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

ESTUDO PRELIMINAR (DEMANDAS DE TIC) Nº STIC 06/2022 - TRE-ES/PRE/DG/STI/CIS/SRCD

(este documento deve seguir as orientações da Resolução TRE/ES nº 261/2018)

SUMÁRIO

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1 - CARACTERIZAÇÃO DA DEMANDA

1.1 - Descrição Sucinta

Aquisição de uma solução de Segurança para Servidores (Linux e Windows), com XDR e Sandbox, com manutenção e garantia (update e upgrade).

1.2 - Justificativa da necessidade e Resultados

A aquisição da solução em questão visa proteger os servidores de rede contra ameaças conhecidas como: objetos maliciosos Browser Helper (BHOs), sequestradores de navegadores, ransomware, keyloggers, backdoors, rootkits, cavalos de tróia, worms, dialers, fraudtools, adware e spyware. Também inclui proteção contra ameaças virtuais, tais como URLs infectadas e maliciosas, spam, fraude e ataques de phishing, identidade online (privacidade), ataques bancários on-line, ameaças persistentes avançadas (APT).

Uma das camadas de proteção é realizada pelo sistema de antimalware, atualmente chamado de sistema de proteção de estações de trabalho e servidores. Seguindo as tendências de evolução de atividades maliciosas, vale ressaltar também o processo evolutivo das soluções de proteção ao ambiente. Atualmente a proteção de XDR, aliada a proteção de tradicional de um antivirus, se tornou um requisito mínimo para proteção adequada do ambiente, provendo maior capacidade de detecção e principalmente de resposta a atividades maliciosas.

O não atendimento da necessidade trará para a rede da Justiça Eleitoral risco de infecções causadas por códigos maliciosos desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas de códigos maliciosos que podem infectar ou comprometer um computador são:

- Pela exploração de vulnerabilidades existentes nos programas instalados;
- Pela auto execução de mídias removíveis infectadas, como pendrives;
- Pelo acesso às páginas Web maliciosas, utilizando navegadores vulneráveis;
- Pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas;
- Através de mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

Com esta contratação pretende-se assegurar que os serviços de TIC sejam prestados de forma satisfatória protegendo os servidores de rede e mitigando as ameaças que possam comprometer a segurança da informação.

2 - ESPECIFICAÇÃO DOS REQUISITOS FUNCIONAIS

2.1 - Requisitos Relacionados ao Negócio

A solução deve:

- Possuir proteção avançada antimalware para estações de trabalho e servidores de rede.
- Possuir proteção contra execução de aplicações maliciosas.
- Realizar análise e bloqueio da execução de aplicações baseada em comportamento.
- Monitorar as atividades de criptografia de arquivos para evitar ataques de ransomware.
- Possuir proteção contra ataques direcionados e 0Day.
- Possuir proteção para a solução de correio eletrônico com capacidade de atendimento ao tráfego de e-mail gerado.

2.2 - Requisitos de Capacitação, Ambientais, Culturais e Sociais

A contratação deve prover a transferência de conhecimento para capacitar os servidores da STI a operacionalizar a ferramenta.

2.3 - Requisitos de Manutenção

Não há requisitos de manutenção dos itens adquiridos, exceto quando houver mudança de versão do sistema operacional.

2.4 - Requisitos Temporais

As licenças adquiridas serão no modo de subscrição com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.

2.5 - Requisitos de Segurança

A empresa contratada deverá respeitar as diretrizes constantes da Política de Segurança da Informação da Justiça Eleitoral (Resolução TSE Nº 23.501/2016), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral do Espírito Santo aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;

O Tribunal Regional Eleitoral da Espírito Santo terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;

Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX).

3. ESPECIFICAÇÃO DOS REQUISITOS TECNOLÓGICOS

3.1 - Características para Servidores Linux

3.1.1. Deve possuir compatibilidade com Plataforma 64-bits para as seguintes distribuições:

- Red Hat Enterprise Linux 6.7 e superior;
- Ubuntu 16.04 LTS e superior;
- CentOS 6.7 e superior;
- Debian GNU / Linux 8.6 e superior;
- Oracle Linux 7.3 e superior;
- SUSE Linux Enterprise Server 15 e superior.

