13616296 08006.000003/2021-38

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

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA - IN 01/2019 - 08006.000003/2021-38

HISTÓRICO DE REVISÕES			
Data	**Versão**	**Descrição**	**Autor**
07/01/2021	1.0	Finalização da primeira versão do documento	Osmar Ribeiro Torres

INTRODUÇÃO
Em conformidade com o art. 10 da Instrução Normativa SGD/ME n° 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/CRS
E-mail	ivanildo.jr@mj.gov.br
Telefone	61-2025-3566

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE 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

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

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

Joédes Cardoso da Silva

3 - IDENTIFICAÇÃO DA DEMANDA

Necessidade de Contratação:

Contratação de Serviço de Centro de Operações de Segurança - SCO (Security Operations Center - SOC) com fornecimento suporte 24h por dia e 7 dias por semana abrangendo: aplicativos, equipamentos, Blue Team, Red Team e treinamentos para a equipe de gestão de SIC do MJSP.

ALINHAMENTO AO PDTIC 2021-2023

Código da necessidade atendida	Unidade	Área	Tipo	Identificação da Necessidade	Ação	Descrição da Ação
N0264	DTIC/SE	DTIC/CGGOV	Contratação	Segurança e Risco	A077	Contratação de serviço de SOC

ALINHAMENTO AO PAC 2021, DOC SEI (13249519)	
Código do PGC/ME	**Ação do PDTIC**
21202	Adquirir Segurança e Risco

4 - MOTIVAÇÃO/JUSTIFICATIVA

O Ministério da Justiça e Segurança Pública - MJSP - não possui em seu portfólio de serviços de TIC uma equipe de monitoramento, detecção, análise e bloqueio relacionados a área de segurança da informação e comunicação que esteja disponível 24 horas por dia e 7 dias por semana.

A função de bloqueio tem sido realizada de forma bastante limitada pela equipe terceirizada do NOC - Network Operations Center (Centro de Operação de Rede). Porém, a função do NOC não é afeta às questões de segurança da informação, mas sim relacionadas ao monitoramento da infraestrutura de rede e de seus serviços, ou seja, destina-se a identificar e solucionar problemas capazes de comprometer a performance ou a disponibilidade de rede.

Um SOC - Security Operations Center, por sua vez, verifica, analisa, classifica, detecta, monitora e resolve incidentes que podem vir a se tornar uma ameaça à estrutura digital e de segurança cibernética de uma organização de forma ininterrupta (24 horas por dia e 7 dias por semanas). Ameaças como vazamento de informações, comprometimento de dados, monitoramento de ataques, contramedidas em ataques, análise de segurança de rede, dentre diversos outros, são alguns exemplos de seus serviços.

Além disso, um SOC também provê serviços de BlueTeam e RedTeam, responsáveis, respectivamente, por corrigir incidentes de segurança encontrados ou defender ativamente contra ataques na infraestrutura digital de uma organização e, divulgar falhas em sua estrutura interna por meio de análise ativa da infraestrutura digital, na figura de hacker ético.

Segundo a norma ABNT ISO/IEC 27001:2006, segurança da informação seria a "preservação da confidencialidade, integridade e disponibilidade da informação [...] ". Ainda utilizado-se dessa norma podemos extrair que confidencialidade é a "propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados". Integridade é a "propriedade de salvaguarda da exatidão e completeza de ativos" e disponibilidade seria a "propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada".

Esse conceitos sofreram ao longo do tempo melhorias de forma que podemos citar como exemplo que a confidencialidade, para se concentrar apenas em uma propriedade, não se trata apenas de a informação ser ou não secreta, mas também, do nível de acesso a essa informação em termos de como e quando essa informação pode ser acessada em torno de um grau ou nível de confidencialidade.

Quando associam-se essas propriedades aos serviços prestados por um NOC, percebe-se que o NOC, como dito alhures, não possui essa competência uma vez que não é responsável pela manutenção da Tríade de Segurança e suas subpropriedades como a privacidade, autenticidade, identidade, não

repúdio, auditoria e *accountbility,* documentação, cabendo a um SOC lidar com esses detalhes da segurança da informação.

