cigás Companhia de Gás do Amazonas

COMPANHIA DE GÁS DO AMAZONAS
1000
cigás

PROCESSO ADMINISTRATIVO: N. 014/2023.
INTERESSADO: COMITÊ PERMANENTE DE LICITAÇÃO - CPL
OBJETO: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇO DE CENTRO DE OPERAÇÕES DE SEGURANÇA (SOC)

DESPACHO N. 151/2024 - GETIN/CIGÁS

Trata-se de pedido de revogação desta GETIN sobre o procedimento licitatório realizado para a contratação de empresa especializada na prestação de serviço de Centro de Operações de Segurança (SOC).

A necessidade de revogação do certame se justifica, sobretudo, pelo interesse público em otimizar os recursos, buscando a melhor aplicação do orçamento da Companhia. Embora as propostas comerciais recebidas estivessem dentro do preço médio de mercado, a implementação de soluções internas de segurança da informação, em conjunto com os recursos tecnológicos já existentes, demonstra-se mais vantajosa para a Administração Pública.

A revogação além de estar em consonância com o princípio da eficiência administrativa, atende integralmente à necessidade da Administração, uma vez que permite a alocação mais eficiente dos recursos e o fortalecimento da estrutura de segurança da informação da CIGÁS, nos seguintes termos, quais sejam:

- ✓ **Custo-Benefício:** para melhor otimização do orçamento, algumas demandas serão absorvidas pelo time técnico atual, mediante soluções tecnológicas a serem implementadas, proporcionando um melhor custo-benefício à organização, ao mesmo tempo que contribuirá para a otimização de despesas e atendimento mais adequado às exigências da Companhia;

- ✓ **Alternativas mais viáveis:** a análise detalhada conduzida pela equipe de tecnologia da informação apontou alternativas internas e soluções híbridas viáveis que oferecem condições de atender à demanda por monitoramento e segurança, mantendo padrões aceitáveis de segurança da informação. Essas alternativas foram apresentadas como mais vantajosas financeiramente e com implementação eficiente.

Nesse sentido, destaca-se que a Companhia encontra-se em fase avançada de implementação das seguintes ferramentas:

- EDR (Endpoint Detection and response): A solução EDR implementada monitora continuamente todos os endpoints da CIGÁS (computadores, notebooks, servidores) em busca de atividades maliciosas. Através de técnicas avançadas de análise comportamental e inteligência artificial, o EDR é capaz de detectar e bloquear ameaças em tempo real, como malware, ransomware e tentativas de intrusão. Além disso, a solução fornece informações detalhadas sobre incidentes de segurança, permitindo uma resposta rápida e eficiente. A solução EDR se integra com o SIEM para fornecer uma visão completa da segurança dos endpoints;

- IOCs (Indicadores of Compromise): A CIGÁS implementou um sistema de gerenciamento de IOCs que coleta e analisa indicadores de ameaças conhecidas, como hashes de arquivos maliciosos, URLs maliciosas e endereços IP suspeitos. Esses indicadores são integrados ao SIEM e ao EDR, permitindo a detecção proativa de ameaças e a correlação de eventos para identificar ataques em andamento. O sistema de IOCs é atualizado continuamente com informações de diversas fontes, incluindo feeds de inteligência de ameaças e bancos de dados de segurança;

- MDR (Managed Detection and response): O serviço de MDR fornece monitoramento 24/7 dos sistemas da CIGÁS por uma equipe de especialistas em segurança. Esses especialistas analisam os alertas gerados pelo SIEM e pelo EDR, investigam atividades suspeitas e respondem a incidentes de segurança de forma proativa. O serviço de MDR inclui a triagem e a priorização de alertas, a análise de causa raiz de incidentes, e a implementação de medidas de contenção e remediação;

- Firewall (Adequação de regras de segurança): A CIGÁS atualizou seu firewall para um modelo de última geração com recursos avançados de segurança, como inspeção profunda de pacotes (DPI), prevenção de intrusão (IPS) e filtragem de conteúdo. As regras de firewall foram revisadas e otimizadas para bloquear tráfego malicioso e permitir apenas conexões legítimas. Além disso, foram implementadas novas funcionalidades de segurança, para aumentar a proteção da infraestrutura de rede;

- SIEM (Security Information and Event Management): O SIEM realiza a coleta e agrega logs de segurança de diversas fontes, como servidores, firewalls, dispositivos de rede e aplicações. O SIEM correlaciona os eventos de segurança, gera alertas em tempo real sobre possíveis ameaças e fornece dashboards e relatórios com informações relevantes sobre a segurança da informação da CIGÁS. O SIEM está integrado com as demais soluções de segurança, como o EDR e o sistema de IOCs, para uma visão completa e centralizada da segurança;

cigás Companhia de Gás do Amazonas

COMPANHIA DE GÁS DO AMAZONAS 1002 Folha

Em suma, a revogação do pregão em se considerando a priorização de soluções internas, que se complementam para formar uma estrutura robusta, trazendo como benefício uma solução integrada de Segurança da Informação, constituem uma decisão estratégica para a CIGÁS. Essa decisão visa atingir os objetivos de segurança da informação de forma mais eficiente e econômica, em total consonância com os princípios da Administração Pública.

Ante o exposto, encaminham-se os autos à Diretoria Administrativo-Financeira da CIGÁS, com a indicação da GETIN para a revogação do Pregão Eletrônico, nos termos elencados acima, priorizando soluções internas que atendam de forma eficaz às demandas, visando primordialmente otimizar o uso dos recursos da Companhia, em consonância com os princípios da economicidade e eficiência que regem a Administração Pública.

Manaus, 27 de novembro de 2024.

Bruna Oliveira da Silva
Analista de Segurança da Informação

Marcelo Nogueira de Alencar
Gerente de Tecnologia da Informação