



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

TERMO DE REFERÊNCIA (TIC) Nº - STIC 09/2023 V2 - TRE-ES/PRE/DG/STI/CIS/SGIR

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

SUMÁRIO

1. Caracterização do Objeto.
2. Fundamentação da Contratação.
3. Estratégia da Contratação.
4. Definição das Responsabilidades do Contratante.
5. Definição das Responsabilidades da Contratada.
6. Modelo de Execução do Contrato.
7. Modelo de Gestão do Contrato.

QUADRO INFORMATIVO

OBJETO:	Licenciamento com suporte técnico e direito de atualização (no modelo de subscrição) para solução de Gestão de Vulnerabilidades dos Ativos de Tecnologia da Informação utilizada pelo TRE-ES.
CATMAT/CATSER:	27502
QUANTITATIVOS:	1 Solução licenciada para 500 endereços IP's
CARACTERÍSTICAS:	Nome do Produto: Tenable.sc Continuous View Part Numbers - TSCCV-M e TSCCV-STNDC-M Deve permitir suporte técnico e direito de atualização do software e da base de vulnerabilidades por 60 meses;

1. CARACTERIZAÇÃO DO OBJETO

1.1. DEFINIÇÃO DO OBJETO

Licenciamento com suporte técnico e direito de atualização (no modelo de subscrição) para solução de Gestão de Vulnerabilidades dos Ativos de Tecnologia da Informação utilizada pelo TRE-ES.

1.2. REQUISITOS DA CONTRATAÇÃO

O contratação em questão deve atender os seguintes requisitos técnicos mínimos:

- Fornecer suporte técnico e direito de atualização de software para a solução de Gestão de Vulnerabilidades **Tenable.sc Continuous View** on premise no modelo de subscrição por 60 meses;
- A contratada deve disponibilizar um canal (0800 ou número similar gratuito ou site da contratada/fabricante) para abertura de chamados técnicos de suporte;
- Part Numbers do software- TSCCV-M e TSCCV-STNDC-M;
- No ato da abertura do chamado técnico, a contratada disponibilizará um número identificador do chamado que permita acompanhar o andamento da solicitação;
- O atendimento inicial do chamado de suporte deve ocorrer em no máximo 2 horas;
- O licenciamento deve ser vinculado à conta do TRE-ES (**Customer ID = 889020**) no portal da fabricante Tenable (<https://community.tenable.com/>);
- O licenciamento deve ser vinculado ao hostname TRE-ES-37-2020;
- A solução deve ser licenciada para 500 endereços IP's;

1.3. QUANTIFICAÇÃO OU ESTIMATIVA PRÉVIA

ITEM	QUANT	CLASSIFICAÇÃO	CÓDIGO *
1	01 UN	Custeio	CATSER 27502

(*) Em caso de divergência entre as especificações do objeto descritas no CATMAT, CATSER e as especificações constantes neste termo de referência, prevalecerão as últimas.

1.4. ESTIMATIVA DE PREÇO

Item	Valor Total do Item (R\$)
01	295.406,00

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. JUSTIFICATIVA DA NECESSIDADE E RESULTADOS

A gestão de vulnerabilidades é um processo que se preocupa com a descoberta e remediação de vulnerabilidades que podem estar presentes nos sistemas de informação. Uma vulnerabilidade pode surgir pela utilização de uma versão comprometida de um software ou por uma configuração inadequada de uma aplicação. Essa vulnerabilidade pode ser explorada por um atacante para prejudicar a disponibilidade, integridade e confidencialidade dos ativos de informação. Existem inúmeras ações maliciosas que podem explorar um vasto número vulnerabilidades existentes. Dentre elas podemos citar:

- Utilização de usuários e senhas padrões: A maioria de aplicações possuem usuários e senhas padrões, de conhecimento público, que caso não sejam alteradas ou desabilitadas podem ser utilizadas por invasores para acessar os sistemas e obter informações importantes ou sigilosas;

- Problemas de criptografia: Ocorre quando aplicações ou sites utilizam algoritmos de criptografia "fracos" que possibilitem ao invasor quebrar a chave e obter dados sensíveis que podem ser utilizados para obter acesso a servidores, banco de dados, sistemas essenciais, etc.

