TRIBUNAL REGIONAL ELEITORAL DO PARANÁ

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO - SECTI

ASSESSORIA DE SEGURANÇA CIBERNÉTICA - ASC

ESTUDO TÉCNICO PRELIMINAR

Processo Administrativo **nº 029797/2022**

CONTRATAÇÃO DE LICENÇAS ADICIONAIS DE EPS (EVENTOS POR SEGUNDO) E RENOVAÇÃO DO SOFTWARE DE SIEM (SECURITY INFORMATION EVENT MANAGEMENT)

Curitiba, 27 de Setembro de 2022

Histórico de Revisões

Data	Versão	Descrição	Autor
30/08/2022	1.0	descrição do ETP	Lucas Barke
06/10/2022	1.1	inclusão de serviço de configuração	Lucas Barke

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

INTRODUÇÃO

Este documento apresenta o estudo técnico preliminar (ETP) da contratação que objetiva assegurar a viabilidade técnica da contratação e embasar o Termo de Referência, conforme previsto na Lei nº 8.666/93, art. 6°, inc. IX.

Atualmente o TRE-PR utiliza o sistema de SIEM, chamado QRadar da empresa IBM, para coleta e correlação de log´s de ativos de tecnologia da informação e comunicações (TIC), com o objetivo de identificar vulnerabilidades de segurança da informação e permitir auditoria de utilização de recursos de TIC.

O sistema referido foi contratado em 2018, conforme PAD´s: 13447/2018 e 1885/2019, com capacidade para receber 2.600 eventos por segundo e 20 mil fluxos de rede por minuto, e desde então vem sendo amplamente utilizado pelas equipes da Secretaria de Tecnologia da Informação, possuindo inúmeras regras de correlação de log´s e identificação de ofensas à segurança da informação.

No entanto, o ambiente computacional de ativos de tecnologia da informação no TRE-PR cresceu exponencialmente nos últimos anos. Atualmente existem cerca de 3500 computadores, 400 servidores (máquinas virtuais), 8 firewalls de grande porte na sede e mais 157 firewalls no interior do estado, além de outros ativos de rede como switches, roteadores NAC (Network Access Control), Access Point, e diversos servidores físicos.

Com o aumento expressivo do ambiente computacional dos últimos anos, os 2.600 eventos por segundo, assim como os 20 mil eventos de fluxo de rede por minuto, não são suficientes para atender a realidade deste tribunal na atualidade.

Ademais, para atender as demandas de segurança da informação previstas na Estratégia Nacional de Segurança Cibernética do Poder Judiciário(Resolução CNJ nº 396/2021) e atender a recente Instrução Normativa (IN) nº 03/2022 do TRE-PR que contempla a necessidade do tribunal armazenar, por no mínimo 12 meses, todos os log´s de todos os equipamentos de TIC, torna-se necessária a expansão da capacidade da ferramenta.

Para adequar a quantidade de eventos(log´s) e fluxo de rede recebidos para realidade atual deste tribunal, iniciou-se este estudo técnico que prevê o aumento imediato para, no mínimo, 7.600 eventos por segundo e quantidade compatível de fluxo de rede para a nova realidade do Tribunal Regional Eleitoral do Paraná, com previsão de registro de preços para posterior aumento do quantitativo de eventos em caso de necessidade devido ao crescimento do ambiente.

1 – DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.1 - Identificação das necessidades de negócio

1	Permitir que o software de SIEM atualmente utilizado pelo Tribunal Regional Eleitoral do Paraná centralize e correlacione log´s de todos os ativos de informação, como computadores, servidores e equipamentos de Rede, atendendo a IN 03/2022 que orienta o armazenamento de *log´s* ativos por 180 dias e inativos por 12 meses, de todos os ativos da informação.
2	Proporcionar correlação de log´s de atividade de todos os ativos de informação, permitindo identificação de vulnerabilidades de Segurança da Informação.
3	Permitir automatização na resposta a incidentes de segurança da informação através de ferramenta de SOAR (Security Orchestration, Automation and Response) proporcionando atuação rápida e eficaz, 24 horas, 7 dias por semana, em caso de suspeita de incidente de segurança.
4	Renovação do licenciamento do software IBM QRadar, unificando as atuais 5 licenças para mesma data a fim de proporcionar melhor gestão do software contratado e garantir continuidade do serviço prestado pelos 36 meses subsequentes.
5	Adequar arquitetura, utilizando modelo distribuído, para comportar quantidade necessária de eventos por segundo recebido.
6	Realizar revisão da arquitetura com implantação de novas configurações para otimização do tempo de resposta e automação de resposta com uso do SOAR.

