15854445 08006.000003/2021-38

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

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO
PROCESSO Nº 08006.000003/2021-38

INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

O presente estudo tem por objetivo demonstrar a viabilidade técnica e econômica da contratação de empresa especializada para o fornecimento de **Serviço de Centro de Operações de Segurança - SCO (Security Operations Center - SOC) com funcionamento e suporte 24h por dia e 7 dias por semana, Serviço de tratamento e resposta aos incidentes cibernéticos - CSIRT - Blue Team e Serviço de teste de invasão - Red Team** e garantia dos serviços pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60(sessenta) meses, para o atendimento das necessidades da Diretoria de Tecnologia da Informação e Comunicação - DTIC do MJSP bem como fornecer informações necessárias para subsidiar o respectivo processo.

1. **DEFINIÇÃO DAS NECESSIDADES E REQUISITOS**

1.1. O Ministério da Justiça e Segurança Pública possui um ambiente composto por uma diversidade de tecnologias, pessoas que as acessam, sistemas, locais e informações que juntas elevam a complexidade da gestão de segurança da informação.

1.2. O SIEM a ser utilizado na prestação de serviço, e os softwares de SOAR/NTA/UEBA/CTI, serão fornecidos pelo MJSP. Outros softwares necessários para a prestação de serviço devem ser fornecidos pela Contratada, conforme detalhado em outros itens deste ETP.

1.3. No que diz respeito a diversidade de Tecnologias, quantitativos consolidados, relação de sistemas e outras informações, constam no **relatório de informações sobre a infraestrutura** (14628328).

Tabela 1 - Resumo dos itens de infraestrutura

Itens	Descrição	totais
1.	Equipamentos e tecnologias utilizadas no MJSP	728
2.	Total de estações de trabalho (14868691)	3.125
3.	Total de usuários cadastrados no AD	5.460
4.	Sistemas críticos, essenciais e outros	217
5.	Tecnologias de nuvem contratada Oracle e Microsoft	3
6.	Total de chamados para janeiro e fevereiro 2021 - N3 - Segurança(14656980)	219

Fonte: Relatório de **relatório de informações sobre a infraestrutura** (14628328) e Anexo Planilha de Sistemas Web (15983136).

1.4. As organizações, sejam elas de qualquer segmento ou tamanho, cada vez mais utilizam os serviços da TIC - Tecnologia da Informação e Comunicação como meio para atingirem seus objetivos. Com a transformação digital cada vez mais presente nas organizações, riscos, ameaças e vulnerabilidades que antes não existiam, começaram a surgir. Com dados e informações na nuvem, transações feitas através da internet e redes Wi-Fi, facilitam o dia a dia. Mas também abrem brechas de segurança para ataques de *hackers*, roubo de informações e outras ameaças à segurança virtual.

1.5. De acordo com o relatório de violação de dados de final de ano 2019 da Identity Theft Resource Center - ITRC, houve exposição de registros, sensíveis ou não, em centenas de vazamentos, conforme a figura 1:

INDUSTRY	# OF BREACHES	# OF SENSITIVE RECORDS EXPOSED	# OF NON-SENSITIVE RECORDS EXPOSED
Business	644	18,824,975	705,106,352
Medical/Healthcare	525	39,378,157	1,852
Banking/Credit/Financial	108	100,621,770	20,000
Government/Military	83	3,606,114	22,747
Education	113	2,252,439	23,103
2019 TOTALS:	1,473	164,683,455	705,174,054

Figura 1 - End of Year Data Breach Report 2019 - Identity Theft Resource Center

1.6. De acordo com a figura 2, temos os tipos de violações de dados por método de ataque e segmento da indústria:

# OF DATA BREACHES PER METHOD PER INDUSTRY						
Method	Banking	Business	Education	Government	Medical	Totals
Hacking/Intrusion (includes Phishing, Ransomware/Malware and Skimming)	31	291	29	35	191	577
Unauthorized Access	45	223	59	15	196	538
Employee Error/Negligence/ Improper Disposal/Lost	12	42	15	19	73	161
Accidental Web/Internet Exposure	12	44	7	8	17	88
Physical Theft	2	17	0	2	32	53
Insider Theft	6	12	2	3	10	33
Data on the Move	0	15	1	1	6	23

Figura 2 - End of Year Data Breach Report 2019 - Identity Theft Resource Center

1.7. No segmento governo, o método de ataque mais utilizado foi Hacking/Intrusion com cerca de 42,2%, assim como, em todos os outros segmentos. Não se deve considerar o número de violações de dados de forma absoluta, mas se deve levar em consideração a sensibilidade do dado violado não somente, o prejuízo financeiro imediato associado.

1.8. **Panorama no Brasil - Estatísticas de incidentes**

1.9. No Brasil, o CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil.

1.10. Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.

