TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO SUL
Av. Borges de Medeiros, 1565 - CEP 90110-906 - Porto Alegre - RS - www.tjrs.jus.br

ESTUDO TÉCNICO PRELIMINAR - DEPARTAMENTO DE PRODUÇÃO

Processo Administrativo nº 8.2024.0207/000109-1

Renovação de Licenciamento Perpétuo do Software Kaspersky Endpoint Security for Business Advanced com Kaspersky Endpoint Detection and Response Optimum (EDR) incluso Suporte Técnico do Fabricante por 12 meses.

Histórico de Revisões

Data	Versão	Descrição	Autor
21/06/2024	1.0	Finalização da primeira versão do documento	Marcelo da Silva Strzykalski
16/09/2024	1.1	Finalização da segunda versão do documento visando atender aos apontamentos realizados pela ASSESP (SEI nº 7073031)	Marcelo da Silva Strzykalski
04/10/2024	1.2	Finalização da terceira versão do documento visando atender aos apontamentos realizados pela Governança DITIC (SEI nº 7169656)	Marcelo da Silva Strzykalski
31/01/2025	1.3	Finalização da quarta versão do documento visando atender aos apontamentos realizados pela Seção de Segurança da Informação (SEI nº 7612186)	Marcelo da Silva Strzykalski
14/05/2025	1.4	Finalização da quinta versão do documento visando atender aos apontamentos realizados pela ASSESP (SEI nº 7961727)	Marcelo da Silva Strzykalski
06/06/2025	1.5	Finalização da sexta versão do documento visando atender aos apontamentos realizados pela ASSESP (SEI nº 8065612)	Marcelo da Silva Strzykalski

1 - DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

O Poder Judiciário possui ambiente de TI que contempla uma rede de comunicação de dados com aproximadamente 20 mil dispositivos com considerável rotatividade devido a ações de modernização tecnológica, a maioria formada por estações de trabalho com acesso à internet. É de conhecimento geral que um dos maiores problemas para a segurança das informações e a estabilidade do funcionamento de grandes redes corporativas reside em ameaças de softwares maliciosos que trafegam pela Internet, conhecidos como malwares.

Para a proteção do ambiente de TI de qualquer organização seja pública ou privada, as melhores práticas de segurança computacional e de redes recomendam a utilização de defesas em camadas, ou seja, em diversos níveis. As diferentes soluções de segurança devem estar dispostas em série e se complementarem, formando uma solução coesa e abrangente com capacidade para proteger os recursos de rede, estações de trabalho, usuários e aplicações. Assim, quando uma camada não é capaz de deter ou detectar uma ameaça ou ataque, espera-se que alguma das demais o faça de modo a mitigar os riscos envolvidos.

Um dos níveis implementados pelo Poder Judiciário consiste em solução de proteção de segurança para estações de trabalho e equipamentos servidores de rede. Atualmente, emprega-se o software Kaspersky Endpoint Security for Business Advanced (EPP) com Kaspersky Endpoint Detection and Response Optimum (EDR) para tal finalidade, cuja base de assinaturas de programas maliciosos é atualizada de acordo com a validade das licenças.

As licenças de uso e suporte técnico da plataforma de proteção do fabricante Kaspersky foram adquiridas no pregão eletrônico n° 86/2021-DEC (expediente SEI n° 8.2020.0207/000410-9) resultando na celebração do contrato n° 21/2022-DEC.

Todavia, o contrato supracitado possui vigência de 36 (trinta e seis) meses e expira em 08/02/2025, resultando na interrupção do fornecimento de novas versões dos softwares sem possibilidade de atualização das bases de assinaturas.

Consequentemente, é imprescindível para a segurança cibernética do Poder Judiciário assegurar que as estações de trabalho inclusos servidores de rede possuam softwares de proteção de segurança contra malwares e outras ameaças ativada e atualizada, alvo da contratação pretendida.

2 - ANÁLISE DE SOLUÇÕES POSSÍVEIS

A partir de análise no mercado de produtos de segurança de rede que implementam funcionalidades do tipo EPP ou EDR ou similar constata-se a existência de 2 (duas) possíveis soluções para o problema a ser sanado:

ID 1: Renovação das licenças existentes do fabricante Kaspersky permitindo a recontratação dos serviços de garantia técnica do fabricante por 12 meses.

ID 2: Aquisição de nova plataforma EPP ou EDR de outro fabricante por 12 meses.

2.1 - IDENTIFICAÇÃO DAS SOLUÇÕES

ID 1: Renovação das licenças existentes do fabricante Kaspersky permitindo a recontratação dos serviços de garantia técnica do fabricante por 12 meses.

Preliminarmente, razoável afirmar que o conjunto de elementos fáticos explanado na seção 1 pode justificar a necessidade de renovar o quantitativo de licenças de uso e de suporte técnico existente assegurando a recontratação dos serviços de garantia técnica do fabricante por 12 meses.

Não obstante, outro ponto importante a ser reportado consiste no considerável aporte financeiro dispendido pelo Poder Judiciário Gaúcho na aquisição e comissionamento da plataforma EPP/EDR do fabricante Kaspersky existentes por meio da realização do pregão eletrônico n° 86/2021-DEC e da celebração do contrato n° 21/2022-DEC.

De relevância em talcontexto, faz-se importante reportar que a aquisição de plataforma EPP/EDR de outro fabricante implicaria na troca completa da plataforma EPP/EDR ora implantada no ambiente de produção de segurança de rede do Poder Judiciário, implicando assim na perda do investimento financeiro realizado, o qual se aproxima de 4,9 % (a saber, R$ 102.501,80 - ver Tabela 2) e corresponde aos itens 2, 3 e 4 do objeto contratado.

Tal proposição encontra justificativa no fato de que ter-se-ia que contratar o fornecimento, em complemento ao novo sistema EPP/EDR a ser implantado em caso de decisão por nova contratação, dos serviços de instalação, configuração, migração e treinamento no novo sistema a ser implantado, sem comentar os custos financeiros e operacionais bem como os potenciais riscos inerentes à migração para novo sistema EPP/EDR.

A inversão financeira global realizada está sumarizada na Tabela 1 (R$ 2.100.443,00).

Tabela 1 - Valor Final do Ajuste Conforme Ata do Pregão Eletrônico n° 86/2021-DEC (Todos os Itens)

Item	Descrição	Quantidade	Valor Unitário	Valor Total

1	Fornecimento de Licenças de Sistema de Proteção de Estações de Trabalho	17.000	R$ 110,91	R$ 1.885.470,00
2	Serviços de Instalação e Configuração	1	R$ 36.214,37	R$ 36.214,37
3	Serviços de Migração	1	R$ 40.854,10	R$ 40.854,10
4	Serviços de Treinamento	1	R$ 25.433,33	R$ 25.433,33
5	Serviços de Consultoria e Suporte Técnico	360	R$ 312,42	R$ 112.471,20
			Investimento (Total)	**R$ 2.100.443,00**

Tabela 2 - Valores Financeiros Preservados Derivados do Objeto Licitado no Pregão Eletrônico n° 86/2021-DEC (Exceto Itens 1 e 5)

Item	Descrição	Quantidade	Valor Unitário	Valor Total
2	Serviços de Instalação e Configuração	1	R$ 36.214,37	R$ 36.214,37
3	Serviços de Migração	1	R$ 40.854,10	R$ 40.854,10
4	Serviços de Treinamento	1	R$ 25.433,33	R$ 25.433,33
			Investimento (Parcial)	**R$ 102.501,80**

Embora possa ser alegado que possam existir alternativas no mercado de TIC, as evidências coletadas pela área técnica sugerem que a plataforma EPP/EDR do fabricante Kaspersky tem atendido de forma adequada aos casos de uso empregados pelo Poder Judiciário no que tange aos requisitos técnicos que devem ser atendidos por um sistema da categoria EPP/EDR desde seu comissionamento na arquitetura de serviços de segurança em uso.

Razoável afirmar que a recontratação da plataforma EPP/EDR assegura a preservação das receitas orçamentárias consumidas na contratação anterior no percentual supramencionado (≈ 4,9 %) que foram empregadas na contratação dos serviços de instalação, configuração, migração e treinamento da atual plataforma do fabricante Kaspersky.

Por outro lado, cabe reportar que a escolha da marca Kaspersky se deve ao fato de que produtos de fabricantes diferentes não são intercambiáveis, visto que os componentes de *software* que compõem as diversas soluções EPP/EDR não são compatíveis entre si nem tampouco intercambiáveis, portanto, não há como atualizar tecnologicamente um sistema EPP/EDR do fabricante Kaspersky com módulos de *software* de outros fabricantes.

No que tange aos aspectos legais da pretensão contratual, a alínea a) inciso V do art. 40 da Lei nº 14.133/21 determina que as compras, sempre que possível, deverão atender ao princípio da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho, sempre que houver conveniência e oportunidade.

Nessa esteira de entendimento, cumpre mencionar a lição do ilustre professor Marçal Justen Filho, ao comentar o princípio da padronização, *in verbis*:

"A padronização é regra. No caso, a Administração deverá ter em vista aquisições passadas e futuras. A padronização aplica-se não apenas a uma compra específica, especialmente quando se trate de bem de vida útil continuada. Ao selecionar o fornecedor para produtos não consumíveis, a Administração deverá ter em vista produtos semelhantes que já integram o patrimônio público, como também deverá prever eventuais futuras aquisições. Somente assim a padronização produzirá os efeitos desejados, consistentes na redução de custos de manutenção, simplificação de mão-de-obra etc."

(JUSTEN FILHO, Marçal. Comentários à Lei de Licitações e Contratos Administrativos, 13ª ed. São Paulo: Dialética, 2010, p. 176).

No caso concreto, a escolha da marca foi estabelecida, baseada no princípio da padronização, previsto no artigo 40, Alínea a), Inciso I, da Lei 14.133/21, encontrando embasamento no pensamento do aludido doutrinador.

Devendo ser enfatizado que a solução exigida na contratação pretendida consiste em solução padronizada de EPP/EDR que se encontra em funcionamento no ambiente corporativo desde meados de 2022, enquanto o corpo técnico do DITIC já possui capacitação na solução em operação sem maiores percalços na sustentação do serviço resultando em redução de custos com manutenção e mão-de-obra.

Além disso, ao se modificar a solução, existiriam custos adicionais de capacitação do corpo técnico, uma vez que um simples treinamento em nova solução não seria suficiente para dar o mesmo embasamento na solução ao corpo técnico que foi adquirido durante praticamente 3 anos de experiência, sem falar na readequação dos procedimentos operacionais e processos de trabalho relativos à solução de segurança a ser implantada.

Apesar de que não se possa duvidar a despeito das vantagens propiciadas pela padronização, supostamente não haverá qualquer tipo de cerceamento ou limitação aos participantes do certame licitatório. visto haver outros fornecedores da solução pretendida em condições de ofertá-la.

Desta forma, em que pese a existência de outras soluções similares, conclui-se que a escolha da manutenção da solução atualmente implantada, assegurando a atualização tecnológica da plataforma EPP/EDR em operação, poderá trazer ao Poder

Judiciário Gaúcho os seguintes benefícios:

- Aproveitamento da "expertise" da equipe técnica na solução atualmente implantada.
- Baixo custo na absorção de novas tecnologias, tendo em vista a familiaridade com a solução já implantada.
- Amplificação da camada de proteção e disponibilidade da informação.
- Redução do tempo de implantação, tendo em vista que parte da solução já se encontra operacional.
- Eficiência do trabalho, diminuindo custos administrativos.
- Proteção, autenticidade e acessibilidade as informações.
- Várias camadas de proteção fornecidas por empresa líder do mercado de segurança de dispositivos e aplicações.
- Implementação e operações simplificadas com rápida implementação e mínimo de interrupção no ambiente produtivo através do gerenciamento fácil e do uso otimizado dos recursos do sistema EPP/EDR em operação.
- Proteção de rede abrangente contra ameaças maliciosas direcionadas aos sistemas operacionais Windows e Linux em operação no parque tecnológico do Poder Judiciário empregados pela totalidade de aplicações disponibilizadas aos usuários.

