ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

ESTUDOS TÉCNICOS PRELIMINARES - ETP

AQSETIN2023010 - Segurança de Endpoint
PAC: TJCESETIN_2024_0011

1. INTRODUÇÃO

1.1. Este documento tem como finalidade de identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda (DOD), bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

1.2. Com o crescente aumento de ameaças cibernéticas, é imprescindível que o Tribunal de Justiça do Ceará (TJCE) adote medidas de segurança para proteger seus sistemas e dados. A utilização de uma solução de segurança de endpoint é uma medida fundamental para mitigar o risco de ataques cibernéticos.

2. CONTEXTUALIZAÇÃO DA DEMANDA

2.1. **Endpoint.**

2.1.1. Em termos simples, um Endpoint é qualquer dispositivo final que esteja conectado a uma rede de computadores. Esses dispositivos atuam como pontos de acesso para os usuários interagirem com a rede e seus recursos. Tipos de Endpoints:

2.1.1.1. Computadores Desktop e Laptops: São os dispositivos mais comuns usados pelos usuários para acessar a rede e realizar tarefas como navegação na web, criação de documentos e envio de emails.

2.1.1.2. Smartphones e Tablets: Dispositivos móveis que oferecem acesso à rede e a uma variedade de aplicativos, permitindo que os usuários permaneçam conectados e produtivos em movimento.

2.1.1.3. Servidores: Embora sejam frequentemente considerados como recursos da rede, os servidores também podem ser considerados Endpoints, pois fornecem serviços e recursos para outros dispositivos na rede.

2.1.2. Dispositivos de IoT (Internet das Coisas): Dispositivos como câmeras de segurança, termostatos inteligentes e dispositivos médicos conectados à Internet são considerados Endpoints, pois se comunicam com a rede para enviar e receber dados.

2.1.3. Características dos Endpoints:

2.1.3.1. Conectividade: Os Endpoints são capazes de se conectar à rede, seja por meio de conexões com fio (como Ethernet) ou sem fio (como Wi-Fi ou Bluetooth).

2.1.3.2. Processamento de Dados: Muitos Endpoints possuem capacidade de processamento de dados, permitindo que executem aplicativos e realizem tarefas sem depender de um servidor central.

2.1.3.3. Armazenamento de Dados: Alguns Endpoints possuem armazenamento interno, permitindo que armazenem dados localmente. Isso é comum em computadores desktop, laptops, smartphones e tablets.

2.1.3.4. Interatividade: Os usuários interagem diretamente com os Endpoints por meio de interfaces de usuário, como teclados, telas sensíveis ao toque e dispositivos de entrada.

2.1.3.5. Segurança: A segurança dos Endpoints é uma preocupação importante, pois são frequentemente alvos de ataques cibernéticos. Medidas de segurança, como antivírus, firewalls e autenticação de usuários, são comumente implementadas para protegê-los.

2.1.4. Um Endpoint é qualquer dispositivo final conectado a uma rede de computadores, incluindo computadores, dispositivos móveis, servidores e dispositivos de IoT. Eles possuem várias características, como conectividade, processamento de dados, armazenamento de dados, interatividade e segurança,

que os tornam componentes essenciais em uma rede de computadores.

2.1.5. Endpoint Servidores.

2.1.5.1. Endpoint servidores são dispositivos de computação que desempenham um papel central na infraestrutura de rede de uma organização. Ao contrário dos endpoints tradicionais, como computadores desktop e laptops, que são usados por usuários finais, os servidores são projetados para fornecer serviços, armazenar dados e gerenciar recursos de rede. Existem diferentes tipos de servidores, cada um com suas próprias características e funções específicas:

2.1.5.1.1. Servidores de Arquivos: Esses servidores são responsáveis por armazenar e compartilhar arquivos e dados dentro de uma rede. Eles permitem que os usuários acessem e compartilhem documentos, imagens, vídeos e outros tipos de arquivos de forma centralizada e segura.

2.1.5.1.2. Servidores de Aplicativos: Esses servidores hospedam aplicativos e softwares usados pela organização. Eles fornecem recursos computacionais e de armazenamento necessários para executar aplicativos de negócios, como sistemas de gerenciamento de banco de dados, sistemas de gerenciamento de conteúdo e aplicativos de produtividade.

2.1.5.1.3. Servidores Web: Os servidores web hospedam sites e aplicativos web acessíveis pela internet. Eles respondem a solicitações de clientes da web, fornecendo conteúdo estático e dinâmico, como páginas da web, imagens e vídeos, de forma rápida e eficiente.

2.1.5.1.4. Servidores de Banco de Dados: Esses servidores armazenam e gerenciam grandes volumes de dados estruturados e organizados em bancos de dados. Eles oferecem acesso seguro e rápido aos dados para aplicativos e usuários autorizados, garantindo integridade e confiabilidade dos dados.

2.1.5.1.5. Servidores de Email: Os servidores de email gerenciam o envio, recebimento e armazenamento de mensagens de email dentro de uma organização. Eles também podem fornecer recursos adicionais, como filtragem de spam, criptografia de email e colaboração em grupo.

2.1.5.2. As características comuns dos endpoints servidores incluem alta disponibilidade, escalabilidade, segurança avançada e capacidade de

gerenciamento remoto. Esses dispositivos são essenciais para o funcionamento eficiente e seguro de uma organização, e qualquer interrupção ou comprometimento de sua segurança pode ter impactos significativos nos negócios.

2.2. **Segurança da Tecnologia da Informação.**

2.2.1. No mundo digitalizado atual, a segurança da informação e a cibersegurança desempenham um papel crucial na proteção de dados e sistemas contra ameaças virtuais. Esses campos abrangem uma ampla gama de práticas, técnicas e medidas destinadas a garantir a confidencialidade, integridade e disponibilidade das informações, bem como a proteção contra ataques cibernéticos maliciosos.

2.2.2. Segurança da Informação.

2.2.2.1. A segurança da informação é o conjunto de medidas destinadas a proteger as informações de uma organização contra acesso não autorizado, uso indevido, divulgação, interrupção, modificação ou destruição. Seu principal objetivo é garantir que as informações sejam acessadas apenas por indivíduos autorizados e que permaneçam íntegras e disponíveis quando necessário.

2.2.2.2. Princípios da Segurança da Informação:

2.2.2.2.1. Confidencialidade: Garante que as informações só sejam acessadas por pessoas autorizadas. Isso é geralmente alcançado por meio de técnicas como criptografia e controle de acesso.

2.2.2.2.2. Integridade: Assegura que as informações não sejam alteradas de forma não autorizada. Métodos como assinaturas digitais e controles de versão são usados para manter a integridade dos dados.

2.2.2.2.3. Disponibilidade: Garante que as informações estejam acessíveis quando necessário. Isso envolve a implementação de medidas para prevenir interrupções no acesso, como redundância de sistemas e backups regulares.

2.2.2.2.4. Autenticidade: Garante a veracidade e a autenticidade das informações e das fontes que as fornecem. Mecanismos como autenticação de usuários e certificados digitais são usados para garantir a autenticidade das informações.

2.2.2.2.5. Não-repúdio: Garante que uma pessoa não possa negar a autoria ou envolvimento em uma transação. Isso é alcançado através de técnicas como registros de auditoria e assinaturas digitais.

2.2.3. Cibersegurança.

2.2.3.1. A cibersegurança é um ramo específico da segurança da informação que se concentra na proteção dos sistemas de informação contra ataques cibernéticos. Isso inclui a prevenção, detecção e resposta a ameaças e violações de dados.

2.2.3.2. Principais Componentes da Cibersegurança:

2.2.3.2.1. Proteção Perimetral: Implementação de firewalls, filtros de conteúdo e sistemas de detecção de intrusão para proteger a rede contra acesso não autorizado.

2.2.3.2.2. Segurança de Endpoint: Proteção dos dispositivos finais, como computadores, laptops e dispositivos móveis, contra ameaças como vírus, malware e ransomware.

2.2.3.2.3. Gestão de Identidade e Acesso: Controle de acesso aos sistemas e informações por meio de autenticação multifatorial, políticas de senha robustas e gerenciamento de identidades.

2.2.3.2.4. Monitoramento e Análise de Logs: Acompanhamento contínuo das atividades de rede e sistemas para detectar e responder a ameaças em tempo real.

2.2.3.2.5. Resposta a Incidentes: Desenvolvimento e implementação de planos de resposta a incidentes para lidar com violações de segurança de forma eficaz e minimizar o impacto.

2.2.4. Segurança de Dados.

2.2.4.1. A segurança de dados é um componente essencial tanto da segurança da informação quanto da cibersegurança. Envolve a proteção dos dados contra acesso não autorizado, uso indevido, divulgação ou destruição, seja em repouso, em trânsito ou em uso.

2.2.4.2. Principais Práticas de Segurança de Dados:

2.2.4.2.1. Criptografia: Transformação dos dados em formato ilegível, que só pode ser decifrado com uma chave específica, garantindo assim a confidencialidade das informações.

2.2.4.2.2. Controle de Acesso: Restrição do acesso aos dados apenas a usuários autorizados, por meio de autenticação, autorização e políticas de privacidade.

2.2.4.2.3. Backup e Recuperação: Cópia de segurança regular dos dados e implementação de planos de recuperação de desastres para garantir a disponibilidade e integridade das informações em caso de falha ou ataque.

2.2.4.2.4. Máscaras de Dados: Substituição de informações sensíveis por dados fictícios em ambientes de teste ou desenvolvimento para proteger a privacidade e a confidencialidade dos dados reais.

2.2.4.2.5. Gerenciamento de Vulnerabilidades: Identificação e correção de falhas de segurança nos sistemas e aplicativos que podem ser exploradas por invasores para acessar dados sensíveis.

2.2.5. A segurança da informação, a cibersegurança e a segurança de dados são áreas interconectadas que visam proteger os ativos mais valiosos de uma organização: suas informações. A implementação eficaz de medidas de segurança nessas áreas é essencial para garantir a confidencialidade, integridade e disponibilidade dos dados, bem como para proteger contra ameaças cibernéticas em um ambiente digital cada vez mais complexo e interconectado.

2.2.6. Diferentes tipos de ameaças representam variados desafios para a segurança da informação, exigindo estratégias específicas de defesa. Alguns desses tipos de ameaças e vulnerabilidades mais comuns:

2.2.6.1. Malware: Este termo abrange uma variedade de software malicioso, incluindo vírus, worms, trojans, ransomware e spyware. O malware é projetado para danificar, controlar ou roubar informações de um sistema ou dispositivo.

2.2.6.1.1. Vírus: Um vírus é um programa de computador que se replica e se espalha, geralmente anexado a arquivos legítimos. Quando esses arquivos são executados, o vírus infecta o sistema e pode causar danos, como a exclusão de arquivos ou a corrupção de dados.

2.2.6.1.2. Worms: Diferentemente dos vírus, os worms não precisam de um

arquivo hospedeiro para se espalhar. Eles se propagam por redes, explorando vulnerabilidades em sistemas conectados e enviando cópias de si mesmos para outros dispositivos.

2.2.6.1.3. Trojans: Também conhecidos como cavalos de Troia, os trojans são programas maliciosos disfarçados de software legítimo. Eles geralmente são baixados e instalados pelos usuários sem o seu conhecimento e podem conceder acesso remoto ao computador, roubar informações confidenciais ou abrir uma porta dos fundos para ataques futuros.

2.2.6.1.4. Ransomware: Este tipo de malware criptografa os arquivos de um sistema ou dispositivo e exige um pagamento (geralmente em criptomoedas) para restaurar o acesso aos dados. O ransomware pode se espalhar rapidamente e causar danos significativos, afetando desde usuários individuais até grandes organizações.

2.2.6.1.5. Spyware: O spyware é projetado para monitorar as atividades do usuário, como histórico de navegação, teclas digitadas e informações pessoais, sem o seu conhecimento ou consentimento. Esses dados são frequentemente usados para fins de marketing direcionado, roubo de identidade ou espionagem cibernética.

2.2.6.1.6. Engenharia Social: A engenharia social é uma técnica utilizada para manipular pessoas a fim de obter informações confidenciais ou acesso não autorizado a sistemas e redes. Isso pode envolver a criação de pretextos convincentes, como telefonemas falsos, e-mails fraudulentos ou até mesmo invasões físicas a escritórios.

2.2.6.1.7. Phishing: Esta é uma técnica de engenharia social que visa enganar os usuários para que divulguem informações pessoais, como senhas, números de cartão de crédito ou informações de login, geralmente por meio de e-mails, mensagens instantâneas ou sites falsos que se passam por entidades confiáveis.

2.2.6.1.8. Ataques à Infraestrutura: Estes ataques visam comprometer a infraestrutura de TI de uma organização, incluindo servidores, redes e sistemas críticos. Exemplos incluem ataques de negação de serviço (DoS) e ataques de injeção de SQL, que exploram vulnerabilidades em aplicativos da web para acessar ou manipular bancos de dados.

2.2.6.2. O vazamento de dados, a violação de dados, a exfiltração de dados e o sequestro de dados são termos frequentemente utilizados no contexto da segurança da informação, cada um com seus significados distintos, embora relacionados.

2.2.6.3. Um vazamento de dados ocorre quando informações confidenciais são expostas acidentalmente devido a falhas de segurança, sejam elas técnicas ou processuais.

2.2.6.4. Por sua vez, uma violação de dados ocorre quando há acesso não autorizado a informações confidenciais ou sigilosas por parte de um indivíduo não autorizado.

2.2.6.5. Já a exfiltração de dados refere-se ao ato de roubar informações de forma discreta. Isso geralmente ocorre após um vazamento ou violação de dados, mas nem toda violação leva à exfiltração. Os dados só são exfiltrados quando são copiados ou movidos para outro dispositivo sob o controle do invasor.

2.2.6.6. Além disso, o sequestro de dados é uma ameaça em que os dados são criptografados ou bloqueados por um invasor, que exige o pagamento de um resgate para restaurar o acesso aos dados. Esse tipo de ataque é comum em casos de ransomware, em que os dados são "sequestrados" até que a vítima pague o valor exigido pelo invasor.

2.2.6.7. É importante compreender essas distinções para implementar medidas eficazes de segurança cibernética e lidar adequadamente com incidentes de segurança.

2.3. **Visão geral sobre as tendências de cibersegurança.**

2.3.1. Os relatórios divulgados por diversas empresas especializadas em segurança cibernética revelam uma visão abrangente das tendências de cibersegurança em 2022 e 2023, destacando o aumento significativo e a diversificação dos ataques cibernéticos em todo o mundo:

2.3.1.1. A Fortinet divulgou os números totais de ataques cibernéticos do ano de 2022, levantados pelo FortiGuard Labs, seu laboratório de inteligência e análise de ameaças. O Brasil foi o segundo país mais atingido da América Latina, com 103,16 bilhões de tentativas de ataques

cibernéticos, um aumento de 16% com relação a 2021 (com 88,5 bilhões). O país ficou atrás do México (com 187 bilhões) e foi seguido por Colômbia (20 bilhões) e Peru (15,4 bilhões). O total da América Latina e Caribe foi de mais de 360 bilhões de tentativas de ciberataques em 2022.

2.3.1.2. Na comparação entre o último trimestre do ano e o anterior, houve um aumento de 61,7% no número de tentativas de ataques cibernéticos sofridas pelo país. Nos meses de outubro, novembro e dezembro de 2022 foram 30,4 bilhões, contra 18,8 bilhões em julho, agosto e setembro do mesmo ano.