- CRLF Injection: Ocorre quando um invasor pode injetar uma sequência CRLF - "Carriage Return (Retorno de carro)" e "Line Field (Avanço de linha)" - em um fluxo HTTP. Ao introduzir esta injeção de CRLF inesperada, o invasor é capaz de explorar vulnerabilidades de CRLF de forma mal-intencionada para manipular as funções do aplicativo da web.

- Cross-site Scripting (XSS): Acontece quando um invasor explora uma área de um site que possui conteúdos dinâmicos. O invasor consegue rodar seu código dentro do site da vítima, causando o roubo de contas de usuários, controle do navegador da vítima, e muito mais. Esse problema é comum em formulários de contato que permitem a inserção de caracteres utilizados em linguagens de programação como pontos de interrogação ou barras.

- Acesso a diretórios restritos: Ocorre quando o invasor consegue se aproveitar de sites desprotegidos, conseguindo acesso a um grande número de arquivos de sistema, tendo acesso a nome de usuários, senhas, documentos importantes e até mesmo o código fonte do site/aplicativo.

- SQL Injection: Ocorre quando o invasor se aproveita de falhas em sistemas que interagem com bases de dados através de comandos SQL, onde o atacante consegue inserir uma instrução SQL personalizada e indevida dentro de uma consulta (SQL query) através da entradas de dados de uma aplicação, como formulários ou páginas de uma aplicação.

- Varredura em redes (*Scan*): Varredura em redes, ou *scan*, é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

- Interceptação de tráfego (*Sniffing*): Interceptação de tráfego, ou *sniffing*, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*.

- Força bruta (*Brute force*): Um ataque de força bruta, ou *brute force*, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar *sites*, computadores e serviços em nome e com os mesmos privilégios deste usuário.

- Negação de serviço (DoS e DDoS): Negação de serviço, ou DoS (*Denial of Service*), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (*Distributed Denial of Service*). O objetivo destes ataques não é invadir e nem coletar informações, mas sim exaurir recursos e causar indisponibilidades ao alvo.

Devido à complexidade e quantidade de ativos de informação utilizados no nosso ambiente de TIC, o processo de gestão de vulnerabilidades necessita ser suportado por uma solução de gestão de vulnerabilidades.

Em 2020 um grupo da Justiça Eleitoral, formado pelo TSE e vários Tribunais Regionais, adquiriu a solução denominada TenableSC para suprir essa demanda, que é essencial para a Segurança da Informação no âmbito da Justiça Eleitoral. O contrato atual, que permite a atualização e o suporte da solução tem vigência até 21 de fevereiro de 2024 e se a subscrição não for renovada, não conseguiremos mais atualizar a base de vulnerabilidades e o software que compõe a solução, perderíamos o direito de suporte, e não seria possível atingir os objetivos (resultados) esperados:

- Manter a base de vulnerabilidades atualizada para permitir a identificação e priorização de tratamento de vulnerabilidades nos ativos de TIC (roteadores, switches, estações de trabalho, hosts de virtualização, bancos de dados, máquinas virtuais, sistemas operacionais, servidores de aplicação, etc) do TRE-ES;

- Reduzir o nível de risco através da redução da probabilidade de ameaças explorarem vulnerabilidades de nossos ativos.

2.2. ALINHAMENTO ESTRATÉGICO

A solução está alinhada com o [Planejamento Estratégico Institucional](#) no MACRODESAFIO 09 - Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados.

A solução também está alinhada ao PDTIC nos seguintes pontos:

- Princípio 6 - Garantia da segurança em TIC.
- Diretriz 3 - Garantir a disponibilidade, integridade e confidencialidade da informação.

2.3. REFERÊNCIA AOS ESTUDOS TÉCNICOS PRELIMINARES

Estudos Técnicos preliminares constantes do processo SEI 0001592-07.2023.6.08.8000.