Nesse diapasão, cabe enfatizar que por sua vez a nova Lei de Licitações e Contratos (Lei nº 14.133/2021 - Art. 41) provê idêntico dispositivo relativo à exigência de marca permitindo a indicação de marca caso seja necessário manter a compatibilidade com plataforma já adotada pelo órgão ou entidade da Administração, com fulcro no corolário do princípio da padronização, sugerindo suplementarmente que o pleito demandado pela área técnica atende à legislação aplicável, salvo entendimento diverso:

“Art. 41. No caso de licitação que envolva o fornecimento de bens, a Administração poderá excepcionalmente:

I - indicar uma ou mais marcas ou modelos, desde que formalmente justificado, nas seguintes hipóteses:

b) em decorrência da necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração;”

Por outro lado, o Poder Judiciário recentemente contratou a empresa TELETEX COMPUTADORES E SISTEMAS LTDA para fins da prestação dos serviços gerenciados de segurança da informação conforme pregão eletrônico 5/2022 e contrato n° 62/2022-DEC [1], cujo objeto do processo licitatório consiste em:

Lote	Item	Descrição / Especificação	Unidade	Quantidade
1	1	Administração, gerenciamento e monitoração, remotos, do Serviço de Next Generation Firewall (hardware, software e licenças fornecidos pela CONTRATANTE)	Mês	24
	2	Administração, gerenciamento e monitoração, remotos, do Serviço de VPN - Redes Privadas Virtuais (hardware, software e licenças fornecidos pela CONTRATANTE)	Mês	24
	3	Administração, gerenciamento e monitoração, remotos, do Serviço de IDS/IPS - Sistemas de Detecção e Prevenção de Intrusão (hardware, software e licenças fornecidos pela CONTRATANTE)	Mês	24
	4	Administração, gerenciamento e monitoração, remotos, do Serviço de Firewall de Aplicação (WAF) (hardware, software e licenças fornecidos pela CONTRATANTE)	Mês	24
	5	Administração, gerenciamento e monitoração, remotos, do Serviço de Anti-SPAM (hardware, software e licenças fornecidos pela CONTRATANTE)	Mês	24
	6	Administração, gerenciamento e monitoração, remotos, do Serviço de Proxy/Filtro de Conteúdo Web (hardware, software e licenças fornecidos pela CONTRATANTE)	Mês	24
	7	**Administração, gerenciamento e monitoração, remotos, do Serviço de Antivírus Corporativo - ambiente de Desktop e Servidores (software e licenças fornecidos pela CONTRATANTE)**	**Mês**	**24**
	8	Implantação, administração, gerenciamento e monitoração, remotos, do Serviço de Gestão de Vulnerabilidades, com hardware, software e licenças fornecidos pela CONTRATADA	Mês	24

	9	Implantação, administração, gerenciamento e monitoração, remotos, do Serviço de filtro de DNS (Domain Name System), com hardware, software e licenças fornecidas pela CONTRATADA	Mês	24
	10	Implantação, administração, gerenciamento e monitoração, remotos, do Serviço de PAM (Privileged Access Management), com hardware, software e licenças fornecidas pela CONTRATADA	Mês	24
2	1	Implantação, administração, gerenciamento e monitoração, remotos, do Serviço de Network Detection and Response (NDR), com hardware, software e licenças fornecidos, pela CONTRATADA.	Mês	24
	2	Administração, gerenciamento e monitoração, remotos, do Serviço de SIEM (Security Information and Event Management), com porte da solução existente, fornecida pela CONTRATANTE, para nova solução utilizando a stack Elastic Security, com software, licenças e subscrições fornecidas pela CONTRATADA em nome da CONTRATANTE, que será a proprietária da solução desenvolvida.	Mês	24
	3	Serviço de Gestão de Incidentes de Segurança para analisar, remediar, conter e documentar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação, obedecendo os principais frameworks de gestão de incidentes de segurança da informação e boas práticas de mercado	Mês	24
	4	Implantação, administração, gerenciamento e monitoração, remotos, do Serviço de Testes de Invasão, com hardware, software e licenças fornecidos pela CONTRATADA	Mês	24

Particularmente, deve ser enfatizado que o item 7 (destacado em negrito) exige a prestação dos serviços técnicos especializados continuados, durante 24 (vinte e quatro) meses prorrogáveis até o limite de 36 (trinta e seis) meses, das atividades de administração/gerenciamento/monitoração de forma remota dos serviços de EPP/EDR atualmente implementados pela plataforma do fabricante Kaspersky, posto a generalidade do descritivo do item 7 do objeto contratado.

Relevante informar em tal contexto que recentemente foi autorizado pela Administração a celebração do 1º Termo Aditivo de Contrato (documento SEI nº 5950387) assegurando a prorrogação da vigência do contrato celebrado com a empresa supracitada pelo prazo de 12 meses, a contar de 01/04/2024, conforme autos do processo de acompanhamento nº 8.2022.4776/000028-9.

Por sua vez, tal exigência pode ser expressamente identificada no Anexo B do caderno de especificações técnicas do edital, reproduzido a seguir para contextualização:

Anexo B - Caderno de Especificações Técnicas do Edital

ATIVOS DE SEGURANÇA DA INFORMAÇÃO - LOTE 1 E 2

Serviço	**Marca/Modelo do Ativo**	**Quantidade**
Serviço de Next Generation Firewall	Fortinet FortiGate 1500D	4
Serviço de VPN – Redes Privadas Virtuais	Fortinet FortiGate 1500D	2
Serviço de IDS/IPS – Sistemas de Detecção e Prevenção de Intrusos	Fortinet FortiGate 1500D	2
Serviço de Firewall de Aplicação (WAF)	A10 Thunder ADC 5440S	2
Serviço de Anti-SPAM	Postfix + Amavisd	4
Serviço de Proxy/Filtro de Conteúdo Web	McAfee Web Gateway WBG-5500-D	3
Serviço de Antivírus Corporativo – ambiente de Desktop e Servidores	**McAfee Endpoint Threat Defense (ETD) + McAfee Endpoint Threat Protection (ETP) - <u>importante ressaltar que todos os componentes da plataforma antivírus do fabricante McAfee foram migrados para a plataforma do fabricante Kaspersky no 2° semestre de 2022 enquanto a contratação dos serviços gerenciados de segurança da informação foi realizada no início de 2022.</u>**	**18000**
Serviço de SIEM (área de armazenamento atual em 30TB)	McAfee Enterprise Security Manager (ESM)	2
	McAfee Enterprise Log Manager (ELM)	2
	McAfee Event Receiver (ERC)	4

Dessa forma, razoável presumir que a solução proposta resulta em benefício adicional ao garantir a preservação do conhecimento obtido pela equipe de profissionais terceirizados na execução dos serviços gerenciados de segurança cibernética

relacionados aos componentes de software da plataforma EPP/EDR do fabricante Kaspersky regulados pelo contrato n° 21/2022-DEC.

Tal premissa aplica-se por analogia aos servidores do quadro técnico do DITIC que apoiam tais profissionais terceirizados na investigação/diagnóstico e resolução de problemas que exigem maior conhecimento teórico-prático devido sua maior complexidade na plataforma EPP/EDR supracitada.

Em síntese, para escolha da solução mais adequada para a Administração é patente a análise de diversas questões, mas, principalmente, as de ordem técnica e financeira.

Conforme citado anteriormente, o Poder Judiciário despendeu recursos financeiros para a primeira aquisição da solução de segurança cibernética do fabricante Kaspersky, implantando-a em todo o parque tecnológico. Logo, não havendo registros de problemas e necessidade de mudança, enseja-se a continuidade da solução.

De pronto, pode-se afirmar que outra solução de mercado que porventura fosse implantada no ambiente tecnológico do Poder Judiciário poderia gerar riscos, como, por exemplo, incompatibilidades e conflitos entre versões dos componentes EPP/EDR e sistemas operacionais em uso nos computadores, bem como o custo de tempo por parte da equipe técnica para observação e validação da nova solução.

Ressalta-se que os operadores e os técnicos de suporte à solução do quadro e terceirizados foram capacitados para uso do ambiente e a troca do ambiente, além da do fator econômico, ou seja, substituir a solução existente, ainda implicaria na requalificação de toda a equipe, tantos os técnicos quanto dos operadores da solução, mesmo por que a solução de antivírus ainda está em garantia.

Ainda, com a contratação pretendida haveria redução da complexidade do ambiente já que atualmente é empregada uma console única para gerenciamento e administração da solução (Servidor de Administração do KSC). A utilização de ferramentas de diversos fabricantes envolve múltiplas interações entre os agentes que os compõe, causando lentidão em uma pronta resposta.

Por conseguinte, entende-se que a padronização do parque tecnológico é um importante ponto a ser considerado, pois facilita a gestão e a compatibilização destes com os demais dispositivos computacionais existentes no ambiente tecnológico. Assim, com a continuidade da solução fabricante Kaspersky se daria o aproveitamento desse investimento anterior, o que garantiria a economia de recursos financeiros, ou seja, será possível o uso do ambiente atual para a distribuição das licenças que serão adquiridas, bem como a manutenção do parque existente, onde toda gestão e gerência da ferramenta ficarão em tão somente uma única console.

Somado a isso, o aproveitamento de investimento prévio, na aquisição das licenças de plataforma Endpoint Security (EPP) traz uma vantagem competitiva para o fabricante Kaspersky, uma vez que não seria necessário aquisição de novas licenças para proteção dos ativos (computadores, notebooks, celulares, dentre outros) já utilizados no Poder Judiciário, mas somente o direito de atualização das 17.000 licenças existentes.

Com o fito de embasar o cenário proposto, salutar a análise do enunciado nº 270 da Súmula da Jurisprudência do TCU: “Em licitações referentes a compras, inclusive de softwares, é possível a indicação de marca, desde que seja estritamente necessária para atender exigências de padronização e que haja prévia justificação”. Este entendimento, que resguarda, além do parâmetro de qualidade, a facilitação na descrição do objeto almejado, se alinha perfeitamente ao caso em comento, tornando efetivo o princípio da padronização contido no artigo 15, inciso I da Lei 8.666/93, com correspondência explícita ao disposto no art. 40 da nova Lei nº 14.133/21.

Nesta baila, segue entendimento doutrinário do jurista Marçal Justen Filho: “É possível a contratação de fornecedores exclusivos ou a preferência por certas marcas desde que essa seja a solução mais adequada para satisfazer as necessidades coletivas. Não se admite a opção arbitrária, destinada a beneficiar determinado fornecedor ou fabricante.”

Do ponto de vista da economicidade, a renovação das licenças do software de segurança EPP/EDR do fabricante Kaspersky implica não ser necessário o custo adicional para a contratação de treinamento especializado para capacitar os servidores e técnicos envolvidos. É importante esclarecer que a opção pela continuidade da solução já adotada da marca Kaspersky não se dá somente por aproveitamento de investimento prévio, mas principalmente pela qualidade do serviço e dos resultados até então alcançados com uso da plataforma durante o período de vigência do contrato n° 21/2022-DEC.

Do ponto de vista técnico, o DITIC desenvolveu experiência prática em lidar com incidentes e problemas durante os 3 (três) anos em que a solução de segurança Kaspersky para estações de trabalho se encontra em operação no órgão. Razoável inferir que dispor desta experiência na solução atual assegura melhores condições na identificação, efetividade e celeridade na resolução de problemas que se apresentem no decorrer do tempo.

Por fim, o TCU, em diversos julgados, tem se manifestado pela possibilidade excepcional de indicação de marca em licitações, desde que fundadas em razões de ordem técnica ou econômica, devidamente justificadas, como feito in casu, hipóteses nas quais não há ofensa ao princípio da isonomia, nem tampouco restrições ao caráter competitivo do certame (Decisão n. 664/2001 - Plenário; Acórdão n. 1.010/2005 - Plenário e Acórdão n. 1.685/2004 - 2ª Câmara). (TCU, Acórdão 1.122/2010, Primeira Câmara, Rel. Min. Marcos Bemquerer Costa, DOU 12/03/2010). Uma eventual substituição de marca resultaria não somente no descarte precoce de licenças em plenas condições de uso, mas também na perda da *expertise* adquirida pela equipe técnica do DITIC na utilização da solução da fabricante Kaspersky.