1.2 - Identificação das necessidades tecnológicas

1	Ampliar capacidade de armazenamento de log´s e correlações de eventos do software de SIEM, IBM QRadar, permitindo aumento dos atuais 2.600 Eventos por segundo(EPS) para ao menos 7.600 EPS, com possibilidade de ampliação posterior de forma escalonável, visando atender a todos os ativos de informação do TRE-PR.

2	Possuir integração com software de SOAR (S*ecurity Orchestration, Automation and Response*) para automação da resposta a incidentes com base na correlação de log´s entre equipamentos de tecnologia da informação.
3	Renovação do software IBM QRadar, a fim de permitir a quantidade estimada de eventos por segundo para atender a atual necessidade e volume de log´s de equipamentos do TRE-PR.
4	Atender a IN 03/2022-TRE/PR no que tange ao armazenamento e disponibilização de *log´s* (eventos) registrados em todos ativos de informação do Tribunal Regional Eleitoral do Paraná.
5	Permitir a manutenção das regras de correlação e configuração da ferramenta atual sejam mantidas, sem a necessidade de reconfiguração.
6	Realizar revisão da configuração atual, implantar novas configurações na ferramenta a fim de adequar automação da resposta a incidente através do SOAR e permitir maior velocidade na resposta a incidentes.

2. PREVISÃO DA DEMANDA NO PLANO ANUAL DE CONTRATAÇÕES (PAC)

Conforme item 2 do DOD, a demanda está prevista no PAC 2022, ID 22PS003: "Aquisição de licenças de software perpétuas visando atender às demandas oriundas do Projeto de Segurança da Informação da Justiça Eleitoral".

3. HISTÓRICO DAS CONTRATAÇÕES SIMILARES REALIZADAS PELO TRE OU OUTROS ÓRGÃOS

PAD´S de contratações anteriores: 13317/2017, 013447/2018, 001885/2019.

4 - ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO ESTRATÉGICO

Nos moldes da Portaria 311/2021 - TRE/PR, que aprova o Planejamento Estratégico da Justiça Eleitoral do Paraná para o período de 2021-2026, consideram-se os seguintes pilares a serem alcançados:

Processos Internos - OE 3[1]

Fortalecimento da segurança do processo eleitoral

Aprendizado e Crescimento- OE 10

Fortalecimento da estratégia nacional de TIC e de proteção de dados

5 – ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

O *software* de SIEM contratado pelo TRE-PR, chamado IBM QRadar, possui atualmente licença para 2.600 eventos por segundo (EPS), no entanto, com o crescimento do ambiente computacional do tribunal, a quantidade de *log´s* de atividades aumentou consideravelmente e este licenciamento atende a apenas um terço dos eventos gerados pelos ativos de tecnologia da informação, necessitando de pelo menos, mais 5000 EPS, totalizando 7.600 EPS, para o correto cumprimento da IN 03/2022 e necessária correlação de eventos para identificação de vulnerabilidades de segurança da informação.

Além da expansão na quantidade de eventos iniciais, de 2600 para 7600, recomenda-se criação de uma ata de registro de preço, contendo blocos de mil EPS ou quarenta servidores, quando este for o modelo de licenciamento adotado, para permitir crescimento futuro, conforme necessidade de crescimento posterior da ferramenta, acompanhando o crescimento constante da infraestrutura de rede do TRE-PR.

Com o aumento considerável na quantidade de eventos coletados pela ferramenta de SIEM, é de suma importância a disponibilização de ferramenta com módulo de SOAR (Security Orchestration Automation and Response) integrado a fim de permitir a orquestração e resposta a incidentes de forma automática, tendo em vista a necessidade de atendimento rápido para ações de segurança da informação com o objetivo de conter as vulnerabilidades encontradas em horários onde não há expediente de servidores deste tribunal.

