Brasília-DF, 01 de outubro de 2021.

Ao
Tribunal de Justiça do Estado de Goiás
Goiânia - GO

A **System IT Solutions LTDA,** inscrita no CNPJ n.º 05.704.797/0001-21 e inscrição estadual n.º 07.445.783/001-13, estabelecida no SHS QUADRA 06 - CONJ A - BLOCO A SALA 201 - ED. BRASIL 21. CEP: 70.316-102 - BRASÍLIA – DF. Telefone (61) 3322-2222,email: partners@systemits.com , em prosseguimento às tratativas com o **Tribunal de Justiça do estado de Goiás**, apresenta proposta de: **Solução Integrada de Inteligência Cibernética, incluindo Acesso Ilimitado ao Console para Investigação e Análise de Incidentes Cibernéticos, Suporte Técnico, Instalação e Treinamento,** conforme condições, especificações e quantitativos adequados ao escopo do TJGO e em perfeita sintonia com o Anexo I – Termo de Referência – que integra o Edital do **Pregão Eletrônico n.º 080/2020-CLC/PGE e que resultou na ATA DE RESGISTRO DE PREÇOS No 034/2021 – CLC/PGE.**

Atenciosamente,

Fernando França
SYSTEM IT SOLUTIONS LTDA.

(61) 3322-2222
SAC 0800 64 40 007
www.systemits.com
comercial@systemits.com
Ed. Business Center Brasil 21 SHS Qd. 6 Conj. A Bloco A Sala 201
Brasília DF Brasil – CEP: 70322-915

Oferta Especial:

Em consonância com o Acórdão 394/2013-Plenário, TC 044.822/2012-0, relator Ministro Raimundo Carreiro, 6.3.2013 (cópia anexa) que em suma reza: "*É admissível a flexibilização de critério de julgamento da proposta, na hipótese em que o* ***produto ofertado apresentar qualidade superior à especificada no edital****, não tiver havido prejuízo para a competitividade do certame e o preço obtido revelar-se vantajoso para a administração",* e, observando as reais necessidades do TJGO no que tange à Solução Integrada de Inteligência Cibernética, a System ITS firma a seguinte **OFERTA ESPECIAL:**

1 - Ao Tribunal de Justiça do estado de Goiás aderir ao item 3 da supracitada ATA: Sistema de monitoração para cibersegurança (grande porte), originalmente assim composto:

Conjunto de 1 (hum) WDC e 3 (três) WDA – somando quadro appliance distintos com capacidade para analisar até 6 Gbps (seis gigabits por segundo) de tráfego, utilizando placa de captura especializada com 2 portas 10 GbE. Com todas as funcionalidades licenciadas perpetuamente e subscrição de Threat Intelligence durante o período do contrato. Possui capacidade interna de armazenamento de 105 TB para PCAPs e 90 TB para metadados/logs/flows, em drives NVME (capacidade total de armazenamento de 195 TB).

a SYSTEM ITS se compromete a entregar o supracitado item, sem ônus adicionais, com as seguintes configurações:

Conjunto de appliances com 2 (dois) Zerum WDC e 2 (dois) Zerum WDA - somando quatro appliances distintos - com capacidade para analisar até 12 Gbps (doze gigabits por segundo) de tráfego, utilizando placas de captura especializada com 2 portas 10GbE em cada WDC. Conta com todas as funcionalidades licenciadas perpetuamente e subscrição de Threat Intelligence durante o período de contrato. Esse conjunto de appliances prevê capacidade total de armazenamento de 210 Terabytes em drives NVMe, que podem ser utilizados para guardar pacotes, metadados, logs, flows e outros dados de máquina (**36 meses de garantia**)

(61) 3322-2222
SAC 0800 64 40 007
www.systemits.com
comercial@systemits.com
Ed. Business Center Brasil 21 SHS Qd. 6 Conj. A Bloco A Sala 201
Brasília DF Brasil – CEP: 70322-915

2 – Ao Tribunal de Justiça do estado de Goiás aderir ao item 5 da supracitada ARP (Serviços de análise de qualidade operacional) para um total de 22 servidores a System ITS se compromete a entregar, sem ônus adicionais, o serviço de análise de qualidade operacional para até 50 servidores e ainda o serviço de resposta a incidentes de segurança para a totalidade de endpoints do TJGO pelo prazo de **36 meses**.