Visando dimensionar o custo do cenário proposto, para fins de obtenção da estimativa do valor a ser gasto com a contratação em estudo, a equipe de planejamento da contratação efetuou pesquisa de preços em editais publicados no Portal de Compras

Governamentais em busca de contratações similares de outros órgãos públicos, tomando como base os procedimentos administrativos recomendados em:

- Ato 56/2015-P TJRS.
- Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação (subitem 6.1.7).
- Instrução Normativa nº 5/2014-SLTI/MPOG [2] (art. 2º) complementada por esclarecimentos publicados pela SLTI no Guia Versão 1.0/2014 [3] e pela TIControle na Orientação Técnica nº 01/2010 [4].

Mais especificamente, foram reunidas as informações de valores referentes à pesquisa de editais e recentes contratações similares de outros órgãos, a partir do qual foram selecionados editais com graus de similaridade suficientes para fins de comparação de preços praticados, sendo efetuado ao término a normalização dos valores com base na métrica preço mensal por dispositivo protegido conforme segue:

Órgão da Administração	**Licitação**	**Objeto**	**Custo Global**	**Custo Normalizado (Dispositivo protegido/mês)**
Processamento de Dados Amazonas S.A. (PRODAM)	Pregão Eletrônico n° 05-2023	Registro de preços para o fornecimento de licenças de antivírus Kaspersky para compor "prateleira" de produtos e serviços a serem comercializados pela PRODAM a seus clientes e consumidos pela própria PRODAM.	Item 1 - Kaspersky Endpoint Detection and Response Optimum - com validade de 36 meses - 5.000 licenças - valor unitário de R$ 230,00 - valor global de R$ 1.150.000,00	R$ 1.150.000,00 /5.000/36 = R$ 6,39
Tribunal de Justiça do Estado do Maranhão (TJMA)	Pregão Eletrônico n° 08-2023	Contratação de empresa especializada para a renovação das licenças de uso do Software Antvírus Kaspersky Endpoint Security for Business ADVANCED com suporte técnico remoto.	Item 1 - Fornecimento da renovação de licenças de uso do software de antivírus Kaspersky Endpoint Security For Business com upgrade para ADVANCED, com suporte técnico, por 3 anos - 10.000 licenças - valor unitário de R$ 143,00 - valor global de R$ 1.430.000,00	R$ 1.430.000,00/10.000/36 = R$ 3,97
Comissão Nacional de Energia Nuclear (CNEN)	Pregão Eletrônico n° 12-2023	Registro de Preços para a contratação de solução para proteção de endpoints e servidores de rede, incluindo serviços de migração da solução e gerenciamento, por lote único, conforme especificações e quantidades indicadas neste Termo de Referência e seus anexos.	Item 1 - Subscrição de licenças para Proteção de Endpoint - Windows por 24 meses - 4.520 licenças – preço unitário de - valor unitário de R$ 191,00 - valor global de R$ 863.320,00	R$ 863.320,00/4.520/24 = R$ 7,96
Centro Logístico da Aeronáutica (CELOG)	Pregão Eletrônico n° 90008-2024	Contratação e renovação de licenciamento perpétuo do software Kaspersky Endpoint Security – ADVANCED com Kaspersky Endpoint Detection and Response Optimum	Item 1 - Renovação da atualização de licenciamento perpétuo do software Kaspersky Endpoint Security – ADVANCED com Kaspersky Endpoint Detection and Response Optimum (EDR), por 36 meses - 40.000 licenças - preço unitário de R$ 162,92 - valor global de R$ R$ 6.516.800,00	R$ 6.516.800,00/40.000/36 = R$ 4,52
			μ =	**R$ 5,71**

Relevante salientar que tal valor normalizado será empregado como preço unitário referencial na seção que trata da estimativa do valor unitário da contratação.

Por fim, a solução proposta assegura a preservação do conhecimento adquirido pela equipe técnica do DITIC na administração da atual plataforma EPP/EDR e dos investimentos realizados na aquisição das licenças adquiridas em caráter perpétuo do fabricante Kaspersky, as quais tem atendido aos requisitos técnicos exigidos originalmente de forma satisfatória.

ID 2: Aquisição de nova plataforma EPP ou EDR de outro fabricante por 12 meses.

Consiste na aquisição de licenças de solução de proteção contra ameaças cibernéticas de estações e servidores (EPP + EDR) de um fabricante genérico que atenda aos requisitos técnicos a serem mapeados pela equipe técnica no Termo de Referência a ser elaborado e atendidos pela solução a ser ofertada com 12 meses de garantia técnica do fabricante.

Entretanto, a troca de produtos por outro fabricante resulta nos desafios listados abaixo:

- A produção de nova base de conhecimento técnico especializado pela equipe terceirizada/quadro de servidores junto aos novos produtos ofertados durante o período de vigência dos serviços de garantia técnica do fabricante.
- Aumento do tempo de implantação posto que a nova solução deverá ser comissionada do zero no ambiente de centro de dados do contratante resultando em ajustes e readequações de aplicações/serviços e infraestrutura existentes.
- A importação/mapeamento/criação de regras e estruturas criadas durante o ciclo de vida de uso dos novos produtos ofertados.
- Definição dos controles de acesso para manutenção dos níveis de segurança.
- Adequações da camada de proteção e disponibilidade da informação.
- Atualização, manutenção tecnológica e suporte com vistas a atender às novas características técnicas e operacionais da infraestrutura tecnológica existente.
- Atualização tecnológica dos recursos humanos envolvidos na área de segurança (custos com treinamento).

Logo, tal cenário fático torna a solução proposta inviável devido ao considerável esforço necessário na implantação da nova solução com alto risco técnico/operacional.

2.2 - ANÁLISE COMPARATIVA DE SOLUÇÕES

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
A Solução está disponível no Portal do Software Público Brasileiro?	Solução 1			X
	Solução 2			X
A Solução é composta por software livre ou software público?	Solução 1			X
	Solução 2			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
A Solução é aderente às regulamentações da ICP-Brasil?	Solução 1			X
	Solução 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	Solução 1			X
	Solução 2			X

2.3 - PESQUISA DE PREÇOS DE MERCADO

Id	Descrição da solução
1	Renovação das licenças existentes do fabricante Kaspersky permitindo a recontratação dos serviços de garantia técnica do fabricante por 12 meses.
2	Aquisição de nova plataforma EPP ou EDR de outro fabricante por 12 meses.

3 - ANÁLISE COMPARATIVA DE CUSTOS (TCO)

3.1 - CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

Solução Viável 1

Descrição:

ID 1: Renovação das licenças existentes do fabricante Kaspersky permitindo a recontratação dos serviços de garantia técnica do fabricante por 12 meses.

Custo Total de Propriedade - Memória de Cálculo

R$ 5,71 x 17.000 x 12 = R$ 1.164.840,00

Solução Viável 2

Descrição:

ID 2: Aquisição de nova plataforma EPP ou EDR de outro fabricante por 12 meses.

Custo Total de Propriedade - Memória de Cálculo

(R$ 863.320,00 (R$ 191,00 x 4.520 licenças)) / 2 = R$ 431.660,00 (contudo o valor mensal por licença consiste em R$ 7,96 (R$ 431.660,00/4.520/12))

* R$ 863.320,00 / 2 (24 meses) = R$ 431.660,00 por ano (tomando como referência o Pregão Eletrônico n° 12-2023 realizado pela Comissão Nacional de Energia Nuclear (CNEN)), dado o grau de similaridade dos requisitos técnicos da solução elencada com a especificação técnica do objeto do edital supracitado.

3.2 - MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Descrição da solução	Estimativa de TCO ao longo dos anos					Total
	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5	
Solução Viável 1	R$ 1.164.840,00	-	-	-	-	R$ 1.164.840,00 (R$ 5,71 por licença)
Solução Viável 2	R$ 431.660,00	-	-	-	-	R$ 431.660,00 (R$ 7,96 por licença)

4 - REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

- Não dar andamento ao processo de renovação das licenças existentes permitindo a recontratação dos serviços de garantia técnica do fabricante por 12 meses.

5 - DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Após análise comparativa das soluções identificadas, sugere-se a escolha da solução viável 1, visto assegurar a contratação dos serviços de garantia técnica do fabricante Kaspersky mitigando riscos por falhas de software com manutenção corretiva/evolutiva dos módulos EPP/EDR em operação inclusa, provendo melhor relação custo-benefício dado o cenário de uso simplificado da tecnologia EPP/EDR existente na infraestrutura de desktops e servers em funcionamento em todos os prédios do Poder Judiciário Gaúcho.

6. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

6.1 IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

A constante evolução das ameaças cibernéticas torna premente a manutenção de um sistema de proteção contra softwares maliciosos atualizado. Portanto, a proteção dos computadores é um componente cada vez mais vital da estratégia de segurança cibernética de qualquer organização.

Em 2017, o software malicioso conhecido como wannacry se espalhou pelo mundo, atingindo cerca de 230 mil computadores pelo planeta, conforme relatório da fabricante Kaspersky disponível em: <https://www.kaspersky.com.br/resource-center/threats/ransomware-wannacry>. Acesso em: 21 Jun. 2024. Somente no Brasil, mais de 220 empresas foram alvos do malware, conforme notícia do veículo de publicação Valor Econômico apud COAD disponível em: <https://www.coad.com.br/home/noticias-detalhe/79248/mais-de-220-companhias-sao-alvo-de-virus-no-pais >. Acesso em: 21 Jun. 2024.

O Poder Judiciário também teve contato com o malware específico. Porém, graças à existência da solução de antivírus adquirida previamente, o impacto do artefato malicioso foi capaz de ser contido sem maiores prejuízos para sua operação.

Razoável presumir que esse é apenas um exemplo das incontáveis ameaças cibernéticas às quais qualquer organização está submetida atualmente. De acordo com o AV-TEST Institute, um instituto de pesquisa independente para segurança de TI da Alemanha, 450 mil novos softwares maliciosos (malwares) e aplicações potencialmente indesejadas são identificados por dia. Essa estatística mostra que um software de antivírus, sem a contínua atualização de suas bases de dados, se torna, em pouquíssimo tempo, ineficaz contra-ataques cibernéticos.

Além disso, desde 2008 até 2024, o instituto identificou mais de 1.3 bilhões de malwares e aplicações potencialmente indesejadas, conforme estatísticas apontadas disponível em: <https://www.av-test.org/en/statistics/malware/>. Acesso em: 21 Jun. 2024. Não obstante, de acordo com um estudo conduzido pela Utica College, representado pelas informações disponibilizadas na dissertação "LIGGETT, Terry. Evolution of Endpoint Detection and Response Platforms. Dez. 2018, disponível em: <https://www.proquest.com/openview/3177c3dcd44c0586bb0d906f900a1524/1?pq-origsite=gscholar&cbl=18750&diss=y>. Acesso em: 21 Jun. 2024", softwares de antivírus costumam se respaldar, na detecção de novas ameaças, prioritariamente nas suas respectivas bases de assinaturas, o que pode ser limitante na identificação de ameaças desconhecidas e avançadas.

Tal estudo sugere que plataformas de EDR conseguem desempenhar esse papel através da análise de comportamento anômalo e outros indicadores/regras, característica única desse tipo de solução computacional, além de possuir funcionalidades para tratar incidentes de segurança de baixa complexidade de forma automatizada, o que vem aumentando sua demanda na indústria.

Além disso, um estudo realizado pelo Gartner, renomada empresa especializada em consultorias na área de tecnologia da informação e que foi apontado no estudo da Utica College, sugere que organizações vem procurando fazer uma integração de suas soluções de antivírus corporativo, geralmente denominadas “Endpoint Protection Platform” (EPP), com EDR para atender essa demanda emergente na indústria e melhor se protegerem.

Uma solução de segurança computacional do tipo “Endpoint Detection and Response” (EDR) assegura uma abordagem integrada e em camadas para proteção de computadores que combina monitoramento contínuo em tempo real e análise de dados com resposta automatizada baseada em regras, ou seja, detecção e resposta a um incidente de segurança mais rápido pela utilização de inteligência artificial para tal fim. Logo, a implantação de uma solução EDR é essencial para proteger os dispositivos computadores contra ameaças cibernéticas.

Mais especificamente, uma plataforma EDR foi projetada para ir além da defesa cibernética reativa baseada em detecção, ao fornecer aos analistas de segurança ferramentas para identificar proativamente ameaças e proteger os sistemas de informações, viabilizando análises contínuas de dados com reporte a um único sistema centralizado, automatizando a coleta e o processamento de dados, permitindo rapidamente a obtenção do contexto sobre um possível incidente de segurança e a adoção de medidas para solucioná-lo rapidamente, e executando automaticamente determinadas atividades de resposta a incidentes com base em regras predefinidas.

