATIVO**
Bruno Magalhães da Silva Assessor Especial I Matrícula nº 757	**Keycyane dos Santos P. Bittencourt** Coordenador Matrícula nº 762

AUTORIDADE DA ÁREA DE TI
GEFERSON MICHEL SANTOS DE SALES Diretor de Tecnologia da Informação e Inovação Matrícula nº 028

APÊNDICE A

PROVA DE CONCEITO (“PROOF OF CONCEPT” – “POC”) - SISTEMA INTEGRADO DE CIBERSEGURANÇA E PLATAFORMA DE COMPLIANCE E ADEQUAÇÃO À LGPD

1. EXIGÊNCIA DA POC

1.1. A realização de uma Prova de Conceito (PoC) será obrigatória para as plataformas relacionadas aos itens 1 e 3.

2. OBJETIVO

2.1. Validar de forma abrangente a eficácia da solução proposta pela licitante para atender aos requisitos técnicos e funcionais especificados no Termo de Referência (TR). A PoC integrará testes automatizados, análises em tempo real e simulações de cenários reais para demonstrar a capacidade da solução em atender às necessidades da administração pública municipal, por meio da CODEMAR, em termos de cibersegurança e conformidade com a LGPD.

2.2. A PoC é crucial para avaliar a complexidade da solução proposta, minimizando riscos financeiros e operacionais antes da implementação completa. Através da PoC serão identificados potenciais problemas de desempenho, dificuldades de integração com sistemas existentes na Contratante e incompatibilidades com sua infraestrutura tecnológica. A PoC também ajusta expectativas entre a equipe técnica da CODEMAR e o fornecedor, promovendo uma compreensão clara das capacidades e limitações da solução.

2.3. A experimentação direta com a tecnologia, por meio da PoC, facilita a tomada de decisão, fornecendo dados concretos sobre a eficácia e adequação da solução ao contexto da administração pública municipal. Isso garante que a escolha final seja informada e alinhada com os objetivos estratégicos da administração pública, por meio da CODEMAR.

3. EXECUÇÃO

3.1. A licitante com a melhor proposta terá até 5 (cinco) dias úteis, contados da data de convocação pelo agente de licitação / pregoeiro, para iniciar a PoC, que deverá ser conduzida em ambiente virtualizado (nuvem) ou em ambiente de teste físico fornecido ou configurado pela licitante (a ser definido em conjunto com a CODEMAR), exclusivamente para este fim, e deverá ser concluída no mesmo dia que iniciada. O cronograma detalhado para a realização da PoC deverá ser

acordado com a CODEMAR antes do início dos testes.

3.2. A entrega da documentação completa deverá ocorrer em até 5 (cinco) dias úteis após a conclusão da PoC, incluindo relatórios detalhados de cada teste realizado e seus respectivos resultados. Será disponibilizada para inspeção pública no site da CODEMAR.

4. ESCOPO DETALHADO

4.1. O escopo da PoC abrangerá os módulos descritos no Termo de Referência, incluindo, mas não se limitando a:

SOLUÇÃO DE GERENCIAMENTO DE VULNERABILIDADES

4.2. Autenticação

4.2.1. A POC deve incluir testes rigorosos de autenticação, incluindo o uso de chave de hardware (USB) para validar a segurança do acesso à plataforma e a conformidade com as melhores práticas de segurança. Deverá ser demonstrado um método de autenticação robusto e seguro.

4.3. Análise de Vulnerabilidades

4.3.1. Varreduras automatizadas abrangendo os IPs, FQDNS e/ou endpoint informados pela CODEMAR no momento da PoC, utilizando técnicas de varredura autenticada e não autenticada. Detecção e classificação de vulnerabilidades com base em CVSS. Geração de relatórios detalhados com as vulnerabilidades identificadas, suas respectivas severidades, e recomendações de correção priorizadas.

