TERMO DE REFERÊNCIA

1. OBJETO

1.1. Contratação de empresa especializada para prestação de serviços gerenciados em governança em segurança e privacidade da informação, segurança cibernética e fornecimento de solução de antimalware de próxima geração com EDR (Endpoint Detection and Response), incluindo resposta a incidentes, monitoramento de ameaças cibernéticas e atendimento ilimitado 24x7x365, conforme descrição e quantitativos no Item 3 deste Termo de Referência.

1.2. O prazo de vigência da contratação é de 12 meses, devendo ser respeitado o exercício financeiro, nos casos de fornecimento contínuo com celebração do respectivo instrumento contratual, como preconiza o artigo 105 da Lei nº 14.133/2021.

2. JUSTIFICATIVA

2.1. Desde que a Lei Geral de Proteção de Dados (LGPD), Lei n. 13.709/2018, alterada pela Lei n. 13.853/2019 - entrou em vigor, organizações de todo o Brasil vem adaptando suas atividades para atuar em conformidade com a nova legislação, que valoriza a importância da privacidade pessoal.

2.2. Ciente da importância de se adequar à LGPD, a CONTRATANTE necessita implantar diversas mudanças organizacionais para estar aderente à Lei Geral de Proteção de Dados (LGPD), Lei n. 13.709/2018.

2.3. Devido a amplitude das mudanças e a expertise necessária para identificação e tratamento dos riscos à privacidade dos dados pessoais, se faz necessário buscar uma consultoria especializada no assunto para direcionar a CONTRATANTE para aderência a Legislação aplicável.

2.4. Privacidade da informação é inexistente sem que sejam aplicados conceitos de segurança da informação para proteção dos dados pessoais, portanto, assim como, as mudanças necessárias neste momento para a aderência à Lei Geral de Proteção de Dados (LGPD), Lei n. 13.709/2018, se faz necessária manter uma governança contínua em segurança e privacidade da Informação que permita que este assunto não seja algo pontual e sim um processo contínuo para garantir a conformidade da CONTRATANTE.

2.5. E, conforme exigência da Legislação e da Autoridade Nacional de Proteção de Dados (ANPD), a CONTRATANTE necessita indicar uma pessoa como Encarregado de Dados para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), além de manter atividades de privacidade de dados em plena operação.

2.6. Boas práticas de governança corporativa e riscos são metas perseguidas por todas as organizações, incluindo a administração pública. Assim, a CONTRATANTE, na busca constante pela excelência na prestação dos serviços e relacionamento transparente com a sociedade, procura aperfeiçoar o gerenciamento de seus objetivos quando se depara com riscos e obstáculos crescentes, especialmente na busca da adequação das operações às leis e regulamentações aplicáveis.

2.7. Os incidentes de segurança da informação ocorridos nos últimos anos no setor público, demonstram a fragilidade dos órgãos e a necessidade de investimentos em controles eficientes.

2.8. É de conhecimento público e notório, inclusive veiculado nos portais de notícias e veículos de imprensa, que o número de ataques cibernéticos aos órgãos públicos aumentou significativamente nos últimos anos. No estado do Espírito Santo não foi diferente. Os municípios de Vitória, Aracruz, o Tribunal Regional do Trabalho da 17ª Região, dentre outros, foram alvos de ataques cibernéticos que, inclusive, paralisaram a prestação dos serviços até que o ambiente tecnológico pudesse ser restabelecido.

2.9. A CONTRATANTE não dispõe de recursos suficientes para garantir toda a segurança do ambiente tecnológico, fragilizando, dessa forma, a garantia da

confidencialidade, integridade, disponibilidade e privacidade das informações produzidas e armazenadas, o que fragiliza não só este setor em executar suas funções, mas sobretudo a alta gestão.

2.10. A segurança da informação pode ser caracterizada pela aplicação adequada de controles sobre um conjunto de informações ou um ativo de informação com o objetivo de proteger e preservar o valor que este possui para as organizações. Entende-se por informação todo e qualquer conhecimento inscrito, gravado ou codificado em um meio de armazenamento.

2.11. Boas práticas de governança corporativa e riscos são metas perseguidas por todas as organizações, incluindo a administração pública. Assim, a CONTRATANTE, na busca constante pela excelência na prestação dos serviços e relacionamento transparente com a sociedade, procura aperfeiçoar o gerenciamento de seus objetivos quando se depara com riscos e obstáculos crescentes, especialmente na busca da adequação das operações às leis e regulamentações aplicáveis.

2.12. A CONTRATANTE tem buscado constantemente a evolução de seus controles de segurança em seu ambiente de TI e na conscientização de seus colaboradores, aprimorando a governança e suas operações. No entanto, observando o surgimento significativo de novas ameaças cibernéticas e a baixa maturidade em boas práticas de segurança da informação nos órgãos públicos, somando-se, a grande quantidade de vulnerabilidades e a falta da segurança nos controles de acessos em ativos de TI, facilitam ainda mais a execução e a propagação destas ameaças. Com isto, a CONTRATANTE necessita aprimorar seus métodos de monitoramento, identificação e tratamento contínuo dos seus riscos.

2.13. Nos dias atuais, os mecanismos de proteção tradicionais de endpoints demonstram-se ineficientes para o cenário atual e obscuro dos crimes cibernéticos sofisticados, tornando-se imprescindível a adoção de tecnologias de prevenção contra malwares (vírus) utilizando inteligência artificial, auto aprendizagem de máquina e formas de detecção e resposta a incidentes através da análise comportamental sobre técnicas de ataques utilizadas (NGAV – Next Generation Antivírus e EDR – Endpoint Detection and Response).

2.14. Sobre os serviços gerenciados (Managed Security Services – MSS), justifica-se para manter tais mecanismos em conformidade com as melhores práticas que, considerando a expertise do fornecedor contratado, deverá garantir a operação, o monitoramento contínuo e resposta a incidentes de segurança de forma adequada.

2.15. Já a contratação de serviços continuados de governança em segurança e privacidade da informação, justifica-se, pois, a CONTRATANTE precisa aplicar sólidos princípios de gestão para identificação, avaliação e tratamento adequado de seus riscos atuais e emergentes em segurança da informação e na proteção de dados pessoais.

2.16. Por fim, o acréscimo a força de trabalho à equipe de Tecnologia e Segurança da Informação e de Encarregado de Dados (DPO – Data Protection Officer) da CONTRATANTE se dará através dos serviços gerenciados.

2.17. Diante destas informações, justifica-se a contratação do presente objeto.

3. RESULTADOS A SEREM ALCANÇADOS

3.1. Conformidade legal.

3.2. Transparência e responsabilidade.

3.3. Aumento da maturidade perante a segurança e privacidade da informação

3.4. Garantia que os riscos em segurança da informação estejam em níveis aceitáveis.

3.5. Proteção dos ativos de TI da CONTRATANTE contra ameaças e ataques cibernéticos conhecidos e desconhecidos.

4. QUANTIDADE E ESPECIFICAÇÕES GERAIS

4.1. A Tabela abaixo apresenta a descrição e a quantidade estimada sobre cada item que deve ser atendido pela CONTRATADA.

ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE
1	Prestação de serviço contínuo de Governança em Segurança e Privacidade da Informação, incluindo avaliação de maturidade corporativa, gestão de riscos, adequação à LGPD, Encarregado de Dados como serviço, adaptação de processos de negócio, conscientização de colaboradores, desenvolvimento e adequação contínua de políticas, normas, procedimentos e validação de controles em segurança e privacidade da informação com atendimento remoto ilimitado 8x5, pelo período de 12 meses.	Serviço Mensal	12
2	Contratação de empresa especializada no fornecimento de subscrição para solução de Antivírus de Próxima Geração (NGAV), incluindo detecção e resposta a ameaças cibernéticas (EDR), com garantia de atualização por 12 meses.	Subscrição Anual	200
3	Prestação de Serviços Gerenciados de Segurança Cibernética em Endpoints incluindo administração, resposta a incidentes, gerenciamento remoto de plataforma de NGAV+EDR e atendimento 24x7x365 ilimitado pelo período de 12 meses.	Serviço Mensal	12

4.2. A CONTRATANTE irá fornecer a infraestrutura necessária para a CONTRATADA exercer suas atividades.

5. NATUREZA DOS SERVIÇOS

5.1. Os serviços enquadram-se na classificação de serviços comuns e possuem natureza continuada haja vista que os serviços a serem prestados serão executados de forma contínua, não sendo possível o fracionamento da despesa.

6. DETALHAMENTO TÉCNICO

6.1. ITEM 1 – Serviço contínuo de Governança em Segurança e Privacidade da Informação

6.1.1. O serviço tem como principal objetivo identificar, monitorar e tratar os riscos que impactam a confidencialidade, integridade e disponibilidade das informações da CONTRATANTE, garantindo o cumprimento da missão perante a administração pública e a sociedade.

6.1.2. A CONTRATADA deverá executar os Serviços de Governança em Segurança e Privacidade da Informação e de Encarregado de Dados de forma contínua, no formato de atendimento remoto ilimitado 8x5 (oito horas por dia, cinco dias por semana), exceto feriados (nacionais, do estado de Espírito Santo ou do município de Vila Velha), durante toda a vigência do contrato.

6.1.3. A CONTRATADA deverá suportar todos os processos, assim como garantir a conformidade perante a legislação e regulamentação vigente aplicável a CONTRATANTE.

6.1.4. A CONTRATADA deverá suportar os processos que envolvem a privacidade de dados pessoais, visando a proposição de melhorias para a completa aderência aos princípios da Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018).

6.1.5. A CONTRATADA deverá executar as seguintes atividades:

6.1.5.1. Serviços de adequação, análise crítica e atualização contínua de conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei Nº 13.709/2018).

6.1.5.2. Serviços Contínuos de Governança, Gestão de Riscos e Conformidade em Segurança e Privacidade da informação.

6.1.5.3. Serviços Contínuos de Encarregado de Dados.

6.1.6. Sobre os Serviços de adequação, análise crítica e atualização contínua de conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei Nº 13.709/2018):

6.1.6.1. O serviço tem como objetivo adequar e manter a conformidade da CONTRATANTE perante a Lei Geral de Proteção de Dados Pessoais (Lei Nº 13.709/2018).

6.1.6.2. O serviço deverá ser executado considerando as seguintes etapas:

6.1.6.2.1. Etapa 1 – Diagnóstico

6.1.6.2.2. Etapa 2 – Adequação

6.1.6.2.3. Etapa 3 – Gestão contínua

6.1.6.3. As etapas do serviço proposto estão detalhadas nos itens abaixo:

6.1.6.3.1. Etapa 1 – Diagnóstico:

6.1.6.3.1.1. A CONTRATADA deverá realizar a revisão de contratos e políticas corporativas existentes da CONTRATANTE sob o viés da Lei Geral de Proteção de Dados Pessoais e melhores práticas de segurança da informação.

6.1.6.3.1.2. A CONTRATADA deverá realizar o mapeamento de todos os processos da CONTRATANTE que tratam dados pessoais e/ou dados pessoais sensíveis. O mapeamento deverá incluir, pelo menos, os seguintes levantamentos:

6.1.6.3.1.2.1. Levantamento dos processos de negócio que envolvem dados pessoais e o ciclo de vida das informações.

6.1.6.3.1.2.2. Levantamento dos sistemas de informação que tratam dados pessoais, com a identificação dos fornecedores relevantes, dos dados pessoais tratados, das operações de tratamento de dados pessoais com eles realizadas e da infraestrutura tecnológica que as suporta, além dos ciclos de vida associados aos dados pessoais tratados.

6.1.6.3.1.2.3. Levantamento dos controladores, operadores e partes interessadas com quem a CONTRATANTE interage e das relações mantidas com eles.

6.1.6.3.1.3. A CONTRATADA deverá realizar o desenvolvimento do Relatório de Impacto a Proteção de Dados (RIPD) a ser adotado pela CONTRATANTE, de acordo com os seguintes requisitos:

6.1.6.3.1.3.1. A coleta de informações deverá ser realizada através de execução de entrevistas, no formato presencial e/ou remoto, com todas as áreas organizacionais da CONTRATANTE.

6.1.6.3.1.3.2. O Relatório de Impacto a Proteção de Dados (RIPD) deverá possuir, pelo menos, os seguintes itens:

I) Todos os processos de negócio da CONTRATANTE que envolvem operações de tratamento de dados pessoais.

II) Todas as finalidades da execução de cada processo que envolve operações de tratamento de dados pessoais.

III) Todas as descrições para cada etapa do ciclo de vida de cada tratamento de dado pessoal identificado, incluindo: Coleta, Processamento, Análise, Compartilhamento, Armazenamento, Reutilização e Eliminação.

IV) Todas as bases legais aplicáveis que justificam ou justificariam cada operação de tratamento de dados pessoais.

6.1.6.3.1.4. A CONTRATADA deverá realizar o estudo organizacional e tecnológico sobre a segurança da informação para a conformidade com a privacidade e legalidade, conforme especificado abaixo:

6.1.6.3.1.4.1. A CONTRATANTE disponibilizará o inventário de ativos de TI para a CONTRATADA.

6.1.6.3.1.4.2. A CONTRATADA, deverá realizar o estudo e coletar informações adicionais sobre cada ativo, identificando o grau de importância sobre cada ativo para a CONTRATANTE.

6.1.6.3.1.4.3. A CONTRATADA deverá identificar ocorrências sobre incidentes de segurança passados sobre cada ativo.

6.1.6.3.1.4.4. A CONTRATADA deverá avaliar a existência ou não de controles de segurança da informação, segurança cibernética e de privacidade, considerando:

I) Controles estabelecidos pela ABNT ISO/IEC 27001:2022.

II) Controles estabelecidos pela ABNT ISO/IEC 27701:2019.

III) Controles estabelecidos sobre técnicas de ataques cibernéticos definidos pelo MITRE - Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK).

6.1.6.3.1.4.5. A CONTRATADA deverá inspecionar os endpoints da CONTRATANTE para identificar a presença de ameaças cibernéticas (malwares) conhecidas e desconhecidas.

I) A inspeção deverá ser realizada exclusivamente em arquivos presentes em cada endpoint da CONTRATANTE, incluindo arquivos binários, bibliotecas, documentos de textos, scripts, processos em execução, entre outros.

II) A inspeção não deverá bloquear ou tomar nenhuma ação contra as ameaças descobertas e sim apenas identificá-las.

III) A análise de ameaças cibernéticas em endpoints deverá ser realizada através de solução que permita a inspeção através de agentes.

IV) A CONTRATANTE disponibilizará a sua equipe de TI para implementar os agentes da solução utilizada em seus endpoints.

V) A CONTRATADA é a responsável pelo licenciamento das soluções e ferramentas utilizadas para a prestação de serviços, não gerando nenhum ônus adicional para a CONTRATANTE.

VI) Entenda-se como Endpoint, servidores de rede de computadores (físicos e virtuais), estações de trabalho (desktops) e notebooks com sistemas operacionais Windows, Linux e MacOS.