2.3.1.3. Dentre esses ataques, existem algumas abordagens que merecem destaque, como é o caso dos ataques de ransomware. Esse tipo de ataque sequestra as informações confidenciais e exige o pagamento de um valor, geralmente em bitcoins, para que esses dados possam ser devolvidos. Além de causar um grande prejuízo financeiro, esses ataques também demonstram que a empresa não está preparada para lidar com informações confidenciais.

2.3.1.4. Em 2022 os ataques de ransomware sofreram um aumento de 51%, colocando o Brasil na primeira colocação como país que mais sofreu ataques cibernéticos na América Latina. Além dessa ameaça, uma estratégia bastante utilizada que também continua fazendo vítimas é o ataque de phishing, que pode ser aplicado sem recursos sofisticados e causar prejuízos imensuráveis para os usuários e as empresas.

2.3.1.5. O relatório Fast Facts de março de 2023 da Trend Micro revela aumento no número de ataques cibernéticos no primeiro trimestre do ano de 2023, o que representa ameaça considerável à segurança de sistemas e redes de computadores. O mês de março teve o maior número de ataques de 2023, até o momento – 15,8 bilhões -, fechando o trimestre com 43,3 bilhões de ameaças detectadas: um aumento de 31% em relação ao mesmo período do ano de 2022.

2.3.1.6. Além do aumento geral de ataques em março 2023, de 12% em relação ao mês anterior, a taxa de detecção de arquivos também foi a maior no início de 2023, com o bloqueio de 8 bilhões, 850 mil arquivos maliciosos, pouco mais de 1 bilhão e 250 mil a mais do que em fevereiro

2023.

2.3.1.7. Em março 2023, a Tailândia manteve a primeira posição no ranking de países mais atingidos por ransomware (46,1%), seguida pelos Estados Unidos, que tiveram 14,1% das ameaças, Taiwan e Turquia, com 8,6% e 4,3%, respectivamente. O Japão, com 2,7% dos registros, completa o top 5.

2.3.1.8. No Brasil, o setor governamental continua sendo o mais atacado pelo cibercrime, seguido pelos segmentos de educação, tecnologia e saúde.

2.3.1.9. O Brasil também continua sendo o país que mais envia ameaças de extorsão e sextorsão (do termo em inglês sextorsion), que é a chantagem sexual, apresentando 836 registros contra 809 dos Estados Unidos. Esse tipo de ataque apresentou queda considerável em março de 2023, já que tinham sido registrados, no país, em janeiro de 2023, 1.096 casos e 1.845 em fevereiro de 2023. O estudo tem como base endereços de IP únicos."

2.3.1.10. A Check Point Research (CPR), divisão de Inteligência em Ameaças da Check Point Software, alerta que 10% das empresas em todo o mundo sofreram ataques de ransomware, indicando um aumento de 33% em 2023 em relação ao ano de 2022, quando uma em cada 13 organizações sofreu tais ataques.

2.3.1.11. Globalmente, ao longo de 2023, as organizações experimentaram ainda, em média, mais de 60 mil ataques cibernéticos em geral, totalizando 1.158 ataques por organização por semana, um aumento de 1% nos ciberataques, mantendo o aumento significativo observado nos anos anteriores, indicando uma tendência contínua e preocupante no cenário de ameaças digitais.

2.3.1.12. A SonicWall, líder global em segurança cibernética, publicou o Relatório Anual de Ameaças Cibernéticas 2024. Identificou 293.989 variantes de malware Zero day ‘nunca vistas antes’, numa média de 805 por dia.

2.3.2. Aumento de Ciberataques: Nos últimos anos, temos observado um aumento significativo no número e na complexidade dos ataques cibernéticos em todo o mundo, e o Brasil não é exceção. Os ataques podem variar desde malware comum, como vírus e ransomware, até ataques mais sofisticados, como phishing e

ataques de negação de serviço (DoS).

2.3.3. Setores Alvo: Os setores mais visados pelos cibercriminosos incluem instituições financeiras, empresas de tecnologia, governo, saúde e varejo. Esses setores lidam com grandes volumes de dados sensíveis e financeiros, tornando-os alvos atrativos para hackers em busca de lucro ou informações valiosas.

2.3.4. Ransomware em Ascensão: O ransomware tem sido uma das formas mais prevalentes de ataque cibernético nos últimos anos. Os cibercriminosos utilizam malware para criptografar os dados das vítimas e exigem um resgate em troca da chave de descriptografia. Empresas e organizações de todos os tamanhos têm sido alvo desse tipo de ataque, e o Brasil não é exceção.

2.3.5. Vulnerabilidades de Software e Sistemas Desatualizados: Muitos ataques exploram vulnerabilidades conhecidas em software e sistemas desatualizados. Empresas e usuários individuais que não aplicam patches de segurança regularmente estão em maior risco de serem comprometidos por esses tipos de ataques.

2.3.6. Aumento do Uso de Dispositivos Conectados: Com o avanço da Internet das Coisas (IoT), mais dispositivos estão conectados à internet do que nunca. Isso inclui dispositivos domésticos inteligentes, como câmeras de segurança, termostatos e eletrodomésticos. Infelizmente, muitos desses dispositivos têm falhas de segurança, o que os torna vulneráveis a ataques.

2.3.7. Maior Conscientização e Investimento em Segurança Cibernética: Com o aumento das ameaças digitais, empresas, organizações e indivíduos estão se tornando mais conscientes da importância da segurança cibernética. Isso tem levado a um aumento nos investimentos em tecnologias de segurança, treinamento de pessoal e conscientização sobre cibersegurança.

2.4. **Ataques a Tribunais no Brasil.**

2.4.1. No período entre novembro de 2020 e abril de 2022, os tribunais brasileiros enfrentaram 13 ataques cibernéticos perpetrados por hackers, resultando na paralisação das atividades e causando transtornos significativos para advogados e a população em geral. Isso equivale a uma média de um ataque a cada 41 dias.

2.4.2. As invasões aos sistemas de dados e informações ocorreram em vários estados, incluindo São Paulo, Distrito Federal, Pernambuco, Rio Grande do Sul e

Espírito Santo, e afetaram diferentes instâncias judiciais, desde as cortes federais, criminais e eleitorais até as estaduais e do Trabalho. No entanto, os principais alvos foram as cortes superiores, como o Supremo Tribunal Federal, o Superior Tribunal de Justiça e o Tribunal Superior Eleitoral (TSE).

2.4.3. Essa estatística revela uma situação alarmante, uma vez que as bases de dados dos tribunais ficam expostas aos invasores, resultando na inacessibilidade dos serviços prestados tanto para advogados quanto para os cidadãos. Esses ataques causaram atrasos significativos e o adiamento de julgamentos e procedimentos judiciais.

2.4.4. Por exemplo, após um ataque hacker em 30/03/2022, os sistemas do Tribunal Regional Federal da 3ª Região ficaram fora do ar por mais de uma semana. Isso ocorreu em um momento em que o TRF-3 estava prestes a cumprir o prazo constitucional da expedição de precatórios, levando ao adiamento dessa data crucial. Os hackers conseguiram paralisar os sistemas do tribunal federal, afetando ferramentas essenciais como a elaboração de minutas, conferência de dados pelas partes e transmissão de ordens de pagamento de precatórios.

2.4.5. Nos últimos anos, o Brasil tem enfrentado uma série de ataques cibernéticos que visam comprometer a segurança e a operacionalidade dos tribunais e órgãos do poder judiciário. Vamos examinar esses incidentes em ordem cronológica:

2.4.5.1. Novembro de 2020: O Superior Tribunal de Justiça (STJ), em Brasília, foi alvo de um dos maiores ataques de ransomware contra um órgão de Estado no país. O ataque paralisou suas atividades e interrompeu diversos julgamentos que estavam ocorrendo simultaneamente.

2.4.5.2. Janeiro de 2021: O Tribunal Regional Federal da 3ª Região (TRF-3), sediado em São Paulo, foi alvo de um ataque hacker com o objetivo de levar à absolvição de um réu e ao envio de uma quantia considerável em dinheiro.

2.4.5.3. Abril de 2021: O Tribunal de Justiça do Rio Grande do Sul sofreu um ataque cibernético de ransomware, resultando em instabilidade nos sistemas de informática em todo o estado. Cerca de 18 mil computadores foram afetados.

2.4.5.4. Novembro de 2021: O Tribunal de Justiça do Amazonas (TJAM)

confirmou ter sido alvo de hackers, resultando em perturbações nos sistemas de informática.

2.4.5.5. Março de 2022: O Tribunal Regional Federal da 3ª Região (TRF-3) foi novamente atacado, levando à suspensão de suas atividades. Os hackers buscavam forjar assinaturas de juízes em busca de benefício econômico.

2.4.5.6. Julho de 2022: O Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT) foi alvo de um suposto ataque hacker, resultando em quatro dias de instabilidade nos sistemas e na modificação do expediente do órgão.

2.4.5.7. Março de 2023: Um ataque hacker à Ordem dos Advogados do Brasil (OAB) nacional teve efeito-dominó no Tribunal de Justiça de São Paulo, resultando na indisponibilidade dos serviços do Portal e-SAJ.

2.4.5.8. Janeiro de 2023: O Conselho Nacional de Justiça (CNJ) sofreu uma invasão aos seus sistemas, com a inserção de documentos falsos no Banco Nacional de Mandados de Prisão.

2.4.5.9. Janeiro de 2024: O Tribunal de Justiça do Tocantins enfrentou uma tentativa de ataque cibernético, resultando na indisponibilidade de seu site durante parte do dia.

2.4.6. As consequências desses ataques vão além da interrupção das atividades diárias; elas afetam diretamente a confiança no sistema de justiça e o acesso dos cidadãos à justiça de forma eficiente e segura.

2.5. **Tecnologia no Tribunal de Justiça do Ceará.**

2.5.1. O Tribunal de Justiça do Ceará (TJCE), ao longo de seus 150 anos de história, tem se destacado pelos avanços tecnológicos e inovações que têm implementado. Desde a implementação do Sistema de Automação da Justiça (SAJ) em 2009, até a digitalização completa dos processos em 2019, o Judiciário cearense tem buscado acompanhar a evolução da tecnologia para melhorar os serviços oferecidos aos cidadãos.

2.5.2. Um dos marcos mais importantes foi a introdução do Processo Judicial Eletrônico (PJe) em 2014, que otimizou o fluxo de trabalho no tribunal e facilitou a vida dos profissionais do Direito. Durante a pandemia de Covid-19, o TJCE

adotou o regime obrigatório de teletrabalho e implementou o "Balcão Virtual" em 2021, seguindo as diretrizes do Conselho Nacional de Justiça (CNJ). Este serviço digital oferece uma ampla gama de serviços, incluindo informações processuais e funcionamento das unidades judiciárias, promovendo o contato imediato por meio de videoconferência.

2.5.3. Com a digitalização dos processos e a implementação de iniciativas como o teletrabalho, Balcão Virtual e o Juízo 100% Digital, a tecnologia da informação tornou-se um componente crucial no funcionamento do tribunal, garantindo maior agilidade, eficiência e acessibilidade aos serviços judiciais para os cidadãos do Ceará.

2.6. **Segurança da Informação do TJCE.**

2.6.1. No cenário atual de avanço tecnológico, torna-se cada vez mais evidente a necessidade urgente de garantir a segurança dos computadores desktop, laptops, servidores, dispositivos móveis e sistemas utilizados pelos colaboradores do Tribunal de Justiça do Ceará (TJCE).

2.6.2. Com a digitalização de todos os processos judiciais e administrativos, a segurança da informação se tornou um elemento crítico para a manutenção da operacionalidade do tribunal e a proteção das informações confidenciais e sensíveis armazenadas.

2.6.3. O escopo da análise do ambiente de segurança de TI abrange todas as medidas relacionadas à segurança da tecnologia da informação dentro de uma organização, incluindo gerenciamento de identidade e acesso, proteção da rede, segurança dos dispositivos terminais, proteção dos dados, segurança dos aplicativos, gerenciamento de vulnerabilidades e análise de segurança, bem como governança, gestão de riscos e conformidade com regulamentações.

2.6.4. Para o Tribunal de Justiça do Ceará (TJCE), uma solução completa de segurança de TI atua como um escudo digital, integrando uma série de sistemas e tecnologias. Alguns dos principais sistemas incluem:

2.6.4.1. Firewalls de Próxima Geração (Palo Alto Networks): Monitoram, analisam e filtram o tráfego de rede, detectando e detentendo ataques maliciosos.

2.6.4.2. Firewall de Aplicativos Web (WAF) (Citrix NetScaler): Filtra e

bloqueia o tráfego HTTP suspeito para proteger aplicativos e sites da Web.

2.6.4.3. Proxy Reverso (Citrix NetScaler): Balanceia a carga de tráfego e aprimora a segurança de aplicativos da Web.

2.6.4.4. Soluções de Segurança de Endpoint (Kaspersky Endpoint Security): Protegem dispositivos finais contra malware, como vírus e cavalos de Troia.

2.6.4.5. Soluções de Segurança de Email (Microsoft 365): Protegem contra ameaças cibernéticas em e-mails, como phishing e malware.

2.6.4.6. Soluções de Gerenciamento de Vulnerabilidades (Tenable): Detectam e priorizam vulnerabilidades nos sistemas e aplicativos, permitindo correções eficazes.

2.6.4.7. Soluções de Backup e Recuperação de Dados (Veeam): Garantem que os dados sejam armazenados de forma segura, permitindo rápida recuperação em caso de perda.

2.6.5. Juntos, esses sistemas formam uma defesa digital robusta, garantindo que o TJCE esteja protegido contra as ameaças cibernéticas em constante evolução.

2.6.6. No ambiente do Tribunal de Justiça do Ceará (TJCE), o volume de tráfego de dados é bastante significativo, variando entre 6 e 23 terabytes (TB) diariamente. Essa quantidade expressiva de dados em trânsito reflete a intensidade das atividades e operações digitais que ocorrem dentro do ambiente do tribunal.

2.6.7. Além disso, o sistema de segurança do TJCE, representado pelo Firewall principal, registra um alto número de conexões bloqueadas diariamente, situando-se entre 4 e 20 milhões de conexões. Essas conexões bloqueadas podem indicar tentativas de acesso não autorizado ou ameaças potenciais que estão sendo impedidas de penetrar na rede do tribunal.

2.6.8. Em relação à proteção contra ameaças cibernéticas, o sistema de Antivírus do TJCE desempenha um papel crucial. No ano de 2023, foram identificadas e bloqueadas 9851 ameaças pelo sistema de Antivírus, o que representa uma média de mais de 820 ameaças por mês. Essa estatística destaca a importância da vigilância constante e da resposta proativa às ameaças digitais que visam comprometer a segurança do ambiente de TI do tribunal.

2.7. **Segurança de Endpoint do TJCE.**

2.7.1. No âmbito da segurança da informação e tecnologia, o termo "endpoint" refere-se a qualquer dispositivo final que esteja conectado a uma rede corporativa ou à internet. Esses dispositivos englobam computadores desktop, laptops, smartphones, tablets, servidores e outros aparelhos ligados à rede.

2.7.2. Os endpoints são os pontos onde os usuários têm interação direta com a rede, podendo acessar os recursos e dados necessários para suas atividades. Por serem possíveis pontos de entrada para invasores, os endpoints são frequentemente alvos de ataques cibernéticos.

