Ministério da Justiça e Segurança Pública
Secretaria-Executiva
Coordenação de Riscos e Segurança de TIC

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
28/12/2020	1.0	Criação do documento	Joédes Cardoso da Silva, Luis Claudio Rodrigues Morais e Anderson Araújo Alves

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA - IN 01/2019 - 08006.000117/2020-05

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019, a fase de Planejamento da Contratação terá início com o recebimento do Documento de Oficialização da Demanda pela Área de TIC. Este documento deverá ser elaborado pela Área Requisitante da solução.

PREENCHIMENTO PELA ÁREA REQUISITANTE	
1 - IDENTIFICAÇÃO DA ÁREA REQUISITANTE	
Área Requisitante:	Coordenação de Riscos e Segurança de TIC
Responsável pela demanda:	Ivanildo de Oliveira da Silva JR
Matrícula/SIAPE	1535600
E-mail:	ivanildo.jr@mj.gov.br
Telefone	61-2025-3566

2 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE	
Nome	Ivanildo de Oliveira da Silva JR
Matrícula/SIAPE	1535600

Cargo	Policial Rodoviário Federal
Lotação	DTIC/CGGOV
E-mail	ivanildo.jr@mj.gov.br
Telefone	61-2025-3566

IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE SUBSTITUTO	
Nome	Joédes Cardoso da Silva
Matrícula/SIAPE	3730955
Cargo	Analista em Tecnologia da Informação
Lotação	DTIC/CGGOV
E-mail	joedes.cardoso@mj.gov.br
Telefone	61-2025-8045

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE e do INTEGRANTE REQUISITANTE SUBSTITUTO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

IVANILDO DE OLIVEIRA DA SILVA JR

JOÉDES CARDOSO DA SILVA

3 - IDENTIFICAÇÃO DA DEMANDA

Necessidade de Contratação:

Contratação de solução de Gestão de Vulnerabilidades em Ativos de TIC

ALINHAMENTO AOS PLANOS ESTRATÉGICOS - PDTIC 2021-2023

Código	Unidade	Área	Tipo	Subtipo	Ação	Objetivo Estratégico	Descrição	Qtd
N0263	DTIC/SE	DTIC/CGGOV	Contratação	Licença e uso de software	A0064	OE11	Ferramentas de avaliação de vulnerabilidades em ativos	9000

4 - MOTIVAÇÃO/JUSTIFICATIVA

O Ministério da Justiça e Segurança Pública possui um ambiente de Tecnologia da Informação

e Comunicação (TIC) diversificado com vários recursos tecnológicos, sistemas legados e um grande número de usuários desses recursos. Nesse cenário cresce a preocupação relacionada aos problemas com a segurança digital e torna-se necessário a gestão de vulnerabilidades.

Hoje em dia, ainda que uma instituição como o Ministério da Justiça e Segurança Pública tenha um firewall robusto, um sistema de detecção de invasão (IDS) e antivírus/antimalware, os crackers (pessoas que quebram de sistemas de segurança) ainda podem obter acesso aos seus sistemas e dados, explorando as vulnerabilidades. Identificar essas vulnerabilidades antes dos invasores é o propósito da gestão de vulnerabilidades.

Existem diversas maneiras de se estar vulnerável a ciberataques, que são quaisquer tentativas de expor, alterar, desativar, destruir, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um dispositivo. Dentre essas vulnerabilidades citam-se:

- Software desatualizado: Os softwares que tratam de dados que devem ser protegidos, sejam sistemas operacionais ou qualquer outra aplicação, precisam estar atualizados. Essa necessidade decorre do fato de que falhas de segurança descobertas por cibercriminosos normalmente são corrigidas pelos desenvolvedores e disponibilizadas por meio de atualizações (patches).
- Falhas humanas: As falhas humanas podem ocorrer tanto na operação de software, quanto em sua programação. Na operação, erros podem ocorrer principalmente quando, por desatenção, códigos maliciosos são executados ou quando há descuido com senhas, sendo essas muito fracas ou transmitidas de forma não segura. Na área de programação, também podem ocorrer falhas que deixam brechas em softwares.
- Problemas de estrutura: Ainda que os softwares estejam atualizados e sejam operados com zelo, problemas de nível estrutural ou de hardware também podem colocar em risco as informações. Pode-se ter servidores mal configurados, ausência de firewall, antivírus e backup, falta de um profissional capacitado para gerenciar a estrutura de redes e computadores etc.

Um dos maiores ativos do Ministério da Justiça e Segurança Pública são seus dados gerados e armazenados — que muitas vezes são informações confidenciais de servidores, usuários e colaboradores, estratégias de negócios sigilosas ou questões de segurança pública. Portanto, administrar a segurança por meio do gerenciamento de vulnerabilidades não é apenas uma opção, mas uma ação exigida por várias estruturas de conformidade, auditoria e gerenciamento de riscos.

Diante disso, o monitoramento das vulnerabilidades de segurança no ambiente computacional do Ministério é absolutamente necessário para se manter a confidencialidade, a disponibilidade e a integridade das informações e permitir o correto cumprimento dos objetivos estratégicos da instituição e garantir a continuidade do negócio.