TABELA DE PREÇOS

Item	Descritivo	Unidade	Qnt	Valor Unitário	Valor Mensal	Valor Total
3	Sistema de monitoração para cibersegurança (grande porte, com redundância) Com 36 meses de Garantia	Unidade	1	R$ 5.920.800,00	N/A	R$ 5.920.800,00
5	Serviço de análise de qualidade operacional	Endpoints/mês	42	R$ 1.794,51	R$ 75.369,42	R$ 904.433,04
VALOR TOTAL						**R$ 6.825.233,04**

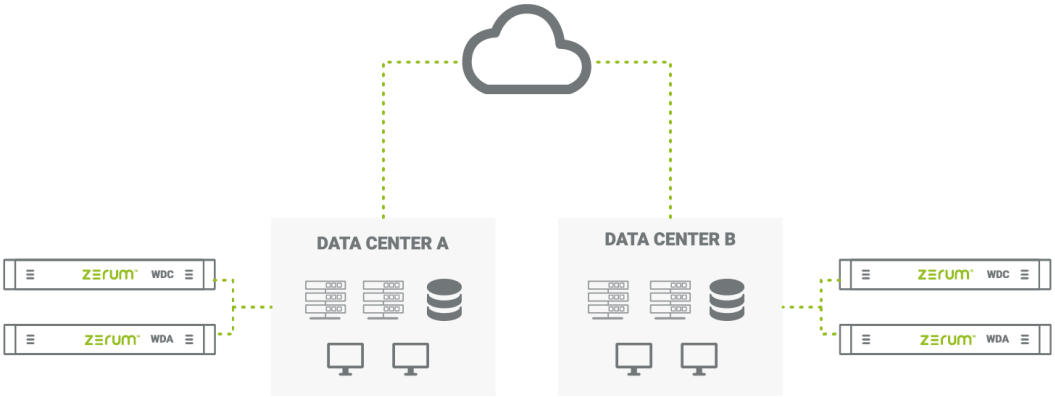
Valor Total da Proposta: R$ 6.825.233,04 (seis milhões, oitocentos e vinte e cinco mil, duzentos e trinta e três reais e quatro centavos).

VALIDADE DA PROPOSTA: 90 (noventa) dias contados da data de sua apresentação.

(61) 3322-2222
SAC 0800 64 40 007
www.systemits.com
comercial@systemits.com
Ed. Business Center Brasil 21 SHS Qd. 6 Conj. A Bloco A Sala 201
Brasília DF Brasil – CEP: 70322-915

ESPECIFICAÇÃO TÉCNICA

Item 3 – SISTEMA DE MONITORAÇÃO PARA CIBERSEGURANÇA (Grande porte com redundância) (com ampliação da oferta especial)



Conjunto de appliances com 2 (dois) Zerum WDC e 2 (dois) Zerum WDA - somando quatro appliances distintos - com capacidade para analisar até 12 Gbps (doze gigabits por segundo) de tráfego, utilizando placas de captura especializada com 2 portas 10GbE em cada WDC. Conta com todas as funcionalidades licenciadas perpetuamente e subscrição de Threat Intelligence durante o período de contrato. Esse conjunto de appliances prevê capacidade total de armazenamento de 210 Terabytes em drives NVMe, que podem ser utilizados para guardar pacotes, metadados, logs, flows e outros dados de máquina.

(61) 3322-2222
SAC 0800 64 40 007
www.systemits.com
comercial@systemits.com
Ed. Business Center Brasil 21 SHS Qd. 6 Conj. A Bloco A Sala 201
Brasília DF Brasil – CEP: 70322-915

Item 4 - SERVIÇO DE RESPOSTA A INCIDENTES DE SEGURANÇA (Oferta especial)

- ✓ Tem por objetivo analisar eventos, orientar a resposta e documentar os incidentes de segurança da informação. Tal serviço deverá ser executado obedecendo aos frameworks do NIST (National Institute of Standards and Technology) e SANS Institute para resposta a incidente de segurança da informação;

- ✓ As equipes de ataque (RED TEAM) e defesa (BLUE TEAM) devem interagir e funcionar de maneira integrada. A equipe de ataque deve compartilhar seu conhecimento no sentido de indicar soluções para vulnerabilidades encontradas e a equipe de defesa deve possuir conhecimento das tácticas e técnicas de ataque para que, por meio da atuação conjunta (PURPLE TEAM), aumente-se a efetividade da proteção do ambiente;

- ✓ Um incidente de segurança é definido como qualquer evento adverso em sistemas computacionais, feito de forma intencional ou acidental, levando a violação de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade;

- ✓ O início do processo de resposta a incidente de segurança se dará das seguintes formas:

a) Sempre que um evento adverso for submetido à Contratada, pelo corpo técnico da Contratante, a qualquer tempo;
b) A partir de consultas diárias ao Sistema de monitoração para cibersegurança, deve identificar situações em que endpoints IP, sistemas ou usuários apresentem comportamentos comprovadamente ou potencialmente nocivos a segurança dos dados.

