TJMG

Demanda 15215

Título:

Continuidade dos serviços de solução de antivirus - proteção Endpoint (CT 169/2017 - CIMCORP)

Gestor da Carteira de Demandas DIRFOR:

DIRFOR

A demanda será conduzida como projeto tradicional?:

Sim

Descrição:

Os serviços de solução de Antivírus estão vigentes no Contrato nº 169/2017, firmado com a empresa CIMCORP COMÉRCIO E SERVIÇOS DE TECNOLOGIA DE INFORMÁTICA LTDA, cuja data de término da vigência contratual é em 20/07/2022, não prorrogáveis.
Trata-se de serviço essencial ao Tribunal, mantendo a proteção à estações de trabalho desktops, notebooks e workstations, além de servidores em ambiente Windows, contra ameaças a segurança que possam explorar vulnerabilidades do ambiente, do sistema operacional ou de aplicações. A solução de segurança provê:
- Proteção contra Vírus conhecidos;
- Proteção por heurística contra vírus ainda desconhecidos;
- Comunicação por alertas;
- Controle centralizado da solução, atualizações e versões de vacinas de todas as estações;
- Distribuição centralizada de definições de vírus e atualizações;
- Repositório centralizado de quarentena;
- Bloqueio poroativo em situações de epidemia;
- Verificação por varredura de unidades de armazenamento fixas e removíveis;
- Inventário de informações das estações gerenciadas;
- dentre outras.

A Solução é composta por
a) Módulo Antimalware;
b) Módulo de Prevenção de Intrusos e Firewall;
c) Módulo de Controle Web;
e) Módulo de Proteção de E-mail;
f) Módulo de Controle de Dispositivos;
g) Módulo de Gerência.

Solicita-se a continuidade do serviço, sendo necessário a revisão dos requisitos técnicos e do modelo de contratação, sugerindo-se:
- A avaliação da separação das soluções de estações de trabalho, servidores e estações virtuais (VDI);

- Solução adequada para o ambiente virtualizado, principalmente as estações virtuais, com modelo de distribuição, gerenciamento e atualização específicos para VDI;
- Ampliação dos perfis profissionais, para atuação proativa na avaliação das ameaças, ações de correção e orientação a usuários;
- Instalar e remover a solução remotamente;
- Remuneração variável, sobre q auantidade de equipamentos em uso e suportada pelo serviço;
- Atender ao parque do Tribunal e sua expansão pelo período máximo de vigência da contratação;
- Dentre outras melhorias.

Motivação:

Os serviços de solução de Antivírus estão vigentes no Contrato nº 169/2017, firmado com a empresa CIMCORP COMÉRCIO E SERVIÇOS DE TECNOLOGIA DE INFORMÁTICA LTDA, cuja data de término da vigência contratual é em 20/07/2022, não prorrogáveis.
Solicita-se a continuidade do serviço, sendo necessário a revisão dos requisitos técnicos e do modelo de contratação, sugerindo-se
Trata-se de serviço essencial ao Tribunal, mantendo a proteção à estações de trabalho desktops, notebooks e workstations, além de servidores em ambiente Windows, contra ameaças a segurança que possam explorar vulnerabilidades do ambiente, do sistema operacional ou de aplicações. A solução de segurança provê:
- Proteção contra Vírus conhecidos;
- Proteção por heurística contra vírus ainda desconhecidos;
- Comunicação por alertas;
- Controle centralizado da solução, atualizações e versões de vacinas de todas as estações;
- Distribuição centralizada de definições de vírus e atualizações;
- Repositório centralizado de quarentena;
- Bloqueio poroativo em situações de epidemia;
- Verificação por varredura de unidades de armazenamento fixas e removíveis;
- Inventário de informações das estações gerenciadas;
- dentre outras.

Demonstrativo dos benefícios e resultados a serem alcançados:

a) Aumentar a satisfação dos usuários com os serviços prestados pela TIC;
b) Proteção das estações de trabalho, notebooks, servidores, ambiente virtual e storages da rede corporativa do TJMG;
c) Melhorar o controle de disponibilidade, confidencialidade, integridade e autenticidade dos serviços informatizados na rede corporativa do TJMG.
d) Ágil identificação de falhas de segurança na rede corporativa do TJMG;
e) Efetuar ações conjuntas que busquem a melhoria contínua dos serviços de TIC;
f) Apoiar na gestão dos ativos de TIC e Gerenciamento da Configuração;
g) Utilizar solução tecnológica para suportar a crescente maturidade na Governança de TI, um dos pilares da Governança Corporativa;
h) Prover suporte técnico e ação proativa contra ameaças