Além dos itens descritos acima, é necessário a contratação de prestador de serviço, em pacotes de 40 horas, para implantação do novo licenciamento e ferramenta de SOAR junto ao serviço de revisão das regras atuais e de automação e orquestração da resposta a incidentes.

[1] O DOD (doc. nº 375831/2022), também menciona o OE 03.

6 – ANÁLISE DE SOLUÇÕES

1º Cenário - Ampliação da quantidade de eventos e fluxo de rede com adequações de arquitetura para modelo atual.

Adequar capacidade de Eventos por segundo(EPS) do software de SIEM - IBM QRadar, com adaptação da arquitetura de servidores para absorver a nova capacidade, renovando o licenciamento e unificando o licenciamento em uma única contratação.

Desde 2018 o TRE-PR utiliza a ferramenta de SIEM da IBM, chamada QRadar, no entanto esta ferramenta possui atualmente contratados, licenciamento de apenas 2.600 EPS que são insuficientes para a quantidade de *log´s* produzidos por todos os ativos de rede, conforme determina a IN 03/2022, além de possuir fluxo de rede (FPM) limitado em 20 mil por minuto.

A sugestão apresentada é ampliar a capacidade da ferramenta, em mais 5000 EPS, totalizando 7.600 EPS e mais 20 mil FPM (Flows Per Minute), adequando o modelo de arquitetura distribuída dos servidores para receber nova capacidade de *log´s* sem afetar desempenho de correlação de ofensas já configuradas, além de permitir expansão futura, através de ATA de registro de preços, em pacotes de 1.000 EPS a fim de permitir adequação do volume de *log´s,* conforme necessidade ocasionada pela ampliação de equipamentos e ativos de rede durante a vigência deste contrato.

- **Prós**: Adequação da quantidade de eventos recebidos e analisados pela ferramenta, atendendo ao que determina a norma (IN 03/2022), e permitindo correlação entre equipamentos e análise de possíveis vulnerabilidades.

- **Contras**: Dificuldade no gerenciamento e fiscalização contratual.

Atualmente este contrato já possui cinco “Part Numbers” diferentes, com vencimentos em datas diferentes, e adicionar um sexto aumentaria a complexidade de gestão, o que a princípio não seria um empecilho. Porém, isto resultaria, nos dois próximos exercícios, necessidade de nova contratação de renovação de “part numbers” previstos para expirar em 2023 e 2024; o que traria maior ônus para a Administração.

2º Cenário - Adequar a capacidade da ferramenta, dos atuais 2.600 EPS para 7.600 EPS, renovando licenciamento para novo modelo “Cloud Pack”, unificando em um único licenciamento todas as capacidades necessárias, simplificando a gestão contratual e permitindo a utilização do módulo de SOAR (Security Orchestration Automation and Response) que permite a automatização da resposta de incidentes, com base na análise e correlação de log´s.

Neste cenário, além dos 5.000 EPS iniciais, recomenda-se a elaboração de uma ATA de registro de preços, com pacotes de 1.000 EPS para acréscimo futuro de acordo com o crescimento do parque tecnológico, permitindo adequação às necessidades futuras deste tribunal.

Prós:

- Adequação da quantidade de eventos recebidos e analisados pela ferramenta, atendendo ao que determina a IN 03/2022), e permitindo correlação entre equipamentos e análise de possíveis vulnerabilidades.
- Permite a orquestração e automação da resposta a incidentes através do módulo de SOAR integrado à ferramenta.
- Renovação do licenciamento de eventos, unificando em um único "Part Number", com data de vencimento unificada, simplificando a gestão contratual.

Contras:

- Custo elevado devido ao modelo de licenciamento por EPS, onde o crescimento exponencial do ambiente tecnológico do TRE-PR certamente necessitará de futuras contratações de pacotes de EPS para atender a constante crescente demanda.