- ✓ Após o incidente de segurança ser aberto, será de responsabilidade do grupo de resposta a incidente de segurança (Blue Team) da Contratada, analisar os logs, pacotes, flows e demais artefatos coletados, a fim de no primeiro instante identificar do que se trata o incidente e avaliar o risco dele;

- ✓ Uma vez realizadas as análises iniciais do incidente, o grupo de resposta a incidente de segurança (Blue Team) da Contratada, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do Contratante;

- ✓ Como próximo passo o grupo de resposta a incidente de segurança (Blue Team) da Contratada, deverá comunicar ao time de segurança da informação do Contratante as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente;

- ✓ A severidade do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do

(61) 3322-2222
SAC 0800 64 40 007
www.systemits.com
comercial@systemits.com
Ed. Business Center Brasil 21 SHS Qd. 6 Conj. A Bloco A Sala 201
Brasília DF Brasil – CEP: 70322-915

negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente;

- ✓ Após análises iniciais do incidente, caberá ao grupo de resposta a incidente de segurança (Blue Team), realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e todos os seus artefatos coletados;

- ✓ Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente de segurança (Blue Team) da Contratada, deverá definir uma estratégia para a mitigação e contenção do ataque em questão;

- ✓ Ao longo do processo de resposta ao incidente de segurança, a Contratada através do grupo de resposta a incidente de segurança (Blue Team), deve documentar toda e quaisquer evidências e identificação dos serviços e usuários envolvidos. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso.

- ✓ A análise deve ser realizada com o objetivo de identificar pessoas, locais e/ou eventos relacionados, correlacionando todas as informações reunidas, e gerando como produto final um laudo sobre o incidente de segurança em questão;

- ✓ Caso seja necessária a reconstrução do ataque, este deve ser realizado pela Contratada em ambiente controlado, usando-se, por exemplo, de sandbox (mecanismo de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança da informação). Tal ambiente deve ser de propriedade e controle da Contratada;

- ✓ O grupo de resposta a incidente de segurança (Blue Team) da Contratada, deve documentar as lições aprendidas no incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos;

- ✓ O serviço de resposta a incidentes será responsável por monitorar, configurar e operar o Sistema de monitoração para cibersegurança, visando a análise de logs, flows e pacotes de rede;

- ✓ O regime de execução deste serviço deverá ser 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano);

- ✓ A Contratada irá prover inteligência de proteção contra-ataques cibernéticos e serviços de pesquisa e desenvolvimento de inteligência de proteção contra ataques cibernéticos, sendo responsável por:

a) Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela Contratada;
b) Criar e revisar periodicamente regras (casos de uso) para detecção de ataques no Sistema de monitoração para cibersegurança, realizando as adaptações e evoluções necessárias;

(61) 3322-2222
SAC 0800 64 40 007
www.systemits.com
comercial@systemits.com
Ed. Business Center Brasil 21 SHS Qd. 6 Conj. A Bloco A Sala 201
Brasília DF Brasil – CEP: 70322-915

c) Implementar procedimentos para triagem de alertas e resposta a incidentes.

Item 5 - SERVIÇO DE ANÁLISE DA QUALIDADE (oferta especial)