1.11. O CERT.br mantém estatísticas sobre notificações de incidentes a ele reportados. Estas notificações são voluntárias e refletem os incidentes ocorridos em redes que espontaneamente os notificaram ao CERT.br. Os dados sumarizados são apresentados na figura 3.

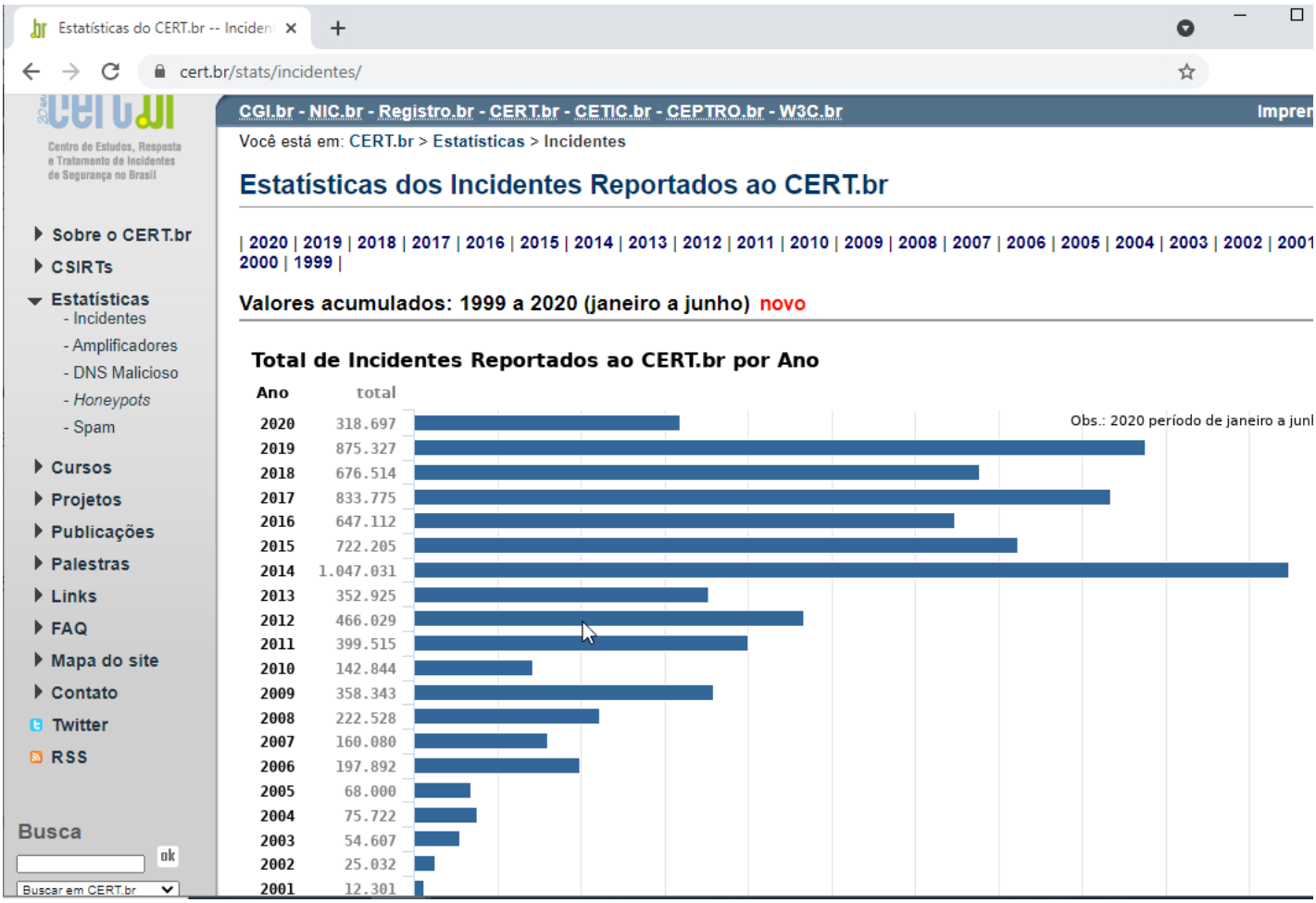

Figura 3 - Total de incidentes reportados, Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/ acesso em 13/05/2021.

1.12. **Incidentes Reportados ao CERT.br -- Janeiro a Junho de 2020**

1.13. A Tabela 2 apresenta os Totais Mensais e Anual Classificados por Tipo de Ataque.

Tabela - 2: Totais Mensais e Anual Classificados por Tipo de Ataque.