3º Cenário: Elevar licenciamento da ferramenta QRadar para o novo modelo "Cloud Pack", com os benefícios citados no Cenário 2, porém alterando o modelo de licenciamento, atualmente mensurado em EPS, para modelo contabilizado por quantidade de servidores de rede, possibilitando aumento da quantidade de eventos por segundo e fluxo de rede forma ilimitada, proporcionando maior escalabilidade e adequação da ferramenta com constante crescimento no volume de *log´s* gerados na rede do TRE/PR.

Prós:

- Eventos por segundo e Fluxo de rede ilimitados.
- Permite a orquestração e automação da resposta a incidentes através do módulo de SOAR integrado à ferramenta.
- Mudança no modelo de licenciamento de eventos, desta forma calculado pela quantidade de servidores de rede, e não mais por eventos por segundo.
- Permite crescimento no volume de dados, sem gerar custo adicional para este tribunal.
- Redução no custo do modelo de licenciamento.

Contras:

- Não se aplica.

4º Cenário: Contratar nova ferramenta de SIEM, para substituir o atual IBM QRadar, com quantidade

de eventos adequados à necessidade atual para atender a demanda do TRE-PR, incluindo módulo de SOAR para orquestração e automação da resposta a incidentes atendendo a demanda deste tribunal.

Prós:

- Não se aplica.

Contras:

- Prejuízo ao erário devido a mudança de solução e perda do investimento já realizado em capacitação e horas técnicas utilizadas na contratação e configuração da ferramenta atual, já em uso neste tribunal há 4 anos.

5º Cenário: Manter a utilização da ferramenta atual, sem evolução do contrato e adequação da quantidade de eventos recebidos.

Embora a ferramenta esteja em pleno funcionamento há 4 anos neste tribunal, a quantidade de eventos analisados não é suficiente para a demanda atual.

Atualmente dois terços de todos os eventos gerados pelos equipamentos deste tribunal são descartados pela ferramenta e deixam de ser armazenados e correlacionados, gerando baixa credibilidade na análise de vulnerabilidades encontradas através da correlação de log´s e consequentemente impactando na segurança da informação, além de não permitir auditoria através da análise de log´s armazenadas, já que estas são insuficientes para uma completa análise de ações.

Prós:

- Não se aplica.

Contras:

- Perda de informações descartadas pela ferramenta por incapacidade de análise do volume de dados atual.
- Baixa confiabilidade na análise de vulnerabilidades através da correlação de *log´s* devido ao maior número de descarte de informações.

Observação: Para todos os cenários propostos haverá também a contratação de pacotes de 160 horas de serviços do fabricante com escopo aberto e 100 horas da CONTRATADA, para auxílio em configuração, revisão da arquitetura atual e suporte, além dos serviços de instalação das licenças e ferramentas da solução.

6.1 – IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Descrição da solução (ou cenário)
1	Contratação de EPS mantendo o licenciamento atual
2	Contratação de EPS elevando o licenciamento *Cloud Pak*, com SOAR incluso, renovando o licenciamento,no mesmo modelo atual, porém unificando as datas de vencimento dos *Part Numbers* atuais.
3	Contratação de EPS elevando o licenciamento *Cloud Pack*, com SOAR incluso, mudando o licenciamento atual por EPS, para o modelo licenciado por servidores.
4	Contratação de nova solução de SIEM adequada às atuais necessidades do TRE-PR
5	Manter a ferramenta atual sem ampliar os quantitativos de eventos por segundo

6.2 – ANÁLISE COMPARATIVA DE SOLUÇÕES

Requisito	Solução	Sim	Não	N/A
A Solução permite armazenamento, análise e correlaçã todos os *log´s* gerados por todos os equipamentos de TI TRE-PR?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
	Solução 4	X		
	Solução 5		X	
A Solução permite ampliação da capacidade armazenamento e correlação de *log´s*, confo crescimento no número de equipamentos de TIC do PR?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
	Solução 4	X		
	Solução 5		X	
A Solução permite preservação de todas as correlaçõe *log´s* e análises já configuradas na solução atual?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
	Solução 4		X	
	Solução 5	X		
A Solução possui funcionalidade de SOAR (Sec Orchestration Automation and Response) inclusa?	Solução 1		X	
	Solução 2	X		
	Solução 3	X		
	Solução 4	X		
	Solução 5		X	
A Solução possui escalabilidade de eventos	Solução 1		X	

