TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO
Rua João Batista Parra 575 - Bairro Praia do Suá - CEP 29052-123 - Vitória - ES

ESTUDO TÉCNICO PRELIMINAR (TIC) Nº 19/2024 - TRE-ES/PRE/DG/STI/CIS/NSC

(este documento deve seguir as orientações da Resolução TRE/ES n. 63/2023)
Modelo atualizado em: 29/04/2024
SEI nº 0004389-19.2024.6.08.8000

SEÇÃO I - ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

---

1. IDENTIFICAÇÃO DA SOLUÇÃO SOLICITADA

1.1. DESCRIÇÃO

Licença de uso, para 2 usuários, de ferramenta, para análise de comportamento de malware, que permita: a análise da execução do malware em tempo real; o acompanhamento de requisições de rede; o monitoramento dos processos alterados pelo malware; o mapeamento Mitre Att&ck; e crie grafo comportamental.

1.2. MOTIVAÇÃO E RESULTADOS A SEREM ALCANÇADOS

Com a evolução constante das ameaças cibernéticas, as ferramentas tradicionais de segurança podem não ser suficientes para detectar e mitigar ameaças provocadas por malwares avançados. Uma ferramenta de análise de malware permite identificar, analisar e neutralizar essas ameaças antes que causem danos significativos.

A análise de comportamento de um malware em profundidade ajuda a equipe de segurança a desenvolver contramedidas eficazes e a identificar indicadores de comprometimento (IoCs), melhorando a capacidade de detecção e mitigação de ameaças provocadas por malware.

Em resumo, a aquisição de uma ferramenta de análise de malware proporciona uma série de benefícios estratégicos e operacionais que fortalecem a segurança cibernética da organização.

Os resultados que se espera alcançar com a aquisição são:

Aumento significativo na detecção de malware avançado e zero-day (malware para o qual ainda não existe resposta de ferramentas de antivírus tradicionais), com a capacidade de identificar e neutralizar ameaças antes que causem danos.

Capacidades aprimoradas de investigação forense, com a habilidade de realizar análises detalhadas de incidentes e recuperar dados comprometidos.

2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

2.1. IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

1. Proteção Contra Ameaças Avançadas e Persistentes (APT): APTs são um tipo sofisticado de ciberataque que tem como objetivo comprometer uma rede ou sistema de computador de maneira contínua e discreta, mantendo um acesso contínuo e prolongado ao sistema alvo, permitindo que os atacantes permaneçam indetectáveis enquanto exploram e extraem dados sensíveis ao longo do tempo. A utilização de uma ferramenta de análise de malware permite a detecção e mitigação eficaz de APTs e outras ameaças avançadas.

2. Redução do Tempo de Resposta a Incidentes: análises interativas em tempo real permitem uma resposta rápida e precisa, ajudando a conter ameaças antes que causem danos significativos.

3. Melhoria da Eficiência Operacional: automatização da análise de malware, gerando relatórios detalhados e acionáveis, aumentando a eficiência de uma equipe reduzida.

4. Integração com a Infraestrutura de Segurança Existente: facilitando a centralização e correlação de dados.

5. Suporte a Investigações Forenses: por meio do fornecimento de dados detalhados e históricos das atividades de malware.

6. Colaboração e Compartilhamento de Informações: compartilhamento de sessões de análise, facilitando a colaboração e a revisão de ameaças por múltiplas pessoas.

2.2. IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS

1. Análise em Tempo Real: permitir a visualização da análise de malware em tempo real, incluindo ações realizadas pelo malware, como criação de arquivos, chamadas de rede, e modificações no sistema.

2. Interface Interativa: permitir que os usuários interajam com o ambiente de análise, podendo executar ações adicionais para observar diferentes comportamentos.

3. Captura de Rede: capturar o tráfego de rede gerado pelo malware, permitindo análise detalhada de comunicações com servidores de comando e controle (C2) e download de payloads adicionais.

4. Diversidade de Ambientes: possibilitar a escolha entre diferentes sistemas operacionais e configurações de ambiente para a execução de malware, aumentando a probabilidade de capturar comportamentos específicos.