VII) A CONTRATADA deverá gerar um Relatório Executivo sobre as ameaças identificadas.

6.1.6.3.1.5. A CONTRATADA deverá realizar a revisão de políticas, normas e procedimentos atuais de segurança da informação, de tecnologia da informação e segurança cibernética da CONTRATANTE com base nas Normas Técnicas ISO/IEC 27001 e ISO/IEC 27701, mesmo que informais.

6.1.6.3.1.6. A CONTRATADA deverá realizar a Análise de Maturidade perante a Segurança e Privacidade da Informação, conforme especificado abaixo:

6.1.6.3.1.6.1. A CONTRATADA deverá realizar a análise de maturidade em segurança e privacidade da informação na CONTRATANTE.

6.1.6.3.1.6.2. A CONTRATADA deverá desenvolver e aplicar um questionário específico, com no máximo 35 (trinta e cinco) perguntas de simples entendimento, para coletar informações relacionadas a aderência em segurança e privacidade da organização.

6.1.6.3.1.6.3. O tempo médio de resposta de cada colaborador da CONTRATANTE não deverá ultrapassar o tempo de 15 (quinze) minutos.

6.1.6.3.1.6.4. O formado de aplicação do questionário de maturidade deverá ser on-line (via internet) e deverá ser disponibilizado para todos os colaboradores da CONTRATANTE.

6.1.6.3.1.6.5. A CONTRATADA disponibilizará o link do questionário web para a CONTRATANTE.

6.1.6.3.1.6.6. A CONTRATANTE será a responsável por enviar o link do questionário web para os seus colaboradores.

6.1.6.3.1.6.7. Cada colaborador deverá preencher uma única vez o questionário.

6.1.6.3.1.6.8. A CONTRATADA é a responsável pelo licenciamento das soluções e ferramentas utilizadas para a prestação de serviços, não gerando nenhum ônus adicional para a CONTRATANTE.

6.1.6.3.1.6.9. O período de disponibilidade do questionário será previamente combinado e agendado com a CONTRATADA.

6.1.6.3.1.6.10. As questões deverão ser objetivas de múltipla escolha e com respostas simples, considerando:

I) Sim – quando o colaborador entende que há um determinado controle específico de segurança da informação implementado pela CONTRATANTE.

II) Não – quando o colaborador entende que não há um determinado controle específico de segurança da informação implementado pela CONTRATANTE.

III) Não Sei – quando o colaborador não tem certeza de que há um determinado controle específico de segurança da informação implementado pela CONTRATANTE.

6.1.6.3.1.6.11. A CONTRATADA deverá elaborar as perguntas com base nos controles das seguintes normas técnicas:

I) ABNT NBR ISO/IEC 27001:2022.

II) ABNT NBR ISO/IEC 27701:2019.

6.1.6.3.1.6.12. Antes de ser inserido os questionamentos na plataforma de coleta das respostas, a CONTRATADA deverá disponibilizar o questionário para a CONTRATANTE.

6.1.6.3.1.6.13. A CONTRATANTE analisará ou não o questionário a ser aplicado.

6.1.6.3.1.6.14. Após o término do período de coleta de respostas, a CONTRATANTE deverá desativar a coleta de novas respostas e compilar as informações recebidas (respostas dos colaboradores), gerando o relatório de aderência.

6.1.6.3.1.6.15. A CONTRATADA deverá utilizar o método de pesquisa qualitativa para a análise de aderência.

6.1.6.3.1.6.16. A CONTRATADA deverá utilizar o modelo CMMI (Capability Maturity Model Integration), com base no COBIT 5 (Control Objectives for Information and Related Technologies version 5), considerando os seguintes níveis:

I) Inicial.

II) Repetitivo.

III) Definido.

IV) Gerenciado.

V) Otimizado.

6.1.6.3.1.6.17. A CONTRATADA deverá desenvolver e entregar o relatório contendo no mínimo as seguintes informações:

I) Informações do questionário aplicado.

II) Modelo e metodologia aplicadas.

III) Informações de resultados compilados:

a. Total de colaboradores convidados a participar.

b. Total de colaboradores que responderam ao questionário.

c. Total de colaboradores que não responderam ao questionário.

IV) Nível de classificação da CONTRATANTE, contendo:

a. Percentual de "em conformidade".

b. Percentual de "não conformidade".

c. Pontuação global e classificação do nível de maturidade.

d. Recomendações.

6.1.6.3.1.7. A CONTRATADA deverá realizar Análise de Vulnerabilidades técnicas nos ativos de TI da CONTRATANTE com o objetivo de identificar fragilidades que possam impactar a conformidade com a legislação.

6.1.6.3.1.7.1. A análise de vulnerabilidades técnicas deverá ser realizada em ativos de infraestrutura de TI e em aplicações web de forma automatizada.

6.1.6.3.1.7.2. A análise de vulnerabilidades em aplicações web deve ser realizada em tempo de execução, ou seja, deve ser realizada uma análise DAST (Dynamic Application Security Testing) nas aplicações web da CONTRATANTE.

6.1.6.3.1.7.3. A CONTRATADA deverá avaliar no mínimo os padrões de segurança do OWASP Top 10 para as varreduras de aplicações web.

6.1.6.3.1.7.4. As soluções a serem utilizadas pela CONTRATADA para a prestação dos serviços deverão ser referência de mercado. Não serão aceitos relatórios técnicos emitidos por soluções de código aberto (open source).

6.1.6.3.1.7.5. A CONTRATADA é a responsável pelo licenciamento das soluções e ferramentas utilizadas para a prestação de serviços, não gerando nenhum ônus adicional para a CONTRATANTE.

6.1.6.3.1.7.6. Todas as varreduras de vulnerabilidades deverão ser agendadas e programadas juntamente com a CONTRATANTE antes de serem realizadas.

6.1.6.3.1.7.7. As varreduras em ativos de infraestrutura de TI e de aplicações WEB, devem ser realizadas, quando possível, de forma autenticada, com objetivo de identificar vulnerabilidades conhecidas e desconhecidas no ambiente da CONTRATANTE.

6.1.6.3.1.7.8. Para cada vulnerabilidade identificada, a CONTRATADA deverá apresentar evidências da vulnerabilidade através de saídas da verificação realizada pelas plataformas utilizadas (outputs).

6.1.6.3.1.7.9. Cada vulnerabilidade identificada deve possuir a sua classificação de severidades de acordo com o padrão Sistema Comum de Pontuação de Vulnerabilidade versão 3 (CSVSS v3).

6.1.6.3.1.7.10. Para cada vulnerabilidade identificada, a CONTRATADA deve também fornecer informações detalhadas sobre a natureza da vulnerabilidade, evidências da existência da vulnerabilidade e recomendações para mitigá-la.

6.1.6.3.1.7.11. A CONTRATADA deverá analisar criticamente cada vulnerabilidade identificada, tratando possíveis falsos-positivos.

6.1.6.3.1.7.12. A CONTRATADA deve fornecer um plano de ação contendo as principais recomendações de correção das vulnerabilidades descobertas, com foco na redução da exposição cibernética da CONTRATANTE.

6.1.6.3.1.7.13. A CONTRATADA deverá emitir relatórios técnicos contendo todos os resultados das análises de vulnerabilidades realizadas.

6.1.6.3.1.7.14. O resultado das Análises de Vulnerabilidades deve ser utilizado como insumo pela CONTRATADA para a realização da

análise de riscos de segurança e privacidade da informação da CONTRATANTE.

6.1.6.3.1.8. A CONTRATADA deverá realizar Análise de Riscos em Segurança e Privacidade da Informação, conforme especificado abaixo:

6.1.6.3.1.8.1. A CONTRATADA, através das informações coletadas nas atividades anteriores, deverá realizar a análise de riscos sobre a segurança e a privacidade das informações.

6.1.6.3.1.8.2. Para a definição dos critérios de avaliação de riscos, a CONTRATADA deverá considerar a existência de vulnerabilidades e ameaças e a probabilidade, impacto e consequência caso um determinado incidente venha a ocorrer nos ativos da CONTRATANTE.

6.1.6.3.1.8.3. A CONTRATADA deverá considerar o resultado das seguintes questões identificadas na análise de riscos.

I) Ausência ou má configuração de controles definidos pela ABNT ISO/IEC 27001:2022.

II) Ausência ou má configuração de controles definidos pela ABNT ISO/IEC 27701:2019.

III) Não conformidade com a Lei nº. 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

6.1.6.3.1.8.4. A CONTRATADA deverá considerar a seguinte rotulação para cada risco identificado conforme o seu critério:

RISCO		PROBABILIDADE		
		Alta	Média	Baixa
IMPACTO	Alta	Risco Alto	Risco Médio	Risco Baixo
	Média	Risco Médio	Risco Médio	Risco Baixo
	Baixa	Risco Baixo	Risco Baixo	Risco Baixo

6.1.6.3.1.8.5. A CONTRATADA deverá definir juntamente com a CONTRATANTE os critérios para a aceitação dos riscos.

6.1.6.3.1.8.6. A CONTRATADA deverá utilizar pelo menos uma das seguintes metodologias de análise de riscos:

I) ABNT NBR ISO/IEC 27005:2019.

II) ABNT NBR ISO 31000:2018.

6.1.6.3.1.8.7. A CONTRATADA deverá desenvolver os seguintes entregáveis:

I) Relatório da Análise de Riscos.

II) Relatório em formato de planilha, apresentando todos os riscos identificados e seus respectivos controles para remediação.

III) Relatório de Declaração de Aplicabilidade sobre os controles da ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27701:2019.

6.1.6.3.1.9. A CONTRATADA deverá desenvolver um Plano de Ação de atividades necessárias para a adequação da CONTRATANTE, considerando:

6.1.6.3.1.9.1. A CONTRATADA deverá realizar o planejamento de ações necessárias para a adequação da CONTRATANTE.

6.1.6.3.1.9.2. A CONTRATADA deverá desenvolver o Plano de Ação considerando o resultado da análise de riscos em Segurança e Privacidade da Informação.

6.1.6.3.1.9.3. A CONTRATADA deverá classificar as ações de acordo com os seguintes níveis de priorização:

I) Curto Prazo – Prazo de até 1 (um) ano para aderência da recomendação.

II) Médio Prazo – Prazo entre 1 (um) e 3 (três) anos para aderência da recomendação.

III) Longo Prazo – Prazo entre 3 (três) e 5 (cinco) anos para aderência da recomendação.

6.1.6.3.1.9.4. A CONTRATADA deverá identificar o responsável por cada atividade definida no plano de ação.

6.1.6.3.1.9.5. A CONTRATADA deverá realizar a apresentação do plano de ação de forma PRESENCIAL na sede da CONTRATANTE, localizada na R. Antônio Ataíde, 686 - Centro Vila Velha / ES, ou de forma REMOTA a critério da CONTRATANTE.

6.1.6.3.1.10. Na etapa 1 a CONTRATADA deverá disponibilizar para a CONTRATANTE os seguintes entregáveis:

6.1.6.3.1.10.1. Relatório de apontamentos da revisão de contratos e políticas analisadas.

6.1.6.3.1.10.2. Relatório de Impacto a Proteção de Dados (RIPD/DPIA).

6.1.6.3.1.10.3. Relatório da Avaliação de Maturidade em Segurança e Privacidade da Informação.

6.1.6.3.1.10.4. Relatório da Análise de Risco em Segurança e Privacidade da Informação.

6.1.6.3.1.10.5. Plano de Ação sobre os riscos identificados e adequações necessárias.

6.1.6.3.1.11. A CONTRATADA deverá realizar a apresentação dos resultados da Etapa 1 de forma PRESENCIAL na sede da CONTRATANTE, localizada na R. Antônio Ataíde, 686 - Centro Vila Velha / ES, ou de forma REMOTA a critério da CONTRATANTE.

6.1.6.3.2. Etapa 2 – Adequação:

6.1.6.3.2.1. A CONTRATADA deverá adequar a CONTRATANTE conforme as recomendações definidas na Etapa 1, considerando:

6.1.6.3.2.1.1. Adequação Jurídica:

I) A CONTRATADA deverá desenvolver e/ou adequar cláusulas de privacidade em contratos da CONTRATANTE com base na Lei Geral de Proteção de Dados.

II) A CONTRATADA deverá desenvolver e/ou adequar minutas de contratos da CONTRATANTE com base na Lei Geral de Proteção de Dados.

III) A CONTRATADA deverá desenvolver e/ou adequar termos e códigos internos da CONTRATANTE com base na Lei Geral de Proteção de Dados.

IV) A CONTRATADA deverá desenvolver e/ou adequar demais documentos jurídicos da CONTRATANTE com base na Lei Geral de Proteção de Dados.

6.1.6.3.2.1.2. Adequação de Processos:

I) A CONTRATADA deverá orientar e apoiar a CONTRATANTE na adequação de todos seus processos que necessitem de ajustes para a conformidade com a Lei Geral de Proteção de Dados.

6.1.6.3.2.1.3. Adequação da Segurança e Privacidade da Informação:

I) A CONTRATADA deverá desenvolver / atualizar o Manual do Encarregado de Dados (DPO).

II) A CONTRATADA deverá desenvolver / atualizar o Manual da Gestão de Consentimentos.

III) A CONTRATADA deverá desenvolver / atualizar o Manual para garantir o exercício dos direitos dos titulares de dados.

IV) A CONTRATADA deverá desenvolver / atualizar o Manual organizacional com as regras para as operações de tratamento de dados pessoais sensíveis.

V) A CONTRATADA deverá desenvolver / atualizar o Manual de avaliação de risco de privacidade (Privacy Risk Assessment) de terceiros.

VI) A CONTRATADA deverá desenvolver / atualizar o Manual de Comunicação com a Autoridade Nacional de Proteção de Dados (ANPD).

VII) A CONTRATADA deverá desenvolver / atualizar o Manual de Comunicação com o titular de dados pessoais.

VIII) A CONTRATADA deverá desenvolver / atualizar os seguintes documentos, mas não limitando-se a:

a. Política de Segurança da Informação.
b. Política de Privacidade.
c. Política de Cookies.
d. Norma e Procedimentos de Classificação da Informação.
e. Norma e Procedimentos de Retenção e Descarte de Informações.
f. Norma e Procedimentos de Gestão de Incidentes.
g. Norma e Procedimentos de Mesa e Tela Limpa.
h. Norma e Procedimentos de Uso de Recursos de TI.
i. Norma e Procedimentos de Uso de Dispositivos Móveis e Trabalho Remoto.
j. Norma e Procedimentos de Cópia de Segurança.
k. Norma e Procedimentos de Controle de Acesso.
l. Norma e Procedimentos de Gestão de Riscos.
m. Norma e Procedimentos de Segurança na Cadeia de Suprimentos.

IX) A CONTRATADA deverá desenvolver um plano de ação de atividades para adequação das Políticas e Normas de Segurança e Privacidade da Informação desenvolvidas / atualizadas.

X) A CONTRATADA deverá prestar suporte na implementação de todas as Políticas, Normas e Procedimentos de Segurança e Privacidade da Informação desenvolvidas / atualizadas.