Em resumo, os serviços de um NOC normalmente restringem-se a Disponibilidade - com cumprimentos de Acordos de Nível de Serviço de Infraestrutura, seu funcionamento, bem como, o tempo de retorno dos serviços. A detecção, bloqueio, tratamento, auditoria relacionados à segurança da informação relacionam-se a um SOC.

Por não possuir um serviço dedicado à Segurança de TIC, o Ministério da Justiça está sujeito aos riscos associados à ausência de monitoramento contínuo e de uma equipe dedicada e especializada para a contenção e proteção na área de segurança da informação.

O Ministério da Justiça, diante do cenário estratégico que ocupa junto ao Governo Federal apresenta um significativo volume de ataques virtuais sofridos em suas redes corporativas. Associado a isso, por possuir certa capilaridade geográfica, uma vez que atualmente o Ministério da Justiça é responsável pelas redes corporativas do Departamento Penitênciário Nacional - DEPEN, muitos pontos passíveis de comprometimento são encontrados na sua infraestrutura.

Conforme podemos encontrar na Lei nº 13.844/2019, o Ministério da Justiça possui como competências, citando apenas algumas:

- política judiciária;
- políticas sobre drogas;
- defesa da ordem econômica nacional e dos direitos do consumidor;
- nacionalidade, imigração e estrangeiros;
- ouvidoria-geral do consumidor e das polícias federais;
- prevenção e combate à corrupção, à lavagem de dinheiro e ao financiamento do terrorismo e cooperação jurídica internacional;
- coordenação de ações para combate a infrações penais em geral, com ênfase em corrupção, crime organizado e crimes violentos;
- política nacional de arquivos;
- coordenação e promoção da integração da segurança pública no território nacional, em cooperação com os entes federativos;
- coordenação do Sistema Único de Segurança Pública;
- planejamento, coordenação e administração da política penitenciária nacional;
- promoção da integração e da cooperação entre os órgãos federais, estaduais, distritais e municipais e articulação com os órgãos e as entidades de coordenação e supervisão das atividades de segurança pública;
- assistência ao Presidente da República em matérias não afetas a outro Ministério;
- política de organização e manutenção da polícia civil, da polícia militar e do corpo de bombeiros militar do Distrito Federal

Percebe-se pelo exposto na Lei nº 13.844/2019 que uma significativa quantidade de informações sensíveis trafegam na rede corporativa do Ministério da Justiça e, dessa forma, não possuir uma equipe dedicada ao acompanhamento ininterrupto da "saúde" de sua infraestrutura no que diz respeito à Segurança da Informação e Comunicação submete o Ministério e o Governo Brasileiro a um enorme risco de perda de informações, imagem institucional, assim como, o bem estar do povo brasileiro.

Ainda no que diz respeito a sensibilidade dos dados trafegados temos proximidade da vigência da Lei Geral de Proteção de Dados, que prevê multa aos entes públicos por falhas na proteção de seus dados, assim como, determina mecanismos que devem ser seguidos para proteção dos dados pessoais armazenados nos sistemas do Ministério da Justiça.

Sabe-se que quando se trata de segurança da informação não se pergunta se haverá um ataque, mas quando isso acontecerá. Assim, mesmo que uma organização possua equipamentos de proteção de borda como Firewall ou mesmo, sistemas de detecção de intrusão, caso não exista uma equipe presente 24 horas por dia e 7 dias por semana apta atuar preventivamente, ativamente e após o incidente, de nada valerá o investimento em alguns equipamentos.

De acordo com a SANs, instituição que é autoridade mundial em Segurança da Informação, um Blue Team é:

> *"**Blue Team==Defense** The term Blue Team comes from the world of military simulation exercises. During exercises, the Red Team would be those playing the role of the adversary. The Blue Team would be acting as the friendly forces being attacked. So Red Team acts as Offense and Blue Team as Defense. Specifically emphasizing cyber security, the Blue Team's focus is to defend the organization from digital/cyber attacks. In truth, while everything that improves the defensive security posture could be construed as Blue Team, there is an overt emphasis on discovering and defending against attacks." (Destaque nosso)*
>
> *"Time Azul == Defesa O Termo Time Azul é cunhado no mundo da simulação de exercícios militares. Durante os exercícios, o Time Vermelho seria aquele faz o papel do adversário. O Time Azul atuaria como forças aliadas que estão sendo atacadas. Dessa forma, o Time Vermelho atua como o ataque e o Time Azul como a defesa. Enfatizando especificamente a segurança cibernética, o Time Azul foca na defesa da organização dos ataques digitais e cibernéticos. Na verdade, embora tudo o que melhora a postura defensiva de segurança possa ser interpretado como Equipe Azul, há uma ênfase clara na descoberta e defesa contra ataques." (Tradução Livre)*

Dessa forma, a presença de uma equipe de BlueTeam é essencial para promover uma postura defensiva de segurança da informação, sendo responsável, além da defesa propriamente dita, da varredura de toda infraestrutura digital e cibernética do Ministério da Justiça, incluindo seus sitemas corportarivos.

No diâmetro oposto temos o RedTeam que é responsável por "atacar" interna e externamente a infraestrutura de uma organização buscando por vulnerabilidades não detectadas pelo BlueTeam. É essencial que essas equipes sejam compostas por profissionais distintos, preferencialmente que nem se conheçam, visando uma imparcialidade nos resultados, assim como, obter o melhor "retrato" da real situação da organização.

Não menos importante, além da contratação de um **SOC**, de um **BlueTeam** e de um **RedTeam**, há a necessidade de treinamentos do corpo técnico de TIC de um órgão, afinal, a própria Instrução Normativa nº 01 do ME/SEDGD/SGD em seu artigo 3º inciso II afirma que não poderão ser objeto de contratação a gestão de segurança da informação. Além disso, de acordo com a NC nº 05 do Gabinete de Segurança Institucional da Presidência da República é competência dos "Gestores de Segurança da Informação e Comunicações são os responsáveis por coordenar a instituição, implementação e manutenção da infraestrutura necessária às Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais, nos órgãos e entidades da Administração Pública Federal, direta e indireta". Dessa forma, para que o corpo técnico do Ministério da Justiça seja capaz de atender as determinações legais, as recomendações técnicas e de gerir um time de profissionais de altíssima capacitação, como são os necessários para bem desempenhar os papeis de SOC, BlueTeam e RedTeam, é necessária a sua capacitação e certificação constante.

Diante do que foi exposto, 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 que essa contração seja realizada com a maior brevidade possível.

5 – RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

Com a contratação de um Security Operations Center - SOC - com suporte 24h por dia e 7 dias, Blue Team, Red Team e Capacitação irá possibilitar ao Ministério da Justiça e Segurança Pública perseguir os seguintes resultados:

1. Redução de riscos associados perda de dados, comprometimento dos sistemas, imagem institucional do ministério e do governo brasileiro
2. Maior assertividade nos investimentos em soluções de segurnaça da informação efetivamente necessárias
3. Redução dos riscos associados aos ativos críticos
4. Aumento da maturidade de segurança da informação

5. Economia de tempo e redução da complexidade, identificando e saneando a segurança da informação antes da implantação dos sistemas
6. Aumentar a segurança dos seus 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 dos cidadãos
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
15. Manter uma equipe initerrupta de resposta rápida e efetiva a ataques e incidentes de segurança da informação
16. Implantar o estado da arte em termos de segurança da informação
17. Multiplicar o efetivo na área de segurança da informação
18. Elevar o conhecimento técnico e a capacidade de gestão do corpo técnico próprio do Ministério da Justiça
19. Obter uma melhor compreensão da real situação em termos de segurança da informação do Ministério da Justiça de forma periódica por meio de um RedTeam.

