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

ESTUDO TÉCNICO PRELIMINAR (DEMANDAS DE TIC) Nº STIC 14/2021 - 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 Solução de Segurança contra Ataques Cibernéticos e Ransomware.

1.2 - Justificativa da necessidade e Resultados

A contratação justifica-se pela necessidade de manter cópia dos servidores de rede do ambiente de produção armazenados em estrutura segura e isolada logicamente da rede local do TRE-ES, de forma análoga a um cofre, utilizando software de análise que indique a não existência de ransomware oculto e outras ameaças nos dados copiados.

Os objetivos (resultados) esperados são:

1) Manter em ambiente apartado física e logicamente da rede local uma cópia dos principais dados do Tribunal, garantindo que estejam livres de ransomware e outras ameaças conhecidas;

2) Permitir a recuperação de dados íntegros para o ambiente de produção em caso de ataques cibernéticos;

3) Permitir um acesso mais ágil às informações armazenadas no ambiente seguro em caso de impossibilidade de restauração imediata do ambiente de produção.

2 - ESPECIFICAÇÃO DOS REQUISITOS FUNCIONAIS

2.1 - Requisitos Relacionados ao Negócio

- A solução deverá possuir a finalidade específica de armazenar uma réplica dos dados contidos no equipamento de backup primário em uso pelo TRE-ES, DELL IDPA modelo DP4400, com a utilização de algum mecanismo que indique a não existência de ransomware oculto e outras ameaças nos dados copiados;

- Não será permitida oferta de soluções que não sejam compatíveis com o equipamento de backup do TRE-ES, DELL IDPA modelo DP4400.

- A solução ofertada deverá contemplar todos os componentes necessários ao seu pleno funcionamento (ex: fibras óticas, patch cords, transceivers, PDUs, tomadas elétricas, entre outros).

2.2 - Requisitos de Capacitação, Ambientais, Culturais e Sociais

A CONTRATADA deverá providenciar o repasse de conhecimento das ferramentas e componentes da solução ofertada, à equipe técnica da CONTRATANTE.

2.3 - Requisitos de Manutenção e Garantia

A solução deverá possuir garantia de 60 meses.

2.4 - Requisitos Temporais

A solução de chamados técnicos referentes a **problemas de hardware** deve ocorrer em até **4 dias úteis, a partir da abertura do chamado**, mesmo em caso de necessidade de substituição de peças.

O atendimento inicial referente a chamados técnicos sobre **problemas/dúvidas em relação aos softwares** deve ocorrer em até **2 horas após a abertura do chamado**, através do contato de um analista capacitado.

A solução deve ser instalada e configurada em até 60 (sessenta) dias após emissão da ordem de serviço de fornecimento.

3. ESPECIFICAÇÃO DOS REQUISITOS TECNOLÓGICOS

LOTE COM SOLUÇÃO DE SEGURANÇA CONTRA ATAQUES CIBERNÉTICOS E RANSOMWARE			
ITEM	**DESCRIÇÃO**	**QUANT.**	**CLASSIFICAÇÃO**
1	**Sistema de armazenamento/proteção de dados em disco DELL DATA DOMAIN**	01 UN	Investimento
2	**servidor de Rack TIPO 1**	01 UN	Investimento
3	**servidor de Rack TIPO 2**	01 UN	Investimento
4	**Switch de Rede**	02 UN	Investimento
5	**Licença de software DELL CYBER RECOVERY (software de vida útil indefinida)**	01 UN	Investimento
6	**Licença de software DELL CYBER SENSE (software de vida útil indefinida)**	01 UN	Investimento

3.1 - JUSTIFICATIVA PARA FORMAÇÃO DE LOTE

A formação do lote é necessária pois os itens solicitados são interdependentes. A solução só torna-se funcional com a aquisição e instalação de todos os itens. É imprescindível, portanto, que sejam adquiridos em conjunto.

3.2 - JUSTIFICATIVA PARA DEFINIÇÃO DE MARCA/FABRICANTE

A solução de segurança cibernética a ser adquirida deve ser do fabricante DELL pois ela deve se integrar completamente e receber os dados da solução de backup atualmente utilizada pelo TRE-ES, que é composta por um appliance de backup DELL IDPA DP4400. Essa integração torna inviável tecnicamente que equipamentos e softwares de outros fabricantes possam ser utilizados.

