|  |
| --- |
| Contratação de soluções de (1) segurança para ambientes virtualizados e (2) proteção contra ataques direcionados (contra ameaças avançadas persistentes) |

1. **Identificação da Demanda**

|  |  |  |
| --- | --- | --- |
| Demandante | E-mail | Ramal |
| Percival Barbosa Júnior | [percival.bjunior@tjpe.jus.br](mailto:percival.bjunior@tjpe.jus.br) | 3182-0689 |
|  | | |
| Diretoria | Gerência | Unidade |
| Assessoria de Governança – AGTIC | Núcleo de Segurança | NSI |

1. **Escopo da Demanda**
   1. Descrição da Demanda

|  |
| --- |
| * O TJPE vem nos últimos anos investindo pesadamente em soluções de informática que permitam uma melhor prestação dos serviços jurisdicionais. Estas soluções contemplam a disponibilização de novos sistemas e o emprego da infraestrutura necessária para suportá-los. Com o crescimento da infraestrutura e sua elevação para níveis mais sofisticados de soluções tecnológicas, haja vista o volume de atendimento e o desempenho exigido para isso, foi identificado pela SETIC que as soluções de segurança empregadas precisam acompanhar esta nova realidade. * Atualmente o TJPE já conta com contratos de soluções de segurança de perímetro de rede e soluções para as estações de trabalho dos magistrados e servidores. Entretanto, não existe qualquer solução adquirida para mitigar ativamente riscos específicos de segurança da informação nos ambientes de servidores, onde estão centralizadas as soluções que atendem as diversas unidades do TJPE. * Além da identificação e bloqueio de incidentes de segurança, é importante tratar as vulnerabilidades que possibilitam tais incidentes. Não existe atualmente nenhum contrato ativo, de serviço ou produto, no TJPE que forneça relatórios, gerencie, trate de forma automática e com baixo impacto a aplicação de correções nos ambientes de produção de sistemas críticos para o TJPE. * Uma outra lacuna existente em nossos ambientes é a ausência de ferramentas automatizadas de identificação de ameaças conhecidas ou desconhecidas que trabalhe no sentido de evitar ataques persistentes e ameaças do tipo “dia-zero”. * É preciso levar em consideração também que as soluções de segurança precisam de um bom nível de integração e o tempo de reação mais curto possível. Portanto, é importante para o cenário do TJPE que as soluções permitam a integração com ferramentas já existentes, mas que tratam da segurança em outro domínio (ex.: estações de trabalho, solução de spam, etc.), mitigando de os riscos de forma mais abrangente. A integração deve permitir também que eventuais vacinas e regras criadas dinamicamente possam ser propagadas pelas demais ferramentas integradas. * Tão importantes quanto eventuais incidentes de segurança oriundos do ambiente externo ao TJPE são os incidentes causados, de forma intencional ou não, dentro do ambiente do próprio Tribunal. Os riscos de tais incidentes podem ser mitigados por sistemas que gerenciam, monitoram e permitem a auditoria da configuração dos ambientes onde são executadas as aplicações críticas. |
|  |

