DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

Aquisição de Solução de Gerenciamento de Acessos Privilegiados (Privileged Access Management – PAM) e Monitoramento e Análise Comportamental, com possibilidade de proteção, monitoramento, detecção e resposta a atividade de credencial privilegiada, armazenamento de senhas e mitigação de riscos através de gestão de identidade, com serviço de implantação e treinamento *hands on.*

PAMEM202132161

Assinado com senha por ARILSON GALDINO DA SILVA(usuário).
Use 2918825.18735557-2131 para a consulta à autenticidade em https://apps.tjpa.jus.br/sigaex/siga-autenticidade
Documento gerado por JONAS AMERICO ALVES DUARTE *Data e hora: 18/01/2022 11:24

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ	
SETOR DEMANDANTE: Coordenadora de Suporte Técnico – CST	
RESPONSÁVEL PELA DEMANDA: Arilson Galdino da Silva	
MATRÍCULA: 183318	TELEFONE: (91)3289-7181
E-MAIL: arilson.silva@tjpa.jus.br	

1. Justificativa da necessidade e motivação da contratação

Os recentes ataques cibernéticos perpetrado contra o Poder Judiciário, em especial o ocorrido contra o Superior Tribunal de Justiça (STJ), divulgado em 03 de novembro de 2020, chamaram a atenção dos responsáveis pelas instituições ligadas à Justiça e elevaram, como nunca, o grau de alerta do Conselho Nacional de Justiça (CNJ) e dos demais Tribunais para a questão da Segurança Cibernética como requisito fundamental para a continuidade da prestação jurisdicional no Brasil.

Após investigações conduzidas sobre o ataque ao STJ, foi identificado que a técnica de invasão consistiu primeiramente na obtenção de credenciais simples de usuários de rede, para, em seguida, através de uma técnica conhecido como “escalação de privilégios”, ganhar o controle de credenciais de mais alto nível gerencial na rede da vítima. De posse de uma dessas credenciais com poderes administrativos, o atacante efetua a criptografia dos dados armazenados nos servidores da rede. Este tipo de ataque é conhecido como “ramsonware”, através do qual valores pecuniários são exigidos em troca da liberação (descriptografia) dos dados sequestrados e indisponíveis. Em síntese, o atacante obtém por meios ilícitos acesso a alguma credencial de alto poder administrativo da rede da instituição, realizando, em seguida, ações criminosas.

É absolutamente recomendável que tais vulnerabilidades sejam corrigidas o quanto antes. Entretanto, muito frequentemente, é impraticável ou impossível corrigir tais vulnerabilidades, restando apenas a alternativa da adoção de soluções de contorno, como é o caso das soluções de **Gestão de Acessos Privilegiados** ou, na sua terminologia original na língua inglesa, *Privileged Access Management* (PAM).

As soluções que compõem essa classe de aplicativos têm por incumbência gerir, de forma mais segura, o armazenamento de credenciais (nome de usuário e senha, certificados digitais etc.), tomando para si a responsabilidade de intermediar o uso dessas credenciais entre os usuários propriamente ditos (humanos ou outros programas) e as aplicações ou sistemas de autenticação. Além disso, algumas das soluções neste campo são dotadas de “inteligência computacional” capaz de identificar tentativas espúrias de acesso às credenciais com base em regras definidas pelos administradores ou no comportamento temporal dos usuários proprietários da credencial protegida.

Em 07 de junho de 2021, o Conselho Nacional de Justiça publicou a Resolução nº 396 a qual instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Este documento, de caráter cogente para todos os Tribunais nacionais, visa garantir a segurança cibernética do ecossistema digital do Poder Judiciário brasileiro. Entre outras medidas, a Resolução nº 396/CNJ torna obrigatórias, entre outras medidas ligadas à segurança cibernética, ações dos Tribunais no sentido de garantir:

- segurança física e proteção de ativos de tecnologia da informação de forma geral;
- ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e de informações;

PAMEM202132161

Assinado com senha por ARILSON GALDINO DA SILVA(usuário).
Use 2918825.18735557-2131 para a consulta à autenticidade em https://apps.tjpa.jus.br/sigaex/siga-autenticidade
Documento gerado por JONAS AMERICO ALVES DUARTE *Data e hora: 18/01/2022 11:24

- ações destinadas a assegurar o funcionamento dos processos de trabalho, continuidade operacional e a continuidade das atividades fim e administrativas dos órgãos do Poder Judiciário;
- ações de planejamento, de sistematização e de normatização sobre temas atinentes à segurança cibernética.