3.3 - CARACTERÍSTICAS GERAIS

A solução de Segurança contra Ataques Cibernéticos e Ransomware é composta por:

- **Item 1 - 01 (um) sistema de armazenamento/proteção de dados em disco DELL DATA DOMAIN**
- **Item 2 - 01 (um) servidor de Rack TIPO 1**
- **Item 3 - 01 (um) servidor de Rack TIPO 2**
- **Item 4 - 02 (dois) switches de rede**
- **Item 5 - 01 (uma) licença do software DELL CYBER RECOVERY**
- **Item 6 - 01 (uma) licença do software DELL CYBER SENSE.**

Toda a solução ofertada, deverá integrar-se com a solução de backup atualmente existente no ambiente do Tribunal (DELL IDPA DP4400).

Os manuais técnicos referentes a solução deverão ser fornecidos ou disponibilizados eletronicamente;

A solução deverá vir acompanhada de todos os cabos de energia e de conexão lógica para correta instalação, conforme características e serviços descritos neste item.

3.3.1 - Item 1 - O sistema de armazenamento/proteção de dados em disco deverá possuir no mínimo:

- 34 TB (trinta e quatro terabytes) de capacidade de armazenamento;

- Possuir no mínimo 04 (quatro) portas Ethernet de 10 Gbps Base-T e 01 (uma) porta Ethernet de 1 Gbps Base-T;

- Deverá ser do tipo appliance e especifico para backup em disco, não sendo aceito servidores/equipamentos de propósito geral para essa finalidade.

3.3.2 - Item 2 - O servidor rack TIPO 1 da solução deverá possuir, no mínimo:

- 02 (dois) processadores de 2.8Ghz com 16 núcleos cada processador;

- 512GB (quinhentos e doze gigabytes) de memória;

- 10 (dez) discos SAS 10K 12 Gbps de 2.4TB (dois ponto quatro terabytes), cada;

- Controladora de discos SAS, com 8GB de cache;

- 08 (oito) portas Ethernet de 10 Gbps Base-T;

- 01 (uma) porta Ethernet de 1 Gbps Base-T para gerenciamento *out of band*;

- Fontes de alimentação redundantes com capacidade de suportar o funcionamento do servidor em sua configuração ofertada, em caso de falha de uma das fontes;

3.3.3 - Item 3 - O servidor rack TIPO 2 da solução deverá possuir, no mínimo:

- 02 (dois) processadores de 2.4Ghz com 10 núcleos cada processador;

- 128GB (cento e vinte e oito gigabytes) de memória;

- 04 (quatro) discos SAS 10K 12 Gbps de 2.4TB (dois ponto quatro terabytes), cada;

- Controladora de discos SAS, com 2GB de cache;

- 08 (oito) portas Ethernet de 10 Gbps Base-T; 01 (uma) porta Ethernet de 1 Gbps Base-T para gerenciamento *out of band*;

- Fontes de alimentação redundantes com capacidade de suportar o funcionamento do servidor em sua configuração ofertada em caso de falha de uma das fontes;

- Ser entregue com os respectivos licenciamentos: VMware *Essentials Kit* e Windows Server 2019 Standard para todos os processadores/núcleos solicitados para o servidor.

3.3.4 - Item 4 -Os switches deverão possuir, no mínimo:

- 28 (vinte e oito) portas 1/10 GbE Base-T;

- 02 (duas) portas QSFP28, permitindo conexões a 100GbE;

- Throughput de 700 (setecentos) Mpps;

- Capacidade de switching de 900 (novecentos) Gbps.