* 1. Justificativa da Demanda

|  |
| --- |
| * Atualmente o TJPE, por meio da infraestrutura mantida pela SETIC, disponibiliza em torno de 30 instâncias do serviço PJe, cujo o atendimento se diversifica entre o público em geral e a integração com outros órgãos da Administração Pública que operam na Justiça Estadual. Estas três dezenas de nós de serviços foi alcançada em menos de 7 anos, o que mostra uma tendência de crescimento para o uso do PJe. Além do PJe outros serviços críticos, como SICASE, Malote Digital, Consulta Processual, etc. são de importância incontestável para a prestação dos serviços jurisdicionais. Portanto, como qualquer sistema crítico, precisam de soluções que tratem a segurança de maneira crítica, pois isto contribui para a mitigação de riscos e maiores níveis de disponibilidade e garantias de integridade dos dados e serviços. * A indisponibilidade dos serviços críticos de tecnologia pode acarretar prejuízos incomensuráveis para o TJPE, para advogados e, principalmente, para as partes que depositam no Tribunal a confiança para resolução de conflitos. Esta indisponibilidade pode variar de minutos a dias, ou até mesmo semanas, a depender da gravidade do incidente de segurança. * Além da possibilidade de indisponibilidade, incidentes de segurança podem acarretar a perda e o comprometimento da integridade das informações. Em situações como esta, por exemplo, é possível que haja o comprometimento de processos judiciais. Tais danos podem atingir um pequeno número de processos ou até mesmo todo o acervo. * O mercado atualmente já endereça estes problemas e fornece soluções em forma de ferramentas de segurança que podem ser dimensionadas e implementadas nos ambientes das mais diversas instituições para atender a estes requisitos. As funções que cobrem os problemas descritos no item 2.1 podem ser encontradas em diversas arquiteturas. As descrições mais gerais para as ferramentas que endereçam e fornecem soluções para os riscos descritos acima são, de forma geral, divididas em dois tipos, com suas respectivas denominações: (1) solução de segurança para ambientes virtualizados e (2) proteção contra ataques direcionados (contra ameaças avançadas persistentes). |

* 1. Benefícios da Demanda

|  |
| --- |
| * Considerando o exposto nos itens 2.1 e 2.2 o tipo de solução demandada neste documento, se implementada no ambiente do TJPE, pode propiciar vários benefícios. São exemplos: * Maior disponibilidade dos servidores por contarem com proteção contra ameaças cibernéticas (softwares maliciosos ou indivíduos mal-intencionados); * Maior integração entre ferramentas já existentes no âmbito do TJPE, propiciando reações mais amplas e rápidas contra ataques; * Aumento na capacidade prover um ambiente aderente às últimas atualizações da infraestrutura de software utilizada; * Redução dos riscos de perda e comprometimento da integridade de informações; * Redução de riscos para ameaças que possam tornar os servidores virtualizados do TJPE disseminadores de software malicioso; * Maior gerencia sobre aspectos de segurança dos servidores virtualizados do TJPE; * Redução dos riscos de computadores do TJPE servirem involuntariamente em redes de máquinas usadas para crimes digitais; * Redução dos riscos de vazamento de informações sigilosas ou sensíveis do TJPE; * Redução dos riscos de comprometimento de sistemas que atendem aos cidadãos, magistrados, servidores e colaboradores em geral; * Redução de riscos de incidência de ataques ainda não reconhecidos como ataques; * Redução de riscos de incidência de ataques direcionados; * Redução dos riscos de colaboradores terem prejuízos (profissionais, financeiros, materiais, etc.) resultantes de ações criminosas de origem eletrônica. |

1. **Vinculação Estratégica**

|  |  |
| --- | --- |
| Plano Estratégico do TJPE | |
|  | Programa de infraestrutura de Tecnologia da Informação e Comunicação |
|  |  |
|  |  |

|  |  |
| --- | --- |
| Planejamento Estratégico de TIC (PETIC) | |
|  | Promover a Segurança da Informação |
|  | Garantir Infraestrutura de TIC apropriada às atividades judiciais e administrativa |
|  |  |
| Plano Diretor de TIC (PDTIC) | |
|  |  |
|  |  |
|  |  |

1. **Relação com outros Projetos**

|  |  |  |
| --- | --- | --- |
| Projetos | |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
| **Área Demandante** | **Secretaria de TIC** |
|  |  |
| Percival Barbosa Júnior | Juliana Neiva de Gouvea Ribeiro |
| Matrícula: 185.866-1 | Matrícula: 183.825-3 |
|  |  |
| **Recife, 15 de agosto de 2017** | |

Contratação de soluções de (1) segurança para ambientes virtualizados e (2) proteção contra ataques direcionados (contra ameaças avançadas persistentes)