3.1.2. Deve prover as seguintes proteções:

- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;
- Deve ser capaz detectar vírus, worms, trojans, toolkits, adware, auto-dialers e outros tipos de ameaças;
- Deve possuir módulo de proteção baseado em comportamento;
- Deve possuir funcionalidade para identificar as aplicações maliciosas ou não nos servidores com opção de bloquear ou
- permitir;
- Deve ter a capacidade de criar regras para controle de uma aplicação utilizando hash ou nome da aplicação.
- Ter a capacidade de detectar e aplicar as regras necessárias nos módulos e políticas de varredura para cada servidor, de
- forma automática, ou pelo administrador;

3.1.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:

- Via linha de comando;
- Via console administrativa;
- Via GUI;
- Via web;

3.1.4 Deve possuir funcionalidade de scan de drives removíveis para, no mínimo:

- Flash drives;
- HDs externos;

3.1.5 Deve fornecer varredura em compartilhamentos e unidades de rede mapeadas:

- Por arquivos;
- Por pastas/diretórios.

3.1.6. As vacinas devem ser atualizadas, no mínimo, uma vez por dia pelo fabricante;

3.1.7. Deve realizar gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

3.1.8. Deve realizar gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

3.1.9. Deve realizar gerenciamento de Quarentena: Deve bloquear objetos suspeitos;

3.1.10. Deve realizar verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados);

3.1.11. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

3.1.12 Deve possuir capacidade de customizar o uso de memória ou processamento em varreduras agendadas;

3.1.13. Deve possuir capacidade de verificar objetos usando heurística;

3.1.14. Deve possibilitar a realização de backup dos arquivos infectados antes de realizar uma ação;

3.1.15. Deve fazer detecções através de heurística.

3.1.16. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:

- Detecção de phishing e sites maliciosos;
- Bloqueio de download de arquivos maliciosos;
- Bloqueio de adware.

3.1.17. Deve possuir módulo de proteção contra criptografia maliciosa, protegendo contra tentativas de criptografia remota;

3.1.18. Deve possuir recurso contra ataques maliciosos;

3.1.19. Deve possuir recurso para restabelecimento de arquivos contra ataques maliciosos.

3.1.20. Deve realizar busca de vírus e malwares em ambientes Docker e Contâiner;

3.2 - Características para Servidores Windows

3.2.1 - Deve possuir compatibilidade com os Sistemas Operacionais:

- Microsoft Windows Server 2019 Essentials / Standard / Datacenter;
- Microsoft Windows Server 2016 Essentials / Standard / Datacenter;
- Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Microsoft Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Microsoft Windows Server 2008 R2 Foundation / Essentials / Standard / Datacenter SP1;

3.2.2. Deve suportar as seguintes plataformas virtualizadas:

- VMware Workstation 16 Pro;
- VMware ESXI 7.0. e superior;
- Microsoft Hyper-V Server 2019;
- Citrix Hypervisor 8.2 LTSR;

3.2.3. Deve possuir as seguintes características de proteção:

- Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;
- Auto-proteção contra-ataques aos serviços/processos do antivírus;
- Firewall com IDS;
- Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3.2.4. Deve permitir gerenciamento, no mínimo, das seguintes formas:

- Via console administrativa;
- Via web (remotamente);

3.2.5. As vacinas devem ser atualizadas, no mínimo, uma vez por dia pelo fabricante;

3.2.6. Deve possuir a capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

- Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
- Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
- Leitura de configurações;
- Modificação de configurações;
- Gerenciamento de Backup e Quarentena;
- Visualização de logs;
- Gerenciamento de logs;
- Gerenciamento de ativação da aplicação;
- Gerenciamento de permissões (adicionar/excluir permissões acima);
- Bloqueio de inicialização de aplicativos baseado em white lists.