Requisito	Solução	Sim	Não	N/A
segundo(EPS) e fluxo de rede ilimitada?	Solução 2		X	
	Solução 3	X		
	Solução 4			X
	Solução 5		X	

Considerando os cenários aqui citados, com o objetivo de preservar o investimento público, e o tempo despendido no aprendizado e na configuração da ferramenta atualmente em funcionamento que possui inúmeras correlações de *log´s* já configuradas, e a fim de permitir a adequação da quantidade de eventos recebidos, além de atender a IN 03/2022 e possibilitar registro e correlação de *log´s* de todos os equipamentos de tecnologia da informação do TRE/PR, sugere-se que a melhor opção para este tribunal é a **escolha do cenário 3**, por possuir a preservação das configurações já realizadas, a evolução do licenciamento para o modelo *Cloud Pack* que possui, entre outras vantagens, a integração e disponibilização da funcionalidade de SOAR, necessária para a automatização da resposta a incidentes em horários onde não há expediente dos funcionários deste tribunal para o monitoramento reativo, e, principalmente por possuir capacidade de **correlação de eventos e fluxo de rede ilimitados**, por um **valor inferior ao dos demais cenários que utilizam o modelo de licenciamento por quantidade de eventos**.

7 – REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

A Solução proposta no cenário 4 é considerada inviável pela preservação do investimento já realizado no licenciamento do software vigente, além de capacitação da equipe operacional já realizada e tecnologia já configurada em todo ambiente de TIC do TRE-PR.

A Solução proposta no cenário 5, é considerada inviável por não possuir capacidade de total atendimento para pleno funcionamento do objetivo pelo qual foi contratado, tendo em vista que atualmente esta tem capacidade para analisar e correlacionar apenas ⅓ (um terço) dos eventos gerados por todos os equipamentos de TIC do TRE/PR.

8 – ANÁLISE COMPARATIVA DE CUSTOS

Cenário 1	Expansão de EPS (36 meses)	R$ 1.335.185,33

	Renovação da Base	R$ 205.521,18
	Serviço do Fabricante	R$ 206.6440,92
	Total	R$ 1.747.150,43
Cenário 2	Expansão de EPS (36 meses)	R$ 1.234.483,20
	Renovação/Modernização da Base	R$ 392.509,55
	Serviço do Fabricante	R$ 206.440,92
	Total	R$ 1.883.433,67
Cenário 3	Expansão de EPS (36 meses)	R$ 942.507,92
	Renovação da Base	R$ 392.509,55
	Serviço do Fabricante	R$ 206.440,92
	Total	**R$ 1.541.458,39**

9 – DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Esta equipe de planejamento da contratação, com base nas especificações técnicas constantes do presente termo, conclui que **a solução que apresenta maior vantagem técnica e econômica para o TRE/PR** é a de licenciamento baseado na **quantidade de servidores, com eventos por segundo(EPS) e fluxo de rede (Flow) ilimitados**, apresentada acima no **cenário 3**.

A escolha desse modelo de licenciamento é vantajosa por permitir, além da expansão do modelo atual, modernização da base para o modelo cloud pack, possui vantagens tecnológicas como software de SOAR, e crescimento futuro de forma ordenada, baseada em crescimento do parque computacional de servidores e não de eventos gerados (log´s) ou fluxo de rede, possuindo um custo inferior ao modelo de crescimento baseado em eventos utilizado atualmente.

Desta forma, daremos plena utilização à infraestrutura atual, adequando a ferramenta à capacidade necessária, dando cumprimento à referida IN nº 03/2022, evoluindo o licenciamento por meio da modernização da base com possibilidade de adequar a capacidade do software às necessidades atuais e futuras deste tribunal.

Conclui-se, desta forma, que a formação de ata de registro de preços com a modernização do modelo de licenciamento e adequação do volume necessário de eventos e fluxo de rede, prevendo a utilização das tecnologia do cenário 3, atenderá satisfatoriamente às necessidades deste Tribunal.

10. PRAZO DE ENTREGA:

Estima-se até 24/10/2022 a aquisição da solução (consta também no DOD - doc. nº 375831/2022)

11. JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DO OBJETO

Não se aplica, pois se trata de única solução, não podendo ser divisível.