1. **Requisitos da Contratação**
   1. Especificação dos Bens

|  |
| --- |
| * Licenças:   + Licenças de **solução de segurança (incluindo monitoramento e auditoria) para ambientes virtualizados** para um total de 50 máquinas;   + Licenças de **solução de proteção contra ataques direcionados (contra ameaças avançadas persistentes)** para um total de tráfego de no mínimo 4 gigabytes. * Suporte:   + Contrato de suporte para a **solução de segurança (incluindo monitoramento e auditoria) para ambientes virtualizados;**   + Contrato de suporte para a **solução de proteção contra ataques direcionados (contra ameaças avançadas persistentes).** * Treinamento:   + Treinamento na **solução de segurança (incluindo monitoramento e auditoria) para ambientes virtualizados** para 15 participantes;   + Treinamento na **solução de proteção contra ataques direcionados (contra ameaças avançadas persistentes)** para 15 participantes; |

* 1. Justificativa da Solução Escolhida

|  |
| --- |
| * Eventos recentes de tentativas de ataque ao sistema PJe, que poderiam causar sua indisponibilidade e comprometimento de dados, objetivaram a urgência dessa aquisição. A opção pela solução da Trend Micro deveu-se pela facilidade de integração com outras ferramentas do mesmo fabricante, aumentando a capacidade de defesa contra ameaças, e que foram adquiridos através do contrato nº 100/2016-TJPE. |

* 1. Necessidade de Adequação do Ambiente para Execução Contratual

|  |
| --- |
| * Não há necessidade. |

1. **Consultas e Estudos Realizados**

|  |  |  |
| --- | --- | --- |
| Ação Executada | | Documentação Gerada |
|  | POC no Datacenter |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. **Outras Informações**
   1. Local de Entrega:

|  |  |
| --- | --- |
|  | Fórum Desembargador Rodolfo Aureliano – Av. Desembargador Guerra Barreto, s/n, Joana Bezerra, CEP 50080-900 – 1º andar / ala sul, Sala: GEATIV - SETIC. |

|  |  |  |
| --- | --- | --- |
| **Integrante Técnico** | **Integrante Requisitante** | **Integrante Administrativo** |
|  |  |  |
| Marcelo Ferreira Lima | Percival Barbosa Júnior | Liana Beatriz Barreto de Souza |
| Matrícula: 183.733-8 | Matrícula: 185.866-1 | Matrícula: 182.393-0 |
|  |  |  |
| **Recife, 15 de agosto de 2017** | | |

Contratação de soluções de (1) segurança para ambientes virtualizados e (2) proteção contra ataques direcionados (contra ameaças avançadas persistentes)

1. **Riscos do Processo de Contratação**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risco 1** | **Risco: Prolongamento do processo licitatório com interposição de recursos** | | | | | |
| **Probabilidade:**  **Baixo** | |  | **Id** | **Dano** | |
| **1** | Impossibilidade de capacidade da integração das ferramentas adquiridas com as versões existentes das ferramentas existentes no TJPE | |
| **2** |  | |
| **3** |  | |
| **Id** | **Ação Preventiva** | | | | **Responsável** |
| **1** | Reunião com fornecedores para uma correta especificação da solução | | | | NGA/DIOP/NSI |
| **2** | Termo de referência elaborado de forma sucinta e clara | | | | NGA |
| **3** |  | | | |  |
| **Id** | **Ação de Contingência** | | | | **Responsável** |
| **1** | Tramitação célere dos recursos impetrados contra o processo licitatório | | | | NGA |
| **2** |  | | | |  |
| **3** |  | | | |  |