4.4. Inteligência de Ameaças (OSINT)

4.4.1. Coleta de informações de inteligência aberta (OSINT) como parte da avaliação de vulnerabilidades, incluindo:

a) Coleta de IPs: Identificação dos IPs associados à infraestrutura isolada da CODEMAR / Prefeitura.

b) Escaneio de Portas: Identificação de portas abertas e serviços em execução.

c) Informações de Whois e DNS: Coleta de dados de registro de domínio e informações de DNS.

d) Páginas Web e Subdomínios: Identificação e análise de páginas web e subdomínios disponibilizados pela CODEMAR / Prefeitura.

4.5. Testes de Segurança (Pentests)

4.5.1. Simulação de ataques em diferentes níveis, utilizando metodologias Black-box, Gray-box e White-box. Os ataques simulados deverão abranger diferentes vetores, incluindo: SQL Injection, Cross-Site Scripting (XSS) e tentativas de força bruta.

4.6. Simulação de Ataques DDoS

4.6.1. Simulação de ataques DDoS em um ambiente de testes isolado, análise do impacto no desempenho e disponibilidade dos sistemas, avaliação da capacidade de resposta da solução.

4.7. Painel de Prevenção de Phishing

4.7.1. Criação e execução de campanhas simuladas de phishing em um grupo de usuários de teste, análise dos relatórios gerados e avaliação da usabilidade da interface.

4.8. Relatórios e Documentação

4.8.1. Geração de relatórios detalhados com resultados de todos os testes, recomendações de melhoria, e documentação técnica completa da solução. Se proposto, demonstração de mecanismos de validação por blockchain para garantir a integridade e autenticidade dos dados.

4.8.2. A solução deverá apresentar, durante a PoC, um painel de controle intuitivo que forneça uma visão clara e imediata dos resultados das análises e recomendações de segurança. Este painel deverá ser facilmente navegável e permitir a visualização eficiente dos dados. Simultaneamente, a solução deverá gerar alertas em tempo real sobre problemas detectados, categorizados por grau de severidade (por exemplo: baixo, médio, alto, crítico). Cada alerta deverá incluir informações detalhadas sobre:

a) Natureza da vulnerabilidade: Descrição precisa do tipo de vulnerabilidade encontrada (ex: SQL Injection, Cross-Site Scripting, etc.).

b) Sistemas afetados: Identificação precisa dos sistemas ou aplicações impactadas pela vulnerabilidade.

c) Possíveis consequências: Descrição detalhada dos potenciais danos decorrentes da exploração da vulnerabilidade (ex: perda de dados, interrupção de serviços, acesso não autorizado, etc.).

d) Recomendações de ação: Sugestões claras e concisas sobre as medidas

corretivas necessárias para mitigar a vulnerabilidade.

PLATAFORMA DE COMPLIANCE E ADEQUAÇÃO À LGPD

4.9. Mapeamento de dados pessoais, gestão de consentimento, atendimento a requisições de titulares, DPIA/RIPD, políticas e procedimentos de privacidade, gestão de terceiros, diagnóstico de maturidade, banner de cookies, geração de relatórios (RIPD, ROPA, LIA, gerenciais), centralização e visão unificada, personalização e identidade visual, diagnósticos avançados e melhoria contínua, relatórios simplificados e inteligência artificial.

4.10. Testes

4.11. Simulação de cenários de atendimento a requisições de titulares, teste da geração de relatórios, avaliação da usabilidade da plataforma para a gestão de dados pessoais, avaliação da funcionalidade de inteligência artificial, teste da funcionalidade de validade jurídica dos documentos digitais.

5. CRITÉRIOS DE AVALIAÇÃO

A avaliação da PoC levará em consideração os seguintes critérios:

5.1. **Eficácia:** Capacidade da solução em detectar e responder a ameaças e vulnerabilidades.

5.2. **Desempenho:** Tempo de resposta do sistema, uso de recursos, escalabilidade.

5.3. **Usabilidade:** Facilidade de uso e navegação na interface do usuário.

5.4. **Integração:** Sucesso da integração com os sistemas existentes da CODEMAR / Prefeitura.

5.5. **Conformidade:** Cumprimento dos requisitos legais e regulatórios, incluindo a LGPD.

5.6. **Completude da Documentação:** Clareza e abrangência da documentação fornecida.