12. LEGISLAÇÃO APLICÁVEL, NO QUE COUBER (ROL DOS PRINCIPAIS)

Lei 8.666/1993 - Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.

Decreto 7174/2010 - Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.

IN nº 03/2022 - TRE/PR -Dispõe sobre as regras e os procedimentos para a realização da gestão e monitoramento de registro de atividades (logs) no ambiente computacional da Justiça Eleitoral do Paraná

IN nº 01/2019 - SGD/ME - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

IN nº 47/2022 - SGD/ME - Altera a Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da

Informação - SISP do Poder Executivo Federal.

13. SUSTENTABILIDADE

Trata-se de ferramenta já em utilização - aquisição de software, com preservação das configurações já realizadas.

Assim, por se tratar de solução puramente baseada em software, não há critérios de sustentabilidade a serem adotados.

14. FORMA DE SELEÇÃO DO FORNECEDOR, INCLUINDO CRITÉRIOS DE ELABORAÇÃO DA PROPOSTA

A forma de seleção do fornecedor se dará por meio de licitação, nos moldes previstos na legislação vigente. A sugestão para exigência de documentos de aceitação e habilitação, se houver, se dará no Termo de Referência.

A legislação atual prevê que, em sendo bens e serviços comuns, a regra é se licitar na modalidade Pregão, na forma eletrônica.

15. OBRIGAÇÕES DA CONTRATADA

Devem ser consideradas as obrigações a serem previstas no Termo de Referência, não constando nenhuma obrigação específica que deva ser mencionada neste estudo técnico preliminar.

16. PLANO DE GESTÃO E FISCALIZAÇÃO

Não se aplica. Trata-se de aquisição de software.

17. ANÁLISE E INFORMAÇÃO SE HÁ NECESSIDADE DE FORMALIZAR CONTRATO E GARANTIA

Sugere-se a formalização de contrato com garantia

18. PROVIDÊNCIAS PARA ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO

Para o cenário proposto, não se vislumbram adequações ao ambiente computacional atual além

da implantação das novas configurações e funcionalidades.

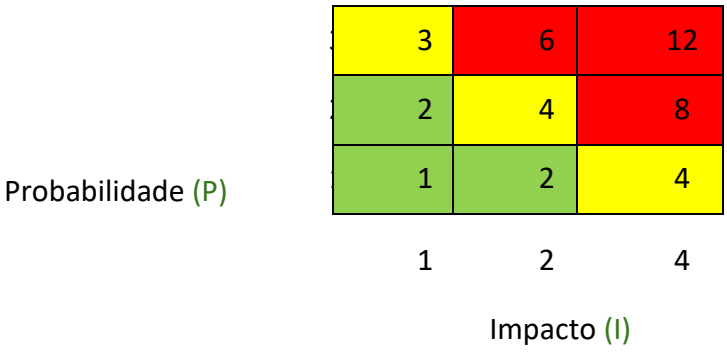
19. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Com base no levantamento inicial, estima-se que o custo total da contratação, incluindo modernização da base , expansão da capacidade de armazenamento de log´s e fluxo de rede, e serviços do fabricante será de R$ 1.541.458,38 (hum milhão, quinhentos e quarenta e hum mil, quatrocentos e cinquenta e oito reais e trinta e oito centavos), cujo orçamento preliminar junto aos possíveis fornecedores, segue em anexo.

20. ANÁLISE DE RISCO

O gerenciamento de riscos permite ações contínuas de planejamento, organização e controle dos recursos relacionados aos riscos que possam comprometer a contratação, execução e gestão contratual.