1. **Riscos da Solução de Tecnologia da Informação**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risco 1** | **Risco: Quantidade insuficiente de licenças** | | | | | |
| **Probabilidade:**  **Baixo** | |  | **Id** | **Dano** | |
| **1** | Impacto (desempenho, indisponibilidade, perda de dados, etc.) da execução de ferramentas no ambiente do TJPE | |
| **2** |  | |
| **3** |  | |
| **Id** | **Ação Preventiva** | | | | **Responsável** |
| **1** | Realização de estudo detalhado e PoC no ambiente do TJPE | | | | NSI/DIOP/SETIC |
| **2** |  | | | |  |
| **Id** | **Ação de Contingência** | | | | **Responsável** |
| **1** | Reunião com fornecedores | | | | DIOP/Fornecedor |
| **2** |  | | | |  |

|  |  |  |
| --- | --- | --- |
| **Integrante Técnico** | **Integrante Requisitante** | **Integrante Administrativo** |
|  |  |  |
| Marcelo Ferreira Lima | Percival Barbosa Júnior | Liana Beatriz Barreto de Souza |
| Matrícula: 183.733-8 | Matrícula: 185.866-1 | Matrícula: 182.393-0 |
|  |  |  |
| **Recife, 15 de agosto de 2017** | | |

Contratação de soluções de (1) segurança para ambientes virtualizados e (2) proteção contra ataques direcionados (contra ameaças avançadas persistentes)

1. **Detalhamento dos Bens e Serviços que Compõem a Solução**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **Descrição** | **QTD** | **UNIDADE** |
| **01** | Solução de proteção para servidores virtuais contemplando: firewall + virtual paching + antimalware para 50 guests  Marca: Trend Micro  Fabricante: Trend Micro  Modelo/Versão: Deep Security Network Security Per Server (DS 9.X) |  |  |
| **02** | Solução de proteção para servidores virtuais contemplando inspeção de logs + monitoramento de integridade para 50 guests  Marca: Trend Micro  Fabricante: Trend Micro  Modelo/Versão: Deep Security System Security Per Server (DS 9.X) |  |  |
| **03** | Solução de segurança para monitoramento, detecção, análise e resposta a ataques desconhecidos e ameaças avançadas persistentes  Marca: Trend Micro  Fabricante: Trend Micro  Modelo/Versão: Deep Security System Security Per Server(DS9.X) |  |  |
| **04** | Implementação assistida |  |  |
| **05** | Suporte Remoto |  |  |

* 1. Justificativa para Parcelamento do Objeto em Lotes

|  |
| --- |
| * Não há necessidade de parcelamento em lotes, haja vista serem itens de mesma natureza, implicando em economia de escala |

1. **Caracterização dos Serviços Continuados**

|  |  |  |
| --- | --- | --- |
| O objeto da contratação se estende necessariamente por mais de um ano? | SIM | Trata-se de serviço continuado, pois a não atualização implica em base de conhecimento ultrapassada, perdendo assim, sua eficácia no combate a vírus e spams. |
| O objeto da contratação é essencial para a continuidade do negócio? | SIM | É item de segurança da informação, sem o qual as informações trafegadas por email e por arquivos estariam desprotegidos |