Dessa forma, pode-se considerar que a manutenção de uma solução de antivírus atualizada, com uma plataforma de EDR integrada, com suporte técnico vigente e profissionais capacitados para sua operação e gerência, é primordial para a preservação dos ativos cibernéticos do Poder Judiciário.

Outra vantagem dessa solução integrada é a diminuição de atuação imediata por partes das Equipes de Tratamento de Incidentes de Rede (ETIRs), uma vez que as funcionalidades de uma plataforma EDR podem suprir essa demanda de pronta resposta em alguns casos mais simples.

Sobretudo, se faz necessário garantir a segurança da informação para os usuários do Poder Judiciário por meio da proteção dos ativos de informática (microcomputadores, servidores, notebooks, dispositivos móveis) por meio do uso de software antivírus (EPP) com funcionalidade EDR integrada, seja no ambiente local, seja no ambiente remoto (teletrabalho).

Dada sua importância na adoção de uma arquitetura de serviços de segurança baseada em padrões e metodologias de mercado, o Poder Judiciário Gaúcho adquiriu 17.000 licenças do antivírus Kaspersky Endpoint Security for Business Advanced (EPP) com Kaspersky Endpoint Detection and Response Optimum (EDR) integrado, as quais foram adquiridas após a homologação do pregão eletrônico n° 86/2021-DEC (expediente SEI n° 8.2020.0207/000410-9) e da celebração do contrato n° 21/2022-DEC:

Descrição	**Quantidade**
Kaspersky Endpoint Detection and Response Optimum Brazilian Edition. 5000+ Node 5year Base Plus License - KL4708KAYT8	17.000

Tanto que o órgão supradito conta hoje com tais licenças instaladas nos servidores de redes e nas estações de trabalho em todas as suas unidades na capital e no interior do Estado, atuando na defesa contra vírus e outras ameaças que surgem constantemente no mundo digital, proporcionando o bom funcionamento dos equipamentos e proteção dos dados neles existentes.

A solução de segurança e proteção do fabricante Kaspersky, já homologada no ambiente do Poder Judiciário, atua na defesa contra vírus, ransowares e outras ameaças que surgem a cada instante na rede mundial de computadores (Internet), permitindo a utilização do software para controle de acesso nas portas USB, identificação, controle de detecção de intrusão, mitigação de ações maliciosas executadas em navegadores web via inspeção SSL, geração e emissão de relatórios e gerenciamento centralizado, além de proporcionar o bom funcionamento e proteção dos dados e informações sigilosas.

Entretanto, o contrato supracitado possui vigência de 36 (trinta e seis) meses e expira em 08/02/2025, resultando na interrupção do fornecimento de novas versões dos softwares sem possibilidade de atualização das bases de assinaturas empregadas pela plataforma EPP/EDR do fabricante Kaspersky.

Consequentemente, se faz necessária a renovação das licenças do software antivírus supramencionado inclusos serviços de suporte técnico do fabricante, justificando-se por ser essencial para viabilizar a proteção adequada e atualizada do ambiente computacional, permitindo preservar os ativos corporativos (hardware, software e, sobretudo dados), garantindo a integridade, a confiabilidade, a segurança e a continuidade das atividades da organização, dirimindo riscos de exposição dos dispositivos institucionais e a disseminação de malwares que possam explorar as vulnerabilidades presentes na infraestrutura do Poder Judiciário, protegendo contra ameaças digitais a partir da identificação de vulnerabilidades para impossibilitar sua exploração.

Todavia, o uso de uma nova plataforma de antivírus necessitaria de considerável esforço na sua implementação, se aproximando a no mínimo 10 meses com base em recente migração que assegurou a substituição da plataforma do fabricante McAfee existente para a nova plataforma do fabricante Kaspersky em meados de 2022, bem como custos com treinamento de pessoal na nova tecnologia, o que torna a escolha por manter a atual plataforma uma opção sensata.

Por fim, a contratação pleiteada visa atender a necessidade de continuidade dos serviços técnicos especializados de sustentação da plataforma EPP/EDR do fabricante Kaspersky na infraestrutura de TIC, em substituição ao contrato n° 21/2022-DEC, com o intuito de:

a) Entregar serviços de TIC alinhados às necessidades de negócio do TJRS.

b) Ampliar a disponibilidade dos sistemas e serviços prestados pelo TJRS.

c) Aprimorar a qualidade e a percepção de entrega de valor dos serviços prestados pelo DITIC.

6.2 IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS

Uma plataforma de proteção de*endpoint* (EPP) consiste em solução implantada em dispositivos clientes (laptop, desktop) para proteger tais dispositivos, evitando *malware* e ataques maliciosos e fornecendo recursos de investigação e correção necessários para responder dinamicamente a incidentes de segurança quando eles ofuscam os controles de proteção.

As soluções EPP tradicionais são fornecidas por meio de um agente cliente gerenciado por um servidor de gerenciamento local. Por sua vez soluções mais modernas utilizam uma arquitetura nativa em ambiente de nuvem computacional que transfere o gerenciamento e parte da carga de trabalho de análise e detecção para o ambiente de computação em nuvem.

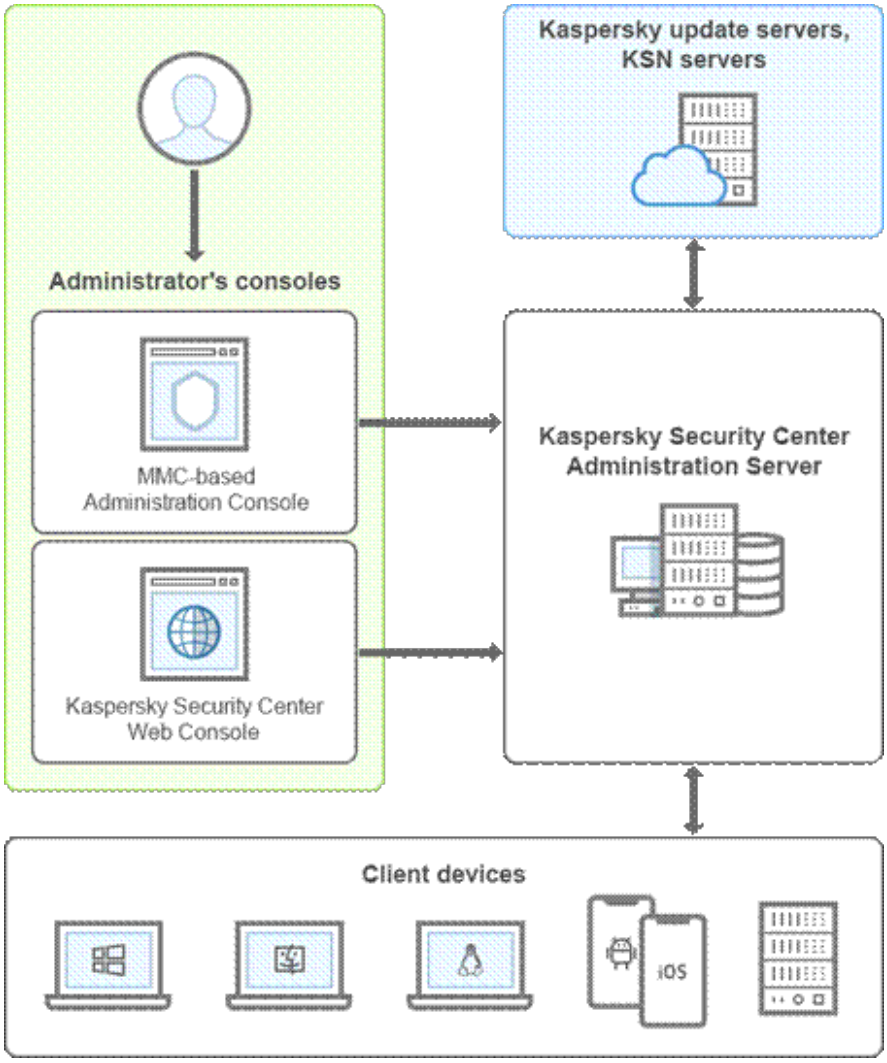
Entretanto, existe uma tendência de que clientes do mercado de segurança e de gerenciamento de risco responsáveis pela proteção de terminais estejam valorizando os recursos de detecção de ameaças avançadas sem arquivo e recursos de investigação e correção (EDR).

Tanto que em recentes quadrantes mágicos da empresa de consultoria Gartner para plataformas de proteção de*endpoints*, os recursos tradicionalmente encontrados no mercado de detecção e resposta de *endpoint* (EDR) agora são considerados componentes essenciais de um EPP que pode abordar e responder a ameaças modernas, conforme linha argumentativa exposta na seção anterior.

Por outro lado, a atual plataforma em operação do fabricante Kaspersky com módulos EPP e EDR inclusos é composta por uma arquitetura de serviços (https://support.kaspersky.com/help/KSC/14.2/en-US/4531.htm) com os seguintes elementos que interagem entre si:

- Console de Administração: fornece uma interface de usuário para os serviços de administração do Servidor de Administração e do Agente de Rede que é implementada como um snap-in do Microsoft Management Console (MMC) permitindo conexão remota ao Servidor de Administração pela Internet.
- Console Web do Kaspersky Security Center: fornece uma interface da web para criar e manter o sistema de proteção da rede de uma organização cliente gerenciada pelo Kaspersky Security Center.
- Servidor de Administração do Kaspersky Security Center (KSC): centraliza o armazenamento de informações sobre os aplicativos instalados na rede e sobre como gerenciá-los permitindo o gerenciamento remoto de aplicativos Kaspersky instalados em dispositivos clientes.

- Servidores de atualização Kaspersky: consistem em servidores web na Kaspersky a partir dos quais os aplicativos Kaspersky baixam atualizações de bancos de dados e módulos de aplicativos.
- Servidores KSN: servidores que contêm um banco de dados Kaspersky com informações constantemente atualizadas sobre a reputação de arquivos, recursos da web e software. Tal elemento arquitetural garante respostas mais rápidas dos aplicativos Kaspersky às ameaças, melhora o desempenho de alguns componentes de proteção e reduz a probabilidade de falsos positivos.
- Dispositivo Cliente Gerenciado: consiste em computador executando Windows, Linux ou MacOS no qual o Agente de Rede está instalado ou um dispositivo móvel no qual um aplicativo de segurança Kaspersky está instalado, permitindo seu gerenciamento por um Servidor de Administração que cria tarefas e políticas para aplicativos instalados nesses dispositivos.
- Ponto de Distribuição: consiste em dispositivo com o Agente de Rede instalado que é usado para distribuição de atualizações, instalação remota de aplicativos e recuperação de informações sobre dispositivos em rede, conectado a um Servidor de Administração do KSC.
- Gateway de Conexão: consiste em Agente de Rede atuando em modo especial usualmente instalado em uma zona desmilitarizada (DMZ) que aceita conexões de outros Agentes de Rede e as encaminha a um Servidor de Administração do KSC através de conexão com tal servidor.



Relevante por fim informar que o Servidor de Administração (ou hierarquia de Servidores de Administração) possui papel preponderante em tal arquitetura, sendo responsável pela descoberta de dispositivos através de *polling* regular via sondagem do Active Directory, a instalação de aplicativos usando uma tarefa de instalação remota, o gerenciamento de tarefas e de políticas [5] em aplicativos instalados dispositivos gerenciados via Agente de Rede pelo Servidor de Administração, atualização de bancos de dados/módulos de software/aplicativos da Kaspersky e distribuição de atualizações para dispositivos clientes automaticamente.

Mormente, deve ainda ser enfatizado que a tecnologia empregada nos produtos de segurança para proteção de estações e servidores incluindo prevenção de ataques avançados vem atendendo satisfatoriamente as necessidades do Poder Judiciário durante a vigência do contrato atual e encontra-se no platô do estado de maturidade de tecnologias do tipo EPP/EDR, por conseguinte não entrará em estado de obsolescência durante o período de execução contratual.

6.3. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

O escopo dos serviços contratados envolve a prestação de atualização de versão e base de assinaturas inclusos serviços de manutenção e assistência técnica da plataforma EPP/EDR do fabricante Kaspersky pelo prazo de 12 meses.