3.3.5 - Itens 5 e 6 - Os softwares da solução ofertada deverão, em conjunto, possuir no mínimo:

- Integração de soluções de varredura, análise, validação e relatórios de integridade de dados e metadados de backup armazenados na cópia offline;

- Estar licenciado para no mínimo 32TB de capacidade;

- Processos de proteção do equipamento de réplica, e permitir ativação do bloqueio e imutabilidade dos dados quando necessário;

- Capacidade de realizar a varredura no conteúdo completo dos arquivos, incluindo metadados e identificar se há comprometimento de dados, incluindo criptografia, ransomware, destruição e corrupção lenta dos arquivos copiados;

- Ferramentas forenses, fazer uso de métodos para encontrar arquivos corrompidos e diagnosticar o ataque a partir da imagem de backup;

- Capacidade de analisar as cópias de backup sem restaurar os dados de backup;

- Capacidade de monitorar a integridade dos dados de backup, enviar relatórios e alertas quando ocorrem mudanças que indicam um incidente cibernético;

- Capacidade de se comunicar com o sistema de armazenamento/proteção de dados em disco, para verificar a integridade dos dados de backup do mesmo;

- Capacidade para operar completamente offline e apartada da rede de produção, exceto ao receber atualizações da réplica dos backups;

- Capacidade de gerenciar as regras de replicação controlada garantindo a réplica segura com “air-gap” de comunicação com o appliance primário (produção) e o sistema de armazenamento/proteção de dados em disco;

- Capacidade de usar criptografia para transferir dados entre os appliances;

- Capacidade de gerenciar e aplicar regras de imutabilidade (WORM) nas imagens de backup;

- Console gráfica capaz de gerenciar e informar o status das imagens de backup, assim como a última cópia válida;

- Capacidade de manter várias cópias de dados de maneira segura;

3.4 - INSTALAÇÃO E CONFIGURAÇÃO

Para instalação e configuração da solução deverão ser fornecidos os seguintes serviços:

3.4.1 - Instalação física dos equipamentos que compõem a solução no rack do datacenter;

3.4.2 - Configuração dos módulos e demais softwares ofertados que compõem toda solução;

3.4.3 - Atualização de firmwares/softwares que compõem a solução;

3.4.4 - Configuração de Credenciais e Acesso e Endereços de Rede;

3.4.5 - Configuração das Interfaces de Gerenciamento;

3.4.6 - Configurar a replicação segura entre os equipamentos primário e secundário;

3.4.7 - Apoiar a equipe de segurança da CONTRATANTE na definição das regras de firewall (se necessário);

3.4.8 - Configurar toda comunicação lógica dos equipamentos ofertados;

3.4.9 - Ativação de Licenças e Features Adquiridas;

3.4.10 - Criação de Pools de Armazenamento e replicação;

3.4.11 - Apresentação de Volumes de Backup para o servidor de backup do ambiente de réplica;

3.4.12 - Elaborar plano e configurar até 3 (três) políticas de replicação seguras;

3.4.13 - Configurar até 3 (três) políticas de agendamento da varredura de verificação e análise;

3.4.14 - Realizar testes e execução das rotinas de validação e envio de alerta das rotinas de varredura;

3.4.15 - Testes de backup e recuperação das 3 (três) políticas;

3.4.16 - Elaborar documentação com procedimentos para validação e recuperação dos backups limpos de malware ou ransomware;

3.4.17 - Elaboração e Entrega de Documentação de Instalação e Configuração após o término dos trabalhos;

3.4.18 - Durante a implementação da solução, providenciar o repasse de conhecimento das ferramentas e componentes da solução ofertada, à equipe técnica da CONTRATANTE, de forma que a administração e operação seja feita de forma independente, contemplando todas as funcionalidades especificadas neste documento de entrega;

3.5 - GARANTIA E SUPORTE

3.5.1 - A solução deverá ter suporte centralizado (software e hardware) em central de atendimento;

3.5.2 - Suporte de hardware pelo período de **60 meses on-site**, incluindo a reposição de peças danificadas, custos operacionais e a mão-de-obra de assistência técnica;

3.5.3 - Direito à suporte e atualização de software/firmware pelo período de **60 meses.** O FABRICANTE deverá disponibilizar durante todo o período de vigência contratual, a versão mais atual, e todas as versões anteriores de BIOS, FIRMWARES e DRIVERS para os equipamentos ofertados e compatíveis com as versões mais recentes dos sistemas operacionais especificados, sem ônus para a CONTRATANTE;

3.5.4 - Atendimentos de hardware e software através de ambiente WEB e/ou serviço telefônico 0800 (ou número similar inteiramente gratuito) para abertura dos chamados, em **regime 24hx7d**;

3.5.5 - Fornecimento obrigatório de número identificador de chamado no ato da abertura, que permita acompanhar o andamento da solicitação.