5. Relatórios Detalhados: gerar relatórios detalhados que incluem informações sobre processos, registros de eventos, atividades de rede, entre outros.

6. Compartilhamento de Sessões: permitir aos usuários compartilhar as sessões de análise com outras pessoas, facilitando a colaboração em investigações de incidentes de segurança.

7. Integração com Outras Ferramentas: permitir a integração com outras ferramentas de segurança para fornecer uma visão mais abrangente e complementar às análises.

8. A solução deve ser fornecida no formato software como serviço: uma solução em nuvem irá dispensar a necessidade de requisitos de hardware local na infraestrutura do TRE-ES, minimizando possíveis gastos posteriores com a contratação.

2.3. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

1. Não haverá compartilhamento de dados pessoais ou dados sensíveis com a contratada.

3. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

1. Necessárias 2 licenças de uso para os dois servidores que atualmente trabalham no Núcleo de Segurança Cibernética.

4. ANÁLISE DAS POSSÍVEIS SOLUÇÕES

4.1. IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Descrição da solução (ou cenário)
1	**Cuckoo Sandbox**
2	**VirusTotal**
3	**Hybrid Analysis**
4	**Joe Sandbox**
5	**FireEye Malware Analysis**
6	**VxStream Sandbox**
7	**Comodo Valkyrie**
8	**ReversingLabs TitaniumCloud**
9	**Detux**
10	**Any.run**

4.2. ANÁLISE COMPARATIVA DAS SOLUÇÕES

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Cuckoo Sandbox		X	
	VirusTotal		X	
	Hybrid Analysis		X	
	Joe Sandbox		X	
	FireEye Malware Analysis		X	
	VxStream Sandbox		X	
	Comodo Valkyrie		X	
	ReversingLabs TitaniumCloud		X	
	Detux		X	
	Any.run		X	

A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Cuckoo Sandbox		X	
	VirusTotal		X	
	Hybrid Analysis		X	
	Joe Sandbox		X	
	FireEye Malware Analysis		X	
	VxStream Sandbox		X	
	Comodo Valkyrie		X	
	ReversingLabs TitaniumCloud		X	
	Detux		X	
	Any.run		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Cuckoo Sandbox	X		
	VirusTotal		X	
	Hybrid Analysis		X	
	Joe Sandbox		X	
	FireEye Malware Analysis		X	
	VxStream Sandbox		X	
	Comodo Valkyrie		X	
	ReversingLabs TitaniumCloud		X	
	Detux	X		
	Any.run		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Cuckoo Sandbox			X
	VirusTotal			X
	Hybrid Analysis			X
	Joe Sandbox			X
	FireEye Malware Analysis			X
	VxStream Sandbox			X
	Comodo Valkyrie			X
	Detux			X
	Any.run			X
	Cuckoo Sandbox			X
	VirusTotal			X

A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Hybrid Analysis			X
	Joe Sandbox			X
	FireEye Malware Analysis			X
	VxStream Sandbox			X
	Comodo Valkyrie			X
	ReversingLabs TitaniumCloud			X
	Detux			X
	Any.run			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Cuckoo Sandbox			X
	VirusTotal			X
	Hybrid Analysis			X
	Joe Sandbox			X
	FireEye Malware Analysis			X
	VxStream Sandbox			X
	Comodo Valkyrie			X
	ReversingLabs TitaniumCloud			X
	Detux			X
	Any.run			X
A solução permite a visualização em tempo real do comportamento do malware	Cuckoo Sandbox		X	
	VirusTotal		X	
	Hybrid Analysis		X	
	Joe Sandbox		X	
	FireEye Malware Analysis		X	
	VxStream Sandbox		X	
	Comodo Valkyrie		X	
	ReversingLabs TitaniumCloud		X	
	Detux		X	
	Any.run	X		
	Cuckoo Sandbox		X	
	VirusTotal		X	