Mês	Total	worm (%)	dos (%)	invasão (%)	web (%)	scan (%)	fraude (%)	outros (%)

jan	**35094**	6703	19	3579	10	54	0	999	2	20704	59	2701	7	354	1
fev	**40229**	8215	20	7424	18	52	0	897	2	21184	52	2319	5	138	0
mar	**63313**	9316	14	16837	26	93	0	1045	1	31633	49	3111	4	1278	2
abr	**55255**	7680	13	6092	11	110	0	1458	2	36287	65	3537	6	91	0
mai	**59820**	10698	17	4815	8	122	0	2225	3	38389	64	3512	5	59	0
jun	**64986**	13033	20	7417	11	184	0	2187	3	39243	60	2844	4	78	0
Total	**318697**	55645	17	46164	14	615	0	8811	2	187440	58	18024	5	1998	0

Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/total.html acesso em 13/05/2021.

1.14. A Figura 4 apresenta de forma gráfica os tipos de ataque.

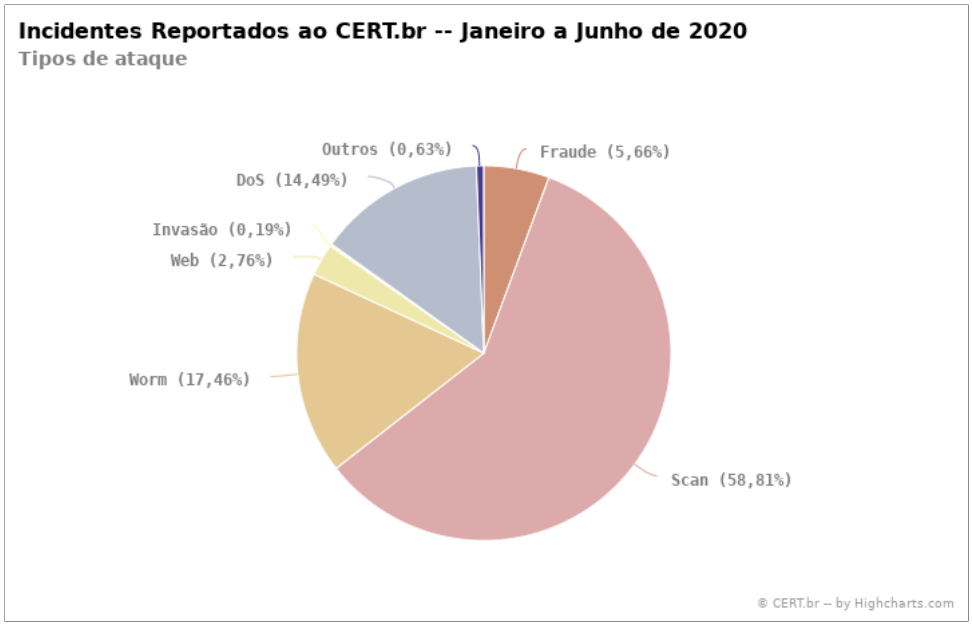

Figura 4 - Tipos de ataque - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html acesso em 13/05/2021.

Legenda:

- **worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **DoS** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

1.15. Obs.: Vale lembrar que **não se deve confundir scan com scam**. Scams (com "m") são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude.

1.16. A figura 5 relaciona os scans reportados por porta .

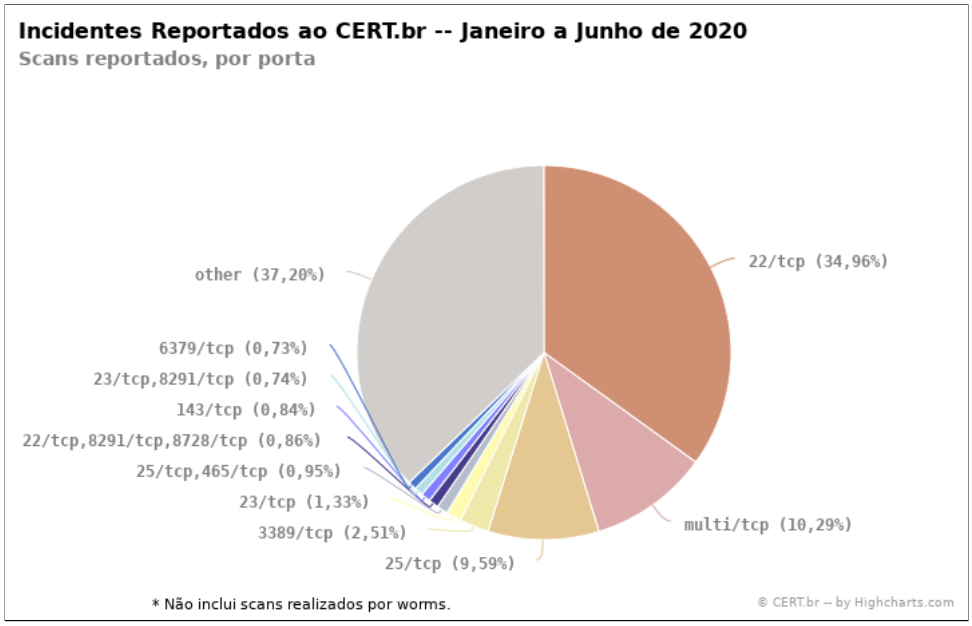

Figura 5 - Scans reportados, por porta - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/scan-portas.html acesso em 13/05/2021.