Os serviços deverão ser prestados pelo fabricante dos softwares com atualização de versões e assinaturas inclusa mão de obra especializada.

Os serviços de manutenção e assistência técnica serão realizados sob demanda, os quais serão requisitados por meio da formalização de abertura de chamado técnico junto ao fabricante.

Os serviços deverão ser prestados durante 24 horas do dia por 7 dias da semana (24 x 7), inclusive finais de semana e feriados.

6.4. PARCELAMENTO OU NÃO DA SOLUÇÃO CONTRATADA

De acordo com a Lei das Licitações e Contratos impõe-se o parcelamento do objeto quando se verifica a existência de parcela de natureza especifica que possa ser executada por empresas com especialidades distintas e for viável técnica e economicamente, desde que vantajoso para a Administração.

Por conseguinte, sugere-se que seja empregado o critério de julgamento baseado no menor preço por item, com uma única empresa sendo a fornecedora dos serviços que compõem o objeto, enquanto os serviços deverão ser prestados pelo fabricante dos softwares de segurança cibernética Kaspersky Endpoint Security for Business Advanced (EPP) e Kaspersky Endpoint Detection and Response Optimum (EDR). Ou seja, os serviços descritos nesta especificação técnica possuem dependência tecnológica intrínseca do fabricante dos softwares de segurança cibernética, uma vez que a Kaspersky, por meio de seus laboratórios de engenharia e de suporte técnico, consiste na única empresa que dispõe de todos os recursos necessários à execução dos serviços.

Sobretudo, cabe enfatizar que o objeto da contratação consiste em item único conforme subitem 2.2. do item 2 do Termo de Referência:

Lote	Item	Descrição/Especificação	Unidade	Natureza	Quantidade
1	1	KASPERSKY NEXT EDR OPTIMUM BRAZILIAN EDITION 5000+ USER 1 YEAR RENEWAL LICENSE - KL4066KAYX9	Unidade	Bem comum	17.000

Por sua vez, a pretensão contratual visa assegurar a prestação dos serviços de garantia técnica pelo fabricante Kaspersky no âmbito das licenças KASPERSKY NEXT EDR OPTIMUM existentes, com fornecimento de mão de obra especializada e manutenção corretiva/evolutiva de software, inclusa atualização de assinaturas de proteção contra ataques cibernéticos.

Relevante destacar em tal contexto que o objeto consiste na contratação de serviços prestados com exclusividade pelo fabricante dos softwares de segurança cibernética Kaspersky, comercializados por revendas autorizadas, afastando eventual justificativa para atuação simultânea de mais de uma empresa.

Embora os serviços sejam efetivamente prestados com exclusividade por mão de obra especializada fornecida pelo próprio fabricante dos softwares de segurança, tais serviços por condições intrínsecas do mercado são comumente comercializados por diversas revendas autorizadas do fabricante, logo, com viabilidade de competição entre diferentes fornecedores (ou seja, revendas do fabricante), sem exclusividade no fornecimento do serviço almejado pela Administração.

Teoricamente, tal cenário fático elucida o motivo de se contratar uma única empresa no caso concreto, justificando o não parcelamento do objeto da contratação.

Por fim, em caráter complementar, a escolha de marca e modelo pode encontrar justificativa nas seguintes razões:

- Padronização visto ser utilizado por diferentes órgãos da Administração Pública.
- Redução de custos de administração e operação.
- Aproveitamento do conhecimento já adquirido pela equipe técnica sobre a solução já contratada.

6.5. CONTRATAÇÕES CORRELATOS E INTERDEPENDENTES

Ver contrato n° 62/2022-DEC (pregão eletrônico n° 5/2022, expediente SEI n°8.2021.0207/000040-1), que versa sobre a contratação de empresa especializada na prestação de serviços gerenciados de segurança da informação.

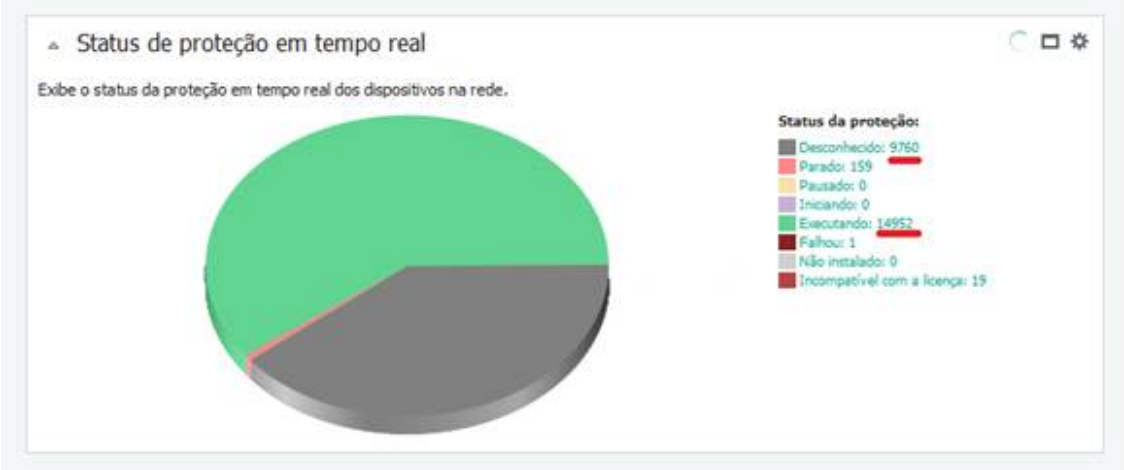
7 - ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

Visando atender à demanda mapeada far-se-á necessário a contratação dos bens e serviços enumerados a seguir:

Item	Descrição	Unidade	Quantidade
1	KASPERSKY NEXT EDR OPTIMUM BRAZILIAN EDITION 5000+ USER 1 YEAR RENEWAL LICENSE - KL4066KAYX9	Licença	17.000

Sobretudo, a quantidade estimada de licenças se fundamenta no consumo atual de licenças da plataforma EPP/EDR do

fabricante Kaspersky, mais especificamente, com base em estatísticas obtidas no servidor de administração KSC-ADMIN-01 da referida plataforma:



De acordo com a figura supracitada, o agente de rede que roda nos computadores que compõem o parque de equipamentos de informática do Poder Judiciário (desktops, notebooks e ultrabooks), sejam locais, nas dependências dos prédios do Judiciário, ou sejam remotos, em uso doméstico, está executando em aproximadamente 15.000 dispositivos (14.942), enquanto temos 9.760 dispositivos em estado desconhecido, eventualmente desligados ou efetivamente descomissionados do parque.

Por outro, pertinente mencionar que os estudos técnicos preliminares (SEI nº 7226468) do edital de pregão eletrônico nº 51/2024 (processo SEI nº 8.2023.0207/000143-5) traz uma estimativa da quantidade de equipamentos obsoletos que necessitam de substituição, baseado em relatórios extraídos do sistema de patrimônio, relacionada na tabela abaixo:

Tipo	Modelo	Tempo de uso (anos)	Quant. a substituir
Computador desktop	Dell Optiplex 7010	11	328
Computador desktop	Dell Optiplex 9020	10	2.620
Computador desktop	HP EliteDesk 800	7	8.508
Computador desktop	Dell Optiplex 7070	4,5	3.646
		Subtotal desktop	**15.102**
Computador portátil	Dell Latitude E6420	13	472
Computador portátil	Lenovo ThinkPad T450s	9	454
Computador portátil	Dell Latitude 5410/5420	3	2.563
		Subtotal portátil	**3.489**
		Total	**18.591**

Como pode ser verificado, a volumetria de equipamentos do tipo desktop (15.102) se aproxima do número de dispositivos com proteção ativada (14.942).

Por outro lado, a volumetria de equipamentos do tipo portátil (3.489) é significativa e exige o consumo de licenças da solução de segurança EPP/EDR do fabricante Kaspersky, sendo que potencialmente muitos equipamentos dessa categoria eventualmente seguem desligados ou efetivamente já foram descomissionados do parque, de tal forma que essa necessidade é vigentemente atendida pelo saldo residual de 2.000 licenças.

Por sua vez, cabe ainda ressaltar que o saldo residual de 2.000 licenças também é usualmente empregado durante a fase de "rolllout" (troca) dos equipamentos com certo grau de obsolescência por equipamentos de informática atualizados, tendo como objetivo manter a celeridade, confiabilidade e qualidade demandadas pela área judicante no exercício de suas atividades, assegurando a proteção do parque.

Razoável presumir que tal cenário complementarmente atende a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) definida pela Resolução nº396-CNJ de 07/06/2021 em seu art. 6º: "São objetivos da ENSEC-PJ (...) IV – permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível."

Assim sendo, é lógico inferir que para atingir tal objetivo, se faz necessário que os equipamentos estejam tecnologicamente atualizados em termos de hardware e software para aplicar as melhores práticas de manutenção e proteção de dados, requisito atendido pela contratação pleiteada incluso o pregão eletrônico nº 51/2024.

8 - PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO, INCLUSIVE QUANTO À CAPACITAÇÃO DE SERVIDORES OU DE EMPREGADOS PARA FISCALIZAÇÃO E GESTÃO CONTRATUAL

Não far-se-á necessário, visto que os servidores já foram capacitados no uso dos softwares empregados no projeto de implantação assegurando o conhecimento técnico necessário na fiscalização e gestão contratual.

9 - ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

O custo estimado da contratação consiste em R$ 1.164.840,00, levando em conta o prazo de vigência contratual de 12 meses, com base em memória de cálculo cujo valor unitário foi formulado com fundamento no preço unitário referencial obtido em contratações similares apresentadas na tabela contida no subitem 2.1, ID 1, reproduzida abaixo:

Solução Viável 1
Descrição:
ID 1: Renovação das licenças existentes do fabricante Kaspersky permitindo a recontratação dos serviços de garantia técnica do fabricante por 12 meses.
Custo Total de Propriedade - Memória de Cálculo R$ 5,71 (valor médio normalizado obtido de contratações públicas similares referente à fornecimento de licenças de antivírus Kaspersky apresentado no subitem 2.1, ID 1) x 17.000 x 12 = R$ 1.164.840,00

10 - DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS E FINANCEIROS DISPONÍVEIS

