TRIBUNAL SUPERIOR ELEITORAL

SEÇÃO DE SUPORTE A APLICAÇÕES

CONTRATAÇÃO DE TIC

DOCUMENTO DE OFICIALIZAÇÃO DE DEMANDA - DOD

Solução de TIC a ser contratada: Trata-se de Registro de Preços para contratação de empresa para fornecimento de Solução de Gestão da Segurança da Informação (**SIEM -** Security Information Management) que tem capacidade para coletar e correlacionar logs para análise posterior. Este projeto inclui o fornecimento de software, serviços de instalação, configuração, suporte técnico, repasse de conhecimento e operação assistida da ferramenta para o Tribunal Superior Eleitoral.

IDENTIFICAÇÃO DA ÁREA REQUISITANTE	
Unidade/Setor:	SESAP - SESOP / COINF / STI
Responsável:	Ivanildo Ferreira Gomes / Marcelo Carneiro

MOTIVAÇÃO E JUSTIFICATIVA DA CONTRATAÇÃO

SIEM significa *Security Information and Event Management*. As ferramentas SIEM geralmente fornecem dois resultados principais: relatórios e alertas. Os relatórios agregam e exibem incidentes e eventos relacionados à segurança, como atividades maliciosas e tentativas de *login* malsucedidas. Os alertas serão acionados se o mecanismo de análise da ferramenta detectar atividades que violam um conjunto de regras, sinalizando, consequentemente, um problema de segurança.

Os maiores benefícios que as ferramentas SIEM oferecem são identificação aprimorada e tempo de resposta por meio da agregação e normalização de dados. Além disso, e tão importante, eles aceleram a detecção de ameaças, alertas de segurança e atendimento aos requisitos de conformidade.

Essa ferramenta tem a capacidade de coletar e normalizar logs que são testados e correlacionados a um conjunto de regras que, se acionadas, criam eventos para análise.

Como o próprio nome sugere, a principal **função** de um **SIEM** é o gerenciamento de eventos. A solução **SIEM**, uma vez implementada de forma completa e eficaz, terá visibilidade completa sobre a rede de uma organização. Isso ajuda a organização a encontrar incidentes ou tentativas de hacking quase em tempo real.

Assim, ela consegue coletar os dados de toda infraestrutura de TI, monitorando os eventos de segurança em tempo real. Esses dados são correlacionados, permitindo uma análise mais complexa.

RESULTADOS A SEREM ALCANÇADOS

Esta contratação visa:

- Prover uma identificação acurada dos eventos do ambiente de TI;
- Detecção de ameaças em menor tempo;
- Visualização centralizada de logs e aplicativos, infraestrutura e rede.
- Fornecimento de relatórios e alertas em tempo real e com precisão.
- Compatibilidade com padrões internacionais (ISO 27000, requisitos de auditoria)

PROJETOS RELACIONADOS

Existe algum projeto em andamento relacionado a esta contratação?

☐ **Sim - Qual?**

☒ **Não**

ALINHAMENTO ESTRATÉGICO

A contratação está alinhada a algum objetivo do planejamento estratégico institucional do Tribunal?

☒ **Sim - Qual?**

Garantir a confiança na Justiça Eleitoral.

Aprimorar continuamente a segurança do processo eleitoral.

Garantir a infraestrutura de Tecnologia da Informação.

☐ **Não**

FONTE DE RECURSOS
O orçamento necessário ao projeto está na previsão orçamentária da COINF/STI.
VINCULAÇÃO AO PDTI
A contratação atende a alguma ação do Plano Diretor de TI?
[X] **Sim - Qual?**
Atendimento ao constante no Art. 1º da Resolução 396 CN (1676014), Parágrafo Único; Relatório - Estratégia Nacional de Cibersegurança v2 (1759818), pág. 14, na qual consta a necessidade de aquisição de ferramentas automatizadas para governança e continuidade do negócio, Correlacionador de Logs. Esta aquisição está em conformidade às iniciativas IN07.04 (nivelar infraestrutura à resolução 90 do CNJ), IN07.E3 (prover a modernização dos serviços e recursos de TIC para adequação à dinâmica do negócio) do Plano Diretor de Tecnologia da Informação (PDTI), além de atender ao objetivo estratégico 7 (garantir a estrutura de TIC apropriada às atividades judiciais, eleitorais e administrativas).
[ ] **Não**

EQUIPE MULTIDISCIPLINAR (se for o caso)	
Integrante:	**Unidade/Setor:**
ENCAMINHAMENTO	

IVANILDO FERREIRA GOMES
CHEFE DE SEÇÃO

Documento assinado eletronicamente em **28/09/2021, às 17:46**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

MARCELO CARNEIRO RODRIGUES
CHEFE DE SEÇÃO

Documento assinado eletronicamente em **28/09/2021, às 17:55**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

Tribunal Superior Eleitoral

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1794609&crc=5F7BEC18, informando, caso não preenchido, o código verificador **1794609** e o código CRC **5F7BEC18**.