2.7.3. Os Endpoints do Tribunal de Justiça do Ceará precisam de proteção por várias razões fundamentais:

2.7.3.1. Natureza Sensível dos Dados: O Tribunal de Justiça do Ceará lida diariamente com uma grande quantidade de informações sensíveis e confidenciais, incluindo dados pessoais de partes envolvidas em processos judiciais, decisões judiciais, informações financeiras e outros dados sigilosos. Essas informações são altamente valiosas e atrativas para hackers e cibercriminosos, que buscam acessá-las para diversos fins ilícitos, como roubo de identidade, fraude financeira e chantagem.

2.7.3.2. Ameaças Cibernéticas em Evolução: O cenário de ameaças cibernéticas está em constante evolução, com novos tipos de ataques sendo desenvolvidos regularmente pelos criminosos digitais. Isso inclui malware sofisticado, ransomware, phishing, ataques de engenharia social e muitas outras técnicas. Os Endpoints do Tribunal de Justiça do Ceará estão constantemente expostos a essas ameaças enquanto os colaboradores realizam suas atividades diárias, tornando essencial a implementação de medidas de proteção eficazes.

2.7.3.3. Ponto de Entrada para Ataques: Os Endpoints, como computadores desktop, laptops, smartphones e tablets, representam pontos de entrada potenciais para ataques cibernéticos. Os usuários interagem diretamente com esses dispositivos e acessam dados críticos da instituição, tornando-os alvos primários para os invasores. Uma vez comprometidos, os Endpoints podem servir como pontos de partida para ataques mais amplos à rede do Tribunal de Justiça do Ceará.

2.7.3.4. Riscos Associados ao Teletrabalho: Com a crescente adoção do teletrabalho, especialmente durante eventos como a pandemia de COVID-19, os Endpoints dos colaboradores do Tribunal de Justiça do Ceará podem estar ainda mais expostos a ameaças cibernéticas. Dispositivos utilizados para acesso remoto à rede institucional podem não ter a mesma segurança de acesso físico que os dispositivos internos mantidos pela instituição, aumentando o risco de comprometimento de dados e sistemas.

2.7.4. Já os endpoints servidores requerem proteção adicional de segurança da informação devido à sua importância crítica na infraestrutura de TI do TJCE. Razões pelas quais os endpoints servidores precisam de mais proteção:

2.7.4.1. Centralidade na Infraestrutura de Rede: Os servidores desempenham um papel central na infraestrutura de rede, fornecendo serviços essenciais e armazenando dados críticos da organização. Um comprometimento da segurança de um servidor pode resultar em interrupções nos serviços, perda de dados e impactos financeiros significativos.

2.7.4.2. Alvos de Ataques Cibernéticos: Os servidores são alvos frequentes de ataques cibernéticos, devido à sua exposição contínua à internet e à sua importância crítica para o funcionamento do Tribunal. Hackers e cibercriminosos visam servidores para roubar dados, interromper serviços.

2.7.4.3. Potencial para Danos Financeiros e Reputacionais: Um comprometimento da segurança de um servidor pode resultar em danos financeiros significativos para o TJCE, incluindo custos de recuperação, perda de informações e multas por violações de dados. Além disso, uma violação de dados pode causar danos à reputação da organização e resultar em perda de confiança dos jurisdicionados.

2.7.5. Além disso, é necessário cumprir com as normas e regulamentos aplicáveis, notadamente:

2.7.5.1. Resolução CNJ Nº 363 de 12/01/2021, que estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais.

2.7.5.2. Resolução CNJ Nº 396 de 07/06/2021, que institui a Estratégia

Nacional de Segurança Cibernética do Poder Judiciário.

2.7.5.3. Resolução do Órgão Especial TJCE nº 15, de 06/07/2023 que regulamenta a Política de Segurança da Informação no âmbito do Poder Judiciário do Estado do Ceará.

2.7.6. Com isso, a proteção dos Endpoints do TJCE é crucial para garantir a segurança e a integridade das informações confidenciais e sensíveis da instituição, protegendo contra ameaças cibernéticas, mantendo a continuidade das operações e preservando a confiança do público e das partes envolvidas nos processos judiciais.

3. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

3.1. **Identificação das necessidades de negócio**
3.1.1. Implementar uma estratégia abrangente de segurança de endpoint avançada: que integre prevenção, detecção e resposta, isso é essencial para garantir a proteção completa da infraestrutura de TI da TJCE. Permite uma abordagem unificada na identificação e resposta rápida às ameaças, abrangendo todos os pontos de entrada e contando com uma interpretação baseada em comportamento para uma segurança mais eficaz. 3.1.2. Correlacionar eventos de segurança em toda a infraestrutura de TI: as soluções de segurança de endpoint avançada podem reduzir drasticamente o tempo necessário para detectar e responder a ameaças. Isso ajuda a minimizar o impacto das ameaças cibernéticas, protegendo proativamente a TJCE contra possíveis danos. 3.1.3. Simplificar a gestão de segurança: isso é outra vantagem dessas soluções integradas. Elas permitem que as equipes de segurança monitorem e gerenciem ameaças de forma mais eficiente, tudo a partir de uma única interface. Isso simplifica as operações de segurança e aumenta a capacidade de resposta da TJCE diante de incidentes de segurança. 3.1.4. Fornecer uma visão completa da segurança cibernética: as soluções de segurança de endpoint avançada capacitam as equipes de segurança da TJCE a tomar decisões mais informadas. Isso resulta em ações mais eficazes para lidar com ameaças e reduzir os riscos de segurança em toda a infraestrutura de TI. 3.1.5. Cumprir regulamentações e normas de segurança cibernética: Ao fornecer uma

visão abrangente das atividades de segurança, elas facilitam a identificação e a mitigação de riscos, garantindo a conformidade com os padrões de segurança estabelecidos.

3.2. Identificação das necessidades tecnológicas

3.2.1. Identificar e bloquear ameaças avançadas e malware em endpoints, incluindo ransomware;

3.2.2. Prevenir e detectar atividades suspeitas em endpoints;

3.2.3. Gerenciar patches e atualizações de segurança;

3.2.4. Gerar relatórios de segurança e conformidade;

3.2.5. Proteger todos os endpoints utilizados pelos colaboradores do TJCE contra uma ampla variedade de ameaças em constante evolução;

3.2.6. Ser compatível com os sistemas operacionais utilizados pelo TJCE;

3.2.7. Possuir recursos avançados de gerenciamento centralizado e monitoramento em tempo real;

3.2.8. Permitir a implementação de políticas de segurança personalizadas;

3.2.9. Possuir suporte técnico e atualizações de software garantidas pelo fabricante.

3.2.10. Ter capacidade de instalar agentes ou sensores para proteger os dados em computadores desktop, laptops, servidores e dispositivos móveis institucionais.

3.2.11. Dispor de capacidade de investigar e corrigir quaisquer ameaças cibernéticas nos dispositivos mencionados que conseguirem burlar os controles de proteção existentes.

3.2.12. Possuir disponibilidade de recursos para reduzir a superfície de ataque, detectar, investigar e responder a incidentes de segurança da informação em computadores desktop, laptops, servidores e dispositivos móveis institucionais.

3.2.13. Aperfeiçoar a investigação de incidentes segurança da informação ao coletar informações detalhadas de comportamentos anormais em computadores desktop, laptops, servidores e dispositivos móveis institucionais.

3.2.14. Haver uma proteção adicional de segurança da informação avançada de Endpoint nos servidores.

3.3. Demais requisitos necessários e suficientes à escolha da solução de TIC

3.3.1. Deve ser compatível com o parque tecnológico em uso no Tribunal de Justiça do Estado do Ceará (TJCE). Essa compatibilidade deve abranger o servidor de administração, console administrativa, estações e servidores Windows, estações e servidores Linux, bem

como dispositivos móveis.

3.3.2. Durante a vigência do suporte, os produtos devem ser acompanhados por garantia e suporte técnico remoto, sem custos adicionais para o TJCE.

3.3.3. A garantia dos produtos deve ser fornecida pelo fabricante do software.

3.3.4. No período de garantia dos produtos, a empresa deve disponibilizar, de forma gratuita, correções, novas versões ou as atualizações mais recentes comercialmente disponíveis dos produtos, além de oferecer suporte técnico remoto.

3.3.5. O suporte técnico remoto deve ser prestado pelo fabricante da solução e deve incluir, no mínimo, atendimento telefônico e suporte por meios eletrônicos (via Internet) para resolver questões de funcionamento e configuração do software adquirido, sem gerar custos adicionais para o TJCE.

3.3.6. A assistência técnica deve ser fornecida em português, sem a necessidade de intérpretes, seguindo o horário de funcionamento do TJCE.

3.3.7. A empresa fornecedora da solução de TI deve tratar todas as informações às quais tenha acesso para cumprir o contrato como "confidenciais". Não é permitido divulgar ou facilitar o acesso a terceiros a essas informações. Essa obrigação permanecerá válida durante todo o período contratual, e o não cumprimento acarretará sanções administrativas e judiciais contra a empresa fornecedora da solução de TI.

3.3.8. As responsabilidades e o conhecimento dos requisitos de segurança serão reafirmados em documentos posteriores pelo TJCE e pela empresa fornecedora da solução de TI, incluindo um termo de compromisso e um termo de ciência.

4. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

4.1. Com base nos dados fornecidos pela Coordenadoria de Gestão de Serviços do Tribunal de Justiça do Ceará (TJCE), podemos observar algumas informações importantes sobre a atualização e renovação do parque computacional:

4.1.1. Computadores:

Equipamento	Marca/Modelo	Qtde.	Data de aquisição	Nº do Contrato	Forma de aquisição	Prazo de garantia	Fim da garantia	Total em uso
Computador	Lenovo/3209-CE1	823	14/01/2013	24/2012	Adesão à ARP Nº 293/2011	36 meses	14/01/2016	274

Computador	Positivo/Master D540	1.136	11/08/2014	36/2013	Doação CNJ Nº 021/2014	48 meses	11/08/2018	542
Computador	Positivo/Master D480	896	03/07/2015	44/2014	Doação CNJ Nº 021/2014	48 meses	03/07/2019	226
Computador	Positivo/C810	812	19/01/2018	31/2017	Adesão à ARP Nº 032/2016	48 meses	19/01/2022	720
Computador	HP/800 G3 DM	1.500	23/10/2018	36/2018	Adesão à ARP Nº 044/2017	48 meses	23/10/2022	1.463
Computador	Positivo/Master D570	212	12/08/2022	03/2022	Doação TRT7 (TD03/2022)	Sem garantia	-	212
Computador	Positivo/C820	1.258	30/04/2019	73/2018	Licitação – P.E. Nº 58/2018	60 meses	30/04/2024	1.258
Computador	Positivo/C6200	3.457	16/12/2019	86/2019	Licitação – P.E. Nº 25/2019	60 meses	16/12/2024	3.457
Computador	Dell/Optiplex 3080	1.000	10/05/2022	30/2022	Adesão à ARP Nº 012/2021	36 meses	10/05/2025	1.000
Workstation	Lenovo/P340	42	03/11/2022	21/2022 22/2022	Pregão Eletrônico Nº 29/2021	60 meses	03/11/2027	42
Workstation	Lenovo/P340	03	25/04/2023	54/2022 58/2022	Pregão Eletrônico Nº 29/2021	60 meses	25/04/2028	03
Computador	Positivo/C4400	2030	05/12/2023	43/2023	Adesão à ARP Nº 01/2022	48 meses	05/12/2027	2030
TOTAL								**11227**

4.1.2. Notebook:

Equipamento	**Marca/Modelo**	**Qtde.**	**Data de aquisição**	**Nº do Contrato**	**Forma de aquisição**	**Prazo de garantia**	**Fim da garantia**	**Total em uso**
Notebook	HP/Probook 440 G5	200	05/12/2018	49/2018	Adesão ARP Nº 36/2017	36 meses	05/12/2021	58

Notebook	HP/Probook 640 G4	357	06/03/2020	94/2019	Adesão ARP Nº 02/2019	60 meses	06/03/2025	357
Notebook	HP/*Ultrabook* 640 G8	105	25/05/2022	08/2022	Adesão ARP Nº 15/2021	36 meses	25/05/2026	105
Notebook	HP/*Ultrabook* 640 G8	245	26/07/2022	08/2022	Adesão ARP Nº 15/2021	36 meses	26/07/2026	245
Notebook	Positivo/Vaio FE14	533	08/11/2023	44/2023	Adesão ARP Nº 018/2022	36 meses	08/11/2026	533
TOTAL								**1298**

4.1.3. Aquisição de Novos Equipamentos em 2023: Pode-se observar que, durante o ano de 2023, o TJCE adquiriu um total de 2030 novos microcomputadores e 533 notebooks, refletindo um investimento significativo na atualização da infraestrutura de TI.

4.1.4. Total de Equipamentos Atuais: Atualmente, o Tribunal possui um total de 11227 computadores e 1298 notebooks em seu parque computacional. Esses números demonstram a extensão da infraestrutura de TI do TJCE e a importância de garantir o funcionamento adequado de cada dispositivo.

4.2. **Renovação e Modernização do Parque Computacional:**

4.2.1. Como parte de um processo contínuo de modernização, o TJCE está retirando os equipamentos mais antigos de seu parque computacional. O objetivo é manter apenas os dispositivos mais recentes, tecnologicamente avançados e ainda dentro do período de garantia, sempre que possível.

4.2.2. Equipamentos a serem retirados: Para os próximos anos, está prevista a retirada de diversos modelos de microcomputadores, totalizando 1.762 unidades, incluindo:

4.2.2.1. Lenovo 3209 (274 unidades)

4.2.2.2. Positivo Master D540 (542 unidades)

4.2.2.3. Positivo Master D480 (226 unidades)

4.2.2.4. Positivo C810 (720 unidades)

4.2.3. Essa medida visa otimizar o desempenho, a segurança e a eficiência

operacional do parque computacional do TJCE, garantindo que os usuários tenham acesso a tecnologias mais modernas e confiáveis.

4.3. Em março de 2024, a Central de Atendimento de TI (CATI) do Tribunal de Justiça do Ceará (TJCE) recebeu o chamado R1642007, com o objetivo de identificar quantos dispositivos precisavam de proteção na rede do TJCE. Os números obtidos foram os seguintes:

4.3.1. Computadores Desktop: Foram registrados 7.182 computadores desktop, que são os sistemas tradicionais de computação utilizados em escritórios e locais de trabalho.

4.3.2. Notebooks: Houve o registro de 941 notebooks, que são dispositivos portáteis frequentemente utilizados por profissionais que necessitam de mobilidade em seu trabalho.

4.3.3. Estações de Trabalho Virtuais: Um total de 145 estações de trabalho virtuais foram identificadas. Essas estações utilizam recursos de virtualização para fornecer ambientes de trabalho aos usuários, muitas vezes de forma remota.

4.3.4. Servidores Virtuais: Foram contabilizados 1.410 servidores virtuais, que são máquinas virtuais usadas para hospedar serviços e aplicativos na infraestrutura de TI do TJCE.

4.3.5. Servidores Físicos: Além disso, foram identificados 250 servidores físicos, que são computadores dedicados ao gerenciamento de redes, armazenamento de dados e execução de serviços essenciais.

4.4. Portanto, somando todos esses dispositivos, chegamos a um total de 9.928 unidades que necessitam de proteção na rede do TJCE.

4.5. É relevante observar que alguns desses dispositivos fazem uso de dual-boot do sistema operacional, o que significa que podem executar dois sistemas operacionais diferentes em um mesmo hardware. Essa situação pode implicar em desafios adicionais de segurança, pois cada sistema operacional precisa ser protegido individualmente contra ameaças cibernéticas.