2.4. RELAÇÃO ENTRE A DEMANDA PREVISTA E A STIC A SER CONTRATADA

Hoje o TRE-ES possui uma solução para Gestão de Vulnerabilidades cujo contrato de subscrição que permite atualização e suporte expira em 21 de fevereiro de 2024. Para que possamos continuar a executar as análises de vulnerabilidades nos ativos TIC e necessário a aquisição de uma nova subscrição da solução atual a partir da data de 22 de fevereiro de 2024.

2.5. JUSTIFICATIVA DA STIC ESCOLHIDA

A solução indicada foi escolhida por ser a única alternativa que atende às necessidades desta contratação.

3. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

3.1. FORMA DE PARCELAMENTO E ADJUDICAÇÃO DO OBJETO

O objeto da licitação será adjudicado ao licitante que ofertar o MENOR PREÇO TOTAL POR ITEM. Não haverá parcelamento do objeto.

3.2. MODALIDADE E TIPO DE LICITAÇÃO

A modalidade de licitação indicada para a contratação em tela é o de **menor preço total por item** e para a habilitação, o licitante deverá:

- 1 – estar inscrito no SICAF, com a documentação obrigatória regularizada;
- 2 – apresentar prova de regularidade com a **Fazenda Municipal** da sede ou do domicílio da empresa licitante;
- 3 – apresentar prova de regularidade com a Justiça do Trabalho;
- 4 – preencher, no momento do envio da proposta comercial, no sistema Compras.gov, a seguinte declaração:

a) De que cumpre o disposto no inciso XXXIII do art. 7º da Constituição da República Federativa do Brasil de 1988, conforme prescreve o inciso V do art. 27 da Lei nº. 8.666/1993.

- 5 – apresentar qualificação técnica;

6 – apresentar qualificação econômico-financeira.

3.3. MARGEM DE PREFERÊNCIA

Não se aplica.

3.4. ADEQUAÇÃO ORÇAMENTÁRIA

DISPONIBILIDADE	Há disponibilidade orçamentária
PROGRAMA DE TRABALHO	02.122.0033.20GP.0032 - Julgamento de Causas e Gestão Administrativa na Justiça Eleitoral no Estado do Espírito Santo
PLANO ORÇAMENTÁRIO	0001 - Julgamento de Causas e Gestão Administrativa
NATUREZA DA DESPESA:	339040 – Serviços Tecnologia da Informação e Comunicação - PJ
SUBITEM DA DESPESA:	07 – Manutenção Corretiva/adaptativa e Sustentação de Softwares
VALOR CONSIDERADO	R\$ 295.406,00 (conforme despacho SECOM 1024664)
PLANO INTERNO:	TIC MANSOF

3.5. VIGÊNCIA DA CONTRATAÇÃO

A contratação deve ter vigência de **60 meses** a partir do dia 22 de fevereiro de 2024.

3.6. QUALIFICAÇÃO TÉCNICA E ECONÔMICO-FINANCEIRA

3.6.1 - Para fins de qualificação técnica a licitante deverá apresentar:

- Atestado(s) e/ou declaração(ões) de capacidade técnica, expedido(s) por pessoa jurídica de direito público ou privado, que comprove(m) ter fornecido licenciamento para a solução de Gestão de Vulnerabilidades **Tenable.sc**, licenciada para no mínimo 250 endereços IP's.

3.6.2 - Para fins de qualificação econômico-financeiro a licitante deverá apresentar:

- Certidão Negativa de Feitos de Falência, Recuperação Judicial ou Recuperação Extrajudicial.

4. DEFINIÇÃO DAS RESPONSABILIDADES DO CONTRATANTE

- Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita;
- Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis;
- Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da STIC.

5. DEFINIÇÃO DAS RESPONSABILIDADES DA CONTRATADA

- Proceder a entrega do objeto em conformidade com as especificações constantes neste Termo de Referência;
- Enviar a documentação que comprova a contratação do suporte técnico para o e-mail rede@tre-es.jus.br;
- Informar os dados do seu domicílio bancário (banco, agência e conta) para o correspondente pagamento;
- Manter as certidões de regularidade fiscal e trabalhista atualizadas junto aos órgãos respectivos, durante toda a execução deste instrumento.
- Cumprir todas as demais obrigações constantes deste Termo de Referência.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. FIXAÇÃO DAS ROTINAS DE EXECUÇÃO DO CONTRATO

6.1.1 - Entrega e Aceite

A entrega dar-se-á com o recebimento da documentação que comprove a contratação do suporte técnico. O Aceite Definitivo ocorrerá após a conferência no site do fabricante se o suporte contratado está aplicado à conta do TRE-ES (**Customer ID = 889020**) no portal da fabricante Tenable, com vigência de **60 meses**.