Detalhamento das características, abrangência, legislação, normativos, restrições de prazo

Abrangência

Todas as estações de trabalho - desktops, notebooks e workstations
Estações virtuais
Servidores Físicos e Virtuais em ambiente Windows
Storages

Prazo
Término do contrato vigente: 20/07/2022

Detalhamento Técnico Inicial:

Aquisição ou contratação de serviços soluções de segurança TI e soluções de segurança da informação para proteção do parque tecnológico do TJMG, incluindo os serviços de instalação, configuração do ambiente, atualização e prestação de serviços de suporte técnico e especializado e as respectivas garantias de funcionalidade das soluções e serviços, conforme especificações técnicas abaixo:
a) Fornecimento de soluções de segurança TI para o do ambiente de TIC e das licenças dos softwares inerentes ao objeto da contratação.
¿ Banco de dados;¿ Computadores, notebooks e estação de trabalho virtuais;¿ Provedores;¿ Servidores físicos e virtuais;¿ STORAGES, armazenamento.
b) Fornecimento soluções de segurança da informação na proteção de dados coorporativos da instituição a ameaças:
¿ Defesa contra ataques de hackers aos sistemas da corporação;¿ Proteção das informações da empresa disponíveis na internet;¿ Prevenção do acesso de indivíduos não autorizados a acessar dados sigilosos.
c) Realização das atividades de instalação, atualização, manutenção e configuração do ambiente:
d) Prestação dos serviços de suporte técnico e especializado.
¿ Ajudar na identificação de ameaças e vulnerabilidades às quais sistemas estão sujeitos! Aplicado técnica, processo ou sistema para identificar pontos de entrada e saída, fluxo de informações, bem como em componentes e ativos utilizados pelo software ou sistema;
¿ Prover soluções em que simule a ação de atacantes mal-intencionados e aplicação de conhecimento de técnicas ofensivas. Conduzir testes contemplando, sobretudo, uma forma de atuação para remediação e prevenção;
¿ Deverá possuir equipe especializada ou contar com suporte de empresa que desenvolve softwares ou faz gestão de sistemas desenvolvidos por terceiros, para avaliação de código-fonte buscando vulnerabilidades tradicionais, mas também características intrínsecas da tecnologia usada no software e que podem ser exploradas em ataques.
¿ Emulações e simulações que combinam técnicas de engenharia social, violação da segurança física e uma série de outros ataques. Assim, oferecendo uma visão clara das áreas a serem aprimoradas, e se caso necessário prover solução que deverá suprir tal necessidade;
¿ Prover soluções para evitar ou mitigar ataques que combinam códigos maliciosos sofisticados com recursos tecnológicos e humanos contra o ambiente tecnológico do tribunal, assim como mecanismos que elevam o nível de segurança contra ataques cibernéticos no ambiente.
¿ Deverá prover solução e especialista em Perícia forense digital, de modo a extrair o máximo de evidências disponíveis, respeitando metodologias da computação forense que podem ajudar a obter material suficiente para conduzirem investigações, sejam internas ou policiais em caso de ataques cibernéticos, ou ofensas promovidos contra a aplicações, soluções e infraestrutura de TIC deste

tribunal;
¿ Possuir equipe especializada com conhecimento de estratégias para a contenção de ataques e para o restabelecimento de ambientes às condições normais. Também ajudando na identificação da origem de um ataque e no planejamento de ações e estratégias futuras de modo a dificultar que um mesmo tipo de incidente volte a ocorrer.
¿ Deverá possuir equipe especializada para regime de contratação de consultoria BANCO DE HORAS para atuar junto a novos projetos para avaliar avaliar e identificar periodicamente pontos que causam desequilíbrio ou riscos para a segurança do ambiente tecnológico e parque computacional deste TRIBUNAL
¿ Observando as melhores práticas da CSA (Cloud Security Alliance) e de provedores de nuvem, Deverá prover solução e serviços para SecDevOps aderentes a norma NIST 800-144 no intuito garantir que o ambiente deste TRIBUNAL esteja em conformidade com melhores práticas de mercado.

Estimativa de Esforço:

Estimativa de Recursos Humanos Envolvidos:

Estimativa de Custo (Aquisição):
3 - Acima de R$ 176.000,00