4.6. **Projeção de uso:**

4.6.1. No chamado, da Central de Atendimento de TI (CATI) do TJCE, R1608163, foi levantado o histórico mensal da quantidade de dispositivos com o aplicativo antivírus instalado ativo em 2023, pode ser observado nas tabelas a seguir:

Ano 2023			
Meses	Relatórios semanais		Médias
Janeiro	Semana 1	8622	8637
	Semana 2	8633	
	Semana 3	8644	
	Semana 4	8647	
Fevereiro	Semana 1	8875	8959
	Semana 2	8952	
	Semana 3	9005	
	Semana 4	9005	
Março	Semana 1	9005	9043
	Semana 2	9043	
	Semana 3	9053	
	Semana 4	8987	
	Semana 5	9127	
Abril	Semana 1	9128	9070
	Semana 2	9022	
	Semana 3	9023	
	Semana 4	9105	
Maio	Semana 1	9059	9127
	Semana 2	9131	
	Semana 3	9153	
	Semana 4	9164	
Junho	Semana 1	9070	9086
	Semana 2	9063	
	Semana 3	9085	
	Semana 4	9099	
	Semana 5	9113	

Ano 2023			
Julho	Semana 1	9118	9134
	Semana 2	9124	
	Semana 3	9134	
	Semana 4	9158	
Agosto	Semana 1	9302	9342
	Semana 2	9347	
	Semana 3	9338	
	Semana 4	9382	
Setembro	Semana 1	9391	9482
	Semana 2	9412	
	Semana 3	9416	
	Semana 4	9563	
	Semana 5	9628	
Outubro	Semana 1	9661	9514
	Semana 2	9502	
	Semana 3	9443	
	Semana 4	9451	
Novembro	Semana 1	9434	9435
	Semana 2	9404	
	Semana 3	9393	
	Semana 4	9507	
Dezembro	Semana 1	9565	9692
	Semana 2	9593	
	Semana 3	9768	
	Semana 4	9768	
	Semana 5	9768	

4.6.2. O histórico mensal da quantidade de dispositivos com o aplicativo antivírus instalado e ativo em 2023 revela uma tendência de crescimento ao longo do ano, com algumas variações observadas em determinados meses. No mês de janeiro, a média mensal ficou em torno de 8637 dispositivos, enquanto em fevereiro houve um aumento para 8959 dispositivos. Em março, ocorreu uma ligeira queda para 9043 dispositivos, seguida por uma alta em abril, com uma média de 9070 dispositivos.

4.6.3. Nos meses subsequentes, observou-se uma oscilação na quantidade de dispositivos ativos, com picos em determinadas semanas. Em agosto, registrou-se uma média de 9342 dispositivos, aumentando para 9482 em setembro. Outubro apresentou uma média de 9514 dispositivos ativos, enquanto em novembro houve uma pequena queda para 9435 dispositivos.

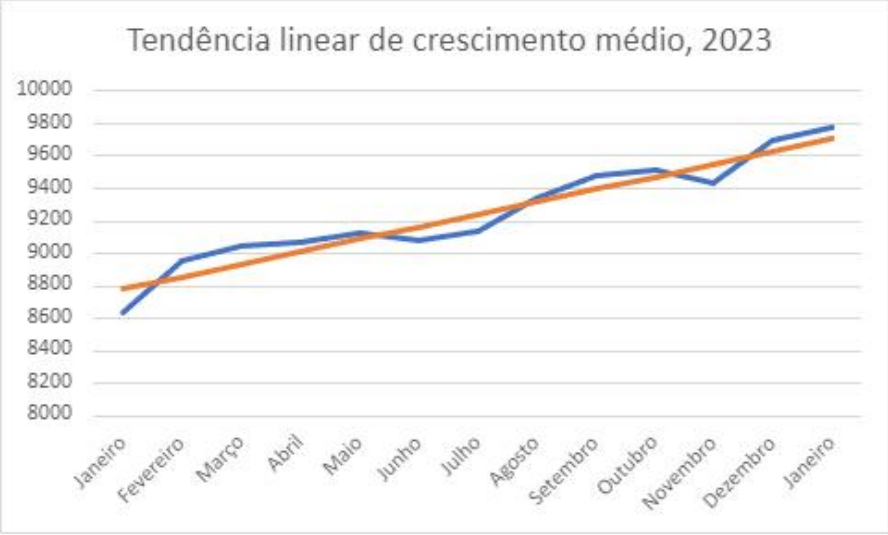
4.6.4. Finalmente, em dezembro, ocorreu um aumento significativo, atingindo uma média de 9692 dispositivos ativos. Esses números refletem a importância da manutenção de um alto nível de proteção cibernética ao longo do ano.

4.6.5. O gráfico abaixo ilustra a compilação da evolução do número médio mensal

de dispositivos com o aplicativo antivírus ativado ao longo do ano de 2023:

4.6.6. Os dados médios mensais de 2023 sobre a quantidade de dispositivos com o aplicativo antivírus ativado mostram uma tendência de crescimento ao longo do ano. Começando com 8.637 dispositivos em janeiro, houve um aumento gradual até alcançar 9.692 dispositivos em dezembro.

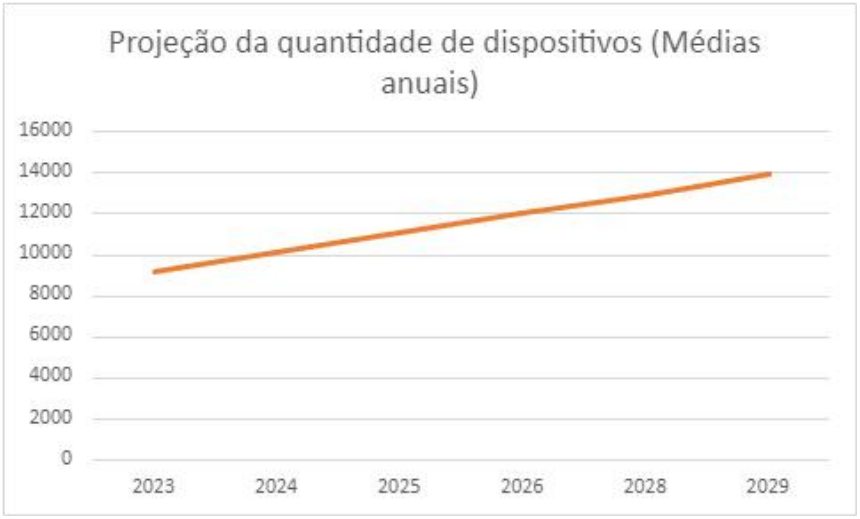
4.6.7. Entre janeiro de 2023 e janeiro de 2024 tivemos tendência linear de crescimento médio de 77 dispositivos ao mês.



4.6.7.1. A tendência linear de crescimento é um padrão de aumento constante ao longo do tempo, onde os valores de uma variável aumentam em uma taxa constante. Essa abordagem é útil para prever valores futuros com

base nos dados históricos e assumindo que a tendência de crescimento permanecerá constante.

4.6.8. Extrapolando esses números para um período de 60 meses, a estimativa é que um total aproximado de 14.000 dispositivos sejam utilizadas ao longo desse período.



4.6.8.1. A extrapolação matemática é um procedimento pelo qual se estima o valor de uma variável além do intervalo de dados disponíveis. Esse termo é usado para descrever a ação de estender uma sequência ou padrão além dos valores conhecidos. A extrapolação é uma técnica empregada para fazer projeções e previsões com base em dados históricos, permitindo antecipar valores futuros com base em informações do passado.

4.7. **Estimativa de demanda:**

4.7.1. Os dados fornecidos apresentam a situação atual do número de dispositivos que precisam de proteção e o histórico mensal da quantidade de dispositivos com o aplicativo antivírus ativado ao longo de 2023, juntamente com médias anuais extrapoladas para os anos subsequentes até 2029. Em 2023, o número médio mensal de dispositivos com o aplicativo antivírus foi de aproximadamente 9.210, com uma tendência de crescimento anual.

4.7.2. A partir daí, a estimativa é que esse número continue aumentando nos próximos anos, atingindo cerca de 10.168 dispositivos em 2024, 11.112 em 2025, 12.060 em 2026, 12.930 em 2028 e 13.957 em 2029. Com isso, é estimado que o

uso médio durante o período será de 12.045 dispositivos, porém, estima-se que poderá haver o um pico de demanda de até aproximamente 14.000 dispositivos no período de 60 meses.

4.7.3. No entanto, o Acórdão 2569/2018 do TCU - Plenário estabelece diretrizes importantes em relação à aquisição de licenças de software. Ele ressalta a necessidade de adquirir apenas o número estritamente necessário de licenças, proibindo o pagamento antecipado por licenças de software. Além disso, sugere que o pagamento dos serviços agregados esteja vinculado às licenças efetivamente utilizadas, especialmente em projetos de alto risco ou de longo prazo. Nessas situações, o número de licenças deve acompanhar a evolução do projeto e ser devidamente documentado nos estudos técnicos preliminares, podendo empregar o Sistema de Registro de Preços, o qual possibilita obter vantagens de escala nas compras, ao mesmo tempo em que permite adquirir os produtos no momento mais adequado.

4.7.4. Já a Lei de Licitações e Contratos Administrativos, Lei nº 14.133/2021, estabelece que a existência de preços registrados implica o compromisso de fornecimento nas condições estabelecidas, porém, não obriga a Administração a contratar. Ela tem a faculdade de realizar uma licitação específica para a aquisição pretendida, desde que devidamente justificada. Além disso, determina que o prazo de vigência da ata de registro de preços seja de um ano, podendo ser prorrogado por igual período, desde que o preço vantajoso seja comprovado.

4.7.5. Dessa forma, caso o produto a ser adquirido seja licenciamento de software, para garantir uma eficiente gestão, é necessário utilizar o registro de preços, observando que seu prazo máximo de validade é de dois anos. No entanto, é crucial registrar o quantitativo para dois anos, mas contratar apenas o uso atual, podendo adicionar mais licenças conforme a necessidade, seguindo as diretrizes estabelecidas pelo TCU e pela legislação pertinente.

4.7.6. Portanto, é importante considerar que o quantitativo previsto deve ser avaliado apenas para um período de até 24 meses. Levando em conta essa previsão, estima-se que a utilização de dispositivos em dois anos será de aproximadamente 12.000.

4.7.7. Para uma análise financeira mais detalhada e precisa, é recomendável considerar o seguinte planejamento para a distribuição da proteção dos dispositivos:

4.7.7.1. Estações de Trabalho e dispositivos móveis: Sugere-se adquirir proteção para um total de 10.000 dispositivos, sendo 9.000 no primeiro ano e mais 1.000 adicionais no segundo ano. Essa estratégia permite uma implementação gradual, alinhada com a demanda prevista para cada período. Assim, a organização pode ajustar seus investimentos de acordo com a evolução das necessidades de proteção.

4.7.7.2. Máquinas Virtuais e Servidores Físicos: Recomenda-se a aquisição de proteção de segurança para 2.000 dispositivos, distribuídas ao longo de dois anos. No primeiro ano, seriam adquiridas 1.500, com um acréscimo de 500 adicionais no segundo ano. Essa abordagem proporciona flexibilidade para atender às demandas específicas desses ambientes, considerando tanto o crescimento projetado quanto as exigências operacionais.

4.7.8. Essa distribuição equilibrada das aquisições de proteção de segurança para dispositivo de Enpoint ao longo de dois anos leva em conta a estimativa de demanda apresentada, garantindo que o investimento seja ajustado às necessidades reais da instituição em cada período. Essa estratégia permite uma alocação eficiente de recursos, maximizando o retorno sobre o investimento e otimizando o desempenho operacional da infraestrutura de TI.

4.7.9. Além disso, a aquisição do serviço de implantação da solução e treinamento é fundamental para garantir o sucesso e a eficácia da nova solução de segurança de endpoint. Existem várias razões pelas quais esse investimento adicional é necessário e justificado:

4.7.9.1. Personalização e Configuração Adequada: Cada ambiente de TI é único, e é essencial que a solução de segurança de endpoint seja configurada de acordo com as necessidades específicas e os requisitos de segurança da organização. O serviço de implantação permitirá que os especialistas ajustem a solução para garantir uma configuração adequada e personalizada, alinhada com as políticas de segurança e os objetivos operacionais.

4.7.9.2. Maximização do Investimento: Uma implantação adequada garante que a organização obtenha o máximo retorno sobre o investimento na nova solução. Os especialistas em implantação podem otimizar a configuração para garantir que todos os recursos e funcionalidades da

solução sejam totalmente utilizados, ajudando a maximizar a eficácia da proteção de endpoint.

4.7.9.3. Redução de Riscos: Uma implementação mal executada pode resultar em lacunas na segurança ou em configurações incorretas que deixam a organização vulnerável a ameaças cibernéticas. O serviço de implantação ajuda a reduzir esses riscos, garantindo que a solução seja instalada e configurada corretamente para proteger adequadamente os endpoints contra ataques.

4.7.9.4. Aceleração da Implementação: Os profissionais de implantação têm experiência e conhecimento especializado na implementação de soluções de segurança de endpoint. Isso permite que o processo de implantação seja concluído de forma mais eficiente e rápida, minimizando o tempo de inatividade e garantindo uma transição suave para a nova solução.

4.7.9.5. Capacitação da Equipe: O treinamento fornecido como parte do serviço de implantação capacita a equipe de TI e os usuários finais a entenderem completamente a nova solução, suas funcionalidades e melhores práticas de uso. Isso ajuda a garantir que a equipe esteja preparada para lidar com ameaças cibernéticas, responder a incidentes de segurança e utilizar efetivamente todas as capacidades da solução.

4.7.10. Em resumo a demanda prevista é apresentada na tabela a seguir.

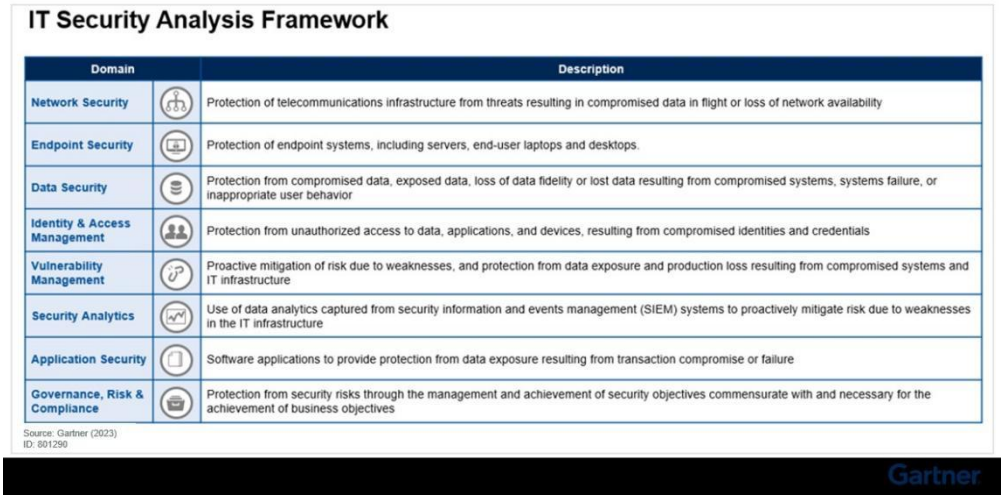
Id	Demanda Prevista	Bem/Serviço	Unidade de Medida	Quantidade
1	Solução de Segurança de EndPoint (desktop, notebook e dispositivos móveis).	Software.	Qtd	10.000
2	Solução de Segurança de EndPoint (Servidores).	Software.	Qtd	2.000
3	Serviços de instalação, configuração e implantação da solução.	Serviço de implantação.	Qtd	1
4	Treinamento.	Treinamento.	Qtd	1

5. ANÁLISE DE SOLUÇÕES POSSÍVEIS

5.1. **Descrição e definições.**

5.1.1. O escopo da análise do ambiente de segurança de TI é uma visão de alto nível dos custos e ao gerenciamento de toda a segurança de tecnologia da informação dentro de uma organização.