1.17. Na Figura 6 são apresentadas as Notificações sobre equipamentos participando em ataques DoS.

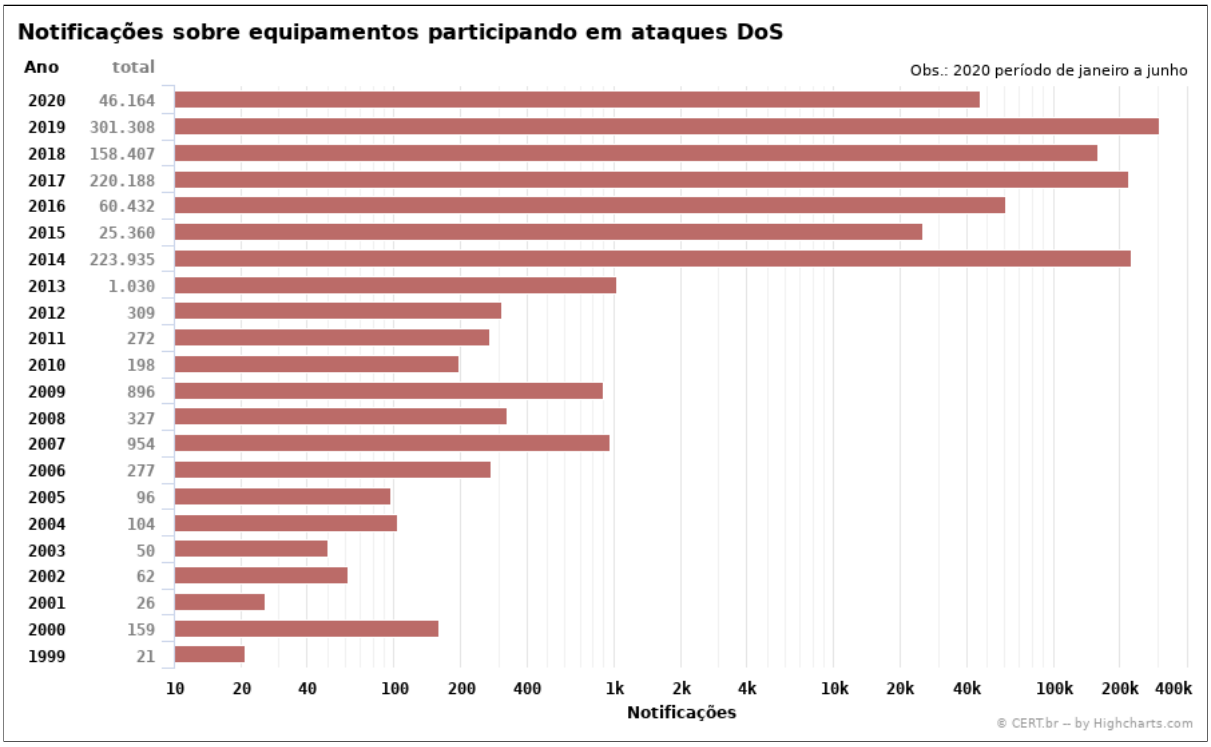

Figura 6 - Notificações sobre equipamentos participando em ataques DoS - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/dos.html acesso em 13/05/2021.