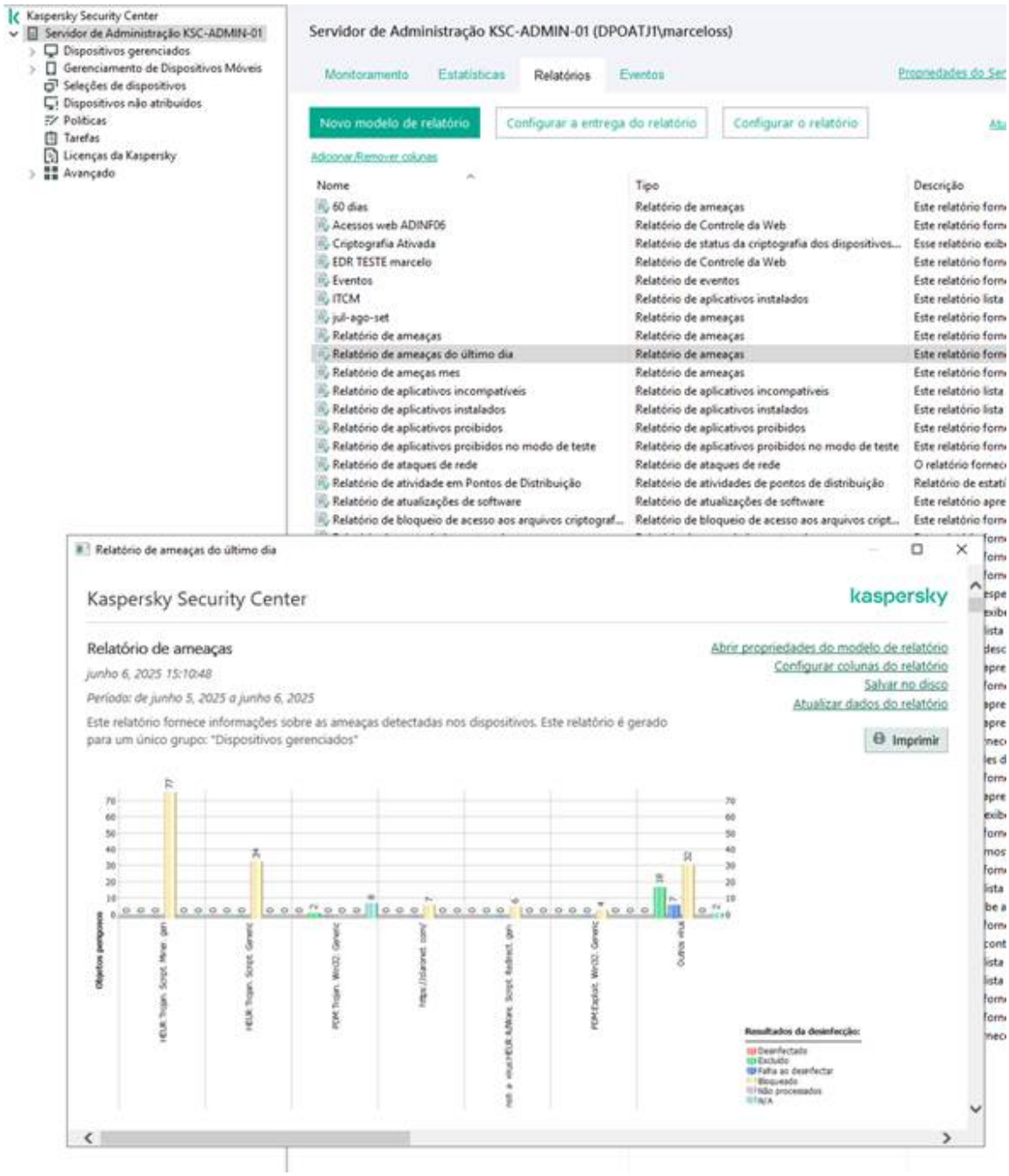
A contratação pretendida visa à contratação dos serviços de garantia técnica do fabricante Kaspersky para 17.000 licenças dos softwares de segurança cibernética Kaspersky Endpoint Security for Business Advanced (EPP) e Kaspersky Endpoint Detection and Response Optimum (EDR) existentes por 12 meses com atualização corretiva e evolutiva de software inclusos atualização das assinaturas de ataques cibernéticos e fornecimento de mão de obra especializada para tal fim, uma vez que somente o fabricante possui o “know how” necessário para executar tais serviços com exclusividade no desenvolvimento de novas versões e vacinas/ assinaturas contra ataques cibernéticos/detecção heurística com fornecimento mão de obra especializada.

Consequentemente, os serviços deverão prover informação, assistência e orientação para: instalação, desinstalação, configuração, substituição e atualização de programas (*software*), aplicação de correções (*patches*), diagnósticos, avaliações e resolução de problemas, ajustes finos e customização, bem como demais atividades relacionadas à correta operação e funcionamento da solução na rede do Poder Judiciário.

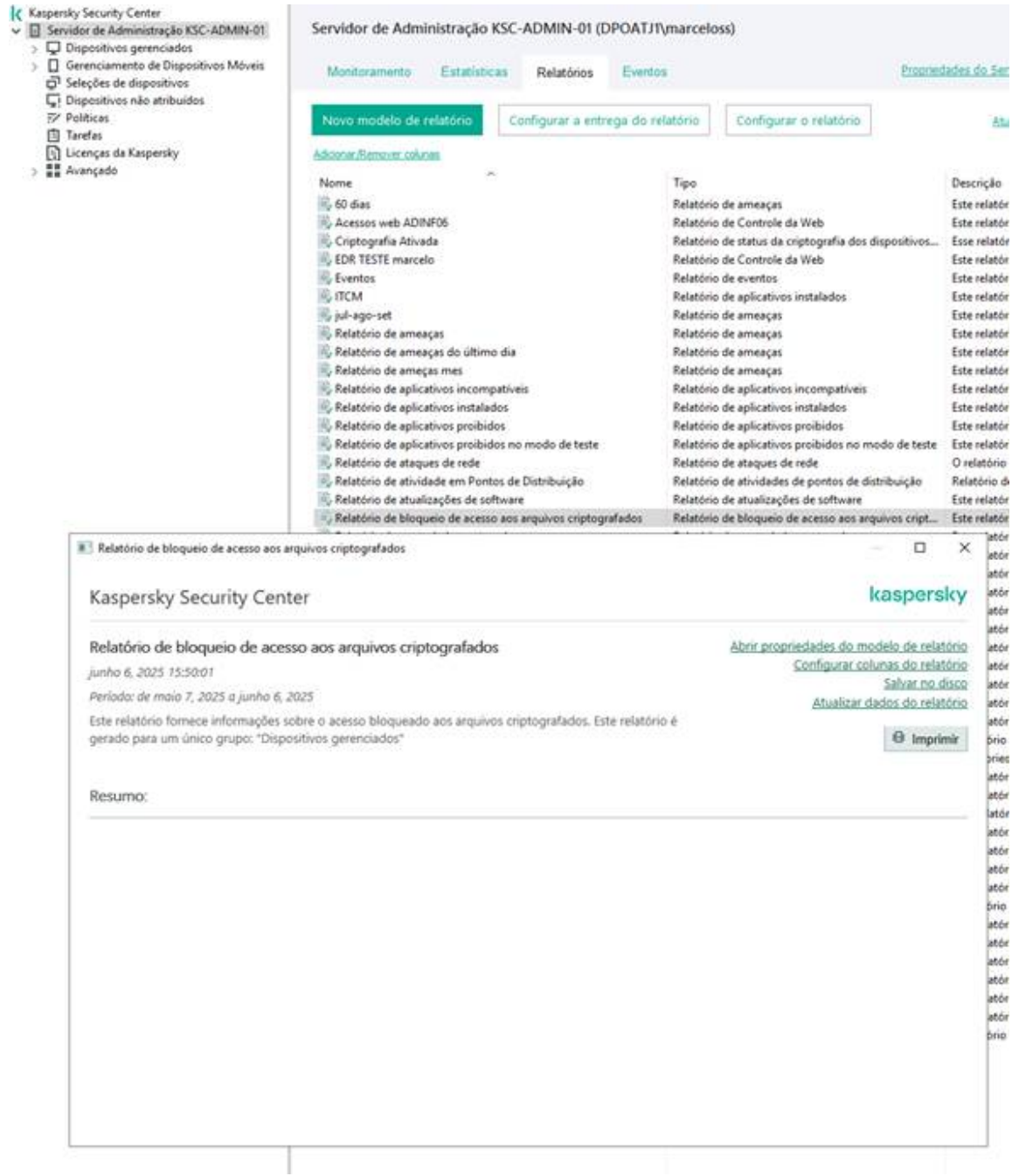
Logo, supostamente tal cenário pode resultar no melhor aproveitamento dos recursos humanos disponíveis, uma vez que os serviços deverão ser executados com exclusividade pelo fabricante, posto que não poderiam ser executados pelo quadro próprio de servidores dado o grau de especialização necessário, os quais dessa forma poderão se dedicar na administração e gestão da plataforma EPP/EDR do fabricante Kaspersky, ou ser remanejados para outras demandas prioritárias da Administração, principalmente nas iniciativas de inovação baseadas em tecnologias de computação em nuvem e inteligência artificial.

Por fim, espera-se que a renovação de licenças do software Kaspersky Endpoint Security for Business Advanced (EPP) com Kaspersky Endpoint Detection and Response Optimum (EDR) integrado permita a obtenção dos benefícios diretos esperados a seguir enumerados, com a indicação dos parâmetros que serão utilizados pela Administração para avaliar se a contratação atingiu seus objetivos:

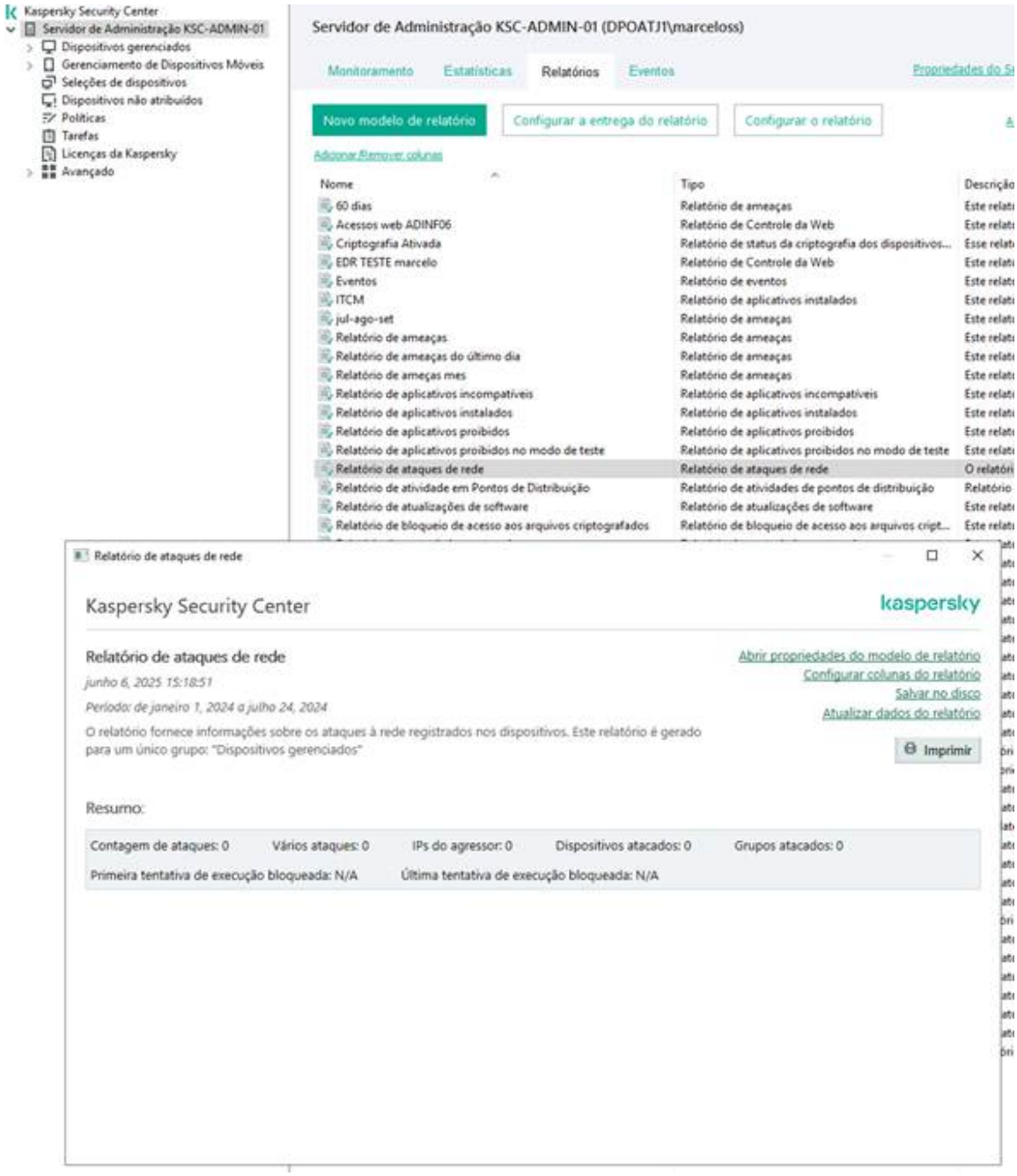
- Garantir a implementação de mecanismos efetivos de proteção contra ameaças cibernéticas: verificar o relatório de ameaças na console do servidor de administração do Kaspersky Security Center (ksc-admin-01.infra.tj.rs)