A solução possui interface interativa	Hybrid Analysis		X	
	Joe Sandbox		X	
	FireEye Malware Analysis		X	
	VxStream Sandbox		X	
	Comodo Valkyrie		X	
	ReversingLabs TitaniumCloud		X	
	Detux		X	
	Any.run	X		
A solução permite captura de pacotes de rede	Cuckoo Sandbox	X		
	VirusTotal		X	
	Hybrid Analysis	X		
	Joe Sandbox	X		
	FireEye Malware Analysis	X		
	VxStream Sandbox	X		
	Comodo Valkyrie		X	
	ReversingLabs TitaniumCloud		X	
	Detux	X		
	Any.run	X		
A solução permite a escolha entre diferentes sistemas operacionais para executar o malware	Cuckoo Sandbox	X		
	VirusTotal		X	
	Hybrid Analysis	X		
	Joe Sandbox	X		
	FireEye Malware Analysis	X		
	VxStream Sandbox	X		
	Comodo Valkyrie		X	
	ReversingLabs TitaniumCloud		X	
	Detux		X	
	Any.run	X		
	Cuckoo Sandbox	X		
	VirusTotal		X	
	Hybrid Analysis	X		

A solução emite relatórios detalhados	Joe Sandbox	X		
	FireEye Malware Analysis	X		
	VxStream Sandbox	X		
	Comodo Valkyrie	X		
	ReversingLabs TitaniumCloud	X		
	Detux	X		
	Any.run	X		
A solução permite o compartilhamento de sessões	Cuckoo Sandbox	X		
	VirusTotal		X	
	Hybrid Analysis	X		
	Joe Sandbox	X		
	FireEye Malware Analysis	X		
	VxStream Sandbox	X		
	Comodo Valkyrie	X		
	ReversingLabs TitaniumCloud	X		
	Detux		X	
	Any.run	X		
A solução permite a integração com outras ferramentas de segurança da informação	Cuckoo Sandbox	X		
	VirusTotal		X	
	Hybrid Analysis	X		
	Joe Sandbox	X		
	FireEye Malware Analysis	X		
	VxStream Sandbox	X		
	Comodo Valkyrie	X		
	ReversingLabs TitaniumCloud	X		
	Detux		X	
	Any.run	X		
	Cuckoo Sandbox		X	
	VirusTotal	X		

É uma solução SaaS (Software como Serviço)?	Hybrid Analysis	X		
	Joe Sandbox	X		
	FireEye Malware Analysis		X	
	VxStream Sandbox		X	
	Comodo Valkyrie		X	
	ReversingLabs TitaniumCloud	X		
	Detux			
	Any.run	X		

4.3. ESTIMATIVA DE CUSTOS PARA CADA SOLUÇÃO

Id	Descrição da solução (ou cenário)
1	Any.run Hunter para 2 usuários: R$ 64.580,00

5. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Cuckoo Sandbox: Trata-se de ferramenta de software livre, disponível para donwload por meio do github, no entanto, segundo a página "https://github.com/cuckoosandbox/cuckoo", a ferramenta está sendo reestruturada e a versão disponível atualmente não está recebendo mais manutenções, dessa forma, não atende às normas de segurança do TRE-ES para a instalação de ferramentas livres.

VirusTotal: Trata-se de um serviço online gratuito, não é software livre, para análise de arquivos e urls. No entanto não possui uma interface interativa nem permite a análise do malware em tempo real, não atendendo aos requisitos tecnológicos especificados nestes Estudos Técnicos Preliminares.

Hybrid Analysis: Trata-se de ferramenta gratuita, apesar de não se tratar de software livre. Não permite a visualização em tempo real do comportamento do malware e nem possui interface interativa, não atendendo aos requisitos tecnológicos especificados nestes Estudos Técnicos Preliminares. A versão paga da ferramenta é o FalconSandbox da CrowdStrike, que faz parte de uma solução completa de antivírus e threat intelligence da CrowdStrike que não são escopo destes Estudos Técnicos Preliminares, incluindo ferramentas que o TRE-ES já possui.

FireEye Malware Analysis: Trata-se de uma solução bem completa, mas que demanda a instalação de equipamentos na infraestrutura do TRE-ES, tornando muito mais onerosa a contratação.

