



TRIBUNAL REGIONAL ELEITORAL DO PARANÁ

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

OBJETO	
Descrição	<p>Contratação de empresa especializada para o fornecimento de solução de Segurança Cibernética, visando o aumento da proteção do ambiente de Rede do Tribunal, sendo composta pelos seguintes itens:</p> <ol style="list-style-type: none">1. Solução de Firewall Camada 7 para proteção Aplicações WEB (WAF - Web Application Firewall);2. Suporte técnico e serviços especializados de implantação.3. Treinamento técnico .
Setor demandante	SSC
Servidor responsável pela oficialização da demanda	<i>Lucas Barke Bruzon</i>

INDICAÇÃO DA DEMANDA NO PLANO ANUAL DE CONTRATAÇÃO
<i>Demanda: 22PO314</i>



TRIBUNAL REGIONAL ELEITORAL DO PARANÁ

MOTIVAÇÃO DA CONTRATAÇÃO E DEMONSTRATIVO DOS RESULTADOS QUE SERÃO ALCANÇADOS (considerando o Planejamento Estratégico)

Justifica-se esta contratação pela necessidade de prestação continuada dos serviços de TIC deste egrégio Tribunal, por meio do aumento da maturidade dos serviços de segurança da informação, mas sobretudo da ATUALIZAÇÃO de tecnologia, capazes de regular o tráfego de rede no TRE-PR, detectar e impedir a transmissão e recepção de tráfego nocivo, identificar, prevenir e bloquear tentativas de intrusão, monitorar e regular as solicitações feitas a aplicações web; fazer a gestão das vulnerabilidades encontradas em sistemas e recursos de TI; monitorar e mitigar eventos que possam afetar a segurança computacional do órgão.

Observaram-se ainda avanços na tecnologia utilizada para explorar vulnerabilidades, notadamente nos eventos recentemente noticiados associados ao aumento de ataques cibernéticos nos órgãos públicos. Destes pode-se salientar os ataques de “dia zero” (Zero Day), nome utilizado na indústria de segurança da informação para ataques utilizados por meio da exploração de uma vulnerabilidade anteriormente desconhecida que afeta de maneira adversa programas, dados, computadores e redes. Códigos maliciosos que exploram tais vulnerabilidades não podem ser detectados pelo método tradicional de assinatura utilizado pela solução ora em uso, ou ainda por outras proteções utilizadas pelo Regional como, por exemplo, Firewall NG e Antivírus. Desta forma, são necessárias novas formas de detecção, como o uso de métodos heurísticos de análise, emulação de código e virtualização, visando mitigar tais ameaças.

Há ainda que se destacar as medidas regulatórias estabelecidas nos últimos anos que necessitam de ferramentas atuais e adequadas para garantir conformidade. Como é o caso da GDPR e a mais recente LGPD (LEI Nº 13.709, DE 14 DE AGOSTO DE 2018), que conhecidamente soluções atuais de segurança precisam estar em aderência.

É justificada, portanto, a modernização do ambiente de Segurança de Rede por meio da aludida solução de segurança, com a adição de novas funcionalidades em face das novas tecnologias que trarão benefícios imediatos a este Egrégio Tribunal, tais como: ferramentas de conformidade regulatória, elevar a capacidade de prevenção de ataques, permitir o monitoramento e avaliação das vulnerabilidades a que os ativos de TI estão sujeitos, possibilitando ainda o bloqueio de ataques antes que estes ocorram; acrescentar uma camada de segurança ao ambiente de sistema a aplicações disponibilizadas em servidores web, mesmo criptografadas; prover a análise avançada de ameaças evasivas e persistentes e análise de tráfego de rede dentro do ambiente de servidores, não apenas no perímetro com as redes externas e com a internet.

Deste modo, a aquisição de uma solução de WAF (Web Application Firewall) se deve à necessidade de proteção do perímetro intranet das aplicações do TRE-PR, tal como a toda e qualquer aplicação com acesso público na Internet. Trata-se, portanto, de recurso capaz de evitar e mitigar ataques de hackers e botnets. A solução também auxiliará na melhoria de gestão e desempenho de acesso aos sites protegidos. Neste contexto, o Manual de Prevenção e Mitigação de Ameaças Cibernéticas e



TRIBUNAL REGIONAL ELEITORAL DO PARANÁ

Confiança Digital (ref. Portaria Nº CNJ 162 de 10/06/2021), disciplina as seguintes ações:

- *Da proteção: o acesso lógico aos ativos seja gerenciado e protegido, possuindo-se mecanismos de segurança de perímetro, como firewalls, Intrusion Prevention Systems (IPS) e **Web Application Firewall (WAF) para restrição de acessos não autorizados**; (grifo nosso)*

Por fim, a Estratégia Nacional de Cibersegurança - 2021 a 2024 (TSE e TREs) no Eixo Estruturante E3, não obstante outros eixos estruturantes que devem ser contemplados pela administração na estratégia de Cibersegurança, salienta da necessidade dos Regionais envidar esforços na contratação de Ferramentas Automatizadas. Dentre as ferramentas indicadas com metas de contratação de Médio Prazo (até o fim de 2022), destaca-se a Ferramentas de Segurança de Borda: WAF (por exemplo, F5, Mod_Security).

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Líder do Planejamento	Lucas Barke Bruzon
Integrante Técnico	
Integrante Administrativo	

QUANTIDADE DE SERVIÇO A SER CONTRATADA

Quantitativo	
Web Application Firewall	2
Suporte	1
Treinamento	6



TRIBUNAL REGIONAL ELEITORAL DO PARANÁ

DATA DESEJADA PARA A DISPONIBILIDADE DO BEM / SERVIÇO

30/08/2022

GRAU DE PRIORIDADE DA DEMANDA

Essencial

VINCULAÇÃO COM OUTRA CONTRATAÇÃO

Demanda faz parte da Arquitetura Nacional de Cibersegurança da Justiça Eleitoral.

OUTROS

Objeto da contratação necessário conforme Estratégia Nacional de Cibersegurança - 2021 a 2024 (TSE e TREs), Eixo Estruturante E3: Ferramentas Automatizadas item ID F05 S / WAF - WEB APP. FIREWALL - INTRANET, Resolução Nº 396 de 07/06/2021, Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) Portaria Nº 162 de 10/06/2021 - Protocolos e Manuais (ENSEC-PJ)

Curitiba, 22 de Abril de 2022

Chefe da Seção Demandante: Lucas Barke Bruzon

Secretário Demandante: Gilmar José Fernandes de Deus