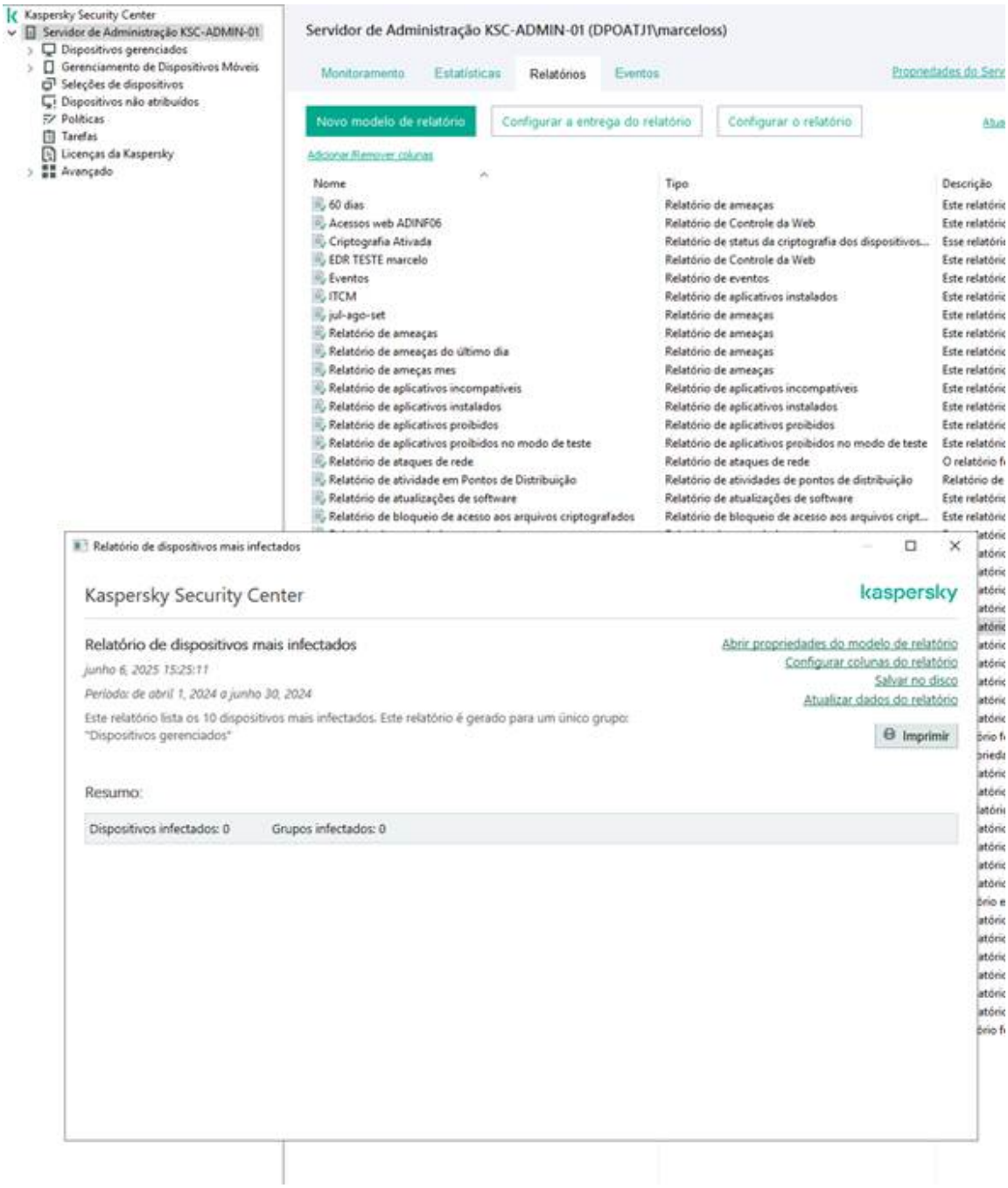
- Garantir que as informações utilizadas nas atividades laborais estejam protegidas contra ataques maliciosos: verificar o relatório de bloqueio de acesso aos arquivos criptografados na console do servidor de administração do Kaspersky Security Center (ksc-admin-01.infra.tj.rs)



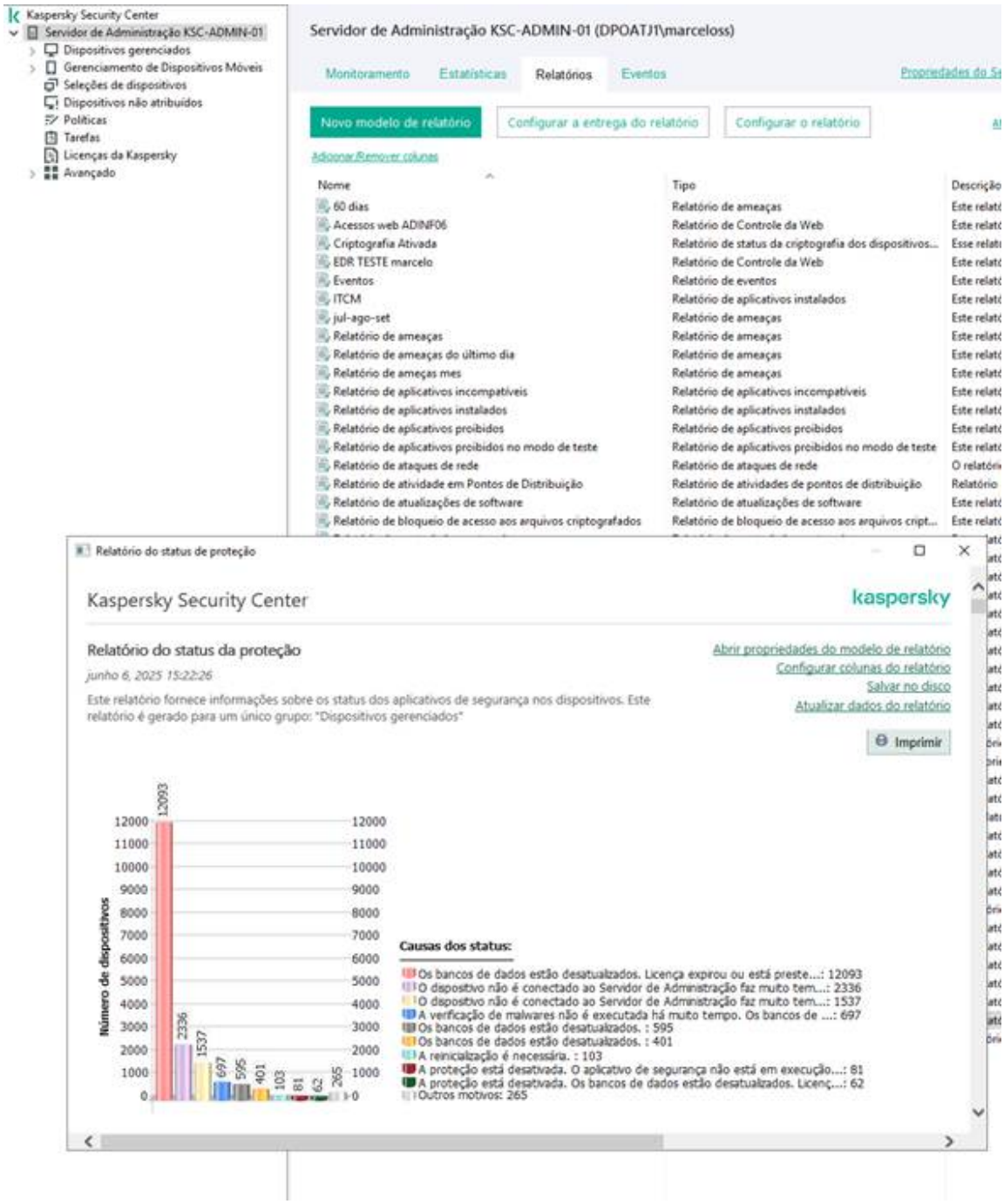
- Proteger com acesso em tempo real as informações sobre *malware*, *phishing*, *spam*, vazamento e roubo de dados digitais: verificar o relatório de ataques de rede na console do servidor de administração do Kaspersky Security Center (ksc-admin-01.infra.tj.rs)



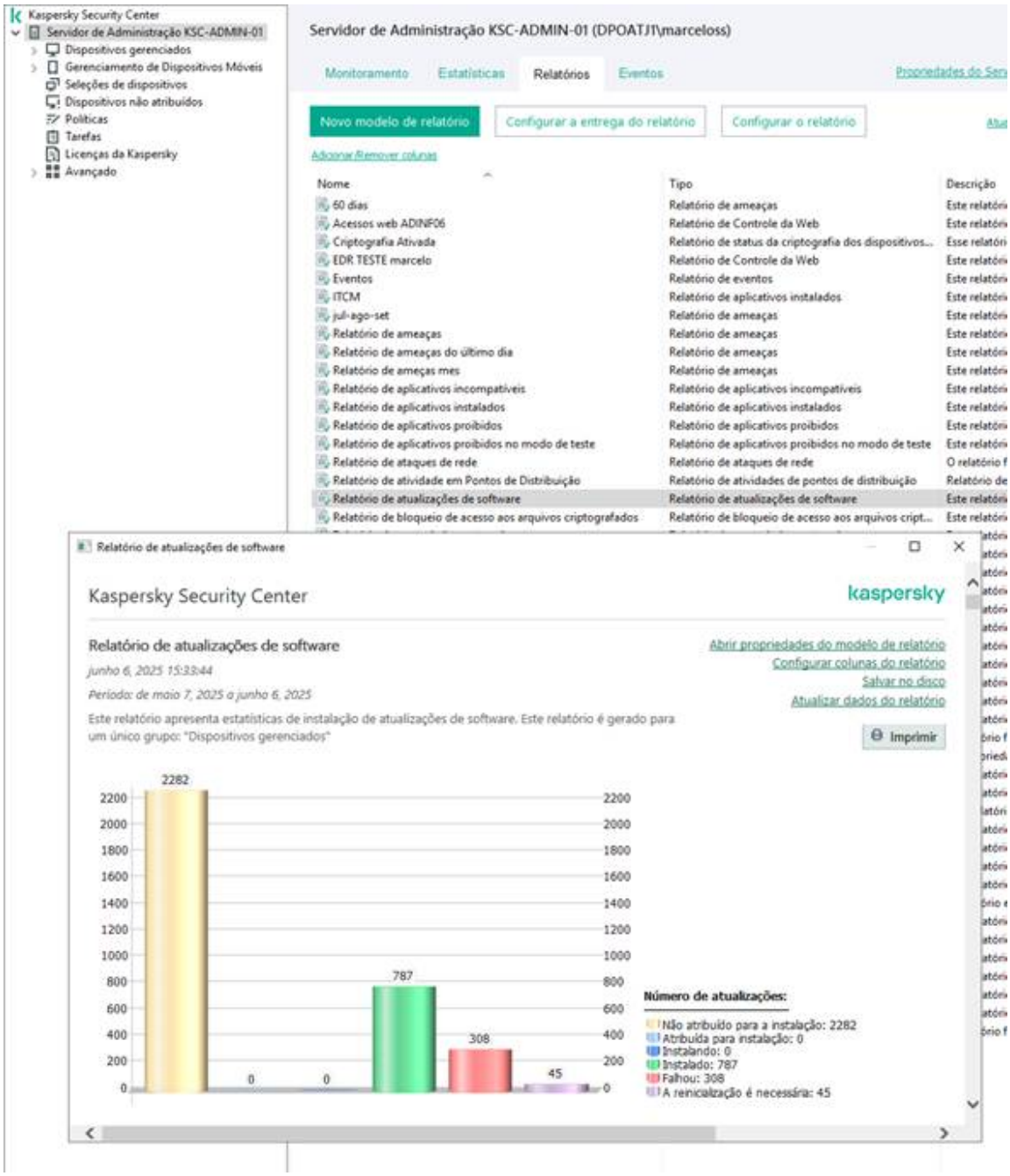
- Aumentar a confidencialidade, integridade, níveis de segurança da informação, eficiência de monitoração de eventos de segurança e disponibilidade das informações: verificar o relatório de dispositivos mais infectados na console do servidor de administração do Kaspersky Security Center (ksc-admin-01.infra.tj.rs)