1.18. Na Figura 7 são apresentadas as Tentativas de Fraudes.

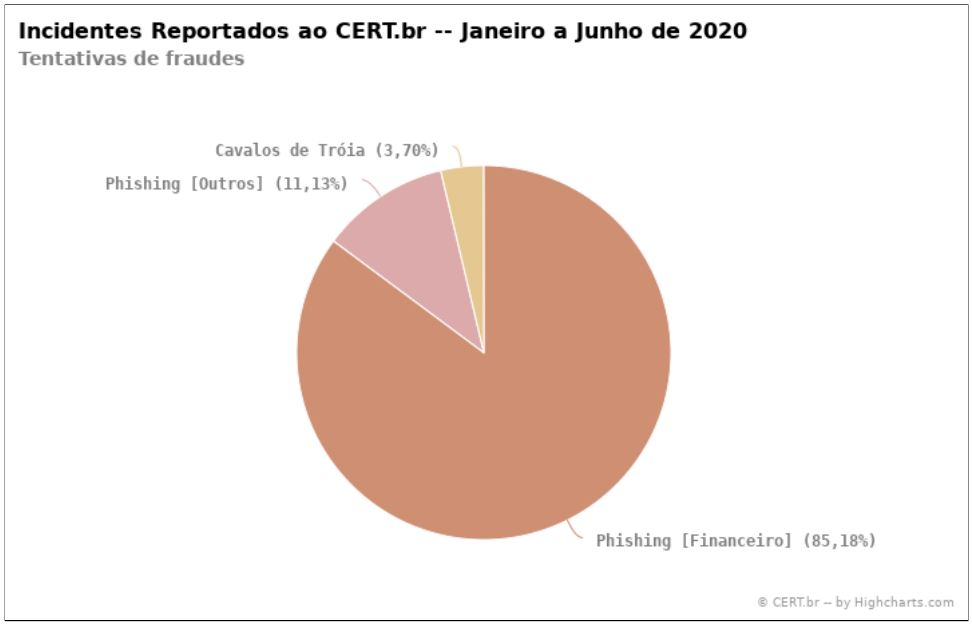

Figura 7 - Tentativas de fraudes - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/fraude.html acesso em 13/05/2021.

1.19. Na Figura 8 são apresentados os totais de incidentes reportados ao CERT.BR.

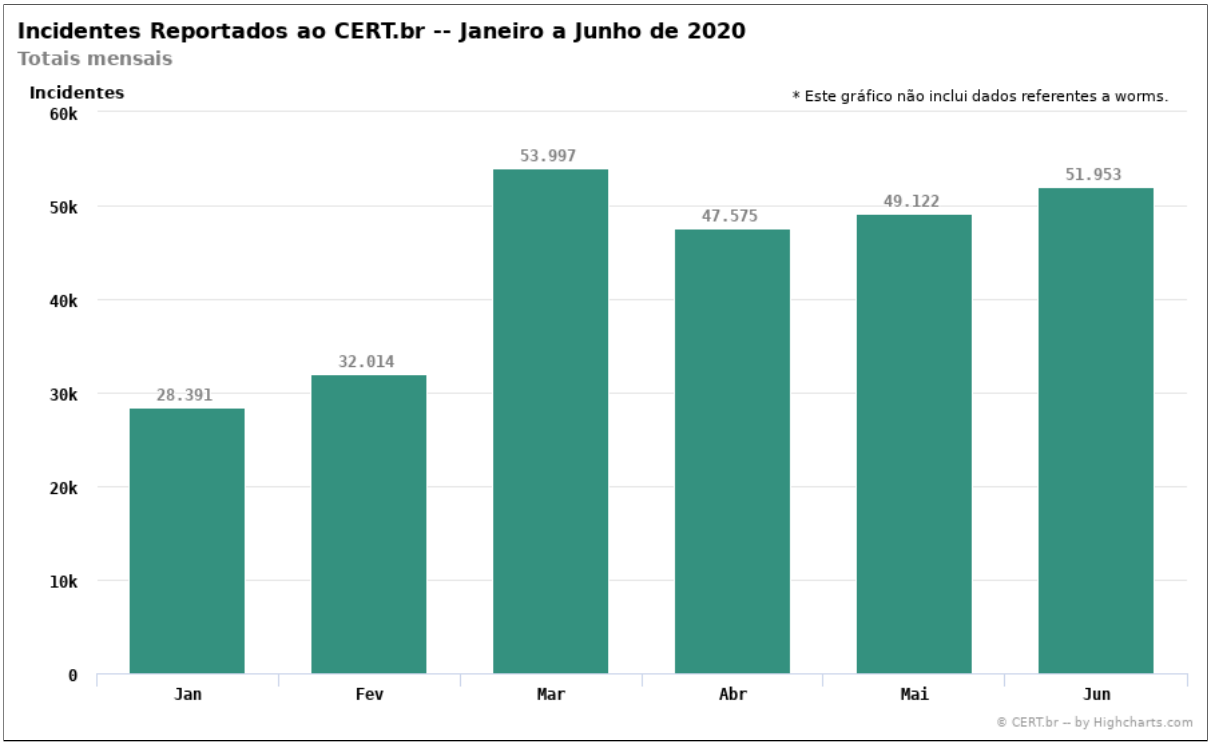

Figura 8 - Totais mensais - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/total-mensal.html acesso em 13/05/2021.