O produto da probabilidade pelo impacto de cada risco gera nove combinações possíveis no contexto da matriz.



id	*Risco*	*Categoria*	*P*	*I*	*Nível Risco*
1	Ausência de recursos orçamentários	Contratação	1	2	Baixo
2	Suspensão/atrasos em face de impugnações/recursos	Contratação	1	4	Médio

3	Impossibilidade de auditorias de comportamento de usuários e sistemas	Operacional	1	4	Médio
4	Não Identificar ataques à segurança cibernética em curso.	Operacional	1	4	Crítico

Risco 1	P	I	P x I = R
Ausência de recursos orçamentários	1	4	1x4 = 4 Médio
Dano Potencial			
1. Manutenção do cenário atual com análise de apenas um terço da necessidade atual.			
2. Risco à segurança da Informação			
3. Impossibilidade de auditoria de segurança da informação			
Ação preventiva			Responsável
Planejamento e análise de contratações com vistas a um correto dimensionamento da necessidade			Equipe de planejamento
Ação de contingência			Responsável
Análise de soluções de mercado incluindo preços praticados em contratações similares			Equipe de planejamento

Risco 2	P	I	P x I = R
Suspensão em face de impugnações	1	4	1x4 = 4 Médio
Dano Potencial			
1. Manutenção do cenário atual com análise de apenas um terço da necessidade atual.			
2. Risco a segurança da Informação			
3. Impossibilidade de auditoria de segurança da informação			
Ação preventiva			Responsável
Análise de editais e impugnações de outros processos licitatórios com vistas a mitigar requisitos inconsistentes.			Equipe de planejamento
Ação de contingência			Responsável
Revisão do edital, análise multissetorial dos requisitos			Equipe de planejamento

Risco 3	P	I	P x I = R
Impossibilidade de auditorias de comportamento de usuário sistemas	1	3	1x3 = 3 Médio

Dano Potencial	
1. Falta de registro e armazenamento de eventos(log´s) de ações de usuários e sistemas.	
2. Impossibilidade de investigação de incidentes cibernéticos.	
Ação preventiva	Responsável
Comunicar a todos os envolvidos sobre a necessidade e urgência desta contratação para a segurança da informação.	Equipe de planejamento
Ação de contingência	Responsável
Armazenar log´s localmente nos cerca de 450 servidores de rede e nos ativos de rede.	Equipe de Rede e Infraestrutur

Risco 4	P	I	P x I = R
Não Identificar ataques à segurança cibernética em curso.	1	4	1x4 = 4 Alto
Dano Potencial			
1. Não identificar ameaças à segurança da informação por falta de dados para análise			
2. Não monitorar ataques à segurança cibernética em curso por falta de correlação de eventos.			
Ação preventiva			Responsável
Comunicar a todos os envolvidos sobre a necessidade e urgência desta contratação para a segurança da informação.			Equipe de planejamento
Ação de contingência			Responsável
Analisar apenas servidores mais críticos, ignorando demais equipamentos excluídos pelo licenciamento atual da ferramenta.			Equipe de planejamento

20. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Os estudos preliminares aqui apresentados evidenciam viabilidade técnica quanto à contratação do novo modelo de licenciamento para modernização do software de SIEM, permitindo utilização de eventos por segundo (EPS) e fluxo de rede(Flow) de forma ilimitada, adequando assim a capacidade do software atual para atendimento das demandas constantes do presente estudo.

21. ASSINATURAS

A Equipe de Planejamento da Contratação foi instituída pelo Doc 384273/2022 , de 26 de Agosto de 2022.

Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC.

Assim a Equipe de Planejamento da Contratação, abaixo nominada, aprova e assina o presente ETP:

INTEGRANTE ADMINISTRATIV	INTEGRANTE TÉCNICO	INTEGRANTE DEMANDANTE
_____	_____	_____
Rachel Ivania Tasca e Lazzari	Lucas Barke Bruzon	Gilmar José Fernandes de Deus
Assessoria Técnica da Secretaria de Administração	**Assessor de Segurança Cibernética**	**Secretário de Tecnologia da Informação**
Curitiba, 28 de Setembro de 2022	Curitiba, 28 de Setembro de 2022	Curitiba, 28 de Setembro de 2022

22. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Declaro viável a contratação da solução do novo modelo de licenciamento para modernização do software de SIEM, permitindo utilização de eventos por segundo (EPS) e fluxo de rede(Flow) de forma ilimitada, adequando assim a capacidade do software atual para atendimento das

demandas constantes do presente estudo.

Curitiba, 28 de setembro de 2022.

_____

Gilmar José Fernandes de Deus

Secretário de Tecnologia da Informação