XI) A CONTRATADA deverá desenvolver / atualizar o Manual do Comitê Gestor de Segurança e Privacidade da Informação da CONTRATANTE.

XII) A CONTRATADA deverá desenvolver / atualizar o Plano de Conscientização contínuo sobre Segurança e Privacidade da Informação.

XIII) A CONTRATADA deverá desenvolver / atualizar a Cartilha de Segurança e Privacidade da Informação abordando todos os assuntos de suas Políticas e Normas de Segurança e Privacidade implementadas.

XIV) A CONTRATADA deverá apoiar a CONTRATANTE em todas as atividades presentes no Plano de Ação desenvolvido na Etapa 1.

6.1.6.3.2.2. Na etapa 2 a CONTRATADA deverá disponibilizar para a CONTRATANTE os seguintes entregáveis:

6.1.6.3.2.2.1. Minutas de contratos, aditivos, termos e demais documentos jurídicos ajustados.

6.1.6.3.2.2.2. Plano de Governança Corporativa em Segurança e Privacidade da Informação, contendo:

I) Manual do Encarregado de Dados (DPO).

II) Manual da Gestão de Consentimentos.

III) Manual para garantir o exercício dos direitos dos titulares de dados.

IV) Manual organizacional com as regras para as operações de tratamento de dados pessoais sensíveis.

V) Manual de avaliação de risco de privacidade (Privacy Risk Assessment) de terceiros.

VI) Manual de Comunicação com a Autoridade Nacional de Proteção de Dados (ANPD).

VII) Manual de Comunicação com o titular de dados pessoais.

6.1.6.3.2.2.3. Políticas, Normas e Procedimentos de Segurança e Privacidade da Informação.

6.1.6.3.2.2.4. Cartilha de Segurança e Privacidade da Informação.

6.1.6.3.2.2.5. Manual do Comitê Gestor de Segurança e Privacidade da Informação.

6.1.6.3.2.2.6. Plano de Ação sobre controles técnicos para atender as diretrizes estabelecidas nas Políticas, Normas e Procedimentos de Segurança e Privacidade da Informação desenvolvidas/adequadas.

6.1.6.3.2.2.7. O Plano de Ação deverá ser desenvolvido somente após a aprovação da CONTRATANTE sobre as diretrizes estabelecidas nas Políticas e Normas de Segurança e Privacidade da Informação. A CONTRATADA deverá realizar os ajustes necessários solicitados pela CONTRATANTE, até o momento em que todas as documentações sejam completamente aprovadas.

6.1.6.3.2.3. A CONTRATADA deverá realizar a apresentação dos entregáveis da Etapa 2 de forma PRESENCIAL na sede da CONTRATANTE, localizada na R. Antônio Ataíde, 686 - Centro Vila Velha / ES, ou de forma REMOTA a critério da CONTRATANTE.

6.1.6.3.3. Etapa 3 – Gestão Contínua:

6.1.6.3.3.1. Após a aprovação de cada documentação criada ou atualizada, segue-se o processo de gestão contínua, onde a CONTRATADA deverá manter capacitados todos os servidores e terceiros envolvidos nos processos de trabalho de acordo com as adequações necessárias.

6.1.6.3.3.2. O processo de gestão contínua é sustentado pelos serviços de Governança, Gestão de Riscos e Conformidade em Segurança e Privacidade da Informação e pelo serviço de encarregado de dados.

6.1.7. Sobre os Serviços Contínuos de Governança, Gestão de Riscos e Conformidade em Segurança e Privacidade da informação.

6.1.7.1. O serviço deverá garantir, durante toda a vigência do contrato, que todos os riscos relacionados à segurança e privacidade da informação sejam mapeados e gerenciados.

6.1.7.2. A CONTRATADA deverá manter atualizado o inventário de ativos de informação. A CONTRATANTE define ativos de informação como qualquer meio de armazenamento, processamento e transporte de informações bem como os locais onde se

encontram esses meios e as pessoas que a eles têm acesso. Ex. ativos de TI, recursos humanos, documentos, entre outros.

6.1.7.3. A CONTRATADA deverá identificar continuamente ameaças e vulnerabilidades nos ativos de informação.

6.1.7.4. A CONTRATADA deverá analisar o impacto, probabilidade e consequência das ameaças e vulnerabilidades identificadas nos ativos de informação, identificando ou não um risco a Segurança da Informação da CONTRATANTE.

6.1.7.5. A CONTRATADA deverá avaliar quantitativamente a criticidade do risco, considerando os seguintes níveis de risco:

6.1.7.5.1. Risco Alto: Quando a consequência do risco possibilitar a paralização total das operações da CONTRATANTE.

6.1.7.5.2. Risco Médio: Quando a consequência do risco possibilitar a paralização parcial das operações da CONTRATANTE.

6.1.7.5.3. Risco Baixo: Quando a consequência do risco não impacta significativamente as operações da CONTRATANTE.

6.1.7.6. A CONTRATADA deverá definir os controles aplicáveis para o tratamento dos riscos identificados e apresentar, sempre que for necessário, a CONTRATANTE.

6.1.7.7. A CONTRATADA deverá manter atualizado um documento de declaração de aplicabilidade perante as normas técnicas NBR ISO/IEC 27001 e NBR ISO/IEC 27701, sobre os controles aplicáveis para o tratamento dos riscos.

6.1.7.8. A CONTRATADA deverá definir, em comum acordo com a CONTRATANTE, os critérios para aceitação dos riscos a serem identificados e gerenciados durante a prestação dos serviços.

6.1.7.9. A CONTRATADA deverá gerenciar continuamente a mitigação do risco através da priorização, avaliação e implementação dos controles necessários para remediação, assim como identificar e avaliar os riscos residuais.

6.1.7.10. A CONTRATADA deverá desenvolver e manter atualizado um Manual de Gestão dos Riscos em segurança e privacidade da informação da CONTRATANTE, contendo no mínimo:

6.1.7.10.1. Metodologias, frameworks e métodos definidos para identificar, analisar e avaliar os riscos.

6.1.7.10.2. Critérios definidos para aceitar, transferir, evitar e mitigar os riscos (Plano de Tratamento de Risco).

6.1.7.11. A CONTRATADA deverá garantir que as políticas, normas, processos, procedimentos e demais documentos de Segurança e Privacidade da Informação sejam criados, ajustados, implementados e mantidos para garantir o tratamento dos riscos gerenciados através das seguintes atividades:

6.1.7.11.1. A CONTRATADA deverá definir diretrizes conforme os controles estabelecidos na declaração de aplicabilidade perante as normas técnicas NBR ISO/IEC 27001 e NBR ISO/IEC 27701.

6.1.7.11.2. A CONTRATADA deverá definir e apoiar na implementação e atualização de controles técnicos para cumprir as diretrizes estabelecidas. Exemplos: tecnologias como de backup, firewalls, classificação de dados, DLP, antimalwares, controle de acesso, etc.

6.1.7.11.3. A CONTRATADA deverá definir e implementar controles administrativos para cumprir as diretrizes estabelecidas. Exemplos: ajustes administrativos, modificações de processo de trabalho, capacitações, contratos, etc.

6.1.7.12. A CONTRATADA deverá garantir que os controles para o tratamento dos riscos gerenciados estejam em conformidade com as diretrizes estabelecidas e suportadas pela Política de Segurança da Informação através das seguintes atividades:

6.1.7.12.1. A CONTRATADA deverá realizar auditoria interna sobre os controles de segurança e privacidade da informação.

6.1.7.12.2. A CONTRATADA deverá coordenar a execução de testes de segurança da informação conduzidas internamente e externamente.

6.1.7.12.3. A CONTRATADA deverá validar os controles técnicos relacionados à proteção de dados pessoais.

6.1.7.13. A CONTRATADA deverá garantir que a CONTRATANTE esteja apta a identificar, tratar e responder proativamente e com agilidade a incidentes de segurança e privacidade da informação.

6.1.7.14. A CONTRATADA deverá elaborar, atualizar, gerenciar e testar continuamente um Plano de Resposta a Incidentes, contemplando a Gestão de Incidentes de Segurança e Privacidade da Informação da CONTRATANTE através das seguintes atividades:

6.1.7.14.1. A CONTRATADA deverá definir processo de identificação e notificação de incidentes.

6.1.7.14.2. A CONTRATADA deverá definir o processo de resposta a incidentes em conformidade com o framework NIST 800-61.

6.1.7.14.3. A CONTRATADA deverá definir processo exclusivo para o tratamento e resposta a incidentes que envolvam de dados pessoais e dados pessoais sensíveis.

6.1.7.14.4. A CONTRATADA deverá mapear os ativos de informação críticos.

6.1.7.14.5. A CONTRATADA deverá definir os tipos de incidentes.

6.1.7.14.6. A CONTRATADA deverá classificar os incidentes.

6.1.7.14.7. A CONTRATADA deverá elaborar o plano de comunicação de incidentes.

6.1.7.14.8. A CONTRATADA deverá elaborar o plano de comunicação exclusivo a incidentes que envolvam dados pessoais e dados pessoais sensíveis.

6.1.7.14.9. A CONTRATADA deverá criar, manter e testar os procedimentos de resposta a incidentes (Playbooks).

6.1.7.14.10. A CONTRATADA deverá definir e capacitar a equipe de resposta a incidentes.

6.1.7.14.11. A CONTRATADA deverá estruturar o ponto único de contato para registro e acompanhamento de incidentes.

6.1.7.14.12. A CONTRATADA deverá definir, implementar e capacitar colaboradores sobre a estrutura de notificação, identificação e resposta a incidentes.

6.1.7.15. A CONTRATADA deverá garantir que as atividades do encarregado pelo tratamento de dados pessoais (DPO – Data Protection Officer) sejam apoiadas pela equipe de Governança em Segurança e Privacidade da Informação através das seguintes atividades:

6.1.7.15.1. A CONTRATADA deverá apoiar as respostas sobre auditorias internas e externas relacionadas a Análise de Impacto a Privacidade (PIA - Privacy Impact Assessment).

6.1.7.15.2. A CONTRATADA deverá apoiar na investigação e coleta de evidências sobre incidentes que envolvam dados pessoais e dados pessoais sensíveis.

6.1.7.15.3. A CONTRATADA deverá apoiar na resposta ao direto do titular.

6.1.7.15.4. A CONTRATADA deverá apoiar na comunicação e resposta a solicitações perante a Autoridade Nacional de Proteção de Dados (ANPD).

6.1.7.15.5. A CONTRATADA deverá apoiar na elaboração / atualização de Políticas de Privacidade e Política de Cookies.

6.1.7.15.6. A CONTRATADA deverá apoiar em métodos de coleta de consentimentos de titulares de dados pessoais.

6.1.7.15.7. A CONTRATADA deverá apoiar a área jurídica da CONTRATANTE em demandas relacionadas a tratamento e proteção de dados pessoais e dados pessoais sensíveis.

6.1.7.15.8. A CONTRATADA deverá apoiar no mapeamento do fluxo de informações que tratam dados pessoais e dados pessoais sensíveis em processos administrativos (Data Mapping).

6.1.7.15.9. A CONTRATADA deverá apoiar na elaboração do Relatório de Impacto de Dados Pessoais (RIPD).

6.1.7.15.10. A CONTRATADA deverá propor e apoiar nos métodos de comunicação e divulgação sobre a proteção de dados pessoais e dados pessoais sensíveis na CONTRATANTE.

6.1.7.16. A CONTRATADA deverá garantir que todos os colaboradores estejam cientes sobre suas responsabilidades e em conformidade com a Segurança e Privacidade da Informação da CONTRATANTE através de uma gestão contínua de maturidade.

6.1.7.17. A CONTRATADA deverá garantir que um programa de capacitação contínua em segurança e privacidade da informação seja implementado e gerenciado continuamente na CONTRATANTE, através das seguintes atividades:

6.1.7.17.1. A CONTRATADA deverá realizar semestralmente a avaliação de maturidade da CONTRATANTE perante a segurança e privacidade da informação com base nos controles estabelecidos na NBR ISO/IEC 27001 e NBR ISO/IEC 27701. Esta atividade deverá ser realizada através de pesquisas internas com todos os colaboradores da CONTRATANTE a partir do início do contrato, utilizado a metodologia CMMI (Capability Maturity Model Integration) com base no COBIT 5 (Control Objectives for Information and Related Technologies version 5).

6.1.7.17.2. A CONTRATADA deverá gerenciar a evolução da maturidade da CONTRATANTE perante a segurança e privacidade da informação com base nos controles estabelecidos na NBR ISO/IEC 27001 e NBR ISO/IEC 27701.

6.1.7.17.3. A CONTRATADA deverá elaborar / atualizar o programa de capacitação continuada interna em Segurança e Privacidade da Informação.

6.1.7.17.4. A CONTRATADA deverá elaborar / atualizar a Cartilha de Segurança e Privacidade da Informação da CONTRATANTE em conformidade com as políticas e normas estabelecidas.

6.1.7.17.5. A CONTRATADA deverá estabelecer / atualizar insumos de conteúdo para a área de comunicação (marketing) para a realização de campanhas de endomarketing sobre Segurança e Privacidade da

Informação, em periodicidades e volumetrias de conteúdo a serem definidas pela CONTRATANTE.

6.1.7.17.6. A CONTRATADA deverá estabelecer / atualizar premissas de segurança e privacidade da informação no processo de integração de colaboradores e terceiros.

6.1.7.17.7. A CONTRATADA deverá realizar campanhas de conscientização sobre Segurança e Privacidade da Informação com base em todas as adequações realizadas. A campanha de conscientização, deverá conter, pelo menos, as seguintes atividades:

6.1.7.17.7.1. Divulgação da Cartilha de Segurança e Privacidade da Informação.

6.1.7.17.7.2. Realização de, pelo menos, 2 (dois) workshops a cada 6 (seis) meses sobre Segurança e Privacidade da Informação, de forma presencial, na sede da CONTRATANTE, localizada na R. Antônio Ataíde, 686 - Centro Vila Velha / ES, ou de forma remota a critério da CONTRATANTE, respeitando os seguintes requisitos:

6.1.7.17.7.2.1. Para os workshops realizados de forma remota, eles deverão ser gravados e disponibilizados para a CONTRATANTE em até 2 (dois) dias úteis após a realização.

6.1.7.17.7.2.2. O tema dos workshops deverá contemplar assuntos relacionados à Segurança da Informação e ao Tratamento de Dados Pessoais.

6.1.7.17.7.2.3. Os workshops deverão respeitar no mínimo as seguintes regras:

I) Possuir duração de 1h (uma hora) por turma.

II) O público dos workshops deverá ser segmentado por pelo menos 2 (duas) turmas.

III) Cada workshop deverá ser conduzido por pelo menos dois palestrantes específicos, sendo 1 (um) para ministrar palestras relacionadas à Segurança da Informação e 1 (um) para ministrar

palestras relacionadas ao tratamento de dados pessoais.