3.2.6. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

- Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
- Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

3.2.7.Deve possuir capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

3.2.8. Deve bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;

3.2.9. Deve possuir capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros);

3.2.10. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

3.2.11. Deve possuir funcionalidade de análise personalizada de logs do Windows;

3.2.12 Deve possuir capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

3.2.13. Deve possuir capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

3.2.14. Deve possuir capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

3.2.15. Deve possuir capacidade de adicionar pastas para uma zona de exclusão, a fim de excluí-las da verificação. Capacidade, também, de adicionar arquivos à lista de exclusão;

3.2.16. Deve possuir capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

3.2.16. Deve possuir capacidade de verificar somente arquivos novos e alterados;

3.2.17. Deve possuir capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários);

3.2.18. Deve possuir capacidade de verificar objetos usando heurística;

3.2.19. Deve possuir capacidade de configurar diferentes ações para diferentes tipos de ameaças;

3.2.20. Deve possuir capacidade de agendar uma pausa na verificação;

3.2.21. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

- Perguntar o que fazer, ou;
- Bloquear acesso ao objeto;
- Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- Caso positivo de desinfecção:
- Restaurar o objeto para uso;
- Caso negativo de desinfecção:
- Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

3.2.22. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

3.2.23. Deve possibilitar a escolha da pasta onde serão guardados os backups e arquivos em quarentena;

3.2.24. Deve possibilitar a escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

3.2.25. Em caso de detecção de sinais de de uma infecção ativa, deve possuir capacidade de, automaticamente:

- Executar os procedimentos pré-configurados pelo administrador;
- Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.

3.2.26. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

3.2.26. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;

3.2.27. Deve possuir capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning);

3.2.28. Deve possuir capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

3.3. Características XDR (EDR Extendido) para servidores

3.3.1. A funcionalidade de EDR e cliente de antivírus devem ser integradas sendo configurado pela mesma gerência;

3.3.2. A ferramenta de EDR deve fazer detecção através do comportamento;

3.3.3. Deve fazer o correlacionamento de eventos entre computadores na rede (IoC Scanning);

3.3.4. Deve detectar elevação de privilégio;

3.3.5. Deve enviar objetos para verificação em Sandbox de formar manual e automática;

3.3.6. O EDR deve permitir coletar informações forenses do endpoint tais como:

- Dados;
- Dumps de memória;
- Estado do sistema operacional;
- Processos iniciados;
- Conexões estabelecidas;
- Arquivos criados;
- Registro modificado;
- Tentativas de conexão com um host remoto;
- Tentativa de login com sucesso;
- Tentativa de login com falha.

3.3.7. Para segurança entre a comunicação entre o EDR e a Console de gerenciamento um certificado deve ser utilizado;

3.3.8. O EDR deve ser capaz de executar tarefas para todo o ambiente e para dispositivos específicos, contendo no mínimo as capacidades abaixo:

- 23.1.6.19. Parar um processo;
- 23.1.6.20. Deletar um objeto;
- 23.1.6.21. Quarentenar um arquivo;
- 23.1.6.22. Recuperar um arquivo;
- 23.1.6.23. Prevenir a execução de um arquivo;
- 23.1.6.24. Executar um script;
- 23.1.6.25. Isolar o host completamente e de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

3.3.9. Deve ser possível realizar a customização de indicador de ataques IoA;

3.3.10. Deve ter capacidade de apresentar informações relacionadas ao MITRE ATT&CK para cada um dos eventos detectados no ambiente, caso possuam;

3.3.11. Deverá possuir modulo de pesquisa para descoberta de ameaças (Threat Hunting);

3.3.12. Deverá possuir acesso ao portal de inteligência de ameaças da própria fabricante.

3.3.13. No portal deverá ser possível buscar informações sobre indicadores de ataques, consultas de domínios na base global de ameaças do próprio fabricante;

3.3.14. Deve possuir funcionalidade integrada de emulação para malware, onde as ameaças sejam analisadas em Sandbox, em ambiente controlado, em nuvem própria do fabricante ou em ambiente computacional da Justiça eleitoral;

3.3.15. Deverá realizar emulação em Sandbox nos seguintes sistemas operacionais:

- Windows 7, 64-bit;

- Windows 10, 64-bit;

3.3.16. Deverá ser possível prevenir ataques de forma automatizada baseada na resposta da Sandbox;

3.4 - Serviço de Instalação, Configuração e Transferência de Conhecimento

3.4.1. A CONTRATADA será inteiramente responsável pela instalação da solução antivírus, bem como pelas despesas diretas ou indiretas para execução das atividades pela sua equipe técnica;