6.1.2 - Prazos e local de entrega

A documentação que comprova a contratação do suporte técnico deve ser encaminhada por meio digital para o email: rede@tre-es.jus.br, no prazo 30 (trinta) dias, contados a partir do recebimento da nota de empenho ou da assinatura do instrumento contratual.

6.1.3 - Recebimento Provisório e Definitivo da Solução

O recebimento provisório dar-se-á com o recebimento por e-mail da documentação comprobatória da contratação do suporte. O recebimento definitivo ocorrerá após a conferência no site do fabricante se o suporte contratado está aplicado à conta do TRE-ES (**Customer ID = 889020**) no portal da fabricante Tenable, com vigência de 60 meses.

O recebimento definitivo dar-se-á em um prazo máximo de 10 dias úteis após o recebimento provisório, com o atesto do documento fiscal.

6.2. DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI Nº 13.709/2018)

- É vedada às partes a utilização de todo e qualquer dado pessoal, repassado em decorrência da execução contratual, para finalidade distinta da contida no objeto da contratação, sob pena de responsabilização administrativa, civil e criminal;
- Para fins de execução do objeto contratado e de cumprimento de obrigação legal ou regulatória, o Contratante poderá proceder ao tratamento dos dados pessoais dos representantes legais da Contratada, inclusive para publicação nos portais de Transparência do Contratante;

6.3. FORMA DE PAGAMENTO

O pagamento será realizado em uma única parcela, correspondente ao valor contratado, mediante depósito bancário na conta corrente da contratada, até o 5º (quinto) dia útil após a apresentação de documento fiscal, devidamente atestado pelo setor competente deste Tribunal, desde que não haja fator impeditivo provocado pela contratada.

6.4. MODELOS DE TERMOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO

Não se aplica à presente contratação.

7. MODELO DE GESTÃO DO CONTRATO

7.1. FIXAÇÃO DOS CRITÉRIOS DE ACEITAÇÃO

- Devem ser respeitados os prazos de entrega previstos no subitem 6.1.2;
- Devem atender completamente as especificações técnicas deste Termo de Referência;

7.2. INDICAÇÃO DOS PROCEDIMENTOS MÍNIMOS DE TESTE E INSPEÇÃO

Não existem procedimentos mínimos de teste e inspeção. Devem ser seguidos somente os critérios do item 6.1.3, referente aos procedimentos para recebimento provisório e definitivo.

7.3. RETENÇÕES OU GLOSAS

Não se aplica à presente contratação.

7.4. SANÇÕES ADMINISTRATIVAS

Descumprimento	Percentual	Limite	Percentual total	Base de incidência
Atraso no início da execução do contrato	0,5% por dia	20 dias	10%	Valor do contrato
Prazo excepcional no início execução do contrato	0,5% por dia	20 dias	10%	Valor do contrato
Atraso no atendimento inicial de chamado de suporte	0,4% por hora	75 horas	30%	Valor do contrato
Inexecução total ou parcial	-----	-----	30%	Valor do contrato
Qualquer outra obrigação (por ocorrência)	-----	-----	1%	Valor do contrato

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 Pádua Filho)

Vitória, 02 de outubro de 2023.



Documento assinado eletronicamente por **MARCOS VENTUROT FERRERIRA**, Integrante Administrativo, em 03/10/2023, às 12:47, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **LUCAS RIBEIRO CARLIN**, Integrante Técnico, em 03/10/2023, às 14:22, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ROMMEL BAI SILV**, Integrante Demandante, em 03/10/2023, às 14:22, 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 **1033874** e o código CRC **AE0DC357**.