1. **Procedimento para Gestão e Fiscalização do Contrato**

|  |
| --- |
|  |
| * Ler atentamente o termo de Contrato, o edital, assim como os anexos, principalmente quanto a (ao):   + - especificação do objeto;     - prazo de execução do serviço, observada a primeira Ordem de Serviço emitida pela Diretoria de Informática;     - Acordo de níveis de Serviço     - cronograma dos serviços. * Providenciar o formulário próprio para registro das ocorrências relacionadas à fiscalização do Contrato; * Ter cópia de toda documentação relativa ao acompanhamento do Contrato; * Acompanhar a execução dos serviços, tendo como base os direcionamentos registrados no termo de Contrato, exercendo rigoroso controle sobre a qualidade e o cronograma de execução dos serviços; * Receber a fatura de cobrança, conferindo:   + - se as condições de pagamento do Contrato foram obedecidas;     - se o valor cobrado corresponde exatamente àquilo que foi efetuado;     - se a Nota Fiscal tem validade e se está corretamente preenchida;   + se está acompanhada das guias de quitação do FGTS/INSS sobre a mão-de-obra empregada (no caso de manutenção, serviço de engenharia, limpeza, etc.), conforme determina o Contrato; * Atestar, se for especificado, em conjunto com outro servidor ou comissão, a prestação do serviço efetivamente realizado; * Encaminhar a Nota Fiscal ao Núcleo de Gestão de Finanças e Contratos – SETIC que posteriormente enviará ao setor financeiro para pagamento; * No caso de dúvidas quanto ao ATESTO, deve-se buscar obrigatoriamente auxílio para que se efetue corretamente a atestação; * Notificar o descumprimento de cláusulas contratuais, principalmente quanto ao prazo, com o fim de aplicação das sanções cabíveis; * Manter contato regular com o preposto/representante da Contratada, com vistas a permitir o fiel cumprimento do Contrato. * Acompanhar as emissões de Ordem de Serviço * Atestar fatura/nota fiscal verificando se os prazos de entrega, especificações e quantidades estão compatíveis com o instrumento contratual; * Emitir pareceres técnicos relativos à repactuação solicitada pela contratada e sobre a qualidade do serviço prestado e/ou material recebido; * Registrar em formulário impresso ou eletrônico todas as ocorrências relacionadas com a execução do contrato, providenciando as medidas necessárias à regularização das falhas ou problemas constatados; * Notificar a contratada em caso de descumprimento de obrigações contratuais, estabelecendo prazo para providências; |

1. **Formas de Pagamento**

|  |  |
| --- | --- |
|  | Pagamento mensal após a emissão do empenho |

1. **Forma de Seleção do Fornecedor**

|  |  |
| --- | --- |
| Forma de Contratação | Justificativa |
| Pregão Eletrônico | Por ser bem comum, deve ser aplicado pregão, conforme Lei 10.520 de 17 de Julho de 2012 |

1. **Critérios de Seleção do Fornecedor**

|  |  |
| --- | --- |
| Requisito | Justificativa |
| * Atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado, no qual o licitante interessado já forneceu/prestou bem/serviço compatível com o solicitado * Ser empresa parceira da Trend Micro |  |

|  |  |  |
| --- | --- | --- |
| **Integrante Técnico** | **Integrante Requisitante** | **Integrante Administrativo** |
|  |  |  |
| Marcelo Ferreira Lima | Percival Barbosa Júnior | Liana Beatriz Barreto de Souza |
| Matrícula: 183.733-8 | Matrícula: 185.866-1 | Matrícula: 182.393-0 |
|  |  |  |
| **Recife, 15 de agosto de 2017** | | |

Contratação de soluções de (1) segurança para ambientes virtualizados e (2) proteção contra ataques direcionados (contra ameaças avançadas persistentes)

1. **Transição Contratual**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Serviços | Com que antecedência o gestor do contrato deverá analisar a possibilidade e o interesse da administração na prorrogação do contrato ou na eventual condução de uma nova contratação? | 6 meses antes do fim do contrato |

1. **Segurança da Informação e Controle de Acesso**

|  |
| --- |
| * Durante a prestação do objeto, a Contratada deverá observar a Política de Segurança da Informação definidas pelo Tribunal. * A contratada deverá firmar Termo de Responsabilidade e Sigilo com a Segurança da Informação conforme minuta em anexo. |

|  |  |  |
| --- | --- | --- |
| **Integrante Técnico** | **Integrante Requisitante** | **Integrante Administrativo** |
|  |  |  |
| Marcelo Ferreira Lima | Percival Barbosa Júnior | Liana Beatriz Barreto de Souza |
| Matrícula: 183.733-8 | Matrícula: 185.866-1 | Matrícula: 182.393-0 |
|  |  |  |
| **Recife, 15 de agosto de 2017** | | |