Tais ações tem por objetivo:

1. tornar o Judiciário mais seguro e inclusivo no ambiente digital;
2. aumentar a resiliência às ameaças cibernéticas;
3. estabelecer governança de segurança cibernética e fortalecer a gestão e coordenação
4. integrada de ações de segurança cibernética nos órgãos do Poder Judiciário; e
5. permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.

A contratação, alvo deste instrumento de oficialização de demanda, tem por objetivo exatamente a aquisição de recurso tecnológico capaz compor solução de segurança que se destina a atender os objetivos expressos e comandados pelo CNJ aos Tribunais através do ENSEC-PJ.

Dessa forma, é de fundamental importância que o Tribunal de Justiça do Estado do Pará seja capaz de identificar as falhas e vulnerabilidades aos quais está desprotegido, com a finalidade de gerenciar os riscos e, assim, impedir que estas sejam exploradas, uma vez que o poder judiciário estadual tem expandido sua capacidade de sustentação, adicionando novos ativos para garantir um serviço jurisdicional de excelência.

2. Descrição sucinta da solução pretendida

A solução pretendida é um *Privileged Access Management* (PAM), ou seja, um **Sistema de Gerenciamento de Acesso Privilegiado**. Tal solução é usualmente conhecida por uma de suas funcionalidades mais frequentes, qual seja **Cofre de Senhas** embora a solução seja mais ampla que apenas a atividade de guarda de senhas.

Soluções tipo PAM são destinadas a mitigar os riscos inerentes à divulgação ou perda da confidencialidade de credenciais de alto poder administrativo no ambiente computacional das organizações, assumindo e mediando o controle do acesso, uso, abrangência e registro de ocorrência do uso de credenciais de administradores de rede e de outros dispositivos sensíveis, para os quais a obtenção por parte de elementos mal intencionados (hackers e demais criminosos cibernéticos) representaria perdas significativas no campo pecuniário, seja no campo da imagem da instituição frente à opinião pública e mesmo frente às exigências legais de continuidade da prestação jurisdicional.

De uma forma mais geral, uma solução PAM tem o objetivo de assumir o controle de credenciais (nomes de usuários e senhas, certificados digitais, chaves criptográficas etc.) usadas para gerenciar sistemas ou para ter acesso a recursos sensíveis e de grande impacto para a organização, como os que foram atacados no STJ em 2020. De posse e controle das credenciais, o sistema passa a controlar, restringir, registrar, e constranger a conformidade com normas de segurança que antes não poderiam, ou seriam muito difíceis de serem exercitados, tornando tais credenciais muito mais resistentes à ataques cibernéticos e tornando seu uso auditável e passível de análise através de algoritmos de inteligência artificial em busca de padrões que possam indicar ataques ou perigo de perda de segurança.

A solução a ser contratada deve possuir, dentre outras características, funcionalidade de isolamento de sessões e credenciais, capacidade de auditoria, mitigação de ameaças, aplicação de políticas, autenticação multifator, além da proteção contra o ataque *pass the hash* (PtH) em servidores.

PAMEM202132161

Assinado com senha por ARILSON GALDINO DA SILVA(usuário).
Use 2918825.18735557-2131 para a consulta à autenticidade em https://apps.tjpa.jus.br/sigaex/siga-autenticidade
Documento gerado por JONAS AMERICO ALVES DUARTE *Data e hora: 18/01/2022 11:24

A entrega da solução deve conter, além dos ativos de software, serviços de configuração inicial para atender ao cenário previsto e também treinamento tipo *hands on* da solução para integrantes da equipe técnica do TJPA focada em segurança da informação.