6.1.7.17.7.2.4. A CONTRATADA deverá realizar o controle de presença dos participantes em cada turma.

6.1.7.17.7.2.5. A CONTRATADA deverá fornecer certificado de participação para cada participante dos workshops.

6.1.7.18. A CONTRATADA deverá garantir que a Gestão da Segurança e Privacidade da Informação seja eficaz, através das seguintes atividades:

6.1.7.18.1. A CONTRATADA deverá estruturar e coordenar o comitê gestor de segurança e privacidade da informação através das seguintes atividades:

6.1.7.18.1.1. Desenvolver / atualizar o Manual do Comitê Gestor de Segurança e Privacidade da CONTRATANTE.

6.1.7.18.1.2. Estabelecer e priorizar as demandas e dar encaminhamento às deliberações do comitê às demais áreas da CONTRATANTE.

6.1.7.18.1.3. Incentivar que a análise crítica da segurança e privacidade da informação seja realizada por todos os membros do comitê periodicamente.

6.1.7.18.1.4. Convocar, presidir e registrar, através de atas, as reuniões do comitê.

6.1.7.18.1.4.1. As reuniões de comitê deverão ocorrer a cada 2 (dois) meses (bimestralmente), com duração mínima de 1h (uma hora).

6.1.7.18.1.4.2. Emergencialmente, o comitê poderá ser convocado a se reunir em casos de incidentes que impactam significativamente a CONTRATANTE.

6.1.7.18.1.4.3. As reuniões serão realizadas de forma remota, devendo ser gravadas e disponibilizadas para a CONTRATANTE em até 2 (dois) dias úteis após a realização.

6.1.7.18.2. A CONTRATADA deverá realizar a avaliação contínua de desempenho de Segurança e Privacidade da Informação através da

implementação e acompanhamento dos indicadores de desempenho (KPIs - Key Performance Indicator) sobre os riscos, maturidade corporativa e eficácia de controles de segurança e privacidade da informação.

6.1.7.18.3. Mensalmente, a CONTRATADA deverá desenvolver e apresentar no mínimo os seguintes relatórios:

6.1.7.18.3.1. Relatório sobre os indicadores de desempenhos.

6.1.7.18.3.2. Relatório da gestão de riscos.

6.1.7.18.3.3. Relatório da gestão de incidentes no período.

6.1.7.19. A CONTRATADA deverá garantir que a Gestão da Segurança e Privacidade da Informação seja eficaz, utilizando as seguintes normas técnicas e frameworks:

6.1.7.19.1. Norma Técnica Brasileira ISO/IEC 27001 (Sistema em Gestão de Segurança da Informação).

6.1.7.19.2. Norma Técnica Brasileira ISO/IEC 27701 (Sistema em Gestão de Privacidade da Informação).

6.1.7.19.3. Norma Técnica Brasileira ISO/IEC 27005 (Gestão de Riscos em Segurança da Informação).

6.1.7.19.4. Center for Internet Security versão 8 – CIS Controls v8.

6.1.7.19.5. NIST Cybersecurity Framework – NIST CSF.

6.1.8. Sobre os Serviços Contínuos de Encarregado de Dados:

6.1.8.1. A CONTRATADA deverá possibilitar sua indicação e exposição como Encarregado de Dados e atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

6.1.8.2. O nome e contato do Encarregado de Dados, indicado pela CONTRATADA, será divulgado pela CONTRATANTE em sua Política de Privacidade e nos meios de comunicação onde a CONTRATANTE divulgue sua Política de Privacidade.

6.1.8.3. A CONTRATADA deverá garantir que todos os riscos relacionados à privacidade da informação sejam mapeados e gerenciados através das seguintes atividades:

6.1.8.3.1. A CONTRATADA deverá manter atualizado o mapeamento do fluxo de informações que tratam dados pessoais e dados pessoais sensíveis em processos administrativos (Data Mapping).

6.1.8.3.2. A CONTRATADA deverá identificar continuamente ameaças e vulnerabilidades à privacidade dos dados pessoais e dados pessoais sensíveis nos processos administrativos da CONTRATANTE.

6.1.8.3.3. A CONTRATADA deverá analisar o impacto, probabilidade e consequência das ameaças e vulnerabilidades identificadas nos processos administrativos, identificando ou não um risco a Privacidade da Informação da CONTRATANTE.

6.1.8.3.4. A CONTRATADA deverá avaliar quantitativamente a criticidade do risco, considerando os seguintes níveis de risco:

6.1.8.3.4.1. Risco Alto: Tratamento de dados pessoais e/ou dados pessoais sensíveis sem medidas técnicas e administrativas adequadas para proteção dos dados.

6.1.8.3.4.2. Risco Médio: Tratamento de dados pessoais e dados pessoais sensíveis com poucas medidas técnicas, administrativas adequadas para proteção dos dados.

6.1.8.3.4.3. Risco Baixo: Tratamento de dados pessoais com poucas medidas técnicas, administrativas e operacionais adequadas para proteção dos dados.

6.1.8.3.5. A CONTRATADA deverá definir os controles aplicáveis para o tratamento dos riscos identificados e apresentar, sempre que for necessário a CONTRATANTE.

6.1.8.3.6. A CONTRATADA deverá definir, em comum acordo com a CONTRATANTE, os critérios para aceitação dos riscos a serem identificados e gerenciados durante a prestação dos serviços.

6.1.8.3.7. A CONTRATADA deverá gerenciar continuamente a mitigação do risco através da priorização, avaliação e implementação dos controles necessários para remediação, assim como identificar e avaliar os riscos residuais.

6.1.8.3.8. A CONTRATADA deverá desenvolver e manter atualizado um manual de gestão dos riscos privacidade da informação da CONTRATANTE, contendo no mínimo:

6.1.8.3.8.1. Metodologias, frameworks e métodos definidos para identificar, analisar e avaliar os riscos.

6.1.8.3.8.2. Critérios definidos para aceitar, transferir, evitar e mitigar os riscos (Plano de Tratamento de Risco).

6.1.8.4. A CONTRATADA deverá garantir que todas as responsabilidades do Encarregado de Dados da CONTRATANTE, sejam executadas e cumpridas. Sendo elas:

6.1.8.4.1. A CONTRATADA deverá responder auditorias internas e externas relacionadas a Análise de Impacto a Privacidade (PIA - Privacy Impact Assessment).

6.1.8.4.2. A CONTRATADA deverá apoiar na investigação e coleta de evidências sobre incidentes que envolvam dados pessoais e dados pessoais sensíveis.

6.1.8.4.3. A CONTRATADA deverá receber as reclamações e comunicações dos titulares de dados pessoais, prestar os devidos esclarecimentos e adotar as providências necessárias.

6.1.8.4.4. A CONTRATADA deverá realizar a comunicação e responder às solicitações perante a Autoridade Nacional de Proteção de Dados (ANPD).

6.1.8.4.5. A CONTRATADA deverá apoiar na elaboração da Política de Privacidade e Política de Cookies.

6.1.8.4.6. A CONTRATADA deverá ser responsável por manter o processo de coleta de consentimentos de titulares de dados pessoais.

6.1.8.4.7. A CONTRATADA deverá apoiar a área jurídica da CONTRATANTE em demandas relacionadas a tratamento e proteção de dados pessoais e dados pessoais sensíveis.

6.1.8.4.8. A CONTRATADA deverá manter o Relatório de Impacto de Dados Pessoais (RIPD) atualizado.

6.1.8.4.9. A CONTRATADA deverá orientar os colaboradores, terceiros, fornecedores, parceiros institucionais e demais partes que interagem com a CONTRATANTE, a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

6.1.8.4.10. A CONTRATADA deverá apoiar o Comitê Gestor de Segurança e Privacidade da Informação em suas deliberações.

6.1.8.4.11. A CONTRATADA deverá identificar e avaliar as principais ameaças à proteção de dados pessoais, bem como propor melhorias e, quando aprovado, apoiar a implantação de medidas corretivas para reduzir riscos.

6.1.8.4.12. A CONTRATADA deverá atender as demais atribuições, conforme orientação da Autoridade Nacional de Proteção de Dados, definidas em normas complementares publicadas pelo referido órgão, atualizações da Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018) e demais normas, regulamentos e legislações de Privacidade de Dados que possam ser aplicáveis a CONTRATANTE no futuro.

6.1.8.4.13. A CONTRATADA deverá estar ciente das atualizações e novidades legislativas que envolvem o tema de Privacidade, Proteção de Dados Pessoais e Segurança Digital e realizar treinamentos para os colaboradores da CONTRATANTE.

6.1.8.4.14. A CONTRATADA deverá realizar a auditoria de privacidade dos parceiros da CONTRATANTE.

6.1.8.4.15. A CONTRATADA deverá participar do Fluxo de Resposta a Incidentes de Segurança da Informação que envolvam Dados Pessoais.

6.1.8.4.16. A CONTRATADA deverá formular relatórios e manuais, gerenciando todas as mudanças necessárias para manter o ciclo de vida da Governança em Privacidade da Informação da CONTRATANTE.

6.1.8.4.17. A CONTRATADA deverá participar, quando solicitado, de demais reuniões das áreas da CONTRATANTE.

6.1.8.5. A CONTRATADA deverá garantir que as atividades de governança, gestão de riscos e conformidade em segurança e privacidade da informação sejam apoiadas pelo Encarregado de Dados designado.

6.1.8.6. A CONTRATADA deverá evidenciar a eficiência de suas atividades através das seguintes atividades:

6.1.8.6.1. A CONTRATADA deverá definir os indicadores de desempenho do Encarregado de Dados juntamente com a CONTRATANTE.

6.1.8.6.2. Mensalmente, a CONTRATADA deverá desenvolver e apresentar no mínimo os seguintes relatórios:

6.1.8.6.2.1. Relatório sobre os indicadores de desempenhos definidos.

6.1.8.6.2.2. Relatório da gestão de riscos em Privacidade da Informação.

6.1.8.6.2.3. Relatório da gestão de incidentes no período.

6.1.8.6.2.4. Relatório da gestão de consentimentos.

6.1.8.6.2.5. Outros relatórios a serem solicitados pela CONTRATANTE.

6.1.8.7. A CONTRATADA deverá garantir que sejam aplicadas as melhores práticas de mercado considerando no mínimo a aplicabilidade das seguintes normativas técnicas e frameworks de mercado:

6.1.8.7.1. Norma Técnica Brasileira ISO/IEC 27001 (Sistema em Gestão de Segurança da Informação).

6.1.8.7.2. Norma Técnica Brasileira ISO/IEC 27701 (Sistema em Gestão de Privacidade da Informação).

6.1.8.7.3. Norma Técnica Brasileira ISO/IEC 27005 (Gestão de Riscos em Segurança da Informação).

6.2. ITEM 2 – Subscrição de solução de Antimalware e de Detecção e Resposta a Ameaças Cibernéticas (EDR)

6.2.1. Detalhamento do Módulo de Antimalware (NGAV):

6.2.1.1. A solução de proteção para endpoint deve prover proteção contra ameaças conhecidas e desconhecidas. As ameaças devem ser

identificadas e neutralizadas, incluindo o código executável, scripts e exploits.

6.2.1.2. Os agentes da solução devem ser compatíveis com no mínimo os seguintes sistemas operacionais:

6.2.1.2.1. Windows XP.

6.2.1.2.2. Windows 7 (32 e 64 bits).

6.2.1.2.3. Windows 8 e Windows 8.1 (32 e 64 bits).

6.2.1.2.4. Windows 10 (32 e 64 bits).

6.2.1.2.5. Windows 11.

6.2.1.2.6. Windows Server 2003 R2.

6.2.1.2.7. Windows Server 2008.

6.2.1.2.8. Windows Server 2008 R2.

6.2.1.2.9. Windows Server 2012 (64 bits).

6.2.1.2.10. Windows Server 2012 R2 (64 bits).

6.2.1.2.11. Windows Server 2016 (64 bits).

6.2.1.2.12. Windows Server 2019 (64 bits).

6.2.1.2.13. Windows Server 2022 (64 bits).

6.2.1.2.14. MacOS Catalina (10.15).

6.2.1.2.15. MacOS Mojave (10.14).

6.2.1.2.16. MacOS Big Sur (11).

6.2.1.2.17. MacOS Monterey (12).

6.2.1.2.18. RHEL 6 (64 bits).

6.2.1.2.19. RHEL/CentOS 7.8 (64 bits).

6.2.1.2.20. RHEL/CentOS 7.9 (64 bits).

6.2.1.2.21. RHEL/CentOS 8.3 (64 bits).

6.2.1.2.22. RHEL/CentOS 8.4 (64 bits).

6.2.1.2.23. RHEL/CentOS 8.5 (64 bits).

6.2.1.2.24. RHEL Enterprise 8.6 (64 bits).

6.2.1.2.25. RHEL Enterprise 9 (64 bits).

6.2.1.2.26. SUSE (SLES) 12 SP5(64 bits).

6.2.1.2.27. SUSE (SLES) 15 (64 bits).

6.2.1.2.28. Ubuntu 18.04 (64 bits).

6.2.1.2.29. Ubuntu 20.04 (64 bits).

6.2.1.2.30. Ubuntu LTS 20.04 (64 bits).

6.2.1.2.31. Ubuntu 22.04 LTS (64 bits).

6.2.1.2.32. Amazon Linux 2 (64 bits).

6.2.1.2.33. Debian 10 (64 bits).

6.2.1.2.34. Debian 11 (64 bits).

6.2.1.2.35. Oracle Linux Server 6 (64 bits).

6.2.1.2.36. Oracle Linux Server 7 (64 bits).

6.2.1.2.37. Oracle Linux Server 8 (64 bits).

6.2.1.2.38. Oracle Linux Server 9 (64 bits).

6.2.1.2.39. Oracle Linux Server UEK 6 (64 bits).

6.2.1.2.40. Oracle Linux Server UEK 7(64 bits).

6.2.1.2.41. Oracle Linux Server UEK 8 (64 bits).

6.2.1.2.42. Oracle Linux Server UEK 9 (64 bits).

6.2.1.3. A instalação da solução de Antivírus de Próxima Geração (NGAV) deve aceitar parâmetros de configuração e distribuição, como instalação silenciosa e definição de diretório de instalação.

6.2.1.4. Não será permitido que o instalador baixe parte do pacote de instalação da Internet ou de um servidor local.

6.2.1.5. Deve permitir identificar dispositivos que não possuem o agente instalado.

6.2.1.6. Deve permitir a utilização de senha para prevenir a desinstalação do produto nas estações/servidores.

6.2.1.7. Deve possuir serviço de proteção contra finalização (kill) do processo da ferramenta. Também deve impedir que outros aplicativos efetuem a finalização do serviço.

6.2.1.8. Todas as funcionalidades desta ferramenta devem ser ativadas por um único produto que facilita a instalação, a configuração e o gerenciamento.

6.2.1.9. Deve ter a capacidade de realizar a análise somente dos arquivos copiados na máquina, de uma análise completa da máquina após a

instalação e adicionalmente deve ser possível configurar análises recorrentes de arquivos.