5.1.2. Isso inclui gerenciamento de identidade e acesso, segurança de rede, segurança de endpoint, segurança de dados, segurança de aplicativos, gerenciamento de vulnerabilidades e análise de segurança, governança, risco e gerenciamento de conformidade:



IT Security Analysis Framework

Domain	Description
Network Security	Protection of telecommunications infrastructure from threats resulting in compromised data in flight or loss of network availability
Endpoint Security	Protection of endpoint systems, including servers, end-user laptops and desktops.
Data Security	Protection from compromised data, exposed data, loss of data fidelity or lost data resulting from compromised systems, systems failure, or inappropriate user behavior
Identity & Access Management	Protection from unauthorized access to data, applications, and devices, resulting from compromised identities and credentials
Vulnerability Management	Proactive mitigation of risk due to weaknesses, and protection from data exposure and production loss resulting from compromised systems and IT infrastructure
Security Analytics	Use of data analytics captured from security information and events management (SIEM) systems to proactively mitigate risk due to weaknesses in the IT infrastructure
Application Security	Software applications to provide protection from data exposure resulting from transaction compromise or failure
Governance, Risk & Compliance	Protection from security risks through the management and achievement of security objectives commensurate with and necessary for the achievement of business objectives

Source: Gartner (2023)
ID: 801290

Gartner

5.1.3. O cenário de segurança cibernética em rápida evolução exige uma plataforma robusta de proteção de endpoint (EPP) para proteger as organizações contra uma gama crescente de ataques sofisticados. Muitas organizações explorarão novos produtos de detecção e resposta de EPP/ endpoint (EDR), mesmo que seja apenas para ver se os atuais ainda são uma boa escolha e atendem a todos os seus requisitos quando chegar a hora de renovar.

5.1.4. Cada organização é única e fatores como setor, tamanho, região geográfica e objetivos de negócios específicos desempenham um papel importante na definição dos requisitos de segurança de endpoint.

5.1.5. Endpoint, em termos de segurança da informação e tecnologia, refere-se a qualquer dispositivo terminal conectado a uma rede corporativa ou de internet, como computadores desktop, laptops, smartphones, tablets e servidores. Esses são os pontos onde os usuários interagem diretamente com a rede e acessam recursos e dados.

5.1.6. No entanto, os endpoint também são frequentemente alvos de ataques

cibernéticos, pois representam pontos de entrada potenciais para invasores. Portanto, a proteção dos endpoints é crucial para garantir a segurança da rede, envolvendo a implementação de medidas como antivírus, firewalls de host e soluções de detecção e resposta para defender esses dispositivos contra ameaças como malware, ransomware e phishing.

5.1.7. Consequentemente, a proteção dos endpoints é uma prioridade essencial para garantir a segurança de uma rede corporativa ou da internet. Isso implica a implementação de medidas de segurança, como antivírus, firewalls, soluções de detecção e resposta, entre outras tecnologias, visando proteger esses dispositivos contra uma variedade de ameaças cibernéticas, incluindo malware, ransomware, ataques de phishing e outros tipos de ataques.

5.1.8. Identificar ameaças na infraestrutura de uma organização e responder a elas em tempo hábil requer ferramentas e serviços de detecção e resposta que permitam a descoberta, mitigação e contenção de ameaças

5.1.9. O TJCE estabeleceu o Contrato n° 54/2021 com o Gartner, com objetivo de fornecer serviços técnicos especializados de pesquisa e aconselhamento imparcial em Tecnologia da Informação, através de pesquisas revelando para que servem as tecnologias, onde deverão ser usadas, quais benefícios apresentarão, e em que situações devem ser empregadas. A Consultoria do Gartner define uma plataforma de proteção de endpoint (EPP) como um software de segurança projetado para proteger endpoints gerenciados de usuários finais – incluindo PCs desktop, laptops e dispositivos móveis – contra ataques maliciosos conhecidos e desconhecidos. Além disso, os EPPs fornecem recursos para que as equipes de segurança investiguem e remediem incidentes que escapam aos controles de prevenção. Os produtos EPP são entregues como agentes de software implantados em endpoints e conectados a interfaces centralizadas de análise e gerenciamento de segurança.

5.1.10. Os EPPs fornecem um controle de segurança defensivo para proteger os endpoints do usuário final contra infecções por malware conhecidas e desconhecidas. Os recursos de prevenção de EPP são implantados como parte de uma estratégia de defesa profunda para ajudar a reduzir a superfície de ataque e minimizar o risco de comprometimento do endpoint. Os recursos de detecção e resposta de EPP são usados para descobrir, investigar e responder a ameaças de endpoint que escapam à prevenção de segurança, muitas vezes como parte de

plataformas de operações de segurança mais amplas.

5.1.11. Os recursos padrão de um EPP são:

5.1.11.1. Prevenção e proteção contra ameaças à segurança, incluindo malware que usa técnicas de ataque baseadas em arquivos e sem arquivo.

5.1.11.2. A capacidade de detectar e prevenir ameaças usando análise comportamental da atividade do dispositivo, aplicação, identidade e telemetria do usuário.

5.1.11.3. Instalações para detectar e investigar incidentes e obter orientação para remediação quando as ameaças escapam aos controles de prevenção.

5.1.11.4. Gerenciamento e relatórios de controles de segurança do sistema operacional, como firewall de host e controle de dispositivos.

5.1.11.5. Funcionalidade integrada de detecção e resposta de endpoint (EDR).

5.1.12. Os recursos opcionais frequentemente presentes nos EPPs incluem:

5.1.12.1. Relatórios de risco baseados em inventário, configuração e gerenciamento de políticas de dispositivos endpoint.

5.1.12.2. Instalações para avaliar vulnerabilidades em endpoints e relatar ou gerenciar a instalação de patches ou mitigação de controles de segurança.

5.1.12.3. Funcionalidade estendida de detecção e resposta (XDR) integrada nativamente com módulos complementares, como proteção de identidade, segurança de e-mail, proteção de servidor e carga de trabalho.

5.1.12.4. Suporte estendido para sistemas operacionais incomuns ou em fim de vida.

5.2. **Visão geral do mercado**

5.2.1. À medida que as técnicas dos invasores evoluem, os provedores de proteção de endpoint são desafiados a acompanhar o ritmo. Os recursos de EDR comportamental agora são padrão; no entanto, a proteção de endpoint deve ser integrada às informações contextuais de toda a pilha de infraestrutura de segurança para enfrentar as ameaças em evolução. A crescente complexidade das soluções EPP, EDR e agora XDR, combinada com a lacuna de competências em segurança cibernética, impulsiona o aumento da procura por serviços geridos. Ao mesmo tempo, os esforços de consolidação de fornecedores colocam maior ênfase em soluções abrangentes de segurança do espaço de trabalho, em vez de produtos

pontuais. Como resultado, os produtos de proteção de terminais são cada vez mais avaliados no contexto destas estratégias de segurança mais amplas.

5.2.2. Em 2023, a inovação dos fornecedores concentrou-se principalmente em melhorias na eficácia da detecção, detecção e resposta a ameaças de identidade, gerenciamento de configuração de segurança e no conjunto mais amplo de recursos integrados da plataforma de segurança do espaço de trabalho. A maioria dos fornecedores nesta pesquisa oferece controles adicionais de segurança do espaço de trabalho e soluções XDR que auxiliam nos esforços de consolidação de fornecedores de segurança. No entanto, a amplitude e profundidade desses controlos auxiliares, a qualidade da integração do ecossistema e a experiência geral do utilizador final diferem entre fornecedores.

5.2.3. Os fornecedores também estão trabalhando para melhorar a facilidade de uso, aumentar o nível de integração de suas ofertas e reduzir o impacto de suas soluções no desempenho dos endpoints para fornecer uma experiência de administração mais integrada. Alguns fornecedores fornecem seus produtos para equipes de operações de segurança maduras e totalmente equipadas, enquanto outros fornecem soluções mais fáceis de usar, com orientações e sugestões mais contextuais.

5.2.4. Os líderes do mercado de proteção de endpoints continuam a se concentrar na evolução da proteção para infraestruturas modernas. As organizações que continuam a proteger a infraestrutura legada ou aquelas que exigem implantações locais devido à residência de dados muitas vezes lutam para encontrar fornecedores que ainda possam oferecer suporte a ambientes isolados e com arquitetura restrita, oferecer opções de implantação local ou oferecer suporte a um amplo espectro de sistemas operacionais legados.

5.2.5. As tendências amplas do mercado que estão impulsionando a adoção de ofertas de EPP incluem:

5.2.5.1. Consolidação da plataforma de segurança cibernética: as organizações desejam reduzir a complexidade, melhorar a postura de segurança e aumentar a eficiência da equipe. As soluções XDR fornecem um conjunto unificado de ferramentas de detecção e resposta a incidentes que integra dados de eventos e alertas de vários produtos de segurança. As organizações também precisam de configuração priorizada e orientação reforçada para melhorar a postura de segurança, reduzindo

configurações incorretas em seus controles de segurança.

5.2.5.2. Ransomware e defesa contra ameaças: O ransomware continua sendo a ameaça mais significativa para todas as organizações. Os operadores de ransomware estão a deixar de depender exclusivamente da encriptação para outras formas de extorsão cibernética, incluindo corrupção de dados irrecuperáveis, corrupção de hardware, roubo de dados e mineração de dados. Além disso, a maioria dos ataques modernos explora o uso indevido de credenciais e técnicas de sobrevivência para contornar soluções baseadas em assinaturas, tornando obrigatórias capacidades robustas de proteção comportamental, EDR e restauração de arquivos para uma solução EPP.

5.2.5.3. Trabalho remoto e adoção da nuvem: O trabalho remoto acelerou significativamente a adoção de ofertas entregues na nuvem, que agora representam 90% da base instalada, de acordo com a pesquisa de fornecedores do *Gartner Magic Quadrant*. Os potenciais compradores devem procurar indicadores de que as soluções são verdadeiramente concebidas para entrega nativa na nuvem e não representam servidores de gestão que foram simplesmente transferidos para a nuvem.

5.2.6. A proteção é a primeira linha de defesa em uma abordagem de segurança multicamadas para construir um EPP/EDR. Inclui recursos de prevenção, como um firewall baseado em host para controlar comunicações indesejadas em portas restritas. Poderia incluir controles de dispositivos periféricos para carregar malware através de dispositivos USB infectados para reduzir a superfície de ataque, bem como recursos de proteção, como antimalware, antiransomware e análise de comportamento contra ataques não baseados em malware.

5.2.7. A prevenção não pode ser 100% eficaz o tempo todo no cenário de ameaças em rápida evolução. Portanto, uma organização deve avaliar as capacidades de EDR de um produto da mesma forma que a prevenção.

5.2.8. Plataformas de proteção de endpoint (EPPs) e detecção e resposta de endpoint (EDR) são apostas importantes para proteção contra ataques. Combinadas com detecção e resposta estendida (XDR) e detecção e resposta a ameaças de identidade (ITDR), essas soluções se concentram na detecção proativa e na resposta mais rápida em um ambiente de ataque cada vez mais sofisticado.

5.2.9. Apesar das alegações dos fornecedores de melhoria na busca e correlação de

ameaças, as organizações muitas vezes exigem serviços gerenciados para se beneficiarem totalmente da implementação de EDR.

5.2.10. Os modelos de entrega de SaaS da maioria dos fornecedores de EPP exigem recursos de integração adicionais para oferecer suporte a organizações com infraestruturas de arquitetura de segurança complexas e híbridas.

5.2.11. O perímetro de segurança mudou para os usuários e seus dispositivos. Os dispositivos de computação do usuário final tornaram-se um ponto de entrada para os invasores obterem acesso inicial à infraestrutura de TI corporativa, exigindo uma ênfase renovada na proteção de endpoints.

5.2.12. As capacidades do EPP evoluíram ao longo do tempo para incluir recursos adicionais de proteção e prevenção e detecção. Os fornecedores estão consolidando mais funções de segurança em uma única plataforma.

5.2.13. Os EPPs continuam a se transformar de ofertas básicas de proteção antimalware em soluções completas de segurança para espaços de trabalho. Devido a esta mudança e ao aumento de ataques sofisticados e direcionados (como ransomware operado por humanos), a gestão, a monitorização e a automação são agora críticas. Há também o XDR — uma evolução adicional que traz visibilidade de ponta a ponta em mais disciplinas de segurança.

5.2.14. A maioria das organizações já adotou EPPs entregues em nuvem, e apenas algumas indústrias e regiões geográficas altamente regulamentadas ainda priorizam soluções locais para satisfazer as necessidades de seus ambientes arquitetonicamente restritos. Os fornecedores também estão investindo principalmente em soluções baseadas na nuvem, em vez de soluções locais, e alguns não oferecem mais suporte ou desenvolvem melhorias de recursos de EPP locais. Muitas organizações só agora estão fazendo a transição para soluções SaaS. Estas organizações devem considerar a capacidade destas ferramentas locais focadas na proteção para expandir as competências para novas áreas – como a deteção e a resposta, uma vez que faltam muitas ferramentas nesta área.

5.2.15. Com o avanço das soluções proteção de endpoint, tornou-se necessário evoluir para plataformas avançadas de segurança cibernética que protejam contra uma ampla variedade de ameaças em constante evolução.

5.2.16. Nesse contexto, as soluções de detecção e resposta de endpoint (EDR) e com funcionalidades estendida de detecção e resposta (XDR) apresentam-se como uma alternativa essencial para garantir a segurança dos endpoints.

5.2.17. Uma solução de EDR é necessária para garantir a segurança dos endpoints. A solução de EDR permite o monitoramento em tempo real, a detecção de ameaças, a investigação de incidentes e a análise avançada de comportamentos suspeitos das estações de trabalho.

5.2.18. Já a solução de segurança de XDR oferece uma abordagem de segurança multicamadas, combinando várias técnicas de proteção, como prevenção de ameaças, detecção comportamental, análise de tráfego e inteligência de ameaças. Isso garante uma proteção abrangente contra uma ampla variedade de ameaças cibernéticas, independentemente do tipo de ambiente de TI.

5.2.19. O XDR é ideal para servidores de aplicações em máquinas virtuais ou físicos devido à sua capacidade avançada de proteção, detecção e resposta a ameaças cibernéticas, sua adaptabilidade a ambientes virtualizados e sua abordagem de segurança multicamadas.