3.5.6 - A solução de chamados técnicos referentes a **problemas de hardware** deve ocorrer em até **4 dias úteis, a partir da abertura do chamado**, mesmo em caso de necessidade de substituição de peças.

3.5.7 - O atendimento inicial referente a chamados técnicos sobre **problemas/dúvidas em relação aos softwares** deve ocorrer em até **2 horas após a abertura do chamado**, através do contato de um analista capacitado.

3.5.8- O contato inicial através dos mecanismos previstos em **3.5.4**, mediante a informação do identificador previsto em **3.5.5**, determina o início da contagem dos prazos previstos nos subitens **3.5.6** e **3.5.7**.

3.5.9 - O fechamento do chamado técnico pela contratada, com anuência do contratante, caracterizará o fim da contagem do prazo de solução de hardware/software.

3.5.10 - A empresa, na execução do contato, sem prejuízo das suas responsabilidades contratuais e legais, poderá utilizar a estrutura técnica e operacional do fabricante do equipamento ou subcontratar uma assistência técnica na Região da Grande Vitória, ES, exclusivamente para cumprir o atendimento e suporte de hardware e software;

3.5.11 - Todos os equipamentos deverão ser novos e de primeiro uso e estar na linha de produção atual do FABRICANTE. Não serão aceitos componentes, partes e peças recondicionados, usados ou que não sejam comprovadamente, originais.

3.5.12 - Visando ampliar a proteção dos dados da instituição, em caso de falha ou defeito de disco(s) da solução, a CONTRATADA deverá realizar a substituição, mantendo, sem custos adicionais, o(s) disco(s) substituído(s) na posse da CONTRATANTE.

4. IDENTIFICAÇÃO E COMPARAÇÃO DAS SOLUÇÕES ADERENTES AOS REQUISITOS

4.1. Solução Única – Aquisição de Solução de Segurança contra Ataques Cibernéticos e Ransomware

Descrição da Solução: Aquisição de solução composta por 01 (um) sistema de armazenamento/proteção de dados em disco DELL DATA DOMAIN, 02 (dois) servidores do Tipo Rack, 02 (dois) switches de rede e os softwares DELL CYBER RECOVERY e CYBER SENSE.

Fornecedor da Solução: Empresas do Mercado.

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

Orçamento da Solução: Após consultas realizadas estima-se o valor da solução em **R$ 1.000.000 (Um milhão de reais).**

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

Aquisição de Solução de Segurança contra Ataques Cibernéticos e Ransomware

5.2 - Justificativa/Motivação da Escolha

Trata-se de aquisição de solução composta de hardware e software para aumentar a segurança contra Ataques Cibernéticos e Ransomware, conforme justificativa constante no item 1.2, visando atender a demanda descrita no item 5.4 deste ETP.

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 atualmente uma solução de Backup do fabricante DELL, modelo IDPA DP 4400. Esta solução armazena as cópias de segurança em um Appliance de Backup (equipamento de armazenamento de dados que acumula o software de backup e os componentes de hardware em um único dispositivo). Mesmo possuindo diversos mecanismos de segurança, como esta solução está instalada na mesma rede lógica dos clusters de servidores, ela também está *"ascessível*", e portanto vulnerável, a um ataque cibernético que consiga invadir a rede de computadores do TRE-ES. Para que possamos ampliar os mecanimos de segurança existentes, possuímos uma demanda para manter uma cópia dos servidores de rede de produção armazenados em ambiente seguro e isolado logicamente da rede local do TRE-ES, de forma análoga a um cofre, utilizando software de análise que monitore e indique a não existência de ransomware oculto e outras ameaças nos dados copiados.