VxStream Sandbox: Trata-se de solução que demanda instalação na infraestrutura do TRE-ES, não possui interface interativa e nem permite a análise de malware em tempo real. Além disso, faz parte de uma solução maior de antivirus para a qual o TRE-ES já possui contratação.

Comodo Valkyrie: A solução não permite a visualização em tempo real do comportamento do malware, não possui interface interativa, não permite a captura de pacotes de rede, não permite a escolha entre diferentes sistemas operacionais para executar o malware. Não atendendo, portanto, vários requisitos tecnológicos especificados nestes Estudos Técnicos Preliminares.

ReversingLabs TitaniumCloud: A solução não permite a visualização em tempo real do comportamento do malware, não possui interface interativa, não permite a captura de pacotes de rede, não permite a escolha

entre diferentes sistemas operacionais para executar o malware. Não atendendo, portanto, vários requisitos tecnológicos especificados nestes Estudos Técnicos Preliminares.

Detux: Trata-se de software livre, específica para emular o sistema operacional Linux. A solução não permite a visualização em tempo real do comportamento do malware, não possui interface interativa, não permite a escolha entre diferentes sistemas operacionais para executar o malware. Não atendendo, portanto, vários requisitos tecnológicos especificados nestes Estudos Técnicos Preliminares.

Joe Sandbox Cloud: A solução não permite a visualização em tempo real do comportamento do malware e não possui interface interativa, não atendendo aos requisitos tecnológicos especificados nestes Estudos Técnicos Preliminares.

Any.run: Ferramenta de análise de malware que atende a todos os requisitos de negócio especificados nos Estudos Técnicos Preliminares, no entanto, a versão gratuita publica todos os arquivos analisados disponibilizando-os online para qualquer usuário, sendo necessária a aquisição de uma licença para que as análises possam ser privadas. Dessa forma, para evitar publicação de dados na internet, seria necessária a contratação de uma licença de uso para garantir que todos os envios sejam privados. **A versão Any.run Hunter para 2 usuários atende a demanda.**

6. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

A única solução considerada tecnicamente viável, que atende a todos os requisitos de negócios especificados nestes Estudos Técnicos Preliminares foi a Solução Any.run, cujo custo da licença Hunter para 2 usuários pelo período de 1 ano é R$ 64.580,00.

6.1. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

1. Any.run Hunter para 2 usuários:

a) Descrição da solução: Solução fornecida como software como serviço (SaaS) que permite análise de malware em tempo real, oferecendo uma interface interativa que permite interagir com a sandbox durante a execução do malware possibilitando simular comandos de usuários que poderiam ativá-lo. Também é possível monitorar o acesso do malware à rede, possibilitando a captura de pacotes de rede para uma melhor análise de comportamento. A solução permite a simulação em diferentes sistemas operacionais, emite relatórios detalhados sobre o arquivo analisado e permite o compartilhamento de sessões que facilitam o trabalho em conjunto de mais de um analista. Além disso, é possível sua integração com outras ferramentas de segurança por meio de API.

b) Custo Total de Propriedade da solução 1 – Memória de Cálculo

Apenas o custo para a licença Hunter para 2 usuários: R$ 64.580,00.

6.2. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

O custo estimado é apenas para a contratação da solução pelo período de um ano: R$ 64.580,00.

7. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Após realizar a análise e comparar todas as soluções encontradas como software livre, gratuitas ou de mercado, foi identificado que a solução Any.run é a que melhor atende à demanda, por apresentar todos os requisitos de negócio e requisitos técnicos especificados nestes Estudos Técnicos Preliminares.

7.1. ANÁLISE DA DEPENDÊNCIA TECNOLÓGICA

Não haverá dependência tecnológica. A solução deve funcionar fora da rede do TRE-ES e ao final da contratação deverá ser avaliada a necessidade de renovação.

7.2. COMPOSIÇÃO DE BENS ou SERVIÇOS DA SOLUÇÃO

Serviço. Software como serviço. Licenças de uso por período determinado, na infraestrutura local ou na nuvem.

7.3. INDICAÇÃO DA NECESSIDADE DE PARCELAMENTO DO OBJETO

Não há.

8. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

R$ 64.580,00 ao ano.

9. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Declaramos que a contratação da solução Any.run Hunter para 2 usuários é viável, tendo sido escolhida por apresentar todos os requisitos de negócio e requisitos técnicos especificados nestes Estudos Técnicos Preliminares. trazendo os seguintes benefícios:

- Aumento significativo na detecção de malware avançado e zero-day (malware para o qual ainda não existe resposta de ferramentas de antivírus tradicionais), com a capacidade de identificar e neutralizar ameaças antes que causem danos.
- Capacidades aprimoradas de investigação forense, com a habilidade de realizar análises detalhadas de incidentes e recuperar dados comprometidos.

SEÇÃO II - ANÁLISE DE SUSTENTAÇÃO E TRANSIÇÃO CONTRATUAL

---

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

1.1 – Recursos Materiais

Não há.

1.2 – Recursos Humanos

Não há.

2. ESTRATÉGIA DE CONTINUIDADE CONTRATUAL

Ao final do contrato a equipe de contratação deverá avaliar a necessidade de realizar a renovação.

3. ESTRATÉGIA DE TRANSIÇÃO CONTRATUAL

Não há risco de perda de dados ou necessidade de solicitar retenções ao final do contrato.

4. ESTRATÉGIA DE INDEPENDÊNCIA

Não haverá dependência tecnológica. A solução deve funcionar fora da rede do TRE-ES e ao final da contratação deverá ser avaliada a necessidade de renovação.

SEÇÃO III - MAPA DE GERENCIAMENTO DE RISCOS

1. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

A tabela a seguir apresenta uma síntese dos riscos identificados e classificados:

Id	Risco	Relacionado ao(à):	P	I	Nível de Risco (P × I)
R01	Falta de clareza pelo demandante quanto aos requisitos do software a ser adquirido	Planejamento da Contratação	2	4	8
R02	Atraso no processo administrativo de contratação.	Planejamento da Contratação	2	3	6
R03	Ausência de recursos orçamentários ou financeiros.	Planejamento da Contratação	4	4	16
R04	Atraso ou suspensão no processo licitatório em face de impugnações.	Seleção do Fornecedor	5	4	20
R05	Valores licitados superiores aos estimados para a contratação dos serviços.	Seleção do Fornecedor	3	4	12

Legenda: P = Probabilidade; I = Impacto.
* A qual natureza o risco está associado: fases do Processo da Contratação ou Solução Tecnológica: Planejamento, Seleção do Fornecedor, Gestão do Contrato.
** **Probabilidade**: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000). Usualmente usa-se uma escala de 1 a 5, sendo 1= muito baixo, 2= baixo, 3= médio, 4= alto, 5= muito alto.
*** **Impacto**: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009). Usualmente usa-se uma escala de 1 a 5, sendo 1= muito baixo, 2= baixo, 3= médio, 4= alto, 5= muito alto.
**** **Nível de Risco**: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009). Obtido pelo produto da probabilidade pelo impacto.

2. AVALIAÇÃO E TRATAMENTO DOS RISCOS IDENTIFICADOS

Risco 01:	Falta de clareza pelo demandante quanto aos requisitos do software a ser adquirido	
Probabilidade:	Baixa	
Impacto:	Alto	
Dano 1:	Falta de empresas para participar da licitação que possam atender à demanda	
Tratamento:	Mitigar.	
Id	**Ação Preventiva**	**Responsável**
P1	Estudo das ferramentas disponíveis no mercado para identificar todas as que possam atender à demanda	Equipe de Planejamento da Contratação
P2	Identificação de potenciais fornecedores	Equipe de Planejamento da Contratação
Id	**Ação de Contingência**	**Responsável**
C1	Alocação integral da Equipe de Planejamento da Contratação para prestar esclarecimentos durante o processo licitatório	Integrante Técnico

Risco 02:	Atraso no processo administrativo de contratação.
Probabilidade:	Baixa
Impacto:	Média
Dano 1:	Falta de recursos orçamentários para a contratação