5.3. **Contratações públicas de proteção de Endpoint.**

5.3.1. A tabela a seguir oferece exemplos de contratações públicas efetuadas nos últimos 12 meses, relacionadas à solução de segurança de Endpoint. As contratações foram categorizadas com base em diversos critérios, incluindo se são renovações, se incluem funcionalidades de EDR (Resposta e Detecção de Ameaças) ou XDR (Detecção e Resposta Estendida), a quantidade registrada e a duração do suporte fornecido:

Identificação	**Objeto**	**Renov.**	**EDR**	**XDR**	**Qtd**	**Tempo (meses)**
ATA DE REGISTRO DE PREÇOS 02/2023, referente ao Pregão Eletrônico Nº 05/2023, da PRODAM – Processamento de Dados Amazonas S.A, com vigência até 27/07/2024.	Kaspersky Endpoint Detection and Response Optimum – com validade de 36 meses.	Não	Sim	Não	5.000	36
Pregão Eletrônico Nº 9/2023, CONSELHO FEDERAL DE	Contratação de solução de tecnologia da informação e comunicação visando a	Sim	Não	Não	370	36

CONTABILIDADE Código da UASG: 383500, de 03/08/2023.	renovação das licenças de uso da solução de segurança antivírus Kaspersky Endpoint Security para estações de trabalho (endpoints), servidores e dispositivos móveis, gerenciados por solução centralizada no modelo onpremisse, garantia, suporte técnico e atualizações por 36 (treinta e seis) meses.					
ATA DE REGISTRO DE PREÇOS referente ao Pregão Eletrônico Nº 006/2023 – TC O TRIBUNAL DE CONTAS DO ESTADO DO RIO GRANDE DO NORTE, de 16/08/2023.	Ata de Registro de Preços para posterior aquisição de 700 (setecentas) licenças do software Kaspersky Endpoint Security for Business Advanced (PLUS), com direito a atualizações pelo período de 36 (trinta e seis) meses.	Sim	Não	Não	700	36
PREGÃO ELETRÔNICO Nº 11/2023, MMA-IBAMA - DEFIN/DF, homologado em 22/08/2023.	Contratação de solução de proteção (Next Generation Antivírus - NGAV) baseada em agente com funcionalidade de EDR com suporte, garantia e atualização por 36 meses.	Não	Sim	Não	180	36
Pregão Eletrônico Nº 41/2023, GOVERNO DO ESTADO DA BAHIA, Procuradoria Geral de Justiça do Estado da Bahia, Código da UASG: 926302, de 18/09/2023.	Contratação de SOLUÇÃO DE SEGURANÇA DE ENDPOINT, marca FORTINET, Item: Endpoint-based Licenses - EPP/APT (LICENCIAMENTO POR 36 MESES)	Não	Sim	Sim	300	36
Pregão Eletrônico Nº 101/2023, Ministério do Planejamento e Orçamento,	Contratação de empresa para a prestação de serviço de locação de software Microsoft	Não	Sim	Sim	1.545	36

Fundação Instituto Brasileiro de Geografia e Estatística, Fundação IBGE - Administração Central - RJ, Código da UASG: 114601, de 19/09/2023.	na modalidade EAS por 36 (trinta e seis) meses, Item Licença Defender Endpoint Server Sub.					
Pregão Eletrônico Nº 3/2023, PRESIDÊNCIA DA REPÚBLICA, Advocacia Geral da União, Diretoria Geral de Administração Diretoria de Logística e Gestão Documental, Código da UASG: 110792, de 06/10/2023.	Contratação de solução de tecnologia da informação e comunicação de Segurança Avançada Integrada de Prevenção, Detecção e Resposta.	Não	Sim	Sim	18.000	12
Pregão Eletrônico Nº 15/2023, MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS, Arquivo Nacional, Código da UASG: 200247, de 06/10/2023.	Registro de preços para contratação de empresa especializada em licenciamento e suporte da solução de Proteção de Endpoint Sophos Central Intercept X Advanced para estações de trabalho e servidores pelo período de 36 (trinta e seis) meses.	Sim	Sim	Sim	850	36
Pregão Eletrônico Nº 29/2023, UASG 926677 - CAMARA MUNICIPAL DE CAMPINAS, de 10/11/2023.	Renovação de licença (assinatura) da solução de proteção Eset Protect Advanced pelo prazo de 36 (trinta e seis) meses	Sim	Não	Não	700	36
Pregão Eletrônico Nº 10/2023, UASG 925398 - TRIBUNAL DE CONTAS DO EST. DO ESPÍRITO SANTO, de 27/10/2023.	Licença de subscrição da solução de segurança Symantec Endpoint Protection por 24 meses.	Sim	Não	Não	700	24

Pregão Eletrônico Nº 35/2023, Tribunal de Contas do Estado de Rondônia, Código da UASG: 935002, de 31/10/2023.	Renovação de licenças do software Antivírus Symantec Endpoint Protection, contemplando suporte e atualizações pelo período de 12 (doze) meses.	Sim	Não	Não	1.300	12
Pregão Eletrônico Nº 72/2022, MINISTÉRIO PÚBLICO DO ESTADO DO MATO GROSSO, homologado em 31/10/2023.	Aquisição de novas Licenças de EDR com suporte e garantia para 36 meses.	Não	Sim	Não	3.000	36
Pregão Eletrônico Nº 72/2022, MINISTÉRIO PÚBLICO DO ESTADO DO MATO GROSSO, homologado em 31/10/2023	Aquisição de novas Licenças de XDR com suporte e garantia para 36 meses.	Não	Sim	Sim	500	36
Pregão Eletrônico Nº 5/2023, CONSELHO REGIONAL DOS REPRESENTANTES COMERCIAIS DO ESTADO DO PARANÁ - CORE/PR, Código da UASG: 926647, de 21/11/2023.	Software de Antivírus Cliente Servidor Kaspersky Endpoint Security for Business Advanced (50 licenças).	Não	Não	Não	50	60
Pregão Eletrônico Nº 2/2023, MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA E COMÉRCIO EXTERIOR, INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL, UASG 183038 - MICT-INPI-INST.NAC.DA	Licenças de solução de segurança do tipo Endpoint Protection (Antivírus, proteção contra Ransomware, Proteção Web, Firewall de Host) com Gerência centralizada, incluindo garantia, suporte e atualização por 36 (trinta e seis) meses.	Não	Não	Não	1.835	36

PROPR.INDUSTRIAL/RJ, de 24/11/2023.						
Pregão Eletrônico Nº 27/2023, Tribunal Regional Federal da 2ª Região, Justiça Federal de 1ª Instância - ES, Código da UASG: 90014, de 14/12/2023.	Renovação da solução de segurança de proteção de endpoint Kaspersky Endpoint Security for Bussiness Select Brazilian Edition.	Sim	Não	Não	1.100	15,5
Pregão Eletrônico Nº 12/2023, MINISTÉRIO DA DEFESA, Comando do Exército, Gabinete do Comandante do Exército, Centro de Inteligência do Exército, Código da UASG: 160062, de 01/12/2023.	Ampliação dos recursos do software Netwitness com a aquisição do componente de Detectação e Resposta em Endpoints Endpoint Detection and Response (EDR).	Não	Sim	Não	50	36
Pregão Eletrônico Nº 170/2023, - PREFEITURA MUNICIPAL DE SANTA MARIA/RS, homologado em 19/12/2023.	Solução XDR baseado em inteligência artificial com instalação, configuração e suporte, para 36 meses.	Não	Sim	Sim	5.000	36
Pregão Eletrônico Nº 12/2023, GOVERNO DO DISTRITO FEDERAL - GDF, SECRETARIA DE ESTADO DE SEGURANCA PUBLICA DO GOVERNO DO DISTRITO FEDERAL, Código da UASG: 450107, de 21/12/2023.	Licença Antivirus Desktop om EDR com instalação, configuração, suporte técnico, manutenção e garantia de 36 (trinta e seis) meses.	Não	Sim	Não	500	36
Pregão Eletrônico Nº	Licenciamento: - Trellix	Sim	Sim	Sim	1.060	36

54/2023, SECRETARIA ESPECIAL DE PORTOS, Companhia Docas do Estado de São Paulo, Código da UASG: 399003, de 28/12/2023.	Complete EndPoint Protection Business.					
Pregão Eletrônico Nº 30/2023, PREFEITURA MUNICIPAL DE SAQUAREMA, Código da UASG: 985909, de 25/01/2024.	SOLUÇÃO DE PROTEÇÃO, DETECÇÃO E RESPOSTA A INCIDENTE DE ENDPOINT, subscrição pelo período de 36 (trinta e seis) meses.	Não	Sim	Não	3.500	36
Pregão Eletrônico Nº 90001/2024, MINISTÉRIO PÚBLICO DA UNIÃO, PROCURADORIA GERAL DA JUSTIÇA, Código da UASG: 925129, de 16/01/2024.	Atualização de licença de software antivírus Kaspersky Endpoint Security for Business Select Brazilian Edition, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses	Sim	Não	Não	3.000	36
Pregão Eletrônico Nº 90048/2024, Prefeitura Municipal do Rio de Janeiro, Código da UASG: 986001, de 12/03/2024.	LICENÇA DO ANTIVÍRUS KASPERSKY ENDPOINT DETECTION AND RESPONSE OPTIMUM BRAZILIAN EDITION	Não	Sim	Não	350	12
Pregão Eletrônico Nº 7/2023, Casa Civil, Instituto Nacional de Tecnologia da Informação, Código da UASG: 243001, de 26/01/2024.	Renovação da solução de proteção de endpoints e servidores utilizados pelo Instituto Nacional de Tecnologia da Informação - ITI, que será composta por software de antivírus para estações de trabalho, dispositivos móveis e para	Sim	Não	Não	8.400	36

	servidores Windows e Linux					
Pregão Eletrônico Nº 15/2023, AGÊNCIA NACIONAL DE TRANSPORTES AQUAVIÁRIOS, homologado em 05/02/2024.	Trend micro cloud one - endpoint security with XDR, com suporte e garantia para 24 meses.	Não	Sim	Sim	1.000	24
Pregão Eletrônico Nº 90001/2024, Uasg: 389088 - CONSELHO REG. DE ENGENHARIA E AGRONOMIA - PR, de 08/02/2024.	Prestação de serviços de licenciamento e instalação de programas de computador do tipo segurança para proteção avançada de e-mails (antispam), segurança para endpoints com detecção e resposta (antivírus) e de correlação, telemetria, detecção e resposta do tipo XDR (extended detection and response).	Não	Sim	Sim	600	36
Pregão Eletrônico Nº 2/2023, CONSELHO REGIONAL DE FARMACIA DO ESTADO DE RORAIMA, Código da UASG: 926623, de 21/02/2024.	Licenciamento de Direitos Permanentes de Uso de Softwarepara Estação de Trabalho Licenças de Software Antivírus Kaspersky Endpoint Security Corporativo ou Norton Antivírus Plus.	Não	Não	Não	10	36

5.3.2. Nos últimos 12 meses, foram realizadas diversas contratações públicas relacionadas à solução de segurança de Endpoint, abrangendo uma variedade de órgãos e instituições. Vamos analisar essas informações em detalhes:

5.3.2.1. Tipos de Contratações:

5.3.2.1.1. Renovações: Alguns órgãos optaram por renovar suas licenças de segurança de endpoint, como o Tribunal de Contas do Rio Grande do Norte e o Tribunal Regional Federal da 2ª Região.

5.3.2.1.2. Novas Contratações: Outros órgãos, como o Governo do Estado da Bahia e a Prefeitura Municipal de Saquarema, realizaram novas contratações para soluções de segurança de endpoint.

5.3.2.1.3. Licenças Específicas: As licitações envolveram diferentes tipos de licenças, desde assinaturas anuais até licenças vitalícias, com suporte e atualizações garantidos por períodos específicos, como 12, 24, 36 ou 60 meses.

5.3.2.2. Funcionalidades Específicas:

5.3.2.2.1. EDR (Resposta e Detecção de Ameaças): Alguns contratos incluíram funcionalidades de EDR, que são essenciais para responder e detectar ameaças de segurança em endpoints. Por exemplo, o MMA-IBAMA e a Secretaria de Seguranca Publica do Governo do Distrito Federal optaram por soluções com funcionalidades de EDR.

5.3.2.2.2. XDR (Detecção e Resposta Estendida): Outras contratações foram para soluções que oferecem XDR, uma abordagem mais abrangente que estende a detecção e resposta para além dos endpoints. Isso foi observado em contratos como o do Governo do Estado da Bahia e o Ministério do Planejamento e Orçamento.

5.3.2.3. Quantidade e Duração:

5.3.2.3.1. O número de licenças contratadas variou consideravelmente, desde algumas dezenas até milhares, dependendo das necessidades de cada órgão.

5.3.2.3.2. A duração dos contratos também variou, com períodos de suporte e atualização que vão de 12 a 60 meses.

5.3.2.4. Órgãos Contratantes:

5.3.2.4.1. Diversos órgãos públicos participaram dessas contratações, incluindo tribunais, prefeituras, ministérios e instituições estaduais e federais, demonstrando a abrangência e a importância da segurança de endpoint em diferentes setores governamentais.

5.3.2.5. Marcas e Soluções Utilizadas:

5.3.2.5.1. Uma variedade de marcas e soluções foram contratadas, incluindo

Kaspersky, Symantec, Fortinet, Microsoft Defender, Sophos, Eset, Trend Micro, entre outras. Isso reflete a diversidade de opções disponíveis no mercado de segurança de endpoint.

5.3.2.6. Tendências e Prioridades:

5.3.2.6.1. Houve uma tendência clara em direção a soluções mais abrangentes, como aquelas que incluem funcionalidades de EDR e XDR, indicando uma crescente preocupação com a detecção e resposta proativa a ameaças de segurança.

5.3.2.7. A duração dos contratos sugere uma preferência por compromissos de longo prazo, garantindo suporte e atualizações contínuas para garantir a eficácia das soluções de segurança.

5.3.3. As contratações públicas revelam um cenário dinâmico e diversificado no qual os órgãos governamentais estão investindo em soluções de segurança de endpoint para proteger suas infraestruturas de TI contra ameaças cibernéticas cada vez mais sofisticadas e frequentes.

5.4. Considerando o mercado e a contratações públicas de proteção de Endpoint, as seguintes alternativas são consideradas para a contratação da solução de segurança de Endpoint para o TJCE:

5.4.1. Renovar e adquirir as licenças da solução atual de Kaspersky Endpoint Security for Business SELECT.

5.4.2. Contratar uma solução de antivírus com EDR/XDR que atenda às necessidades específicas do TJCE.

5.4.3. Não contratar nenhuma solução de proteção de Endpoint, mantendo apenas a solução atual, que ficará sem suporte do fabricante após abril de 2024.

5.4.4. Implantar uma solução de proteção de Endpoint gratuita.

5.5. **Identificação das Soluções**

Id	Descrição da solução (ou cenário)
1	Renovar e adquirir as licenças da solução atual de Kaspersky Endpoint Security for Business SELECT.

2	Contratar uma solução de antivírus com EDR/XDR que atenda às necessidades específicas do TJCE.
3	Não contratar nenhuma solução de proteção de Endpoint, mantendo apenas a solução atual, que ficará sem suporte do fabricante após abril de 2024.
4	Implantar uma solução de proteção de antivírus e EDR/XDR gratuita.

5.6. **Análise Comparativa de Soluções**

Requisito	**Id da Solução**	**Sim**	**Não**	**Não se Aplica**
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	**x**		
	2	**x**		
	3	**x**		
	4	**x**		
A Solução está disponível no Portal do Software Público Brasileiro?	1		**x**	
	2		**x**	
	3		**x**	
	4		**x**	
A Solução é um software livre ou software público?	1		**x**	
	2		**x**	
	3		**x**	
	4	**x**		
A Solução é aderente às políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário?	1			**x**
	2			**x**
	3			**x**
	4			**x**

A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1			**x**
	2			**x**
	3			**x**
	4			**x**
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais definidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus)?	1			**x**
	2			**x**
	3			**x**
	4			**x**

5.7. **Pesquisa de Preços de Mercado**

5.7.1. A pesquisa de mercado está presente no documento acostado aos autos do processo.

6. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

6.1. A solução 1 (Renovar e adquirir as licenças da solução atual de Kaspersky Endpoint Security for Business SELECT) é considerada inviável.