Neste contexto, busca-se implementar uma solução de serviços e software capaz de testar os ativos de TI e as aplicações web periodicamente em busca de quaisquer vulnerabilidades, sejam elas relativas à atualização de sistemas operacionais e servidores de aplicação, configurações de serviços ou outras falhas técnicas. Além disso, é preciso que a solução forneça relatórios para que seja possível o acompanhamento deste trabalho de identificação e mitigação de riscos.

Assim, a contratação de uma solução de gestão de vulnerabilidade e auditoria de configuração de ativos de rede e de análise dinâmica em aplicações WEB é imprescindível para que o Ministério da Justiça e Segurança Pública possa prover a segurança dos dados e ativos presentes em todo seu parque tecnológico.

5 – RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

A contratação de solução de gestão de vulnerabilidade e auditoria de configuração de ativos de rede e de análise em aplicações WEB irá possibilitar ao Ministério da Justiça e Segurança Pública perseguir os seguintes resultados:

1. Redução de custos associados à análise de vulnerabilidades
2. Maior assertividade nos investimentos em soluções de TI efetivamente necessárias
3. Redução dos riscos associados às vulnerabilidades críticas de ativos
4. Aumento da maturidade de segurança da informação
5. Economia de tempo e redução da complexidade, identificando e corrigindo as vulnerabilidades
6. Aumentar a segurança dos ativos eliminando os pontos cegos
7. Desenvolvimento de relatórios e apurações especiais; e painéis gerenciais para apoio à tomada de decisão dos gestores, quanto ao risco da instituição.
8. Garantir a segurança da informação e comunicação no âmbito do Ministério da Justiça e o sigilo das informações do cidadão
9. Implantar e fortalecer as equipes de tratamento de incidentes de segurança nas redes de computadores
10. Implantar ações que promovam o envolvimento da alta administração do órgão em relação às diretrizes e ações de Segurança da Informação e Comunicação
11. Definir e implantar mecanismos mais efetivos de responsabilização de colaboradores por eventos relacionados à Segurança da Informação e Comunicação
12. Contribuir para o aumento da capacidade de resiliência dos ativos de informação e das infraestruturas críticas
13. Instituir práticas de auditoria de Segurança da Informação e Comunicações
14. Atualizar a Política de Segurança da Informação e Comunicações

6 – FONTE DE RECURSOS

PLOA 2020 Fonte: 0100 Programa de Trabalho: 04122003220000001 Ação: 2000 PO: 000C Plano Interno: GL67OPCGLTI

ENCAMINHAMENTO

Encaminhe-se ao DIRETOR DE TECNOLOGIA DA INFORMAÇÃO para providências.

IVANILDO DE OLIVEIRA DA SILVA JR

PREENCHIMENTO PELA ÁREA DE TECNOLOGIA DA INFORMAÇÃO	
7 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO	
Nome	Anderson Araújo Alves
Matrícula/SIAPE	2045478
Cargo	Analista de Governança de Dados
Lotação	DTIC/CGGOV
E-mail	anderson.aalves@mj.gov.br
Telefone	61-2025-8045

IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO SUBSTITUTO	
Nome	Luis Claudio Rodrigues Morais
Matrícula/SIAPE	3214091
Cargo	Analista de Governança de Dados
Lotação	DTIC/CGGOV
E-mail	luis.morais@mj.gov.br
Telefone	61-2025-8045

Por este instrumento declaro ter ciência das competências do INTEGRANTE TÉCNICO e do INTEGRANTE TÉCNICO SUBSTITUTO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

ANDERSON ARAÚJO ALVES

LUIS CLAUDIO RODRIGUES MORAIS

ENCAMINHAMENTO

Encaminhe-se à autoridade competente da Área Administrativa, que deverá:

1. Decidir motivadamente sobre o prosseguimento da contratação;
2. Indicar o Integrante Administrativo para composição da Equipe de Planejamento da Contratação, quando da continuidade da contratação; e
3. Instituir a Equipe de Planejamento da Contratação, conforme exposto no inciso IV do art. 2º, e inciso III do §2º do art. 10.

RODRIGO LANGE

PREENCHIMENTO PELA ÁREA ADMINISTRATIVA	
9 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO	
Nome	Vinícius Augusto Bittencourt Dalcól
Matrícula/SIAPE	1764266
Cargo	Administrador
Lotação	CCONT
E-mail	vinicius.dalcol@mj.gov.br
Telefone	2025-7644

Por este instrumento declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como da minha indicação para exercer esse papel na Equipe de Planejamento da Contratação.

VINÍCIUS AUGUSTO BITTENCOURT DALCÓL

Documento assinado eletronicamente por **Joedes Cardoso da Silva**, **Integrante Requisitante - Substituto(a)**, em 15/01/2021, às 10:36, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **LUIS CLAUDIO RODRIGUES MORAIS**, **Analista de Governança de Dados (Big Data)**, em 15/01/2021, às 10:41, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **IVANILDO DE OLIVEIRA DA SILVA JUNIOR**, **Coordenador(a) de Riscos e Segurança de TIC**, em 15/01/2021, às 10:42, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **ANDERSON ARAUJO ALVES**, **Analista de Governança de Dados (Big Data)**, em 15/01/2021, às 10:44, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **VINICIUS AUGUSTO BITTENCOURT DALCOL**, **Integrante Administrativo**, em 15/01/2021, às 15:07, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Rodrigo Lange**, **Diretor(a) de Tecnologia da Informação e Comunicação**, em 15/01/2021, às 15:32, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.