6 – FONTE DE RECURSOS

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

PREENCHIMENTO PELA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

7 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO

Nome	João Marcelo Rodrigues Sant' Ana
CPF	706.056.701-10
Cargo	Cientista de Dados

Lotação	DTIC/CGGOV/CRS
E-mail	santana.joao@mj.gov.br
Telefone	2025 - 3243

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

JOÃO MARCELO RODRIGUES SANT' ANA

7.1 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE TÉCNICO SUBSTITUTO	
Nome	Cintia Mye Yonekawa Yamaguti
Matrícula/SIAPE	3201981
Cargo	Analista de Sistemas
Lotação	DTIC/CGGOV/CRS
E-mail	cintia.yamaguti@mj.gov.br
Telefone	61-2025-3566

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

CINTIA MYE YONEKAWA YAMAGUTI

8 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE	
Nome	Ivanildo de Oliveira da Silva JR
Matrícula/SIAPE	1535600
Cargo	Policial Rodoviário Federal
Lotação	DTIC/CGGOV/CRS
E-mail	ivanildo.jr@mj.gov.br
Telefone	61-2025-3566

Por este instrumento declaro ter ciência das competências do INTEGRANTE REQUISITANTE 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

8.1 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE REQUISITANTE SUBSTITUTO	
Nome	Joédes Cardoso da Silva
Matrícula/SIAPE	3730955
Cargo	Analista em TI
Lotação	DTIC/CGGOV/CRS
E-mail	joedes.cardoso@mj.gov.br
Telefone	61-2025-8045
Por este instrumento declaro ter ciência das competências 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. JOEDES CARDOSO DA SILVA	

PREENCHIMENTO PELA ÁREA ADMINISTRATIVA	
9 - IDENTIFICAÇÃO E CIÊNCIA DO INTEGRANTE ADMINISTRATIVO	
Nome	Gustavo Henrique Corrêa de Paula Maciel
Matrícula/SIAPE	1475463
Cargo	Coordenador de contratos
Lotação	CGL
E-mail	gustavo.maciel@mj.gov.br
Telefone	61-2025-3566
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. Gustavo Henrique Corrêa de Paula Maciel	

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;
3. As atividades atribuídas à autoridade da Área Administrativa poderão ser realizadas em documentos apartados (como Despacho ou Portaria), e devem ser incluídos no processo administrativo da contratação; e
4. 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

DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

PARECER DA AUTORIDADE COMPETENTE

O presente planejamento está de acordo com as necessidades do órgão previstas no PDTIC. Dá-se continuidade à fase Planejamento da Contratação.

Equipe de Planejamento da Contratação:

Integrante Requisitante: Ivanildo de Oliveira da Silva JR

Integrante Requisitante Substituto: Joédes Cardoso da Silva

Integrante Técnico: João Marcelo Rodrigues Sant' Ana

Integrante Técnico Substituto: Cintia Mye Yonekawa Yamaguti

Integrante Administrativo: Gustavo Henrique Corrêa de Paula Maciel

De acordo com Decreto n. 9.662, de 1º de Janeiro de 2019, que aprovou a Estrutura Regimental do Ministério da Justiça e Segurança Pública, a Diretoria de Tecnologia da Informação e Comunicações - DTIC equipara-se à Subsecretaria de Administração e à Subsecretaria de Planejamento e Orçamento. Assim, o rito processual observado pela SAA, no tocante ao "Parecer da Autoridade Competente do DOD" passa a ser de competência da DTIC, não havendo necessidade para a submissão de tais expedientes à Secretaria-Executiva. Referência Despacho nº 533/2019/SE (7975690).

Conforme o art. 30, § 3º da IN 04/2014 SLTI/MP a equipe da contratação será automaticamente destituída quando da assinatura do contrato.

_____

Rodrigo Lange

Diretor de Tecnologia da Informação e Comunicação

SIAPE nº 1558579

Documento assinado eletronicamente por **Gustavo Henrique Correa de Paula Maciel**, **Coordenador(a) de Contratos**, em 07/01/2021, às 16:41, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Cintia Mye Yonekawa Yamaguti**, **Analista em Tecnologia da Informação**, em 07/01/2021, às 16:53, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Joao Marcelo Rodrigues SantAna**, **Cientista de Dados (Big Data)**, em 07/01/2021, às 17:08, 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**, **Integrante Requisitante**, em 07/01/2021, às 17:15, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Joedes Cardoso da Silva**, **Integrante Requisitante - Substituto(a)**, em 07/01/2021, às 17:15, 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 07/01/2021, às 17:22, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **13616296** e o código CRC **37D72C3C**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

Referência: Processo nº 08006.000003/2021-38 SEI nº 13616296