6.1.1. A solução de segurança e proteção Kaspersky atualmente implementada no ambiente de rede do Tribunal de Justiça do Estado do Ceará (TJCE) desempenha um papel crucial na defesa contra vírus e outras ameaças, proporcionando o controle sobre portas USB, arquivos infectados e a geração de relatórios, tudo isso sob uma administração centralizada. Contudo, a licença atual corresponde apenas ao plano básico oferecido pelo fabricante, o que não é mais adequado às crescentes demandas dos dispositivos conectados à rede do TJCE.

6.1.2. Observa-se que a solução atual não incorpora diversas funcionalidades essenciais para o ambiente de segurança cibernética contemporâneo. Entre essas funcionalidades ausentes, destacam-se a análise da causa raiz, que possibilita uma investigação aprofundada de ciberataques para uma avaliação completa dos vetores e uma resposta eficaz; a visibilidade e análise profunda de ameaças; a resposta automatizada e a verificação cruzada de rastreamento de vestígios de ataques; a detecção e resposta de incidentes de segurança em endpoints; o gerenciamento de criptografia; o controle adaptativo de anomalias e

gerenciamento de correções; a defesa para aplicativos e servidores de terminal; instalação de software de terceiros e de sistema operacional.

6.1.3. Ademais, a solução atual carece de características de mercado fundamentais, tais como a capacidade de detectar e prevenir ameaças por meio da análise comportamental da atividade do dispositivo, aplicação, identidade e telemetria do usuário; relatórios de risco baseados em inventário ou indicador de comprometimento, configuração e gerenciamento de políticas de dispositivos endpoint; recurso para avaliar vulnerabilidades em endpoints e gerenciar a instalação de patches ou mitigação de controles de segurança; e funcionalidade estendida de detecção e resposta (XDR) integrada nativamente ou com módulos complementares.

6.1.4. Diante dessas lacunas, torna-se evidente que as necessidades tanto de negócio quanto tecnológicas não estão sendo adequadamente atendidas. No âmbito das necessidades de negócio, destaca-se a importância de correlacionar eventos de segurança, ter funcionalidade integrada de detecção e resposta de endpoint e garantir a identificação e resposta rápida às ameaças, abrangendo todos os pontos de entrada e contando com uma interpretação baseada em comportamento. Já no que diz respeito às necessidades tecnológicas, é fundamental prevenir e detectar atividades suspeitas em endpoints, gerenciar patches e atualizações de segurança e possuir disponibilidade de recursos para reduzir a superfície de ataque e responder a incidentes de segurança da informação de maneira eficiente.

6.1.5. Nesse contexto, torna-se imperativo realizar um upgrade para uma solução de segurança de Endpoint de nova geração, que incorpore características avançadas como EDR/XDR. Tal medida é essencial para garantir uma proteção adequada e sempre atualizada ao ambiente computacional do TJCE, assegurando a preservação de ativos, incluindo hardware, software e, principalmente, dados sensíveis. Consequentemente, é inegável que a manutenção da integridade, confiabilidade, segurança e continuidade das operações organizacionais do TJCE a longo prazo requer a implementação de uma solução de segurança de Endpoint avançada.

6.2. A solução 3 (Não contratar nenhuma solução de proteção de Endpoint, mantendo apenas a solução atual de antivírus, que ficará sem suporte do fabricante após abril de 2024) é considerada inviável.

6.2.1. Atualmente, a instituição possui dois pacotes de licenças Kaspersky Endpoint Security for Business SELECT: uma com 6.500 licenças, válida até dezembro de 2023 (CT Nº 28-2020), e outra com 2.500 licenças, válida até abril de 2024 (CT Nº 09-2021), totalizando 9.000 licenças para uso.

6.2.2. Essas licenças atuais são do tipo perpétuas, o que implica que, após o término do suporte, o antivírus continuará funcionando, porém, as atualizações no software e nas vacinas e assinaturas de vírus serão interrompidas. Tal cenário levanta sérias preocupações de segurança cibernética, considerando a constante evolução das ameaças digitais e a importância de manter as defesas atualizadas para garantir a proteção adequada dos sistemas e dados.

6.2.3. Outro ponto a ser considerado é o impacto nas operações da organização. Falhas de segurança e ataques cibernéticos podem interromper as operações normais, resultando em tempo de inatividade, perda de produtividade e danos à reputação. Além disso, incidentes de segurança podem acarretar prejuízos financeiros significativos, incluindo gastos com recuperação de dados, reparos de sistemas comprometidos e custos legais.

6.2.4. Além disso, a quantidade atual de licenças não é mais capaz de abranger todos os dispositivos em uso na rede de dados do TJCE, tornando-se necessário adquirir licenças adicionais para garantir a cobertura atual e futura. O fim do suporte aos softwares que compõem a solução atual de antivírus, em abril de 2024, pode ter diversas implicações negativas para a segurança e o funcionamento dos sistemas e dispositivos do TJCE.

6.2.5. Sem atualizações de segurança regulares, os softwares desatualizados podem se tornar vulneráveis a novas ameaças cibernéticas, como vírus, malware e ataques de hackers. Além disso, o software desatualizado pode apresentar falhas de desempenho, como lentidão, travamentos e incompatibilidades com outros programas e sistemas operacionais. Há também preocupações com a conformidade, uma vez que muitos setores exigem a utilização de software atualizado e suportado para proteger dados sensíveis e informações confidenciais.

6.2.6. Sem o suporte do fabricante, o TJCE não pode obter assistência técnica para resolver problemas e realizar manutenções necessárias. É importante notar que as soluções de antivírus e proteção de endpoint evoluíram constantemente ao longo das últimas décadas, com o desenvolvimento de novas tecnologias e técnicas para lidar com ameaças cada vez mais sofisticadas no cenário de segurança cibernética.

6.2.7. É crucial destacar que todas as áreas da instituição, sejam administrativas ou judiciais, estão sujeitas a diversos riscos de segurança que podem ter repercussões significativas. Tais riscos incluem a possibilidade de interrupção de processos críticos de negócios, queda na produtividade, aumento dos custos operacionais e danos à reputação e eficácia do serviço judiciário como um todo.

6.2.8. O avanço das soluções de antivírus e das plataformas de proteção de endpoint (EPP) evidencia a necessidade premente de evolução para plataformas mais avançadas de segurança cibernética. Tais plataformas não apenas fornecem proteção contra uma ampla variedade de ameaças em constante evolução, mas também oferecem recursos adicionais para detecção e resposta proativas a incidentes de segurança.

6.2.9. É importante ressaltar que a sofisticação dos cibercriminosos está em constante crescimento, o que torna as proteções existentes vulneráveis a ataques cada vez mais elaborados. Portanto, contar apenas com uma solução de antivírus desatualizada representa um risco significativo para a segurança da instituição, uma vez que pode deixá-la exposta a ataques bem-sucedidos e suas consequências devastadoras.

6.3. A solução 4 (Implantar uma solução de proteção de antivírus gratuita) é considerada inviável.

6.3.1. Não se percebe maturidade suficiente nas opções gratuitas para atender na íntegra o presente projeto, para que possa garantir a segurança das informações confidenciais e sensíveis da instituição, além de cumprir com as normas e regulamentos aplicáveis, como a Lei Geral de Proteção de Dados (LGPD), que exige medidas de segurança adequadas para proteger as informações pessoais.

6.3.2. Soluções gratuitas oferecem suporte técnico limitado ou nenhum suporte. No caso de uma instituição governamental, é essencial ter acesso a suporte técnico confiável e rápido para resolver problemas de segurança com eficácia.

6.3.3. As soluções gratuitas podem não ser tão eficazes na detecção e prevenção de ameaças avançadas e sofisticadas, o que é vital para proteger informações críticas.

6.3.4. Portanto, para uma instituição como o TJCE, que lida com informações críticas e é alvo potencial de ataques cibernéticos, investir em uma solução de segurança paga, com recursos avançados, suporte e atualizações regulares, é uma escolha mais segura e adequada para proteger seus sistemas e dados.

7. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

7.1. Os valores utilizados neste item foram baseados nos valores médios apurados no documento de pesquisa de mercado.

7.2. Cálculo dos Custos Totais de Propriedade

Solução 2
Custo Total de Propriedade – Valores médios da pesquisa financeira
Custo de aquisição das licenças R$ 6.493.680,00 **Custo de implementação** Serviços de instalação, configuração e implantação da solução. R$ 137.030,26 Treinamento. R$ 54.733,33 **Custo de manutenção** Não há custos de manutenção relevantes, já que o suporte e garantia estão inclusos no custo de aquisição.

7.3. Mapa Comparativo dos Cálculos Totais de Propriedade (TCO)

7.3.1. Com base na análise quantitativa realizada neste estudo técnico, recomenda-se a aquisição de proteção para um total de 10.000 estações de trabalho e dispositivos móveis. No primeiro ano, seria adquirida proteção para 9.000 destes dispositivos, com um acréscimo de 1.000 unidades previsto para o segundo ano. Quanto às máquinas virtuais e servidores físicos, sugere-se a aquisição de proteção para um total de 2.000 unidades, distribuídas ao longo de dois anos. No primeiro ano, seriam adquiridas 1.500 unidades, com um acréscimo de 500 unidades previsto para o segundo ano.

7.3.2. Com isso, a estimativa de custo para o primeiro ano seria de R$ 4.086.540 referentes à aquisição de proteção para 9.000 estações de trabalho e dispositivos

móveis, mais R$ 1.464.810,00 referentes à proteção de 1.500 máquinas virtuais e servidores físicos, além de R$ 137.030,26 para serviços de instalação, configuração e implantação da solução, e R$ 54.733,33 para treinamento da solução, totalizando uma estimativa de investimento de R$ 5.743.113,59 no primeiro ano.

7.3.3. Para o segundo ano, a estimativa de custo seria de R$ 454.060,00 para a aquisição adicional de proteção para 1.000 estações de trabalho e dispositivos móveis, mais R$ 488.270,00 para a proteção de mais 500 máquinas virtuais e servidores físicos, totalizando R$ 942.330,00 no segundo ano e R$ 6.685.443,59 ao todo.

7.3.4. Essa estratégia possibilita uma implementação gradual, alinhada com a demanda prevista para cada período, oferecendo à organização a flexibilidade de ajustar seus investimentos conforme as necessidades de proteção evoluem. Na tabela a seguir, apresenta-se a Estimativa de Cálculos Totais de Propriedade (TCO) ao longo dos anos:

Solução	**Estimativa de TCO ao longo dos anos**					**Total**
	Ano 1	**Ano 2**	**Ano 3**	**Ano 4**	**Ano 5**	
Solução 2	R$ 5.743.113,59	R$ 942.330,00	R$ 0,00	R$ 0,00	R$ 0,00	**R$ 6.685.443,59**

8. IDENTIFICAÇÃO DA SOLUÇÃO ESCOLHIDA

8.1. Solução Escolhida

8.1.1. Contratar uma solução de antivírus com EDR/XDR que atenda às necessidades específicas do TJCE.

8.2. Justificativa da solução escolhida

8.2.1. A identificação das necessidades de negócio do TJCE destaca a importância de implementar uma estratégia abrangente de segurança de endpoint avançada. Essa abordagem unificada permite prevenção, detecção e resposta às ameaças, com interpretação baseada em comportamento para uma segurança mais eficaz. Além disso, correlacionar eventos de segurança em toda a infraestrutura de TI reduz o tempo de detecção e resposta, minimizando os danos potenciais. A simplificação da gestão de segurança e a visão completa da segurança cibernética

oferecida por essas soluções capacitam as equipes de segurança a tomar decisões informadas e a lidar com ameaças de forma mais eficaz. Por fim, o cumprimento das regulamentações e normas de segurança cibernética é facilitado, garantindo a conformidade com os padrões estabelecidos.

8.2.2. A identificação das necessidades tecnológicas do TJCE inclui a capacidade de identificar e bloquear ameaças avançadas e malware, prevenir atividades suspeitas, gerenciar patches e atualizações, e gerar relatórios de segurança. É crucial proteger todos os endpoints utilizados pelos colaboradores contra ameaças em constante evolução, ser compatível com sistemas operacionais, oferecer recursos avançados de gerenciamento e suporte técnico garantido. Além disso, a solução deve permitir a instalação de agentes ou sensores, investigar e corrigir ameaças, reduzir a superfície de ataque e aperfeiçoar a investigação de incidentes, incluindo uma proteção adicional para servidores.

8.2.3. O cenário atual de segurança cibernética exige uma abordagem multifacetada e em constante evolução para proteger os endpoints contra ameaças cada vez mais sofisticadas. Os fornecedores de proteção de endpoint enfrentam desafios significativos para acompanhar o ritmo das técnicas dos invasores, levando ao desenvolvimento de recursos avançados, como EDR comportamental e soluções XDR integradas.

8.2.4. Em 2023, houve um foco considerável na melhoria da eficácia da detecção e resposta a ameaças, bem como na integração de recursos mais amplos de segurança do espaço de trabalho. Os fornecedores buscam facilitar a administração e a integração de suas soluções, ao mesmo tempo em que reduzem o impacto no desempenho dos endpoints.

8.2.5. As tendências do mercado destacam a consolidação da plataforma de segurança cibernética, a defesa contra ransomware e outras ameaças, bem como a crescente adoção do trabalho remoto e da computação em nuvem. As soluções de proteção de endpoint continuam a evoluir para se tornarem plataformas abrangentes de segurança cibernética, integrando recursos de prevenção, detecção e resposta em um único ambiente.

8.2.6. Diante desse panorama em constante mudança, é essencial que as organizações adotem abordagens proativas e avançadas para proteger seus ambientes de TI contra uma ampla variedade de ameaças. As soluções de proteção

de endpoint desempenham um papel crucial nesse contexto, mas devem ser complementadas por uma estratégia de segurança cibernética abrangente e em camadas.

8.2.7. Nos últimos 12 meses, observamos uma diversidade de contratações públicas relacionadas a soluções de segurança de Endpoint, abrangendo diferentes tipos de órgãos e instituições. Estas incluíram tanto renovações de licenças existentes, como novas contratações para soluções de segurança de endpoint, com variedade nas funcionalidades, quantidade e duração dos contratos.

8.2.8. As tendências revelam uma preferência por soluções mais abrangentes, como aquelas que oferecem funcionalidades de EDR e XDR, refletindo uma crescente preocupação com a detecção e resposta proativa a ameaças de segurança. Além disso, a maioria das contratações indicou uma preferência por compromissos de longo prazo, visando garantir suporte e atualizações contínuas.

8.2.9. Considerando o mercado e as contratações públicas de proteção de Endpoint, as opções consideradas para o TJCE incluem renovar e adquirir licenças da solução atual de Kaspersky Endpoint Security, contratar uma solução de antivírus com EDR/XDR, ou optar por não contratar nenhuma solução ou implantar uma solução gratuita.

8.2.10. No entanto, as opções de renovação da solução atual e de não contratar nenhuma solução foram consideradas inviáveis devido à inadequação das soluções atuais e ao aumento dos riscos de segurança. Da mesma forma, soluções gratuitas foram consideradas inadequadas devido à falta de suporte técnico confiável e eficácia na detecção e prevenção de ameaças avançadas. Portanto, para proteger seus sistemas e dados de forma eficaz, é recomendável que o TJCE opte por uma solução de segurança paga, com recursos avançados, suporte e atualizações regulares.