6.2.1.10. Não serão aceitas soluções que detectam o malware apenas quando da execução da aplicação.

6.2.1.11. O funcionamento da solução deve operar analisando a execução da ameaça em potencial, nas camadas do Sistema Operacional (O/S), Memória e prevenindo a entrada de códigos maliciosos.

6.2.1.12. Deve possuir a capacidade de análise automática do código do arquivo, identificando suas características antes da sua capacidade de execução.

6.2.1.13. A solução deve aplicar análise baseada em algoritmo matemático, para identificar programas maliciosos antes da sua execução.

6.2.1.14. Caso seja identificado um programa malicioso, a sua execução não deve ser permitida.

6.2.1.15. A solução deve identificar e bloquear a execução de códigos executáveis (binários), scripts ou comandos.

6.2.1.16. A solução de proteção de endpoints deve detectar e prevenir qualquer alteração oriunda de código malicioso ou não-autorizado, em programas que estejam sendo executados em memória.

6.2.1.17. Deve-se utilizar a tecnologia de Machine Learning para identificar qualquer ameaça nos arquivos potencialmente perigosos.

6.2.1.18. A análise do malware deve ocorrer em pré-execução, ou seja, o código malicioso deve ser bloqueado antes de executar e infectar a máquina, no processo de detecção e bloqueio em pré-execução não serão aceitas tecnologias que fazem uso de análise de hashing do arquivo ou verificação do arquivo em nuvem.

6.2.1.19. Identificar ameaças avançadas (APTs), chamadas de zero day e ransomwares sem a necessidade de base de assinaturas (DATs), detecção por heurística, detecção por hashing, detecção por comportamento ou sandboxing. Todas as detecções devem ser feitas em tempo real.

6.2.1.20. Deve permitir controlar dispositivos de armazenamento conectados via USB, permitindo bloquear ou liberar o seu acesso. Adicionalmente deve ser possível a criação de exceções na política, pelo número de série, identificador do fabricante e tipo de dispositivo.

6.2.1.21. O controle do acesso via USB, deve ter a capacidade mínima de controlar os seguintes dispositivos:

6.2.1.21.1. Dispositivos Android.

6.2.1.21.2. Dispositivos Apple IOS.

6.2.1.21.3. Dispositivos Still Image como câmeras e Scanners.

6.2.1.21.4. Dispositivos USB Drive (Pen Drive).

6.2.1.21.5. Dispositivos VMWARE USB Passthrough.

6.2.1.21.6. Dispositivos portáteis Windows.

6.2.1.22. A solução não deve depender de base de assinaturas e hashes para identificação de qualquer ameaça.

6.2.1.23. Deve prover proteção em tempo real, independente do estado de conexão da máquina, sendo:

6.2.1.23.1. Online – Com conexão com a Internet.

6.2.1.23.2. Offline – Sem conexão com a Internet.

6.2.1.24. Os módulos de proteção de memória e controle de execução devem prevenir técnicas de ataques do tipo:

6.2.1.24.1. Hijacking.

6.2.1.24.2. File Injection.

6.2.1.24.3. File Overflow.

6.2.1.24.4. In-Memory execution.

6.2.1.24.5. Exploitation - Stack Pivot, Stack protect, Overwrite Code, RAM Scraping e Malicius Payload, System Call Monitoring, Direct System Calls, System DLL Overwrite, Dangerous COM object.

6.2.1.24.6. Process Injection – Remote Allocation of Memory, Remote Mapping of Memory, Remote Write to Memory, Remote Write PE to Memory, Remote Overwrite Code, Remote Unmap of Memory, Remote Thread Creation, Remote APC Scheduled, DYLD Injection (Apenas para MacOS X), Doppelganger e Dangerous Environmental Variable.

6.2.1.24.7. Escalation – LSASS Read, Zero Allocate, Memory Permissions Changes in Other Processes, Memory Permission Changes in Child Processes, Stolen System Token e Low Integrity Process Start.

6.2.1.25. O módulo de proteção de memória deve possuir as seguintes ações em caso de violação:

6.2.1.25.1. Ignorar.

6.2.1.25.2. Alertar.

6.2.1.25.3. Bloquear.

6.2.1.25.4. Terminar.

6.2.1.26. O módulo de controle e análise de scripts deve ser capaz de analisar no mínimo as seguintes linguagens:

6.2.1.26.1. PowerShell.

6.2.1.26.2. Active Scripts – Jscript.

6.2.1.26.3. WScript.

6.2.1.26.4. CScript.

6.2.1.26.5. Macros.

6.2.1.26.6. VBA.

6.2.1.26.7. Python.

6.2.1.26.8. .NETDLR.

6.2.1.27. O módulo de controle e análise de scripts deve possuir as seguintes ações em caso de violação:

6.2.1.27.1. Alertar.

6.2.1.27.2. Bloquear.

6.2.1.28. Caso ocorra alguma identificação de código malicioso em scripts, a ferramenta deve agir no interpretador e prevenir sua execução imediata.

6.2.1.29. Deve ser capaz de finalizar processos e sub processos em execução, caso haja a identificação de algum código malicioso sendo executado nos mesmos.

6.2.1.30. Possuir funcionalidade para análise contra ameaças em background, permitindo análises periódicas no disco contra ameaças

inativas. Esta análise apenas poderá ser realizada quando a estação/servidor estiver em modo ocioso, ou seja, com os recursos disponíveis para execução desta ação.

6.2.1.31. Permitir a verificação de ameaças somente em arquivos novos e modificados.

6.2.1.32. Gerar registro (log) dos eventos de detecção de ameaças em arquivo local, com opção de upload para a console de gerenciamento.

6.2.1.33. Gerar notificações de eventos de ameaças através de alerta via Syslog ou por e-mail.

6.2.1.34. Deve possuir um módulo integrado de Anti-Exploit permitindo identificar e bloquear a execução de Exploits na memória da máquina. Este módulo deve permitir no mínimo a proteção contra ferramentas de injeção de código malicioso, como por exemplo o Shelter, além de detectar e evitar a execução de backdoors.

6.2.1.35. Deve possuir módulo integrado de bloqueio de Exploits onde não deve ser baseado em assinaturas. Deve ser capaz de bloquear estas ameaças utilizando o próprio engine de inteligência artificial e machine learning.

6.2.1.36. No modo desconectado, o endpoint deve fazer a detecção e bloqueio usando unicamente o algoritmo matemático. Não serão permitidas soluções híbridas que utilizem assinaturas (DATs), hashes ou consultas na Internet (Cloud Lookups) para a detecção neste cenário.

6.2.1.37. O endpoint deve ser certificado pela Microsoft como uma ferramenta de antivírus, sendo assim, nas plataformas Windows, a ferramenta deve ser identificada como a solução de antivírus.

6.2.2. Detalhamento do Módulo de Endpoint Detection and Response (EDR):

6.2.2.1. Deve possuir a capacidade de realizar uma conexão remota nas máquinas através da console de gerenciamento para coletar arquivos de logs e para análise forense.

6.2.2.2. Deve possuir regras para detecção de Crypto Hijacking (Crypto mining) usando tecnologia de detecção em processadores Intel (Intel Threat Detection Technology).

6.2.2.3. Realizar obrigatoriamente análise de comportamentos com base nas técnicas, táticas e procedimentos (TTPs) listados no framework MITRE ATT&CK.

6.2.2.4. A nuvem de inteligência da solução utilizada pela console deve ser hospedada em infraestrutura de nuvem em conformidade com a norma NC14 da IN01 do DSIC/GSIPR.

6.2.2.5. O módulo de análise forense e detecção e respostas em endpoints (EDR) deve permitir a monitoração contínua dos eventos, captura e gravação em modo seguro. Este módulo deve permitir analisar o comportamento do usuário ou do malware no endpoint.

6.2.2.6. O módulo deve ter a capacidade de coletar informações dos processos em execução da máquina e o motivo para a finalização dos processos.

6.2.2.7. O módulo deve permitir visualizar através da console Web uma linha do tempo gráfica, contendo toda a sequência de eventos que ocorreram durante a execução do malware, sendo possível ainda expandir os detalhes de cada informação.

6.2.2.8. O módulo deve identificar processos que tenham sido suspensos.

6.2.2.9. Devem ser fornecidas na console de gerenciamento, informações do identificador do processo (Process ID), nome do processo, a linha de comando de execução, o usuário logado que executou o processo, o caminho do executável, e quando disponível o hash MD5 do processo.

6.2.2.10. O módulo deve reportar eventos maliciosos em memória, sendo que devem ser fornecidas no log de eventos os grupos, SID, e quantas vezes o código malicioso tentou executar em memória.

6.2.2.11. O módulo deve detectar a injeção de ameaças em funções e módulos do programa (aplicativo) executado.

6.2.2.12. Deve identificar processos suspeitos que executam em localidades não comuns, como diretórios de dados e lixeira.

6.2.2.13. Deve identificar processos que estabelecem conexões de rede externas e suspeitas (call back).

6.2.2.14. Deve ser reportado no log as conexões de redes externas e suspeitas, a origem da conexão, o destino, o tempo de início e término da conexão.

6.2.2.15. Deve identificar alterações não comuns em áreas do registro da máquina.

6.2.2.16. Deve-se monitorar alterações em tarefas agendadas na máquina.

6.2.2.17. Deve-se monitorar tentativas de escalação de privilégios.

6.2.2.18. Deve possuir a capacidade de realizar busca de ameaças na rede (IOC hunting) por arquivos, hashes, processos, DNS request, powershell trace, wmi trace, eventos do Windows, alterações de chaves de registros e conexões de rede.

6.2.2.19. Deve permitir realizar um isolamento completo da máquina que foi identificada a ameaça, este isolamento evita a propagação da mesma pela rede.

6.2.2.20. Deve permitir realizar um isolamento parcial, permitindo acesso ao equipamento pela console e evitando a propagação da ameaça pela rede.

6.2.2.21. O agente deve ter a capacidade de fazer este isolamento da máquina por si só, sem necessitar de nenhuma integração com outros softwares ou dispositivos de rede para isso.

6.2.2.22. Este isolamento pode ser realizado por um tempo específico não inferior a 5 minutos, onde deve ser possível ao administrador fornecer uma chave para realizar a liberação da máquina isolada. Durante o período de isolamento a máquina não consegue realizar nenhuma conexão de rede ficando completamente sem acesso na rede.

6.2.2.23. O isolamento completo, não deve permitir inclusive o ICMP para a estação isolada, garantindo assim que a ameaça não irá se propagar de nenhuma maneira.

6.2.2.24. Deve ter a capacidade de realizar através da solução o envio do arquivo da ameaça ao sistema de gerenciamento em cloud, para análise posterior, bem como o envio de artefatos pela console.

6.2.2.25. O módulo de análise forense ou EDR deve possuir a capacidade de identificação automática de comportamentos maliciosos executados no endpoint através de um conjunto mínimo de 25 regras para Windows e 10 regras para Mac OS.

6.2.2.26. Deve possuir regras para detecção de pelo menos 65 diferentes técnicas de ataques seguindo a classificação e certificação MITRE.

6.2.2.27. Devem existir pelo menos 6 categorias de regras a serem aplicadas.

6.2.2.28. Deve ser capaz de permitir a criação de regras de detecção customizáveis utilizando linguagem JSON.

6.2.2.29. As regras devem apresentar quatro níveis de criticidade: alto, médio, baixo e informativo.

6.2.2.30. As regras devem identificar pelo menos os seguintes conjuntos de ações:

- **6.2.2.30.1.** Tentativas de mascarar ou matar os processos do módulo de Antivírus de Próxima Geração (NGAV).
- **6.2.2.30.2.** Detecção de Fileless Powershell malware.
- **6.2.2.30.3.** Detecção da execução de comandos maliciosos em Powershell, como comandos que ocultam a execução do Powershell.
- **6.2.2.30.4.** Invocação maliciosa de JavaScritps com Rundll.
- **6.2.2.30.5.** Processos de Sistema Operacional iniciados por usuários que não são SYSTEM.
- **6.2.2.30.6.** Executáveis iniciados do Recycle Bin.
- **6.2.2.30.7.** Executável criado ou lançado como executável do Windows.
- **6.2.2.30.8.** Processos do Windows sendo executados em pastas fora do padrão.

6.2.2.30.9. Processos criados com nomes confusos (tentando se passar por processos do Windows).

6.2.2.30.10. Uso do PSEXEC.

6.2.2.30.11. Modificação de host files.

6.2.2.30.12. Tentativa de invocação do Remote Shell.

6.2.2.30.13. Detecção de executável com múltiplas extensões.

6.2.2.30.14. Tarefas agendadas suspeitas.

6.2.2.31. Após identificar estes comportamentos o módulo de EDR deve ter a capacidade de realizar uma ação automática (sem a intervenção do operador), entre as ações automáticas customizadas, devem estar incluídas:

6.2.2.31.1. Apagar arquivos.

6.2.2.31.2. Realizar Log Off de todos os usuários, usuários remotos e usuários interativos.

6.2.2.31.3. Suspender e terminar processos.

6.2.2.31.4. Gerar log de aplicação.

6.2.2.32. Através do dashboard deve ser possível requisitar e fazer download dos logs e evidências da causa raiz, os arquivos maliciosos ou adicionar os mesmos a quarentena global.

6.2.2.33. Deve permitir o armazenamento de logs do EDR em nuvem e localmente por no mínimo 30 dias.

6.2.2.34. Deve permitir criar ou modificar as regras a critério do usuário.

6.2.2.35. A solução de EDR deve possuir um Engine Python nativo que permite a execução de scripts através da customização de respostas das regras ou por demanda via console. Não serão aceitas soluções que necessitem a instalação adicional do pacote de Python.

6.2.2.36. Deve ser possível iniciar a execução de scripts em Python na máquina infectada quando é detectado um comportamento malicioso, permitindo coletar mais informações forenses como dados do Event Viewer Windows, Registry Hives, Master File Table, histórico do navegador, logs de execução de programas no Windows.

6.2.2.37. Deve possibilitar a criação de Playbooks com um conjunto de Scripts em Python que podem ser configurados nas regras, permitindo a sua execução quando algum evento é detectado.

6.2.3. Detalhamento do Gerenciamento da Solução:

6.2.3.1. Possuir gerência centralizada e integrada, a partir de uma única console, para as todas as ferramentas integradas de segurança em estações de trabalho e servidores, de onde seja possível manter a proteção atualizada, gerar relatórios, visualizar eventos e gerenciar políticas.

6.2.3.2. Deve permitir o acesso a console de gerenciamento Web, através de protocolo seguro (HTTPS).

6.2.3.3. Deve possuir pelo menos 5 (cinco) relatórios na console Web.

6.2.3.4. Deve possuir relatórios que permitam no mínimo: ter um sumário das ameaças identificadas, visão geral das ameaças, visão geral dos equipamentos identificando qual a versão do agente está instalada em cada um deles e quanto tempo estão offline.

6.2.3.5. Possuir comunicação segura através do padrão SSL entre os agentes e a console de gerenciamento da solução de segurança.

