DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

SERAU fls. 2

1- IDENTIFICAÇÃO DA UNIDADE DEMANDANTE DE SOLUÇÃO DE TI (preenchimento a cargo da Unidade demandante)
Unidade Organizacional: DGTEC-DEINF-DIRED.
Identificação da Demanda: Contratação de empresa especializada para atualização, manutenção e suporte da solução de serviços de segurança para o ambiente de segurança da rede corporativa, englobando licenciamento, suporte e banco de horas para a utilização do filtro e analisador de conteúdo web e do sistema de prevenção de intrusão de perímetro (IPS).
Responsável pela Demanda: Marcos Stallone Santos – Diretor da Divisão de Redes
Fonte de Recurso: Fundo Especial – **Nº da Ação do PAG:**
2- ALINHAMENTO ESTRATÉGICO
Objetivo Estratégico da Unidade Demandante: P1 – Garantir a Integridade e a disponibilidade de todos os serviços de TI do Poder Judiciário.
Iniciativas/Necessidades Elencadas no Planejamento Estratégico de TI (PETI): CL1 - Assegurar a qualidade, disponibilidade e eficácia dos serviços de TI com foco na satisfação do cliente. R1 – Manter a infraestrutura de TI segura, apropriada e otimizada.
3- MOTIVAÇÃO/JUSTIFICATIVA
• O contrato atual de suporte a solução de segurança McAfee chega ao seu final em 19/10/2017, completando os 60 meses obrigando a área técnica a fazer nova contratação. • Mensalmente, nosso Sistema de Prevenção de Intrusão (IPS), "Network Security Platform (NSP)", bloqueia, mensalmente, mais de 60 mil ataques originados de vários locais externos diferentes, considerados de alto e médio risco (vide Anexo I). • Caso não exista essa barreira de proteção, o risco de acesso não autorizado e adulteração de dados armazenados em nossos servidores é muito alto, além da possível indisponibilidade dos serviços oferecidos por este Tribunal. • Segue em anexo, tabela de ataques detectados e bloqueados no acesso de usuários externos aos sistemas disponibilizados pelo TJRJ e de conexões originadas pelos usuários internos aos recursos disponibilizados na Internet. Conexões bloqueadas no mês de maio. • Os acessos à Internet originados em nossa rede interna são analisados, acelerados ("cacheados"), filtrados (na existência de download de arquivos com código malicioso) e bloqueados (na detecção de páginas com código malicioso) pelo proxy de acesso à Internet: "Web Gateway". São efetuados, em média, 200 mil bloqueios mensais no acesso a sites, categorizados pelo fabricante como maliciosos (vide Anexo I). • A filtragem é essencial para proteger nossos usuários da rede interna contra ameaças presentes na Internet e no bloqueio do acesso indevido a sites inapropriados.
4- ENCAMINHAMENTO À DGTEC
I - Indico como Integrante Demandante o servidor Marcos Stallone Santos – mat. 19816 – tel. 3133-1813 – e-mail: stallone@tjrj.jus.br. II - À DGTEC, para ciência e encaminhamento ao Comitê de Gestão de Tecnologia da Informação (CGTI). Rio de Janeiro, 27 de julho de 2017. Diretor-Geral da Unidade Demandante

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

SERAU fls. 3

5- ENCAMINHAMENTO AO COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO (CGTI)
(preenchimento a cargo da DGTEC)

I - Indico como Integrante Técnico o servidor Selmo Karacusanscy – mat. 32005 – tel. 3133-4070 – e-mail: selmokaracusanscy@tjrj.jus.br.

II - Ao Comitê de Gestão de Tecnologia da Informação (CGTI) para aprovação.

Rio de Janeiro, 27 de julho de 2017.

Diretor-Geral de Tecnologia da Informação

6- DECISÃO DO COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO (CGTI)

( ) Indefiro a solicitação, que não atende ao Plano de Contratação de STIC e/ou ao PAG.

Explicitação dos motivos: _____

(X) Aprovo o prosseguimento da contratação, considerando a relevância e a oportunidade em relação aos objetivos estratégicos e às necessidades da Unidade Demandante.

À Diretoria-Geral de Logística (DGLOG), para:

I- Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação quando da continuidade da contratação;

II- Constituir a Equipe de Planejamento da Contratação;

III- Dar prosseguimento ao Estudos Preliminares da Solução de TI.

Rio de Janeiro, 28 de julho de 2017.

Comitê Gestor de Tecnologia da Informação

7- PROVIDÊNCIAS DA DGLOG

I- Indico como Integrante Administrativo Marcia de Moura Ferreira, mat.: 01/8052, marciamoura@tjrj.jus.br (nome, matrícula, telefone e *e-mail*);

II- Expeça-se portaria de designação da equipe de planejamento da contratação, conforme indicações neste documento;

III- Ao Protocolo para autuação com retorno a esta DGLOG;

Rio de Janeiro, 02 de agosto de 2017.

Diretor-Geral de Logística

Chefe de Gabinete da DGLOG/TJRJ
Em substituição, conforme
Ato Executivo TJ nº 104/2017

Anexo I

Tabela de ataques detectados e bloqueados no acesso de usuários externos aos sistemas disponibilizados pelo TJRJ e de conexões originadas pelos usuários internos aos recursos disponibilizados na Internet. Quantidade de Conexões bloqueadas no mês de maio de 2017.

Top N Attacks			
#	Attack Name	Severity	Attack Count
1.	Too Many Outbound Rejected TCP Packets	Medium	23179
2.	MALWARE: File Mismatch Detected	Medium	11039
3.	HTTP: Overly Long POST URI in HTTP Request	Medium	7009
4.	HTTP: Microsoft Windows Shell CLSID File Extension Vulnerability	Medium	4312
5.	IP: Connection Limiting Rule Match	Medium	3301
6.	IPv4: TCP Session Hijacking Attempt Detected	Medium	2736
7.	HTTP: KeepAlive Request Detected	Medium	2467
8.	HTTP: Adobe Products PNG file Stack Buffer Overflow	Medium	2130
9.	HTTP: Microsoft Windows HTTP Services Integer Underflow Vulnerability	High	1225
10.	HTTP: Weblogic File Source Read	Medium	870
11.	DNS: ISC BIND RRSIG Record Response Assertion Failure Denial of Service	High	804
12.	P2P: BitTorrent Meta-Info Retrieving	Medium	644
13.	MSSQL: SQL Server Worm Slammer	High	629
14.	HTTP: Microsoft Internet Explorer Remote urlmon.dll Buffer Overflow	Medium	573
15.	HTTP: Mozilla Products Frame Comment Objects Manipulation Memory Corruption	Medium	541
16.	SMTP: Exim SPA Authentication Remote Buffer Overflow	High	352
17.	HTTP: Microsoft Edge Out-of-Bound Vulnerability (CVE-2017-0023)	High	290
18.	HTTP: Repeated Download Detected	Medium	239

Top N Attacks			
#	Attack Name	Severity	Attack Count
19.	HTTP: Acrobat Reader Memory Corruption Vulnerability(CVE-2016-6955)	High	172
20.	HTTP: Adobe Acrobat Memory Corruption Vulnerability(CVE-2016-0936)	High	157

Tabela de sites categorizados pelo Web Gateway, no mês de Mario, conforme o grau de risco do site acessado pelo usuário. As categorias *high risk* e *medium risk* são automaticamente bloqueadas:

Reputation	Número de Web Summary
■ Minimal Risk	12.118.548
■ Unverified	554.366
■ High Risk	124.405
■ Medium Risk	98.933
Total	12.896.252