Para que possamos atender essa demanda é necessário adquirir uma solução de segurança contra ataques cibernéticos que se integre ao ambiente de backup atual do TRE-ES e possa receber os dados, de maneira nativa, do equipamento de backup DELL IDPA DP4400 com vistas a não impactar nas operações do datacenter. Esta solução deve portanto ser obrigatoriamente da fabricante DELL e deve contemplar todos os componentes necessários ao seu pleno funcionamento. A **Solução de Segurança contra Ataques Cibernéticos e Ransomware** especificada atende os requisitos de segurança necessários e armazenará cópias de todos os servidores de produção em um ambiente resiliente, controlado e isolado logicamente da rede local do TRE-ES, possibilitando a recuperação de dados íntegros para o ambiente de produção em caso de ataques cibernéticos.

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:

- Atraso no Trâmite Processual;
- Não cumprimento do prazo de disponibilização dos equipamentos pela contratada;
- Indisponibilidade Orçamentária.

8 - RELAÇÃO DOS RISCOS E AÇÕES DE MITIGAÇÃO

RISCO 1	**ATRASO NO TRÂMITE PROCESSUAL**	
Probabilidade (Alta, média ou baixa)	**Baixa**	
	Efeito (Dano)	***Impacto**
1	Atraso disponibilização da solução de segurança impossibilitando a recuperação rápida dos dados em caso de um ataque cibernético bem sucedido.	**Alto**
	Ações de Mitigação e Contingência	**Responsável**
1	Consultar empresas do ramo sobre a adequação das especificações técnicas.	Integrante Técnico
2	Armazenar cópias dos dados em fitas LTO em cofre seguro.	SRCD/CIS/STI
3	Acompanhar todo o trâmite processual.	Equipe gestora

***Impacto (Baixo, Médio ou Alto)**

RISCO 2	**NÃO CUMPRIMENTO DO PRAZO DE DISPONIBILIZAÇÃO DOS EQUIPAMENTOS PELA CONTRATADA**	
Probabilidade (Alta, média ou baixa)	**Baixa**	
	Efeito (Dano)	***Impacto**
1	Atraso disponibilização da solução de segurança impossibilitando a recuperação rápida dos dados em caso de um ataque cibernético bem sucedido.	**Alto**
	Ações de Mitigação e Contingência	**Responsável**
1	Consultar empresas do ramo sobre adequação do prazo de entrega dos equipamentos.	Equipe gestora
2	Armazenar cópias dos dados em fitas LTO em cofre seguro	SRCD/CIS/STI
3	Acompanhar rigorosamente junto a empresa o andamento da operação de entrega.	Equipe gestora

***Impacto (Baixo, Médio ou Alto)**

RISCO 3	**INDISPONIBILIDADE ORÇAMENTÁRIA**	
Probabilidade (Alta, média ou baixa)	**Média**	
	Efeito (Dano)	***Impacto**
1	Não efetivação da aquisição da solução de segurança, impossibilitando a recuperação rápida dos dados em caso de um ataque cibernético bem sucedido.	**Alto**
	Ações de Mitigação e Contingência	**Responsável**
1	Estudar forma de se manter cópias de segurança travadas (Lock Snapshot) dos servidores de produção no atual appliance de backup.	SRCD/CIS/STI
2	Armazenar cópias dos dados em fitas LTO em cofre seguro.	SRCD/CIS/STI

***Impacto (Baixo, Médio ou Alto)**

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO

9. RECURSOS MATERIAIS E HUMANOS

Os recursos materiais e humanos necessários a esta contratação já estão disponíveis. Os técnicos da Seção de Redes e Comunicação de Dados serão os responsáveis por acompanhar a instalação, atestar os serviços e gerir os equipamentos.

10. DESCONTINUIDADE DO FORNECIMENTO

Não se aplica. Aquisição de solução 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: José Adriani Brunelli Desteffani (substituto: Carlos Alberto da Rocha Pádua Filho)

Vitória, 31 de maio de 2021.

Documento assinado eletronicamente por **MARCOS VENTUROTT FERREIRA**, **Integrante Administrativo**, em 24/06/2021, às 16:13, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUCAS RIBEIRO CARLIN**, **Técnico Judiciário**, em 24/06/2021, às 17:31, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ROMMEL BAIA SILVA**, **Chefe de Seção**, em 24/06/2021, às 17:33, 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 **0573027** e o código CRC **49DE5C30**.

0003216-62.2021.6.08.8000 0573027v67