6.2.3.6. Permitir o gerenciamento através de console Web compatível com Mozilla Firefox e Google Chrome.

6.2.3.7. Deve permitir a definição de níveis diferentes de administração, onde administradores gerenciam, com diferentes níveis de privilégios, grupos de máquinas em diferentes partes do ambiente, havendo, contudo, um grupo de administradores que poderá ter uma visão completa de todo o ambiente instalado.

6.2.3.8. Deve permitir integração com diferentes ferramentas de SIEM, com opção de configurar qual informação será repassada, como:

6.2.3.8.1. Log de Auditoria.

6.2.3.8.2. Dispositivos.

6.2.3.8.3. Proteção de Memória.

6.2.3.8.4. Controle de Scripts.

6.2.3.8.5. Ameaças.

6.2.3.8.6. Classificação de Ameaças.

6.2.3.8.7. Controle de Aplicação.

6.2.3.9. Deve permitir a atualização automática dos agentes, com possibilidade de permitir a homologação da atualização em grupo específico de endpoints e, posteriormente, para o ambiente de produção.

6.2.3.10. Deve suportar a inclusão de certificados digitais para que arquivos assinados com estes certificados estejam dentro de uma lista segura (Safe List) para a execução.

6.2.3.11. Forçar a configuração determinada no servidor para os clientes.

6.2.3.12. Através da console da solução deve ser exibida à lista dos clientes (servidores e estações) que possuem o endpoint instalado, contendo, no mínimo, as seguintes informações, mesmo com as máquinas desligadas:

6.2.3.12.1. Nome da máquina.

6.2.3.12.2. Endereço IP.

6.2.3.12.3. Versão do Sistema Operacional (com a versão do Service Pack).

6.2.3.12.4. MAC Address.

6.2.3.12.5. Usuário.

6.2.3.12.6. Versão do endpoint.

6.2.3.13. A solução de segurança deve prover no mínimo os seguintes indicadores a partir da sua console:

6.2.3.13.1. As 10 máquinas que mais receberam ocorrência de malware.

6.2.3.13.2. As 10 zonas que mais receberam ocorrência de malware.

6.2.3.13.3. Os 10 malwares que mais infectaram a rede.

6.2.3.13.4. Malwares por prioridade.

6.2.3.13.5. Malwares por classificação.

6.2.3.13.6. Históricos de infecções em endpoints.

6.2.3.13.7. Históricos de infecções em zonas.

6.2.3.14. Capacidade de exportar os indicadores para o formato CSV e PNG.

6.2.3.15. Possibilitar a verificação no site "Virus Total", através de link pré-definido no resultado de uma detecção.

6.2.3.16. Possuir módulo que registre em arquivo de log todas as atividades efetuadas pelos administradores, permitindo análises em nível de auditoria.

6.2.3.17. Possuir um painel de controle, contendo em tempo real os indicadores que os administradores da solução julguem necessários para monitorar o ambiente.

6.2.4. Suporte Técnico da Solução

6.2.4.1. A CONTRATADA deverá prestar suporte técnico remoto ilimitado 24x7x365 (vinte e quatro horas, sete dias por semana, trezentos e sessenta e cinco dias, incluindo feriados) para as soluções durante toda a vigência contratual.

6.2.4.2. A CONTRATADA deverá disponibilizar um canal de comunicação para a CONTRATANTE por e-mail e telefone com número 0800.

6.2.4.3. A CONTRATADA deverá possuir um canal direto com as fabricantes das soluções para resolução de problemas técnicos, escalonamento de chamados e solicitações de novas funcionalidades.

6.2.4.4. Eventos e incidentes de segurança da informação devem ser comunicados através de canais predefinidos de comunicação, disponibilizados pelas CONTRATADA/FABRICANTES das soluções, de maneira rápida, eficiente e de acordo com os requisitos legais, regulatórios e contratuais.

6.2.4.5. A CONTRATADA deverá disponibilizar o seu sistema de chamados técnicos (sistema de Help Desk) para que a CONTRATANTE realize as solicitações de atendimentos de suporte das soluções.

6.2.4.6. A CONTRATADA deverá respeitar os seguintes Acordos de Níveis de Serviços (SLAs - Service Level Agreement) para atendimento/suporte sobre as solicitações realizadas pela CONTRATANTE:

SLAS PARA ABERTURAS DE CHAMADOS			
CRITICIDADE	**SLA ATENDIMENTO**	**SLA RESOLUÇÃO**	**DESCRIÇÃO**
URGENTE	15 minutos	2 horas	- Ocorrência de falha ou defeito que impede totalmente a operação do objeto contratado. - Ocorrência de falha ou defeito que afeta a execução do Objeto contratado de forma que o trabalho não possa continuar sem a resolução. - Ocorrência de falha ou defeito que impeça ou cause atraso no andamento do negócio vinculado ao objeto contratado. - Ocorrência de problemas que afetem a segurança do objeto contratado de forma grave e que transgridam a Legislação Vigente. - Ocorrência no objeto contratado que resultem em um impacto crítico de suas operações, com graves restrições.
ALTA	1 hora	12 horas	- Ocorrência de falha ou defeito que impeça de forma parcial a operação ininterrupta e livre de falhas do objeto contratado. - Inoperância parcial do objeto contratado.

SLAS PARA ABERTURAS DE CHAMADOS			
CRITICIDADE	**SLA ATENDIMENTO**	**SLA RESOLUÇÃO**	**DESCRIÇÃO**
			- Ocorrência de falha ou defeito do objeto contratado que, se não resolvida poderá se tornar crítica.
MÉDIA	4 horas	48 horas	- Ocorrência de degradação do desempenho do objeto contratado. - Ocorrência de falha e ou defeito do objeto contratado que cause inconveniência e afete a operacionalidade, a segurança e o desempenho do referenciado objeto. - Impossibilidade de utilização de funcionalidades específicas, que não afetam a operação geral do objeto contratado. - Requisições para apresentação de projeto para solução definitiva de incidentes, que foram caracterizados com prioridade URGENTE e ALTA, resolvidos apenas com solução de contorno.
BAIXA	12 horas	72 horas	- Ocorrência de falha e ou defeito que causa pequenos inconvenientes do objeto contratado.

6.2.4.7. Os prazos do Acordo de Níveis de Serviço poderão ser interrompidos nas seguintes situações:

6.2.4.7.1. Quando a CONTRATADA depender de retorno de informações por parte da CONTRATANTE para execução do atendimento.

6.2.4.7.2. Quando a ocorrência depender do retorno de informações da CONTRATADA mediante concordância da CONTRATANTE.

6.2.4.7.3. Quando o atendimento depender de agendamento para atendimento, onde for acordado data/hora entre CONTRATADA e CONTRATANTE.

6.2.4.8. Os status disponíveis para uso em Incidentes e Requisições são:

6.2.4.8.1. PAUSA do SLA mediante a justificativa:

6.2.4.8.1.1. Aguardando Fornecedor.

6.2.4.8.1.2. Aguardando Cliente/Usuário.

6.2.4.8.1.3. Agendado.

6.2.4.8.1.4. Em Homologação (somente para requisições).

6.2.4.8.2. Os status para RETOMADA do SLA mediante a justificativa:

6.2.4.8.2.1. Em Atendimento.

6.2.4.8.2.2. Encaminhado.

6.2.4.8.2.3. Homologado (somente para requisições).

6.2.4.8.2.4. Não Homologado (somente para requisições).

6.2.4.8.2.5. Reaberto.

6.2.4.9. Pausas e retomadas de tempo de atendimento só ocorrem quando o tempo total não foi excedido.

6.2.4.10. É vedada a transferência do chamado, salvo, para correção de encaminhamento.

6.2.4.11. A CONTRATADA poderá realizar assentamentos ou resolver o chamado a qualquer momento, respeitando os níveis de SLA.

6.2.4.12. Após a resolução da Requisição ou Incidente pela CONTRATADA, a CONTRATANTE terá um prazo de 2 (dois) dias úteis para reabrir o chamado.

6.2.4.13. A reabertura da Requisição ou Incidente será considerada como continuação do atendimento anterior, ou seja, a contagem do prazo de atendimento será retomada e não haverá ônus financeiro para a CONTRATANTE em decorrência de uma possível caracterização de nova demanda.

6.2.4.14. Mensalmente, ou quando solicitado pela CONTRATANTE, a CONTRATADA deverá emitir relatórios sobre os atendimentos técnicos realizados.

6.2.4.15. Semestralmente, a CONTRATADA deverá realizar Health Check das Soluções, compreendendo:

6.2.4.16. Análise do nível de aderência às boas práticas e proteção do ambiente.

6.2.4.17. Análise das políticas e demais configurações implantadas.

6.2.4.18. Para as soluções que possuem agentes, avaliar a comunicação com a console de gerenciamento da solução.

6.2.4.19. Avaliar a integridade da solução em todo ambiente da CONTRATANTE.

6.2.4.20. Validação de features da solução que não estão sendo utilizadas.

6.2.4.21. Validação de consumo de licenças (telemetria).

6.2.4.22. Checagem de logs e correção de problemas.

6.2.5. Requisitos de Homologação das Soluções

6.2.5.1. Juntamente com sua documentação de habilitação técnica, a LICITANTE vencedora da fase de lances, deverá enviar os manuais técnicos, datasheets ou outros documentos oficiais das fabricantes das soluções que permitam comprovar o atendimento aos requisitos técnicos estabelecidos.

6.2.5.2. A LICITANTE vencedora da fase de lances, deverá enviar uma planilha relacionando os requisitos técnicos estabelecidos com a documentação do item anterior, conforme o modelo abaixo (Planilha de Ponto-a-Ponto):

ITEM	REQUISITO	DOCUMENTO DE REFERÊNCIA DO PRODUTO	PÁGINA DO DOCUMENTO	OBSERVAÇÕES

6.2.5.3. Caso a LICITANTE não envie a documentação que permita avaliar se a solução atende os requisitos estabelecidos, a equipe da CONTRATANTE poderá proceder com sua desclassificação.

6.2.5.4. Em sua proposta comercial, as LICITANTES deverão indicar expressamente quais soluções que serão fornecidas.

6.2.5.5. Caso a equipe da CONTRATANTE não consiga identificar o atendimento aos requisitos a partir da documentação enviada, a LICITANTE será convocada para realização de prova de conceito, onde a equipe da CONTRATANTE poderá solicitar a comprovação de todos os requisitos ou daqueles que restarem dúvida quanto ao seu atendimento, sem que isso desobrigue as soluções a atender todos os requisitos técnicos estabelecidos.

6.2.5.5.1. A LICITANTE, juntamente com a CONTRATANTE, deverá realizar a execução e acompanhamento da prova de conceito em formato presencial no seguinte endereço: R. Antônio Ataíde, 686 - Centro, Vila Velha / ES.

6.2.5.5.2. A LICITANTE deverá preparar o ambiente para demonstração em um prazo de 5 (cinco) dias úteis contados da convocação. Os representantes da CONTRATANTE agendaram uma data para o início da homologação da solução, devendo as sessões ocorrerem com duração diária de 4 (quatro) horas consecutivas.

6.2.5.5.3. A comprovação do atendimento aos requisitos técnicos da(s) solução(es) deverá ocorrer no prazo máximo de 10 (dez) dias úteis da solicitação do Pregoeiro.

6.2.5.5.4. Serão de responsabilidade da licitante as atividades e os respectivos gastos relacionados à realização da prova de conceito para a

comprovação do atendimento aos requisitos obrigatórios, incluindo despesas com pessoal, deslocamentos, horas técnicas e hospedagem.

6.2.5.5.5. Durante a realização da prova de conceito, caso não seja possível demonstrar a comprovação aos requisitos, dentro do prazo, poderá ser concedido novo prazo de até 2 dias úteis para conclusão da demonstração, desde que não haja requisitos não atendidos até o fim do prazo de 10 (dez) dias úteis.

6.2.5.5.6. Não caberá, sob qualquer hipótese, o pagamento de indenização de qualquer espécie pela rejeição da amostra que não esteja em conformidade com os requisitos estabelecidos.

6.3. ITEM 3 – Serviços Gerenciados de Segurança Cibernética em Endpoints.

6.3.1. A CONTRATADA deverá executar os serviços Gerenciados de Segurança Cibernética em Endpoints de forma contínua, no formato de atendimento remoto ilimitado 24x7x365 (vinte e quatro horas, sete dias por semana, trezentos e sessenta e cindo dias, incluindo feriados), durante toda a vigência do contrato.

6.3.2. A CONTRATADA deverá disponibilizar um canal de comunicação para a CONTRATANTE por e-mail e telefone com número 0800.

6.3.3. A CONTRATADA deverá disponibilizar o seu sistema de chamados técnicos (sistema de Help Desk) para que a CONTRATANTE realize as solicitações de atendimentos sobre o serviço de Gerenciamento de Segurança Cibernética em Endpoints.

6.3.4. O serviço Gerenciamento de Segurança Cibernética em Endpoints tem como objetivo manter o nível de segurança adequado dos endpoints da CONTRATANTE, provendo proteção avançada contra ameaças conhecidas e desconhecidas (Zero Day), bem como a resposta adequada em caso de incidentes cibernéticos em endpoints.

6.3.5. A CONTRATADA deverá documentar, implementar e validar todas as atividades sobre o serviço de Gerenciamento de Segurança Cibernética em Endpoints.

6.3.6. A CONTRATADA deverá gerenciar a solução de Proteção de Endpoints (NGAV + EDR), para executar as atividades do serviço de Gerenciamento de Segurança Cibernética em Endpoints na CONTRATANTE.

6.3.7. O serviço de Gerenciamento de Segurança Cibernética em Endpoints deverá contemplar todos os tipos de endpoints suportados pela solução de Proteção de Endpoints (NGAV + EDR).

6.3.8. A CONTRATADA deverá garantir que nenhum endpoint da CONTRATANTE fique descoberto da Solução de Proteção de Endpoints (NGAV + EDR), salvo em casos de licenciamento excedido.

6.3.9. A CONTRATADA deverá contemplar atuação proativa, por meio da administração e operação diária da solução e pelo contato entre as equipes técnicas da CONTRATANTE.

6.3.10. A CONTRATADA deverá monitorar continuamente a identificação e neutralização de ameaças cibernéticas nos endpoints da CONTRATANTE.

6.3.11. A CONTRATADA deverá realizar estudo aprofundado sobre ameaças e comportamentos suspeitos identificados e/ou neutralizados pela solução, validando se as ameaças e/ou comportamentos são legítimos ou falsos positivos.

6.3.12. A CONTRATADA deverá realizar a liberação de aplicações, arquivos e scripts específicos classificados como confiáveis pela CONTRATANTE ou pela análise de falsos positivos (política de lista branca – Whitelist).

6.3.13. A CONTRATADA deverá garantir o bloqueio do uso de unidades de armazenamentos removíveis via USB (Universal Serial Bus), realizando liberações exclusivamente solicitadas e autorizadas pela CONTRATANTE.

6.3.14. A CONTRATADA deverá atuar na contenção de ameaças identificadas pela solução, acionando a CONTRATANTE quando necessário.