1.20. Na Figura 9 são apresentados os totais de incidentes reportados ao CERT.BR, considerando a origem do ataque.

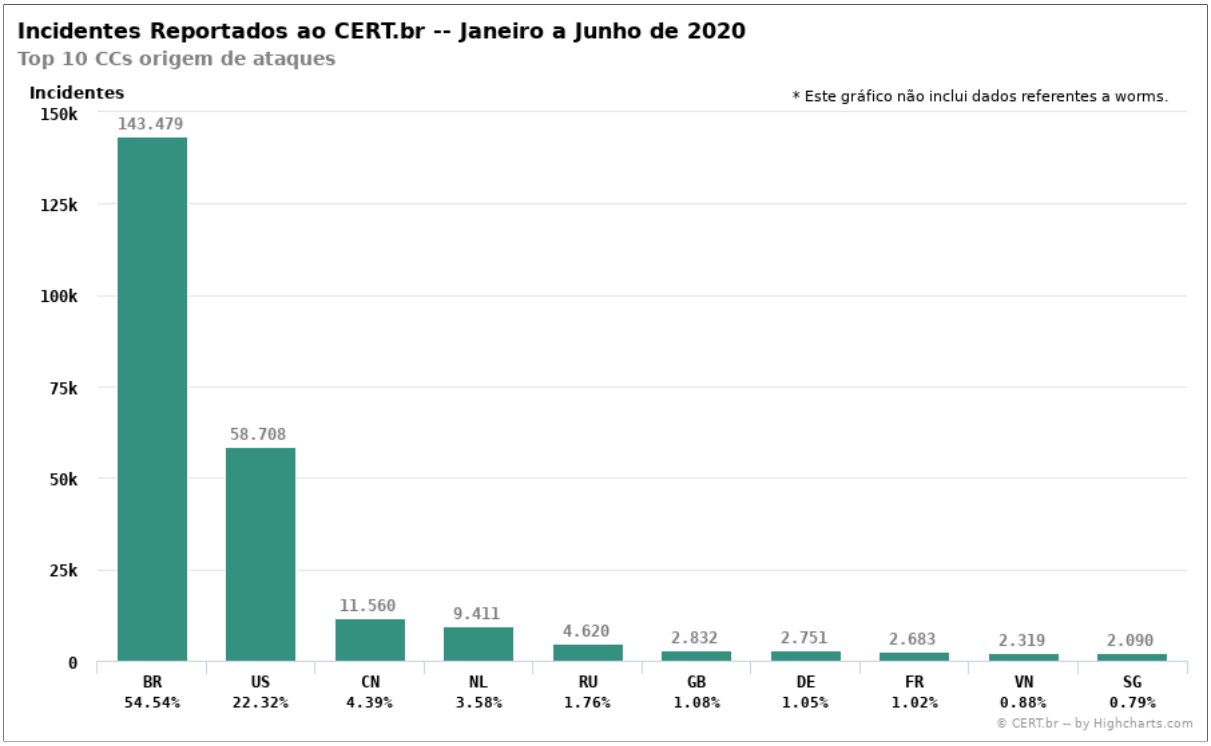

Figura 9 - Top 10 Country Codes origem de ataques - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/top-cc.html acesso em 13/05/2021.

1.21. Diante desse cenário complexo e misto, a contratação de uma equipe dedicada ao monitoramento, prevenção e reposta a incidentes de segurança se torna imprescindível.

1.22. É possível perceber a função de um *Security Operations Center - SOC,* a partir do trecho extraído da brochura do *Kaspersky for Security Operations Center,* conforme a seguir:

> "As businesses learn to better protect themselves, criminals are simultaneously devising increasingly sophisticated techniques to penetrate their security barriers. Attracted by the unprecedented financial rewards that cyberattacks can deliver, growing numbers of threat actors are actively seeking and targeting undiscovered security flaws. In this environment, many organizations are establishing Security Operations Centers (SOCs) to combat security issues as they arise, providing a swift response and a decisive resolution." (https://media.kaspersky.com/en/business-security/enterprise/brochure-soc-powered-by-kl-eng.pdf)

> "À medida que as empresas aprendem a se proteger melhor, os criminosos estão simultaneamente planejando cada vez mais técnicas sofisticadas para penetrar em suas barreiras de segurança. Atraídos pelas recompensas financeiras sem precedentes que os ciberataques podem oferecer, um número crescente de atores de ameaças está ativamente buscando e direcionando falhas de segurança não descobertas. Nesse ambiente, muitas organizações estão estabelecendo Centrais de Operações de Segurança SOCs para combater os problemas de segurança à medida que surgem, fornecendo uma resposta rápida e uma resolução decisiva." (tradução livre)

1.23. Partindo dessa percepção, um SOC (utilizaremos o acrônimo em inglês), é um ente centralizado com a função de monitoramento contínuo de ameaças, análise dessas ameaças, bem como, para prevenção e mitigação de incidentes de cibersegurança.

1.24. A crescente demanda pela eficiência na segurança da informação fez com que as organizações passassem a lidar com o assunto de forma mais estratégica. A formação de um Blue Team e um Red Team é um bom exemplo disso.

1.25. Com atribuições específicas, as equipes promovem um trabalho de cibersegurança em nível mais elevado nas empresas. Cada uma delas tem sua importância e o alinhamento entre as duas traz inúmeros benefícios.