3.4.2. A instalação das consoles de gerência da solução será realizada remotamente no ambiente do TRE-ES;

3.4.3. Deverá ser realizada a instalação dos softwares em 5 (cinco) servidores, remotamente;

3.4.4. A instalação da solução no ambiente do Contratante não poderá interferir no bom funcionamento de outros sistemas previamente instalados;

3.4.5. A instalação da solução deverá ser realizada em horário de expediente de cada sítio, podendo ocorrer no período de 8h às 20hs;

3.4.6. O processo de instalação e configuração da solução deverá ser acompanhado por servidores do TRE-ES;

3.4.7. Para garantir que a instalação não afete o ambiente do CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos certificados pelo fabricante;

3.4.8. A CONTRATADA deverá se reunir com a equipe técnica do CONTRATANTE, por solicitação desta, e elaborar um plano de migração, em até 10 (dez) dias úteis, contendo as etapas, modelos, arquiteturas, funcionalidades e configurações da solução que serão implantadas durante a execução do serviço de migração;

3.4.9. Caso alguma instalação mostre-se não funcional ou apresente problemas, será feita a comunicação do CONTRATANTE para a CONTRATADA, por e-mail ou abertura de chamado. A instalação deverá ser refeita em até 2 (dois) dias úteis a contar da comunicação feita pelo CONTRATANTE;

3.4.10. A CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica do CONTRATANTE, por meio de treinamento oficial nas tecnologias da solução, com carga horária total de 40 (quarenta) horas;

3.4.11. A carga horária diária será de 4h (quatro horas). O treinamento deverá ocorrer em dias úteis e em horário comercial;

3.4.12. A transferência de conhecimento deverá ser realizada de forma remota ou poderá ser realizada nas dependências do TRE-ES conforme decisão do CONTRATANTE;

3.4.13. A transferência de conhecimento deverá conter conteúdo teórico e prático e deverá abordar, no mínimo, os seguintes itens:

- Detalhamento dos componentes da solução, suas interconexões e todas as informações técnicas necessárias para o seu pleno funcionamento;
- Orientar sobre os componentes, procedimentos de instalação e administração da solução unificada de segurança para endpoint e EDR, explorando todas as funcionalidades exigidas na especificação técnica;
- Orientar sobre a topologia lógica da solução implantada, mostrando a interligação dos componentes físicos e virtuais da solução, informando as interconexões realizadas com a infraestrutura existente no CONTRATANTE;
- Orientar sobre os componentes, procedimentos de instalação e administração da solução, explorando as funcionalidades disponíveis na solução ofertada, ainda que não exigidas na especificação técnica.

3.4.14. O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE;

3.4.15. Deverá ser disponibilizado material didático em formato digital, sem custo adicional para o CONTRATANTE. Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês);

3.4.16. Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa e carga horária;

3.4.17. A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelo fabricante dos softwares da solução ofertada.

4. IDENTIFICAÇÃO E COMPARAÇÃO DAS SOLUÇÕES ADERENTES AOS REQUISITOS

A única solução que atende todos os requisitos tecnológicos e a aquisição de antivirus com XDR para servidores.

4.1. Antivirus com XDR para servidores

Descrição da solução: Sistema de antivirus para proteção contra malwares de computador e ameaças conhecidas nos servidores de rede.

Órgão /Entidade Proprietário da Solução: Não se aplica à presente contratação.

Aderência da Solução ao MNI: Não se aplica à presente contratação.

Aderência da Solução ao ICP-Brasil: Não se aplica à presente contratação.

Aderência da Solução ao Moreq-Jus: Não se aplica à presente contratação.

5 - INDICAÇÃO DA STIC ESCOLHIDA

5.1 - Descrição da Solução

Nome: Antivirus com XDR para servidores.

Descrição: Aquisição de uma solução de Segurança para Servidores (Linux e Windows), com XDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses

Valor Estimado: A solução tem um valor anual estimado de R$ 36.800,00 (Trinta e seis mil e oitocentos reais). O valor estimado para 5 anos é de R$ 184.000,00 (Cento e Oitenta e quatro mil reais).