6.3.15. A CONTRATADA deverá realizar análise forense dos eventos, identificando a anatomia da tentativa de ataque e coletando evidências expressivas para a resposta ao incidente.

6.3.16. A CONTRATADA deverá realizar diagnósticos completos nas superfícies de ataques cibernéticos dos endpoints, utilizando o framework MITRE ATT&CK.

6.3.17. Além do monitoramento e resposta a incidentes, o serviço de Gerenciamento de Segurança Cibernética em Endpoints, deverá contemplar as seguintes atividades recorrentemente:

6.3.17.1. A CONTRATADA deverá realizar a operação da Solução de Proteção de Endpoint (NGAV + EDR).

6.3.17.2. A CONTRATADA deverá realizar a definição, criação, implantação, personalização (tunning), exclusão e análise, ou qualquer outra atividade relacionada à manutenção das políticas e grupos de proteção aplicadas aos endpoints.

6.3.17.3. A CONTRATADA deverá realizar a definição, criação, implantação, personalização (tunning), exclusão e análise, ou qualquer outra atividade relacionada à manutenção das regras de bloqueio de comportamentos maliciosos no módulo de Detecção e Resposta em Endpoints (EDR).

6.3.17.4. A CONTRATADA deverá criar relatórios específicos sobre as informações contidas na Solução de Proteção de Endpoint (NGAV + EDR). A CONTRATANTE poderá exigir a criação de relatórios específicos para a CONTRATADA durante toda a vigência contratual.

6.3.17.5. A CONTRATADA deverá garantir o funcionamento ininterrupto dos agentes da Solução de Proteção de Endpoint (NGAV + EDR) instalados nos endpoints da CONTRATANTE.

6.3.17.6. A CONTRATADA deverá realizar o suporte da solução compreendendo ações corretivas, proativas e consultivas.

6.3.17.7. A CONTRATADA deverá analisar criticamente os registros de eventos da solução.

6.3.17.8. A CONTRATADA deverá gerenciar os usuários com acesso a solução e suas permissões.

6.3.17.9. A CONTRATADA deverá realizar testes de atualização dos agentes da solução antes de implementar nos endpoints.

6.3.17.10. A CONTRATADA deverá verificar e testar novas funcionalidades do produto em um ambiente de testes de sua propriedade e, posteriormente, aplicar na CONTRATANTE.

6.3.17.11. A CONTRATADA deverá monitorar o fim da vida útil da solução (End-of-life) e caso surgir alguma informação relacionada, comunicar a CONTRATANTE.

6.3.17.12. Além destas atividades, a CONTRATADA deverá realizar qualquer outra atividade pertinente para a realização do serviço.

6.3.18. A CONTRATADA deverá registrar através de chamados técnicos, todas as suas atividades relacionadas ao serviço de Gerenciamento de Segurança Cibernética em Endpoints.

6.3.19. A CONTRATADA deverá respeitar os seguintes Acordos de Níveis de Serviços (SLAs - Service Level Agreement) para atendimento/suporte sobre as solicitações realizadas pela CONTRATANTE e eventuais incidentes de segurança cibernética em endpoints:

SLAS PARA ABERTURAS DE CHAMADOS			
CRITICIDADE	SLA ATENDIMENTO	SLA RESOLUÇÃO	DESCRIÇÃO
URGENTE	15 Minutos	2 horas	- Chamado referente a incidentes de segurança da informação envolvendo ameaças cibernéticas que resultam a paralização TOTAL de endpoints classificados como críticos para a CONTRATANTE.
ALTA	30 Minutos	4 horas	- Chamado referente a incidentes de segurança da informação envolvendo ameaças cibernéticas que resultam a paralização PARCIAL de endpoints

SLAS PARA ABERTURAS DE CHAMADOS			
CRITICIDADE	SLA ATENDIMENTO	SLA RESOLUÇÃO	DESCRIÇÃO
			classificados como críticos para a CONTRATANTE. - Chamado referente a incidentes de segurança da informação envolvendo ameaças cibernéticas que resultam a paralização TOTAL de endpoints que não possuem criticidade para as operações da CONTRATANTE.
MÉDIA	1 Hora	6 horas	- Chamado referente a incidentes de segurança da informação envolvendo ameaças cibernéticas que NÃO resultam em impactos significativos para os endpoints da CONTRATANTE.
BAIXA	2 horas	24 horas	- Chamado referente a consultas técnicas, dúvidas e monitoramento.

6.3.19.1. Os prazos do Acordo de Níveis de Serviço poderão ser interrompidos nas seguintes situações:

6.3.19.1.1. Quando a CONTRATADA depender de retorno de informações por parte da CONTRATANTE para execução do atendimento.

6.3.19.1.2. Quando a ocorrência depender do retorno de informações da CONTRATADA mediante concordância da CONTRATANTE.

6.3.19.1.3. Quando o atendimento depender de agendamento para atendimento, onde for acordado data/hora entre CONTRATADA e CONTRATANTE.

6.3.19.2. Os status disponíveis para uso em Incidentes e Requisições são:

6.3.19.2.1. PAUSA do SLA mediante a justificativa:

6.3.19.2.1.1. Aguardando Fornecedor.

6.3.19.2.1.2. Aguardando Cliente/Usuário.

6.3.19.2.1.3. Agendado.

6.3.19.2.1.4. Em Homologação (somente para requisições).

6.3.19.2.2. Os status para RETOMADA do SLA mediante a justificativa:

6.3.19.2.2.1. Em Atendimento.

6.3.19.2.2.2. Encaminhado.

6.3.19.2.2.3. Homologado (somente para requisições).

6.3.19.2.2.4. Não Homologado (somente para requisições).

6.3.19.2.2.5. Reaberto.

6.3.19.3. Pausas e retomadas de tempo de atendimento só ocorrem quando tempo total não foi excedido.

6.3.19.4. É vedada a transferência do chamado, salvo, para correção de encaminhamento.

6.3.19.5. A CONTRATADA poderá realizar assentamentos ou resolver o chamado a qualquer momento, respeitando os níveis de SLA.

6.3.19.6. Após a resolução da Requisição ou Incidente pela CONTRADADA, a CONTRATANTE terá um prazo de 2 (dois) dias úteis para reabrir o chamado.

6.3.19.7. A reabertura da Requisição ou Incidente será considerada como continuação do atendimento anterior, ou seja, a contagem do prazo de atendimento será retomada e não haverá ônus financeiro para a CONTRATANTE em decorrência de uma possível caracterização de nova demanda.

6.3.19.8. Mensalmente, a CONTRATADA deverá enviar e, quando necessário, apresentar, pelo menos os seguintes relatórios em PDF:

6.3.19.8.1. Relatório executivo do serviço Gerenciamento de Segurança Cibernética em Endpoints durante o período, contendo pelo menos as seguintes informações:

6.3.19.8.1.1. Resumo do escopo do serviço.

6.3.19.8.1.2. Período contabilizado.

6.3.19.8.1.3. Total de ameaças bloqueadas durante o período, segmentadas por malwares, scripts maliciosos e exploração de memória.

6.3.19.8.1.4. Listagem de todas as ameaças detectadas no período.

6.3.19.8.1.5. Total de ameaças em lista branca (White – List) adicionados no período.

6.3.19.8.1.6. Quantidade de endpoints protegidos e desprotegidos (endpoints monitorados, mas que não possuem nenhuma política de proteção aplicada).

6.3.19.8.1.7. Listagem de endpoints desprotegidos.

6.3.19.8.1.8. Consumo de licenciamento da Solução de Proteção de Endpoint (NGAV + EDR).

6.3.19.8.1.9. Endpoints com maior número de ameaças bloqueadas.

6.3.19.8.1.10. Informações relacionadas as detecções realizadas pelo módulo de Detecção e Resposta em Endpoints (EDR).

6.3.19.8.2. Relatórios de chamados sobre as atividades relacionadas ao serviço de gerenciamento de proteção contra malwares e ataques cibernéticos em endpoints.

6.3.19.8.3. Entre outros relatórios relacionados ao serviço de Gerenciamento de Segurança Cibernética em Endpoints solicitados pela CONTRATANTE.

7. HABILITAÇÃO DA CONTRATADA

7.1. Para fins de habilitação, deverá o licitante comprovar os requisitos de habilitação jurídica, fiscal, social, trabalhista, qualificação econômico-financeira e técnica.

7.1.1. Justificativa para qualificação econômica-financeira: Por tratar-se de serviços de extrema relevância e necessidade para a CMVV, não apenas pelo volume financeiro envolvido, mas sobretudo em face das características do

serviço a ser prestado, cabe à Administração zelar para que seja contratado fornecedor apto a conduzir o contrato resultante desta licitação. Portanto, a boa comprovação financeira da licitante é uma discricionariedade concedida pela norma legal, dada a relevância da presente contratação

7.2. Habilitação Técnica

7.2.1. Justificativa: Por tratar-se de serviços de extrema relevância e necessidade para a CMVV, faz-se necessário as empresas CONTRATADAS demonstrarem por meio de atestados de capacidade técnica que já possuem experiência, em outras instituições públicas ou privadas na prestação dos serviços exigidos neste Edital, conforme qualificação técnica abaixo, incluindo a indicação da(s) parcela(s) de maior relevância técnica do objeto.

7.3. A LICITANTE deverá apresentar todos os documentos comprobatórios relacionados à qualificação técnica para a participação do certame.

7.4. Os documentos de habilitação técnica deverão ser encaminhados, concomitantemente com a proposta e demais documentos de habilitação até a data e horário definidos para a abertura da sessão pública.

7.5. A LICITANTE deverá apresentar os seguintes documentos relacionados à qualificação técnica:

7.5.1. Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto deste Termo de Referência, mediante a apresentação de atestado(s) ou declaração(ões) de capacidade técnica-operacional fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado.

7.5.1.1. O(s) atestado(s) ou declaração(ões) de capacidade técnica-operacional deve(rão) ser elaborado(s) em papel timbrado da(s) pessoa(s) jurídica(s) emissora(s) contendo, no mínimo, as seguintes informações:

7.5.1.1.1. Qualificação da pessoa jurídica emitente contendo razão social completa, CNPJ e endereço.

7.5.1.1.2. Nome, cargo, telefone e e-mail do signatário.

7.5.1.1.3. Data de início e término da prestação de serviços.

7.5.1.1.4. Descrição do escopo dos serviços prestados pela LICITANTE, de forma a comprovar as experiências nas atividades descritas. Esta descrição deverá conter dados que permitam o amplo entendimento dos trabalhos realizados para comparação com os requisitos exigidos por este Termo de Referência.

7.5.1.1.5. Número do contrato vinculado ao serviço atestado, bem como sua vigência.

7.5.1.1.6. Estes documentos, expedidos por pessoas jurídicas de direito público ou privado, em nome da LICITANTE, devem demonstrar que a LICITANTE executa ou tenha executado serviços compatíveis com este Termo de Referência, contemplando no mínimo 50% (cinquenta por cento) do quantitativo.

7.5.1.1.7. Justifica-se este percentual em razão da necessidade de comprovação da capacidade técnico operacional da licitante, diante da complexidade técnica do objeto, quantitativos e suas especificações, onde a potencial LICITANTE deverá comprovar sua aptidão para o desempenho de atividade pertinente e compatível em características, quantidades e prazos, no percentual de, pelo menos, 50% (cinquenta por cento) referente aos quantitativos constantes do quadro dos serviços.

7.5.1.2. Estes documentos, expedidos por pessoas jurídicas de direito público ou privado, em nome da LICITANTE, devem demonstrar que a LICITANTE executa ou tenha executado serviços compatíveis com este Termo de Referência, contemplando:

7.5.1.2.1. Prestação de serviços de Governança em Segurança e Privacidade da Informação.

7.5.1.2.2. Fornecimento de subscrição, implementação e suporte técnico da solução de Antivírus de Próxima Geração (NGAV), incluindo Detecção e Resposta em Endpoints (EDR).

7.5.1.2.3. Prestação de serviço gerenciado de segurança cibernética contemplando administração, gerenciamento de solução de Proteção de Endpoint (NGAV+EDR) e resposta a incidentes.

7.5.1.3. Os atestados ou declaração deverão referir-se a serviços executados nos últimos 2 (dois) anos em ambientes de complexidade similar às da CONTRATANTE.

7.5.1.4. Serão descartados os atestados que não tiverem relação ou similaridade aos requisitos deste Termo de Referência.

7.5.1.5. O(s) atestado(s) ou declaração(ões) técnica-operacional será(ão) desconsiderado(s) caso o emitente se recuse em prestar esclarecimentos e/ou fornecer documentos comprobatórios ou sofrer diligências.

7.5.1.6. No caso de atestado(s) ou declaração(ões) técnica-operacional emitidos por empresas privadas, não serão válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa LICITANTE. São consideradas como pertencentes ao mesmo grupo empresarial as empresas controladas ou controladoras da empresa LICITANTE, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócia ou possua vínculo com a empresa emitente ou empresa licitante.

7.5.2. Declaração facultativa da LICITANTE de conhecimento e vistoria técnica do local onde serão executados os serviços.

7.5.3. Declaração emitida e assinada pela fabricante das soluções especificadas neste Termo de Referência, comprovando que a LICITANTE possui autorização vigente para representar, comercializar, implementar e prestar suporte técnico especializado na devida solução ofertada.

7.5.4. Declaração da LICITANTE indicando os profissionais que atuarão na prestação dos serviços.

7.5.4.1. Os profissionais designados para exercer as atividades descritas neste Termo de Referência, deverão fazer parte do quadro de funcionários da empresa LICITANTE, não sendo aceitos recursos externos.

7.5.4.2. As comprovações dos profissionais deverão se dar mediante apresentação de cópias dos comprovantes de vínculo empregatício ou societário com a empresa LICITANTE.

7.5.4.3. Documentos comprobatórios de aptidão dos profissionais que prestarão os serviços, tais como cópias do currículo profissional, certificações oficiais e diplomas, atendendo no mínimo os itens e perfis dos profissionais citados abaixo:

7.5.4.3.1. Pelo menos 1 (um) profissional designado para a função de Gerente de Projetos, que será o líder e responsável pelas entregas previstas neste Termo de Referência, de modo a garantir a qualidade dos resultados e o atendimento aos requisitos e prazos estipulados, contendo:

7.5.4.3.1.1. Ensino superior completo nas áreas de administração de empresas, Tecnologia da Informação e/ou cursos a fins.

7.5.4.3.1.2. Pós-graduação em Gerenciamento de Projetos.

7.5.4.3.1.3. Certificação Project Management Professional (PMP) emitida pelo Project Management Institute (PMI).

7.5.4.3.2. Pelo menos 2 (dois) profissionais que serão responsáveis pela implementação, integrações, administração, gerenciamento e suporte técnico especializado sobre a solução de Proteção de Endpoint (NGAV + EDR), contendo:

7.5.4.3.2.1. Certificações válidas e oficiais emitidas pela fabricante da solução ofertada.

7.5.4.3.3. Pelo menos 2 (dois) profissionais designado para a função de Consultor em Privacidade de Dados Pessoais, contendo:

7.5.4.3.3.1. 2 (dois) anos de experiência como Encarregado pelo Tratamento de Dados Pessoais (DPO – Data Protection Officer).