3. Alinhamento entre a demanda e o Plano de Anual de Contratação e o Planejamento Estratégico Institucional (PEI) e/ou Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETIC) do TJPA

O alinhamento desta contratação está exarado no Planejamento Estratégico do Tribunal de Justiça do Estado do Pará - Macrodesafio Objetivo Estratégico: Inovação e Modernização da Infraestrutura de TIC. Programa: 1417 – Infraestrutura e Gestão de TIC (Objetivo 2: Modernizar a Infraestrutura de TIC); Ação: 8651 – Atualização, Expansão e Manutenção da Infraestrutura de Tecnologia do Poder Judiciário (1° Grau), estando prevista no **Plano de Contratações de Soluções de TIC 2021**, na linha 44, onde lê-se a descrição "*Contratação de serviço de PAS – Privileged Account Secutiry, incluindo acompanhamento operacional.*"

4. Demonstrativo de resultados a serem alcançados com a solução

Dentre os resultados que são esperados, destacam-se:

- Garantir a confidencialidade, Integridade e disponibilidade das informações e ativos que serão adicionados para a gestão de credenciais;
- Realizar a gestão de acessos privilegiados;
- Mitigar riscos atinentes ao vazamento de credenciais privilegiadas que, em sua maioria, realizam gestão de ativos e serviços essenciais para a manutenção de toda a infraestrutura de Tecnologia da Informação e Comunicação, deste Egrégio Tribunal;
- Estruturar por meio de cofre de senhas as credenciais dos administradores de ativos, bem como das principais aplicações judiciais e administrativas;
- Promover segurança e proteção lógica dos principais dispositivos, situados tanto no Datacenter do TJPA, quanto nas estações e ativos de trabalho, que formam a infraestrutura tecnológica do Poder Judiciário do Estado do Pará;
- Evitar indisponibilidade, diminuição de desempenho, vazamento de credenciais, bem como interrupções não programadas;
- Propiciar o excelente funcionamento ininterrupto, assim como a disponibilidade dos serviços de tecnologia da informação, indispensáveis ao implemento da função jurisdicional.

5. A previsão de data em que deve ser iniciado o fornecimento dos bens ou a prestação dos serviços, observando os prazos estabelecidos no Plano de Contratações

O fornecimento de produtos e serviços deverá ocorrer no prazo de até 30 dias, após formalização e assinatura do contrato.

6. Indicação dos integrantes das equipes de planejamento, de apoio e de gestão e fiscalização da contratação

6.1. Equipe de planejamento da contratação	
Integrante Demandante Nome: ARILSON GALDINO DA SILVA Matrícula: 183318 Telefone: (91)3289-7181	Integrante Técnico Nome: Daniel Azevedo Ferreira Matrícula: 116394 Telefone: (91) 99386-7010

PAMEM202132161

Assinado com senha por ARILSON GALDINO DA SILVA(usuário).
Use 2918825.18735557-2131 para a consulta à autenticidade em https://apps.tjpa.jus.br/sigaex/siga-autenticidade
Documento gerado por JONAS AMERICO ALVES DUARTE *Data e hora: 18/01/2022 11:24

E-mail: arilson.silva@tjpa.jus.br	E-mail: daniel.ferreira@tjpa.jus.br

6.2. Equipe de apoio da contratação	
Integrante Demandante Nome: ARILSON GALDINO DA SILVA Matrícula: 183318 Telefone: (91)3289-7181 E-mail: arilson.silva@tjpa.jus.br	Integrante Técnico Nome: Daniel Azevedo Ferreira Matrícula: 116394 Telefone: (91) 3289/7177 E-mail: daniel.ferreira@tjpa.jus.br

6.3. Equipe de gestão e fiscalização da contratação		
Gestor do Contrato Nome: THIAGO DO ROSÁRIO DE CASTRO Matrícula: 174394 Telefone: (91)3289-7189 E-mail: thiago.rosario@tjpa.jus.br	Fiscal Demandante Nome: ARILSON GALDINO DA SILVA Matrícula: 183318 Telefone: (91)3289-7181 E-mail: arilson.silva@tjpa.jus.br	Fiscal Técnico Nome: Daniel Azevedo Ferreira Matrícula: 116394 Telefone: (91) 3289-7177 E-mail: daniel.ferreira@tjpa.jus.br

Belém, 28 de agosto de 2021

Arilson Galdino da Silva
Coordenador de Suporte Técnico

PAMEM202132161

Assinado com senha por ARILSON GALDINO DA SILVA(usuário).
Use 2918825.18735557-2131 para a consulta à autenticidade em https://apps.tjpa.jus.br/sigaex/siga-autenticidade
Documento gerado por JONAS AMERICO ALVES DUARTE *Data e hora: 18/01/2022 11:24