1.26. O Red Team é formado com o objetivo de realizar testes de ciberataque na empresa. Estamos falando de profissionais com alto conhecimento sobre as principais ameaças e ataques existentes, sendo capazes de simular tentativas de penetrar na rede e ou sistemas. Com isso, eles se tornam capazes de identificar vulnerabilidades e, consequentemente, eliminá-las.

1.27. Resumidamente, eles assumem o papel de alguém que tentaria atacar a empresa — o que geralmente pode envolver a contratação de alguém de fora, sem o olhar acostumado àquele ambiente. Os ataques podem envolver engenharia social para enviar phishing aos funcionários, por exemplo.

1.28. O papel do Blue Team é justamente se opor aos ataques, inclusive aqueles ensaiados pelo Red Team. Assim, ele deve desenvolver estratégias para aumentar as defesas, modificando e reagrupando os mecanismos de proteção da rede para que eles se tornem mais fortes.

1.29. Um time desse tipo deve ter também um alto nível de conhecimento sobre a natureza das ameaças da rede. Entretanto, eles devem ser capazes não só de eliminar brechas, mas de reformular a infraestrutura de defesa como um todo.

1.30. Podemos extrair o que se entende por Blue Team, Red Team e Purple Team a partir das definições da autoridade mundial no tema, SANs:

- Blue Team:

> "[...] 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". (https://wiki.sans.blue/#!index.md)

> "[...] focado em defender a organização de digital/cyber ataques. Na verdade, enquanto tudo que promova a postura defensiva de segurança possa ser entendida como Blue Team, há uma ênfase na descoberta e defesa contra esses ataques. " (Tradução Livre)

- Red Team:

> "[...] would be those playing the role of the adversary. [...] So Red Team acts as Offense and Blue Team as Defense." (https://wiki.sans.blue/#!index.md)

"[...] serial aqueles que atuam o papel de adversários. [...] Então o Red Team atua como ofensiva e Blue Tema como defensiva." (Tradução Livre)

- Purple Team:

"[...] They typically report to a as a "third" team; think of it as a concept aimed at bringing the red and blue teams together to create purple team exercises. Red teams and blue teams should be encouraged to work as a joint team, to share insights beyond just reporting, to create a strong feedback loop, and to look for detection and prevention controls that can realistically be implemented for immediate improvement. " (https://www.sans.org/purple-team?msc=ptcourse-faq-lp)

"[...] Eles se denominam como o 'terceiro' time; pense nisso como um conceito que visa reunir as equipes vermelhas e azuis para criar exercícios de purple team. Equipes vermelhas e azuis devem ser incentivadas a trabalhar como uma equipe conjunta, para compartilhar ideias além somente gerar relatórios, a criar um forte ciclo de feedback, e a procurar controles de detecção e prevenção que possam ser implementados realisticamente para melhoria imediata."

1.31. A SANS - System Administration, Networking and Security é uma empresa especializada em segurança da informação e treinamento de cybersegurança. Definição o que é SANS :

SANS is the most trusted and by far the largest source for cybersecurity training in the world. We offer training through several delivery methods including OnDemand (self paced) and instructor-led both Live Online (virtual) and In-Person. Our cybersecurity courses are developed by industry leaders in numerous fields including network security, digital forensics, offensive operations, cybersecurity leadership, industrial control systems, and cloud security. Courses are taught by real-world practitioners who are the best at ensuring you not only learn the material, but that you can apply it immediately when you return to the office. In addition to top-notch training, we offer certification via GIAC, an affiliate of the SANS Institute featuring over 35 hands-on, technical certifications in cyber security. We offer a Master's Degree, graduate and undergraduate certificate programs through SANS Technology Institute, as well as numerous free resources including newsletters, whitepapers and webcasts.

SANS é a mais confiável e de longe a maior fonte de treinamento em segurança cibernética do mundo. Oferecendo treinamento por meio de vários métodos de entrega, incluindo OnDemand (individualizado) e ministrado por instrutor ao vivo online (virtual) e presencial. Os cursos de segurança cibernética são desenvolvidos por líderes do setor em diversos campos, incluindo segurança de rede, análise forense digital, operações ofensivas, liderança em segurança cibernética, sistemas de controle industrial e segurança em nuvem. Os cursos são ministrados por profissionais do mundo real que são os melhores em garantir que você não apenas aprenda o material, mas também que possa aplicá-lo imediatamente ao retornar ao escritório. Além do treinamento de alto nível, oferece certificação via GIAC, uma afiliada do SANS Institute com mais de 35 certificações técnicas práticas em segurança cibernética. Oferece programas de certificado de mestrado, pós-graduação e graduação por meio do SANS Technology Institute, bem como diversos recursos gratuitos, incluindo boletins, white papers e webcasts.