7.5.4.3.3.1.1. Exclusivamente para este profissional, a comprovação de experiência como Encarregado de Dados Pessoais

deverá ser realizada através de atestado(s) ou declaração(ões) expedidos por pessoas jurídicas de direito público ou privado, em nome do PROFISSIONAL.

7.5.4.3.3.2. Ensino superior completo em Direito e cursos a fins.

7.5.4.3.3.3. Pós-Graduação em Direito Digital.

7.5.4.3.3.4. Certificação Data Protection Officer (DPO) emitida pela EXIN.

7.5.4.3.4. Pelo menos 1 (um) profissional designado para a função de Consultor em Segurança da Informação, contendo:

7.5.4.3.4.1. 3 (três) anos de experiência como consultor em Segurança da Informação.

7.5.4.3.4.2. Ensino superior completo na área de segurança da informação.

7.5.4.3.4.2.1. Na ausência de formação superior na área de segurança da informação, possuir graduação na área de tecnologia da informação e pós-graduação em segurança da informação/segurança cibernética.

7.5.4.3.4.3. Pelo menos uma das seguintes certificações:

7.5.4.3.4.3.1. ISC2 CISSP – Certified Information System Security Professional.

7.5.4.3.4.3.2. ISC2 ISSAP – Information System Security Architect Professional.

7.5.4.3.4.3.3. CompTIA Security+.

7.5.4.3.4.3.4. CISM – Certified Information Security Manager.

7.5.4.3.5. Pelo menos 1 (um) profissional designado para a função de Consultor em Sistema de Gestão de Segurança da Informação, contendo:

7.5.4.3.5.1. 3 (três) anos de experiência em consultoria em segurança da informação.

7.5.4.3.5.2. Ensino superior completo na área de segurança da informação.

7.5.4.3.5.2.1. Na ausência de formação superior na área de segurança da informação, possuir graduação na área de tecnologia da informação e pós-graduação em segurança da informação/segurança cibernética.

7.5.4.3.5.3. Pelo menos uma das seguintes certificações:

7.5.4.3.5.3.1. Certificação de formação de Auditor Interno em Sistema de Gestão de Segurança da Informação ISO/IEC 27001.

7.6. A CONTRATANTE poderá, a seu critério, solicitar esclarecimentos e/ou documentos comprobatórios e, ainda, efetuar diligências, a fim de verificar as informações apresentadas pela LICITANTE.

8. DA DOTAÇÃO ORÇAMENTÁRIA

8.1. Os recursos necessários ao pagamento das despesas decorrentes do objeto deste Pregão correrão a cargo das seguintes dotações orçamentárias e elementos de despesas:

01.01.00 - CAMARA MUNICIPAL
01.031.0001.2.001- MANUTENÇÃO DAS ATIVIDADES DA CÂMARA MUN. DE V
3.3.90.39.11 LOCAÇÃO DE SOFTWARES

9. OBRIGAÇÕES DA CONTRATADA

9.1. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade especificadas neste Termo de Referência e em sua proposta;

9.2. Reparar, corrigir, remover ou substituir às suas expensas, no total ou em parte, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução;

9.3. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto;

9.4. Utilizar empregados habilitados e com conhecimentos técnicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

9.5. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade à CONTRATANTE;

9.6. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a CONTRATADA relatar à CONTRATANTE toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;

9.7. Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração;

9.8. Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços, prestando os esclarecimentos que julgar necessários;

9.9. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto contratado.

9.10. Deter instalações, aparelhamento e pessoal técnico adequados e disponíveis para a realização do objeto contratado;

9.11. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato;

9.12. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato, abstendo-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca das atividades, objeto deste Termo de Referência, sem prévia autorização do CONTRATANTE;

9.13. Não transferir a outrem, no todo ou em parte, os serviços avençados, sem prévia e expressa anuência do CONTRATANTE;

9.14. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação;

10. OBRIGAÇÕES DA CONTRATANTE

10.1. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;

10.2. Proporcionar todas as condições necessárias ao bom andamento da prestação dos serviços contratados;

10.3. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

10.4. Notificar a CONTRATADA por escrito da ocorrência de eventuais

imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

10.5. Receber o objeto no prazo e condições estabelecidas, através do setor competente e atestar a Nota Fiscal/Fatura;

10.6. Verificar minuciosamente, no prazo fixado, a conformidade da prestação dos serviços recebidos;

10.7. Rejeitar, no todo ou em parte, os serviços realizados em desacordo com este Termo de Referência;

10.8. Pagar à CONTRATADA o valor resultante da prestação do serviço, no prazo e condições no Termo de Referência e proposta comercial;

10.9. Notificar, por escrito, a CONTRATADA, a disposição de aplicação de eventuais penalidades, garantido o contraditório e a ampla defesa.

11. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERANDO O CICLO DE VIDA DO OBJETO ("c", inc. XXIII, art. 6º)

11.1. A descrição da solução como um todo, encontra-se pormenorizada em tópicos específicos dos Estudos Técnicos Preliminares e neste Termo de Referência.

12. REQUISITOS DA CONTRATAÇÃO ("d", inc. XXIII, art. 6º)

12.1 Requisitos Gerais da Contratação

12.1.1 Os serviços serão prestados de acordo com as especificações, padrões técnicos de qualidade, de desempenho e de processos, na forma de serviços continuados, presenciais ou remotos, pagos após apuração do cumprimento dos níveis de serviço estabelecidos, conforme estabelecidos no Estudo Técnico Preliminar e neste Termo de Referência.

12.2 Da exigência da amostra

12.2.1 Não serão exigidas amostras;

12.3 Da exigência de carta de solidariedade

12.3.1 Não será exigida carta de solidariedade

12.4 Subcontratação

12.4.1 Não será admitida subcontratação do objeto contratual.

12.5. Sustentabilidade

12.5.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis

12.6. Garantia da Contratação

12.6.1 Não haverá exigência da garantia da contratação dos artigos 96 e seguintes da Lei nº 14.133, de 2021.

13. MODELO DE EXECUÇÃO DO OBJETO ("e", inc. XXIII, art. 6º)

O SETOR DEVERÁ DESCREVER MINIMAMENTE AS CONDIÇÕES DE EXECUÇÃO DO OBJETO

13.1. Condições de Entrega

13.1.1. O serviço será prestado na Sede da Câmara Municipal de Vila Velha, localizado na Rua Antônio Ataíde, 686, Centro – Vila Velha/ES, CEP 29.100-290;

13.1.2. A entrega dos produtos no local indicado pela CMVV ficará a cargo da CONTRATADA, a quem caberá providenciar o transporte e mão de obra necessária, sem qualquer ônus ao CONTRATANTE;

13.1.3. Os produtos deverão ser novos, não se admitindo, em hipótese alguma, o fornecimento de material alternativo, bem como atender às especificações técnicas exigidas e obedecer rigorosamente:

a) às especificações constantes neste Termo de Referência;
b) às normas da ABNT/INMETRO, conforme especificação e necessidade de cada produto;
c) às prescrições e recomendações dos fabricantes.

13.1.4. Verificada alguma irregularidade, o(s) produto(s) será(ão) devolvido(s), ficando o custo do transporte por conta da CONTRATADA, sem prejuízo da aplicação das penalidades cabíveis;

14. Dos Prazos de Entrega e Critérios De Recebimento

14.1. O prazo de entrega será de até **05 (cinco) dias úteis**, a contar do recebimento da Ordem de Fornecimento e cópia da Nota de Empenho, prorrogáveis por igual período, a critério da fiscalização, mediante solicitação encaminhada antes do vencimento do prazo e devidamente fundamentada e justificada pela CONTRATADA;

14.2. Na hipótese de a CONTRATADA solicitar nova prorrogação, a decisão caberá à Diretoria Administrativa.

14.3. Após a entrega, os produtos serão recebidos:

14.3.1 **PROVISORIAMENTE** pelo Setor de Almoxarifado e Patrimônio, tendo o prazo de **05 (cinco) dias úteis** para verificação da conformidade com as especificações e condições exigidas neste Termo de Referência;

14.3.2. O recebimento provisório dos materiais não implica em sua aceitação.

14.3.3 **DEFINITIVAMENTE** pelo Setor de Almoxarifado e Patrimônio, quando, depois de verificada a conformidade dos produtos, o servidor designado atestará no documento de entrega feito pela empresa o recebimento definitivo em condições satisfatórias, **no prazo máximo de 05 (cinco) dias úteis** a contar do recebimento provisório;

14.3.4 O recebimento definitivo dos produtos não exclui a responsabilidade da CONTRATADA pelo perfeito estado dos produtos fornecidos, cabendo-lhe sanar quaisquer irregularidades detectadas quando da sua utilização no período de garantia do produto.

14.3.5 Os produtos que estiverem em desacordo com as especificações exigidas nesta contratação, apresentarem vício de qualidade ou impropriedade para o uso serão recusados e devolvidos parcial ou totalmente, ficando a CONTRATADA obrigada a substituí-los no prazo de **até 05 (cinco) dias úteis**, contados da data de recebimento da notificação escrita, sem ônus para o CONTRATANTE, sob pena de incorrer em atraso quanto ao prazo de execução;

14.3.6. Durante o prazo de garantia, a CONTRATADA fica obrigada a reparar eventual defeito ou substituição, no prazo máximo de **até 05 (cinco) dias úteis**, a contar da data de notificação do defeito, sem ônus para o CONTRATANTE;

14.3.7. A recusa da CONTRATADA em substituir o(s) produto(s) reprovado(s) nos testes será considerada descumprimento contratual, ensejando a aplicação das penalidades previstas neste Termo de Referência.

15. MODELO DE GESTÃO DO CONTRATO ("f", inc. XXIII, art. 6º)

15.1. O Contrato ou o instrumento que o substituir, deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas previstas na lei, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

15.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato ou o instrumento que o substituir, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

15.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

15.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

15.5. As decisões e providências que ultrapassarem a competência do fiscal deverão ser solicitadas a seus superiores em tempo hábil para a adoção das medidas convenientes.

Preposto

15.6. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres

em relação à execução do objeto contratado, não havendo necessidade do mesmo permanecer nas instalações da Contratante.

15.7. A Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade.

Fiscalização

15.8. O fiscal do Contrato ou do instrumento acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração;

15.9. O fiscal comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual;

15.10. Caso ocorra descumprimento das obrigações contratuais, atuar tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;

Gestor do Contrato

15.11. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato, inclusive, quanto aos registros formais da execução no histórico de gerenciamento do contrato, prorrogações, etc;

15.12. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada;

15.13. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções.

16. DOS CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO ("g", inc. XXIII, art. 6º)

16.1. O recebimento relativo à prestação do serviço será realizado nos termos da Lei nº 14.133/2021.

16.2. O pagamento dos serviços efetivamente prestados, será efetuado em parcelas mensais, até 30 (trinta) dias após o encaminhamento da Nota Fiscal e do Relatório Técnico, devidamente atestados pelo Fiscal do Contrato.

16.3. Os pagamentos ficam condicionados à apresentação dos seguintes documentos juntamente com a Nota Fiscal:

i. Prova de Regularidade conjunta, referente aos Tributos Federais e à Dívida ativa da União, expedida pela Receita Federal do Brasil, de onde for sediada a empresa, devidamente válida.
ii. Prova de Regularidade com a Fazenda Pública do Estado onde for sediada a empresa, devidamente válida.
iii. Prova de Regularidade com a Fazenda Pública do Estado do Espírito Santo, devidamente válida.
iv. Prova de Regularidade com a Fazenda Pública do Município onde for sediada a empresa, devidamente válida.
v. Prova de Regularidade com a Fazenda Pública Municipal do Município de Vila Velha, devidamente válida.
vi. Prova de Regularidade perante o Fundo de Garantia por Tempo de Serviço – FGTS, devidamente válida.
vii. Certidão Negativa Trabalhista.

16.4. Ocorrendo erros na apresentação do(s) Documento(s) Fiscal(ais), ou outra circunstância impeditiva, o(s) mesmo(s) será(ão) devolvido(s) ao responsável técnico da empresa vencedora para correção, sendo que o recebimento definitivo será suspenso, ficando estabelecido que o prazo para pagamento será contado a partir da data de apresentação do novo Documento Fiscal, devidamente corrigido.

17. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR ("h", inc. XXIII, art. 6º)

17.1. Forma de seleção e critério de julgamento da proposta:

a) O fornecedor será selecionado por meio da realização de procedimento de licitatório via Pregão Eletrônico, com adoção do critério de julgamento pelo MENOR VALOR GLOBAL POR LOTE, com fundamento na Lei n.º 14.133/2021.

18. ESTIMATIVAS DO VALOR DE CONTRATAÇÃO ("i", inc. XXIII, art. 6º)

18.1. O custo estimado total da contratação é de R$ 561.600,00 (quinhentos e sessenta e um mil, seiscentos reais, conforme custos apostos no mapa comparativo de preços;

18.2 O valor aceito para contratação deverá estar compatível com o valor de mercado;

18.3 O valor estimado constante neste Termo de Referência foi obtido através de pesquisa mercadológica, expresso no Mapa Comparativo de Preço e documentos que o acompanham.

18.4 Será considerada vencedora a **proposta mais vantajosa**, desde que a empresa ofertante comprove sua regularidade com os encargos trabalhistas, previdenciários, fiscais e comerciais, e tenha como cumprir os prazos e

condições estabelecidos neste Termo de Referência;

Na proposta de preço devem estar incluídos todos os custos e despesas decorrentes da prestação do serviço;

19.ELABORAÇÃO DO TERMO DE REFERÊNCIA

19.1 O Termo de Referência foi elaborado pelo servidor Carlos Hudson Cipreste, lotado no Setor da Tecnologia da Informação.

26/11/2024, Vila Velha – Espirito Santo

Carlos Hudson C Cipreste
Chefe do Departamento de Tecnologia da Informação

TERMO DE REFERÊNCIA APROVADO:

FICA APROVO o conteúdo do presente Termo de Referência. Outrossim, atendidos todos os requisitos legais e administrativos, fica AUTORIZADO os procedimentos para a aquisição que se pretende.

Bruno Lorenzutti
Presidente da Câmara Municipal de Vila Velha

PROTOCOLO DE ASSINATURA(S)

O documento acima foi assinado eletronicamente e pode ser acessado no endereço https://vilavelha.splonline.com.br/autenticidade utilizando o identificador 3200320037003300310003A00540052004100

Assinado eletronicamente por **CARLOS HUDSON DA CONCEIÇÃO CIPRESTE** em **26/11/2024 17:56**
Checksum: **B1A79A450885D3789011A089CB4C27428C537F6541BB14DC3AA2914D0A8A1048**

Assinado eletronicamente por **VEREADOR BRUNO LORENZUTTI** em **26/11/2024 17:58**
Checksum: **E1B8DB3BEC10B15FD87B768E8965DCEABD5BC27276F4D624B2F6F97207F91205**