5.2 - Justificativa/Motivação da Escolha

A solução escolhida é a única que atende a todos os requisitos exigidos;

5.3 - Aderência aos Requisitos

Os requisitos tecnológicos estão aderentes aos requisitos funcionais estabelecidos pelo demandante.

5.4 - Relação entre a Demanda Prevista e a STIC

O TRE-ES possui aproximadamente 160 servidores de redes que precisam de proteção avançada de antivirus, de acordo com a tabela abaixo:

ITEM	QUANTIDADE
Servidores Windows	40
Servidores Linux	120
TOTAL	**160**

Assim o TRE-ES necessitará de 160 licenças de subscrição para a solução de segurança para servidores com XDR.

Em consonância com o que está disposto no Termo de Referência do TSE (0684561) será necessário adquirir:

ITEM	DESCRIÇÃO	QUANTIDADE
3	Solução de Segurança para Servidores (Linux e Windows para ambientes do TSE e 27 TREs), com XDR e Sandbox, com manutenção, garantia (update e upgrade) e suporte por 60 meses, com pagamento de subscrições a cada 12 meses.	160

Cabe ressaltar que os itens referentes a instalação, configuração e transferência de conhecimento já foram adquiridos pelo TSE para todos os TRE´s e atendem completamente os requisitos do presente estudo técnico.

6 - INDICAÇÃO DA NECESSIDADE DE ADEQUAÇÃO AMBIENTAL

Não existem necessidades de adequação ambiental.

ANÁLISE DE RISCOS

7 - IDENTIFICAÇÃO DOS RISCOS

Os principais riscos identificados foram:

- Não cumprimento do prazo de entrega pela contratada;

- Solução não oferecer proteção eficiente contra ataques avançados.

8 - RELAÇÃO DOS RISCOS E AÇÕES DE MITIGAÇÃO

RISCO 1	NÃO CUMPRIMENTO DO PRAZO DE ENTREGA PELA CONTRATADA	
Probabilidade: (Alta, média ou baixa)	**Baixa**	
	Efeito (Dano)	**Impacto:** (Alto, médio ou baixo)
1	Necessidade utilização de computadores com antivírus desatualizados, podendo causar infecções e/ou epidemias de vírus na rede da Justiça Eleitoral.	Alto
	Ações de Mitigação e Contingência	**Responsável**
1	Acompanhar rigorosamente o processo de contratação	Integrante Demandante
2	Interceder junto à contratada a fim de priorizar a entrega das licenças.	Integrante Demandante

RISCO 2	SOLUÇÃO NÃO OFERECER PROTEÇÃO EFICIENTE CONTRA ATAQUES AVANÇADOS	
Probabilidade: (Alta, média ou baixa)	**Baixa**	
	Efeito (Dano)	**Impacto**: (Alto, médio ou baixo)
1	Ocorrência de infecção por vírus e demais malwares, e ineficiência ao mitigá-la colocando em risco a rede da Justiça Eleitoral.	Alto
	Ações de Mitigação e Contingência	Responsável
1	Acompanhamento constante na atualização da solução, além de acionamento do suporte da contratada.	SRCD
2	Acionamento dos canais de suporte da contratada.	SRCD

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO

9. RECURSOS MATERIAIS E HUMANOS

Trata-se de aquisição de licenciamento de software. A instalação e configuração inicial serão realizadas pela contratada.

10. DESCONTINUIDADE DO FORNECIMENTO

Não se aplica. Compra de licenciamento de software em parcela única.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Integrante Demandante: Rommel Baia Silva (substituto: Lucas Ribeiro Carlin)

Integrante Técnico: Lucas Ribeiro Carlin (substituto: Rommel Baia Silva)

Integrante Administrativo: Marcos Venturott Ferreira (substituto: Carlos Alberto da Rocha Padua Filho)

Vitória, 16 de fevereiro de 2022.

Documento assinado eletronicamente por **MARCOS VENTUROTT FERREIRA**, **Integrante Administrativo**, em 17/02/2022, às 18:13, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUCAS RIBEIRO CARLIN**, **Técnico Judiciário**, em 17/02/2022, às 18:17, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ROMMEL BAIA SILVA**, **Chefe de Seção**, em 17/02/2022, às 18:19, 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 **0693031** e o código CRC **96D82C31**.