Tratamento:	Mitigar.	
Id	**Ação Preventiva**	**Responsável**
P1	Diligenciar para que o processo siga os trâmites dentro dos prazos corretos	Equipe de Planejamento da Contratação
Id	**Ação de Contingência**	**Responsável**
C1	Entrar em contato com as outras áreas em que o processo tramitar para solucionar dúvidas e atrasos	Equipe de Planejamento da Contratação

Risco 03:	Ausência de recursos orçamentários ou financeiros	
Probabilidade:	Alto	
Impacto:	Alto	
Dano 1:	Impossibilidade de realizar a contratação	
Tratamento:	Mitigar.	
Id	**Ação Preventiva**	**Responsável**
P1	Incluir a contratação no plano de contratações de TIC	Equipe de Planejamento da Contratação
P2	Diligenciar para que o processo cumpra os prazos para que possa ser realizado com a disponibilidade orçamentária verificada	Equipe de Planejamento da Contratação
Id	**Ação de Contingência**	**Responsável**
C1	Caso não seja possível a contratação no ano corrente, incluir a contratação para o ano seguinte	Equipe de Planejamento da Contratação

Risco 04:	Atraso ou suspensão no processo licitatório em face de impugnações.	
Probabilidade:	Muito Alto	
Impacto:	Alto	
Dano 1:	Fracasso da licitação	
Tratamento:	Mitigar.	
Id	**Ação Preventiva**	**Responsável**
P1	Revisar todo o processo antes de encaminhar para a licitação para detectar e corrigir quaisquer vícios que possam surgir durante a licitação	Equipe de Planejamento da Contratação
P2	Responder prontamente e dentro do prazo a todos os questionamentos elaborados pelos fornecedores	Equipe de Planejamento da Contratação
Id	**Ação de Contingência**	**Responsável**
C1	Caso a licitação venha a fracassar, refazer todo o processo para incluir a contratação para o ano seguinte	Equipe de Planejamento da Contratação

Risco 05:	Valores licitados superiores aos estimados para a contratação dos serviços.	
Probabilidade:	Médio	
Impacto:	Baixo	
Dano 1:	Fracasso da licitação	
Tratamento:	Mitigar.	
Id	**Ação Preventiva**	**Responsável**
P1	Indicação à área responsável pela realização de pesquisa de mercado de potenciais fornecedores para que sejam coletados preços praticados no mercado	Equipe de Planejamento da Contratação
Id	**Ação de Contingência**	**Responsável**
C1	Caso a licitação venha a fracassar, refazer todo o processo para incluir a contratação para o ano seguinte	Integrante Técnico

3 – ACOMPANHAMENTO DAS AÇÕES DE TRATAMENTO DE RISCOS

{ *Espaço para registro e acompanhamento das ações de tratamento dos riscos, que poderá conter eventos relevantes relacionados ao gerenciamento de riscos, conforme exemplo abaixo* }.

Data	Id. Risco	Id. Ação	Registro e acompanhamento das ações de tratamento dos riscos
07/08/2024	R01	P1	Foram realizadas pesquisas sobre as diversas ferramentas disponíveis no mercado para identificar todas as que possam atender à demanda.

4 – APROVAÇÃO E ASSINATURA

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO (Portaria 504 - SEI nº 1216065)

Integrante Demandante: OLGA BAYERL VITA (titular); CARLOS EDUARDO LAQUINE (substituto)

Integrante Técnico: CARLOS EDUARDO LAQUINE (titular); OLGA BAYERL VITA (substituto)

Integrante Administrativo: CARLOS ALBERTO DA ROCHA PADUA FILHO (titular); MARCOS VENTUROTT FERREIRA (substituto)

Vitória, 30 de agosto de 2024.

Documento assinado eletronicamente por **CARLOS ALBERTO DA ROCHA PADUA FILHO**, **Coordenador(a)**, em 05/09/2024, às 18:05, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **OLGA BAYERL VITA**, **Assistente do Núcleo de Segurança Cibernética**, em 05/09/2024, às 18:13, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **CARLOS EDUARDO LAQUINE**, **Integrante Técnico**, em 05/09/2024, às 18:15, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-es.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1227796** e o código CRC **D1987333**.