8.2.11. No contexto da segurança dos endpoints utilizados pelos colaboradores do Tribunal de Justiça do Ceará (TJCE), as soluções de detecção e resposta de endpoint (EDR) e de detecção e resposta estendida (XDR) surgem como essenciais. A contratação de uma solução de EDR é necessária para monitoramento em tempo real, detecção de ameaças e investigação de incidentes nas estações de trabalho. Enquanto isso, a solução de XDR oferece uma abordagem multicamadas, proporcionando proteção abrangente contra ameaças

cibernéticas. O XDR é especialmente vantajoso para servidores de aplicações em máquinas virtuais ou físicas devido à sua capacidade avançada de proteção e adaptabilidade a ambientes virtualizados. Assim, o TJCE estará mais preparado para enfrentar os desafios das ameaças cibernéticas e proteger suas informações sensíveis e confidenciais.

8.2.12. Considerando o cenário de ameaças cibernéticas em constante evolução e a necessidade de proteger os sistemas e dados do TJCE de forma eficaz, é altamente recomendável adquirir uma solução de segurança de endpoint com suporte por um longo período, como 60 meses. Isso garantirá que a instituição tenha acesso a atualizações regulares de segurança e suporte técnico contínuo ao longo do tempo, permitindo uma resposta proativa a ameaças emergentes e a manutenção da integridade e segurança de seus sistemas.

8.2.13. Outro ponto crucial é o custo-benefício a longo prazo. Ao optar por um contrato de suporte de 60 meses, a organização pode obter preços mais vantajosos e previsibilidade financeira a longo prazo, evitando custos adicionais associados à renovação frequente de contratos ou à aquisição de soluções alternativas. Além disso, um compromisso de longo prazo proporciona estabilidade e previsibilidade, ajudando a instituição a planejar seus investimentos em segurança de forma mais eficaz e a garantir uma proteção sólida contra ameaças cibernéticas durante um período prolongado.

8.2.14. Este ETP apresenta uma análise detalhada da situação atual do número de dispositivos que requerem proteção, bem como um histórico mensal da quantidade de dispositivos com o aplicativo antivírus ativado ao longo de 2023. Os dados indicam uma tendência de crescimento anual no número de dispositivos protegidos, estimando um aumento gradual nos próximos anos.

8.2.15. Entretanto, é crucial considerar as diretrizes do Acórdão 2569/2018 do TCU, que enfatiza a necessidade de adquirir apenas o número necessário de licenças de software, evitando pagamentos antecipados e garantindo que os serviços agregados estejam vinculados às licenças efetivamente utilizadas. Além disso, a Lei de Licitações e Contratos Administrativos estabelece regras para a utilização de preços registrados, permitindo à administração pública contratar conforme a necessidade, desde que devidamente justificada.

8.2.16. Assim, para uma gestão eficiente, recomenda-se o uso da Ata de Registro de Preços, contratando apenas o número de licenças necessárias para o período imediato, com a possibilidade de adicionar mais licenças conforme a demanda. No entanto, é essencial observar o prazo máximo de validade máxima da Ata de Registro de Preços, que é de dois anos.

8.2.17. Com base na análise quantitativa da demanda, recomenda-se a aquisição de proteção para um total de 10.000 estações de trabalho e dispositivos móveis, distribuídas ao longo de dois anos. No primeiro ano, seria adquirida proteção para 9.000 destes dispositivos, com um acréscimo de 1.000 unidades previsto para o segundo ano. Quanto às máquinas virtuais e servidores físicos, sugere-se a aquisição de proteção para um total de 2.000 unidades, também distribuídas ao longo de dois anos. Isso resultaria em uma estimativa de investimento de R$ 5.743.113,59 no primeiro ano e R$ 942.330,00 no segundo ano, totalizando R$ 6.685.443,59 ao todo. Essa estratégia permite uma implementação gradual, alinhada com a demanda prevista para cada período, oferecendo à organização a flexibilidade de ajustar seus investimentos conforme as necessidades de quantidade de proteção evoluem.

8.2.18. Além disso, a aquisição do serviço de implantação da solução e treinamento é essencial para garantir uma implementação bem-sucedida da nova solução de segurança de endpoint, maximizando sua eficácia, reduzindo riscos e capacitando a equipe para lidar com desafios de uma implementação e sustentação de segurança cibernética de forma eficiente e eficaz.

8.2.19. A utilização do Sistema de Registro de Preços (SRP) se justifica pela sua eficácia em proporcionar economia, agilidade e transparência nas aquisições públicas, conforme estabelecido na Lei de Licitações e Contratos Administrativos (Lei nº 14.133, de 1º de abril de 2021). O SRP permite que órgãos públicos como o Tribunal de Justiça do Ceará (TJCE) registrem preços para a aquisição de bens e serviços comuns, como licenças de software de segurança de Endpoint, conforme necessário ao longo de um período pré-determinado.

8.2.20. Ao adotar o SRP, o TJCE tem a oportunidade de obter preços mais vantajosos por meio de economias de escala, uma vez que as licenças serão registadas em quantidades maiores, proporcionando ganhos de eficiência e redução de custos. Além disso, o SRP permite flexibilidade para a aquisição conforme a demanda

surgir ao longo do período de vigência da ata de registro de preços, respeitando os princípios da economicidade e da eficiência na administração pública.

8.2.21. A utilização do Sistema de Registro de Preços se mostra como uma alternativa eficaz e alinhada com os princípios da administração pública para a aquisição de licenças de software de segurança de Endpoint.

8.2.22. Enquanto a não realização da Intenção de Registro de Preços (IRP) pode ser justificada pela necessidade de especificidades e adaptação às demandas do TJCE.

8.2.22.1. Identifica-se a necessidade premente de conduzir o procedimento licitatório de forma célere e eficaz. A divulgação da IRP poderia atrair a participação de outros órgãos ou entidades da administração pública, transformando o TJCE em órgão gerenciador. Isso poderia resultar em uma complexidade adicional na gestão das atas, bem como em possíveis atrasos na conclusão do processo licitatório.

8.2.22.2. Além disso, constata-se a ausência de uma estrutura administrativa adequada para gerenciar as Atas de Registro de Preços. A falta de recursos humanos e infraestrutura necessários para administrar eficientemente esse processo poderia comprometer a qualidade e eficácia da gestão das atas, levando a possíveis implicações negativas na execução dos contratos.

8.2.22.3. Assim, diante dessas considerações, recomenda-se, por não divulgar a IRP, visando garantir uma gestão mais eficiente e ágil das licitações, bem como evitar possíveis sobrecargas administrativas decorrentes da participação de outros órgãos ou entidades na gestão da ata de registro de preços.

8.2.23. A solução escolhida consiste em realizar um pregão eletrônico com o objetivo de registrar uma Ata de Registro de Preço. Isso viabilizará a contratação de licenças para uma solução de segurança de Endpoint com funcionalidades de EDR/XDR, incluindo suporte e garantia pelo período de 60 meses. Além disso, o serviço também contempla a implantação da solução e o treinamento necessário para atender às necessidades específicas do Tribunal de Justiça do Ceará (TJCE).

8.2.23.1. Essa abordagem permitirá que o TJCE adquira as licenças de forma vantajosa, através de um processo de licitação transparente e competitivo.

A inclusão de suporte e garantia por um período de 60 meses proporcionará segurança e tranquilidade quanto ao funcionamento e à manutenção da solução ao longo do tempo.

8.2.23.2. Além das licenças, o serviço de implantação e treinamento garantirá que a solução seja implementada de forma eficaz e que os usuários estejam devidamente capacitados para utilizar todas as funcionalidades oferecidas. Isso contribuirá para maximizar o retorno sobre o investimento e garantir a efetividade da solução na proteção dos ativos e dados do TJCE contra ameaças cibernéticas.

9. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

9.1. Aquisição de uma solução de próxima geração, para prever, prevenir, detectar e responder a ciberataques de maneira holística, otimizada, integrada e simplificada, no âmbito do Tribunal de Justiça do Estado do Ceará (TJCE).

9.2. Deve ser fornecido o software de antivírus com EDR/XDR de acordo com o quantitativo previsto, com download do site do fabricante com devido licenciamento.

9.3. Deve ser validada a ferramenta de gerenciamento da plataforma, comprovando perante o fabricante que se trata de uma ferramenta devidamente licenciada;

9.4. A Contratada deverá elaborar e apresentar, para aprovação, o Plano de Instalação de software, envolvendo:

9.4.1. Implantação da solução sem prejuízo a operação de rede atual e minimizando o risco de segurança durante a atualização do antivírus.

9.4.2. Instalação e configuração do software de Gerência da solução.

9.4.3. Criação de regras e grupos de acordo com as melhores práticas de segurança e de acordo com as diretrizes da equipe técnica do TJCE.

9.5. As especificações completas do objeto estão descritas no documento do Termo de Referência.

10. JUSTIFICATIVA PARA O PARCELAMENTO DO OBJETO

10.1. O objeto da solução é formado pelos seguintes itens:

Item	Descrição

1	Solução de Segurança de EndPoint EDR, com manutenção, garantia (update e upgrade), e suporte do fabricante por 60 meses.
2	Solução de Segurança de EndPoint XDR, com manutenção, garantia (update e upgrade), e suporte do fabricante por 60 meses.
3	Serviços de instalação, configuração e implantação da solução.
4	Treinamento.

10.2. Uma vez que a objeto é formado por uma implementação de uma plataforma avançada e integrada de solução de segurança de endpoint, para fins de licitação do objeto deste estudo técnico recomenda-se a adjudicação dos itens em um único lote, o que simplifica a condução das atividades de gestão, fiscalização e controle do contrato, atendendo aos princípios da celeridade, economicidade e eficiência.

11. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

11.1. No contexto da aquisição de uma solução de segurança de Endpoint para o Tribunal de Justiça do Ceará (TJCE), podemos considerar as contratações como correlatas ou interdependentes, que possam impactar ou ser impactadas por essa aquisição:

11.1.1. Implantação do Centro de Operações de Segurança (SOC): O TJCE está em fase de contratação e implantação do SOC, processo nº 8521639-33.2023.8.06.0000. O SOC é um Centro de Operações de Segurança que visa garantir a proteção e integridade dos recursos computacionais da instituição. Esse centro será composto por profissionais altamente qualificados em segurança da informação, desempenhando funções cruciais para monitoramento, detecção e resposta a ameaças cibernéticas. A aquisição das licenças de software de segurança de Endpoint está diretamente relacionada ao funcionamento eficaz do SOC, uma vez que essas licenças contribuirão para a proteção dos dispositivos e sistemas que serão monitorados pelo centro.

11.1.2. Aquisição de novos computadores e notebooks: Recentemente, o TJCE realizou a aquisição de 2.030 novos computadores, processo nº 8508512-28.2023.8.06.00000, e 533 novos notebooks, processo nº 8509007-72.2023.8.06.00000. Essas aquisições são relevantes para a implementação da segurança de endpoint, pois os novos dispositivos precisarão ser configurados e protegidos adequadamente com o software de segurança de endpoint. Além disso, a garantia de 5 anos para os computadores e 3 anos para os notebooks proporciona segurança e suporte contínuo durante o período de utilização desses equipamentos.

11.1.3. Implantação da Solução de Backup: O TJCE também está em processo de contratação e implantação de uma solução de backup, processo nº 8517998-37.2023.8.06.0000. Essa solução envolve a contratação de uma empresa especializada para fornecer licenças de software de cópias de proteção, garantindo a segurança e a integridade dos dados armazenados pelo tribunal. A segurança de endpoint desempenha um papel fundamental nesse contexto, uma vez que contribui para proteger os dados nos dispositivos finais, que também serão protegidos pela solução de backup.

11.1.4. Aquisição de novos appliances de plataforma de segurança em cluster de firewalls tipo chassi (NGFW): O TJCE está projetando a aquisição de Firewalls de nova geração. O NGFW (Next-Generation Firewall) representa uma evolução dos firewalls tradicionais, concebido para oferecer uma segurança avançada e eficaz contra as ameaças cibernéticas contemporâneas. Este sistema apresenta recursos adicionais, tais como inspeção de pacotes em camadas mais profundas, detecção de ameaças baseada em comportamento e controle de aplicativos.

11.1.4.1. Integrado a uma estratégia abrangente de defesa cibernética, o NGFW complementa outras soluções de segurança, tais como sistemas de prevenção de intrusões, soluções de segurança de endpoint, gateways de segurança de e-mail e soluções de gerenciamento de ameaças. No contexto da proteção de endpoint, o NGFW desempenha um papel crucial ao regulamentar o tráfego de entrada e saída na rede, contribuindo para a salvaguarda dos dispositivos finais contra ameaças externas e prevenindo a disseminação de malware pela rede interna. Em suma, o NGFW representa um elemento fundamental na arquitetura de segurança de rede, colaborando de maneira sinérgica com as soluções de proteção de endpoint para garantir uma defesa abrangente contra as ameaças cibernéticas atuais.

11.2. Portanto, todas essas contratações correlatas ou interdependentes estão diretamente ligadas à aquisição da solução de segurança de Endpoint para o TJCE. A implementação bem-sucedida dessas soluções garantirá a segurança, integridade e disponibilidade dos recursos computacionais e dados da instituição, contribuindo para a eficácia das operações e o cumprimento das obrigações legais e regulamentares.

12. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

12.1. Os valores de estimativa de custo total da contratação foram calculados com base nas médias identificadas no estudo de mercado da solução selecionada, considerando os valores unitários médios de cada componente.

12.2. Com base na demanda identificada, estima-se que será de 12.000 unidades de dispositivos a serem protegidos, sendo o quantitativo de 10.000 (dez mil) unidades de software EDR e 2.000 (dois mil) unidades de software XDR.

12.3. Além disso, será requerido o serviço de implantação e treinamento, conforme detalhado na tabela subsequente.

12.4. Os itens designados com ID 1 e 2, na tabela a seguir, podem ser contratados de maneira progressiva, para acomodar a variação natural do número de dispositivos utilizados.

Id	Objeto	Qtd de licenças	Vlr. Unit	Vlr. Total
1	Solução de Segurança de EndPoint EDR, com manutenção, garantia (update e upgrade), e suporte do fabricante por 60 meses.	10.000	**R$ 454,06**	**R$ 4.540.600,00**
2	Solução de Segurança de EndPoint XDR, com manutenção, garantia (update e upgrade), e suporte do fabricante por 60 meses.	2.000	**R$ 976,54**	**R$ 1.953.080,00**
3	Serviços de instalação, configuração e implantação da solução.	1	**R$ 137.030,26**	**R$ 137.030,26**
4	Treinamento.	1	**R$ 54.733,33**	**R$ 54.733,33**
Total				**R$ 6.685.443,59**

13. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

13.1. Declaramos a viabilidade da contratação, conforme justificativa apresentada no item 8.2 deste Estudo Técnico Preliminar, considerando os resultados pretendidos e as metas a serem alcançadas especificadas no Documento de Oficialização da Demanda.

14. APROVAÇÃO e ASSINATURA

14.1. A contratação da solução de segurança de endpoint deverá realizada por meio de pregão eletrônico, conforme previsto na Lei nº 14.133, de 1º de abril de 2021.

Diego Francisco de Mesquita Oliveira - 48802
Integrante Técnico

Heldir Sampaio Silva - 9630
Integrante Requisitante

Andrea Antunes de Carvalho - 3270
Autoridade da Área de TIC
Fortaleza, 17 de maio de 2024.