- ✓ Será executado por profissionais especializados e certificados na ferramenta Sistema de monitoração para cibersegurança e qualidade operacional;
- ✓ Os dados de performance e capacidade a serem analisados deverão ser providos unicamente pelas ferramentas de Network Performance Management (NPM) e Application Performance Management (APM), utilizados pela Contratante. Não cabe a Contratada a instalação ou manutenção dessas ferramentas, apenas o consumo de dados;
- ✓ O serviço será prestado por equipe em regime de teletrabalho, com acesso remoto às ferramentas de monitoração;
- ✓ Cabe ao Contratante assegurar o acesso remoto aos recursos de monitoração, via VPN ou outras tecnologias, para viabilizar o serviço de análise de performance;
- ✓ O serviço será prestado em horário comercial, em dias úteis, conforme calendário local da Contratante;
- ✓ Esse serviço prevê a execução de análise profissional quanto a performance e qualidade de serviço de aplicações Web, banco de dados e infraestrutura;
- ✓ As análises de performance serão feitas de acordo com a prioridade definida pela Contratante;
- ✓ A Contratada terá um prazo de 24 (vinte e quatro) horas corridas para iniciar o serviço de análise após a solicitação formal;
- ✓ Após o início da análise, a Contratada deverá concluir as atividades num prazo máximo de 48 (quarenta e oito) horas corridas;
- ✓ As análises serão realizadas na ordem em que foram solicitadas e, caso a Contratante indique mais de um item por vez, deverá indicar a ordem de prioridade;
- ✓ As análises serão realizadas sequencialmente, respeitando os prazos previstos para início e fim das atividades;
- ✓ Cabe à Contratante definir o escopo da análise, detalhando:

a) Endereços IP dos servidores onde estão os serviços que serão analisados;
b) Nome dos serviços e portas TCP/UDP;
c) Topologia de rede.

- ✓ A análise deve incluir os seguintes aspectos:

(61) 3322-2222
SAC 0800 64 40 007
www.systemits.com
comercial@systemits.com
Ed. Business Center Brasil 21 SHS Qd. 6 Conj. A Bloco A Sala 201
Brasília DF Brasil – CEP: 70322-915

a) Performance de resposta dos servidores de aplicação, banco de dados, webservices e outros componentes da aplicação;
b) Melhoria do tempo de resposta e experiência do usuário final;
c) Requisições com maiores tempos de resposta e sugestões de melhorias;
d) Requisições que apresentaram erros em execução e sugestões de melhorias;
e) Problemas relativos à gargalos em rede e interfaces de comunicação (ex. retransmissões e zero window);
f) Falhas em balanceamento de carga;
g) Falhas em DNS;
h) Erros de autenticação;
i) Lentidão no acesso a FTP ou sistemas NAS (Network Attached Storage), SMB e NFS;
j) Possíveis razões de erros em HTTP, com análise do conteúdo das transações;
k) Queries lentas ou com erros em sistemas de banco de dados, com sugestões de melhorias;
l) Otimização de objetos estáticos (imagens, PDF, vídeos, textos), com melhores práticas de uso de cache e compressão;
m) Latência da comunicação em rede e Round Trip Time;
n) Erros e performance de comunicações criptografadas em SSL/TLS.

- ✓ O resultado das análises será fornecido através de documentação formal e personalizada, contendo todas os levantamentos executados, inclusive com gráficos e tabelas explanatórias e análises da causa-raiz dos problemas encontrados;

- ✓ Toda a documentação produzida irá conter o contato (telefone e e-mail) do especialista responsável pela análise;

- ✓ A Contratante poderá entrar em contato com os especialistas em horário comercial para sanar eventuais dúvidas;

- ✓ A Contratada terá um prazo de 4 (quatro) horas úteis para responder às dúvidas colocadas e fazer possíveis ajustes na documentação produzida.

(61) 3322-2222
SAC 0800 64 40 007
www.systemits.com
comercial@systemits.com
Ed. Business Center Brasil 21 SHS Qd. 6 Conj. A Bloco A Sala 201
Brasília DF Brasil – CEP: 70322-915

APRESENTAÇÃO DA EMPRESA

Razão Social:	System IT Solutions Ltda.
CNPJ/MF Nº:	05.704.797/0001-21
CFDF Nº:	07.445.783/001-13
Endereço:	Ed. Brasil 21 - SHS Quadra 06 Conjunto A Bloco A Sala 201 Brasília/DF – CEP: 70322-915
Telefones:	0800-644-0007 - (61) 3322-2222 - Fax: (61) 3044-4712
E-mail:	comercial@systemits.com

Atenciosamente,

Brasília, 01 de outubro de 2021.

Fernando França
SYSTEM IT SOLUTIONS LTDA.

ASSINATURA(S) ELETRÔNICA(S)

Tribunal de Justiça do Estado de Goiás
Para validar este documento informe o código 457345071214 no endereço https://proad-v2.tjgo.jus.br/proad/publico/validacaoDocumento

Nº Processo PROAD: 202109000294564 (Evento nº 15)

BARBARA FERNANDES
AUXILIAR JUDICIÁRIO
NÚCLEO DE SEGURANÇA E ADMINISTRAÇÃO DE DADOS
Assinatura CONFIRMADA em 02/10/2021 às 23:11