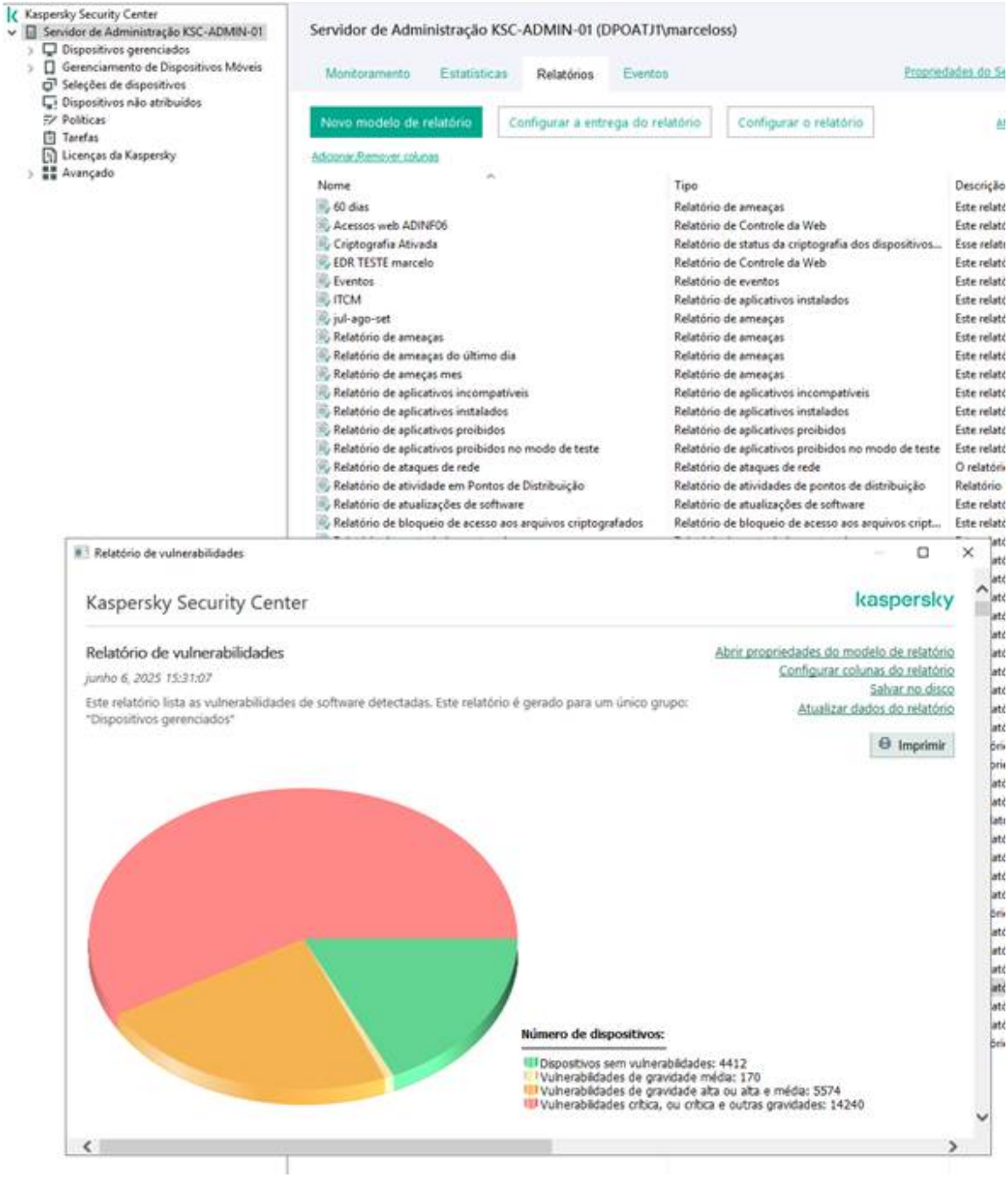
- Minimização do risco de violação da privacidade dos colaboradores e o risco de vazamento de dados confidenciais: verificar o relatório do status da proteção na console do servidor de administração do Kaspersky Security Center (ksc-admin-01.infra.tj.rs)



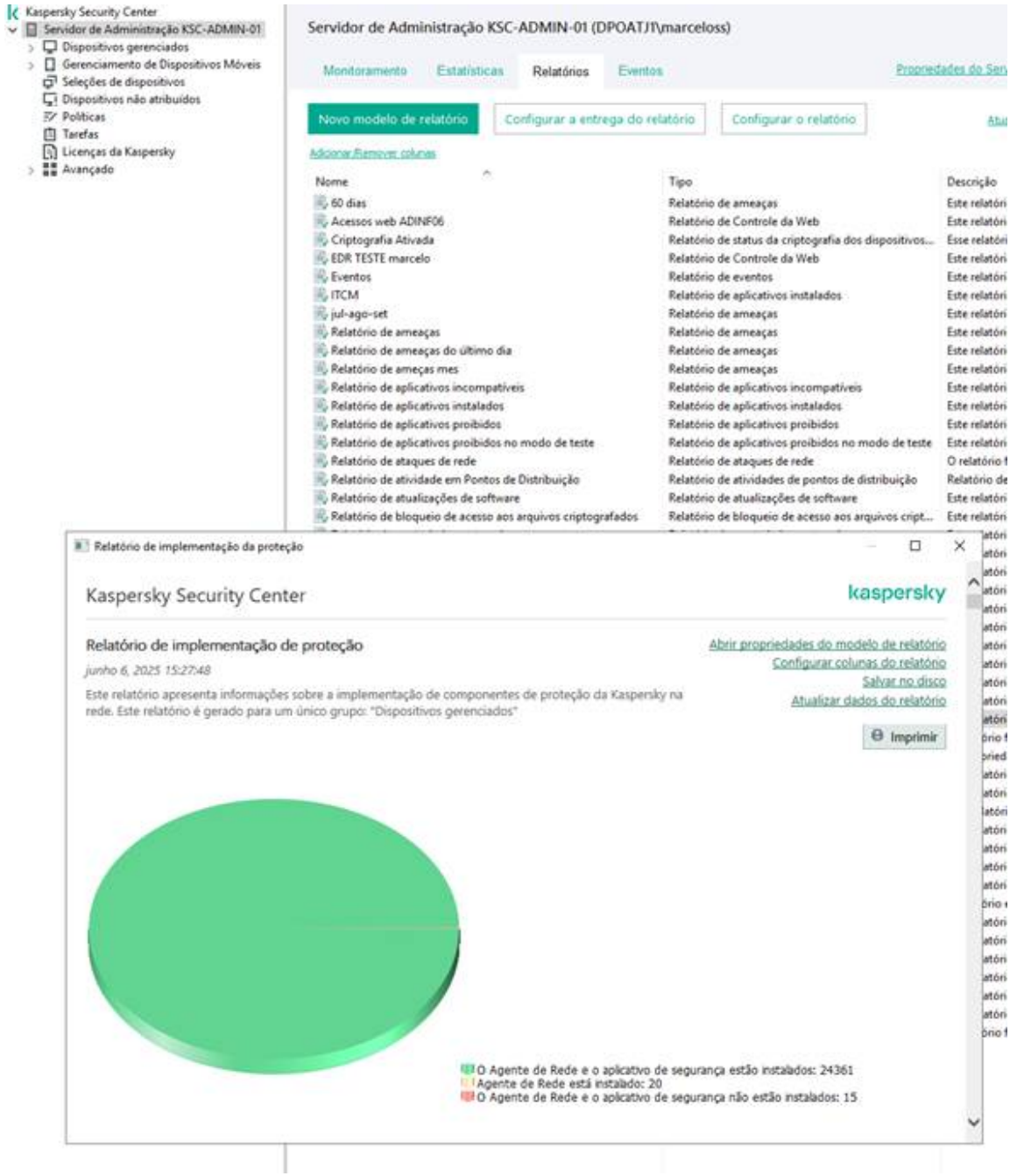
- Promover maior inteligência em relação à distribuição de *software*, gerenciamento de licenças de *software* e conformidade com as políticas de gerenciamento de *software*: verificar o relatório de atualizações de software na console do servidor de administração do Kaspersky Security Center (ksc-admin-01.infra.tj.rs)



- Gerenciamento de *patches* abrangente e automatizado minimizando os riscos de segurança para as vulnerabilidades atuais: verificar o relatório vulnerabilidades na console do servidor de administração do Kaspersky Security Center (ksc-admin-01.infra.tj.rs)



- Melhoria dos serviços e minimização dos problemas de instalação: verificar o relatório de implementação de proteção na console do servidor de administração do Kaspersky Security Center (ksc-admin-01.infra.tj.rs)



11 - DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORES

A análise dos impactos ambientais e respectivas medidas mitigadores será informada pelo ECOJUS.

12 - PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL

A ser definido no Plano Anual de Contratações 2024 da DITIC.

13 - DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Após análise comparativa das soluções identificadas, sugere-se a escolha da solução viável 1, visto assegurar a contratação dos serviços de garantia técnica do fabricante Kaspersky mitigando riscos por falhas de software com manutenção corretiva/evolutiva dos módulos EPP/EDR em operação inclusa, provendo melhor relação custo-benefício dado o cenário de uso simplificado da tecnologia EPP/EDR existente na infraestrutura de desktops e servers em funcionamento em todos os prédios do Poder Judiciário Gaúcho.

ANEXO A

PLANO DE SUSTENTAÇÃO E TRANSIÇÃO CONTRATUAL

1 - RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

1.1 - Recursos Materiais

Não aplicável visto tratar da renovação do suporte de licenças de software contra-ataques maliciosos em estações de trabalho e equipamentos servidores.

1.1.1 - Disponibilidade

Idem.

1.1.2 - Quantidades

Idem.

1.2 - Recursos Humanos

Fornecimento de mão de obra especializada na prestação dos serviços de suporte técnico evolutivo e corretivo.

1.2.1 - Disponibilidade

Contratar os serviços de garantia técnica do fabricante.

1.2.2 - Quantidades / Competências

Prestação dos serviços de suporte técnico evolutivo e corretivo pelo fabricante por 12 meses.

2 – ESTRATÉGIA DE CONTINUIDADE CONTRATUAL

2.1 - Ações de Continuidade, seus respectivos responsáveis e prazos

Em caso de eventual interrupção contratual a estratégia da continuidade do fornecimento se baseará na recontratação dos serviços de garantia técnica do fabricante uma vez que somente esse possui a especialização necessária para executar os serviços exigidos no edital.

3 – ESTRATÉGIA DE TRANSIÇÃO CONTRATUAL

3.1 – Ações de Transição Contratual, seus respectivos responsáveis e prazos

- Entrega de versões atualizadas dos módulos EPP e EDR durante a vigência do contrato com transferência gradativa de conhecimentos sobre o uso e resolução de problemas de tais softwares.

4 – ESTRATÉGIA DE INDEPENDÊNCIA

4.1 - Transferência de Conhecimento

Não aplicável visto tratar de contratação de serviço de garantia técnica do fabricante com exclusividade no fornecimento de mão de obra especializada.

4.2 - Direitos de Propriedade Intelectual

Não aplicável visto tratar de contratação de serviço de garantia técnica do fabricante com exclusividade no fornecimento de mão de obra especializada.

5 – APROVAÇÃO E ASSINATURA

_____

Equipe de Planejamento da Contratação

_____

Autoridade máxima da TIC

[1] Ambos vinculados ao expediente SEI n° 8.2021.0207/000040-1, enquanto a execução do contrato n° 62/2022-DEC está sendo acompanhado no expediente SEI nº 8.2022.4776/000028-9.

[2] IN 5/2014-SLTI/MPOG: Dispõe sobre os procedimentos administrativos básicos para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral. Disponível em http://www.comprasgovernamentais.gov.br/paginas/instrucoes-normativas/instrucao-normativa-no-5-de-27-de-junho-de-2014.

[3] Disponível em http://www.comprasgovernamentais.gov.br/arquivos/caderno/pesquisa_precos-02-09.pdf.

[4] Disponível em http://www.ticontrole.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A14E27750D014E2C2E20C83172.

[5] Rede de segurança Kaspersky, detecção de comportamento, prevenção de exploração, prevenção de invasões de host, mecanismo de remediação, proteção contra ameaças de arquivos, proteção contra ameaças da web, proteção contra ameaças de correio, firewall, proteção contra ameaças à rede, prevenção de ataques BadUSB, proteção AMSI, controle de aplicativos, controle de dispositivos, controle da web e controle adaptativo de anomalias.

Documento assinado eletronicamente por **Marcelo da Silva Strzykalski**, **Assessor(a) Técnico(a)**, em 06/06/2025, às 18:55, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Cátia Cristine Weber**, **Técnico(a) do Poder Judiciário**, em 09/06/2025, às 12:24, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Ronaldo da Silva Rodrigues**, **Chefe de Seção**, em 09/06/2025, às 13:51, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://www.tjrs.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **8081671** e o código CRC **E19308DB**.