1.32. Considerando as definições acima inseridas para Blue Team, Red Team e Purple Team, podemos afirmar, simplificadamente que o Blue Team é o elo de defesa e sua operação, o Red Team seria o ente de ataque o qual checa as defesas implementadas pelo Blue Team. O Purple Team seria o esforço coordenado envolvendo os dois grupos para examinar novas técnicas de invasão, desenvolver defesas melhoradas e enfrentar ataques de equipe vermelha.

1.33. De acordo com o modelo de arquitetura de segurança adaptativa proposto pelo Gartner, uma organização somente obterá sucesso na luta contra os crimes cibernéticos se seu SOC for capaz de predizer, prever, detectar e responder efetivamente as ameaças, conforme podemos visualizar na figura 10 :

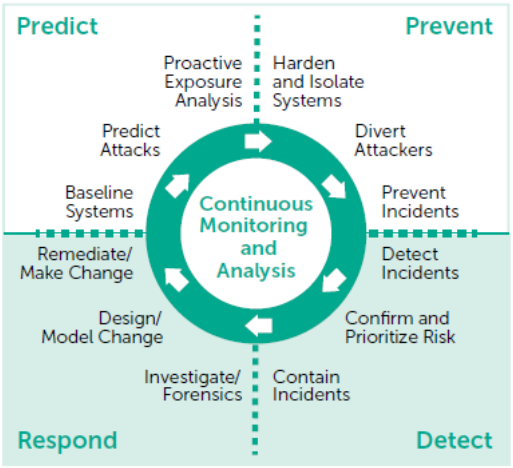

Figura 10 - Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, February 2014. (retirado da brochura do Kaspersky for Security Operations Center)

1.34. Levando esse modelo em consideração o Ministério da Justiça e Segurança Pública objetiva contratar um serviço o qual contemple as equipes de Blue Team, Red Team e Purple Team, de forma 24h por dia e 7 dias por semana para o monitoramento e defesa de primeiro nível, em horário comercial para o suporte de segundo nível, e sob demanda para atividades de Red Team.

1.35. Busca-se com o presente Estudo Técnico Preliminar demonstrar a necessidade que o Ministério da Justiça e Segurança Pública possui em contratar um serviço de SOC, assim como, identificar as necessidades de negócio, tecnológicas, bem como, os demais requisitos necessários e suficientes à escolha dessa solução de TIC. Os quais serão apresentados na tabela 3.

Tabela - 3: Identificação das necessidades de negócio, tecnológicas e demais requisitos

Identificação das necessidades de negócio		**Alinhamento ao PDTIC 2021**
1	Reduzir riscos associados a perda de dados, comprometimento dos sistemas, imagem institucional do ministério e do governo brasileiro	A0077 - Contratação de serviço de SOC
2	Melhorar a assertividade nos investimentos em soluções de segurança da informação efetivamente necessárias	
3	Reduzir os riscos associados aos ativos críticos	

4	Aumentar a maturidade de segurança da informação
5	Economizar tempo e reduzir a complexidade, identificando e saneando a segurança da informação antes da implantação dos sistemas
6	Aumentar a segurança dos ativos reduzindo ou eliminando os pontos cegos
7	Desenvolver relatórios e apurações especiais, 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
10	Definir e implantar mecanismos mais efetivos de responsabilização de colaboradores por eventos relacionados à Segurança da Informação e Comunicação
11	Contribuir para o aumento da capacidade de resiliência dos ativos de informação e das infraestruturas críticas
12	Instituir práticas de auditoria de Segurança da Informação e Comunicações
13	Manter uma equipe ininterrupta de resposta rápida e efetiva a ataques e incidentes de segurança da informação
14	Implantar o estado da arte em termos de segurança da informação
15	Multiplicar o efetivo na área de segurança da informação
16	É necessário que a solução leve em consideração a segurança no serviço em nuvem, garantindo a privacidade e a segurança dos dados

Identificação das necessidades tecnológicas	
1	Monitorar ininterruptamente de forma automatizada a sensibilidade dos dados de acordo com a Lei Geral de Proteção de Dados
2	Monitorar ininterruptamente de forma automatizada os recursos de TI do Ministério da Justiça e Segurança Pública e suas unidades
3	Implantar ferramenta de gerenciamento e correlação de eventos de segurança - SIEM
4	Implantar tecnologias de prevenção, detecção e resposta rápida a incidentes de segurança da informação
5	Prover análise interna e externa dos ativos de TIC, com escopo em segurança da informação, a partir de ferramentas do Ministério da Justiça e Segurança Pública ou próprias
6	Implantar painel em tempo real que demonstre a situação atual em termos de risco e segurança da informação do Ministério da Justiça e Segurança Pública
7	Prover relatórios *Post Mortem* dos ataques à infraestrutura do Ministério da Justiça e Segurança Pública
8	Sugerir melhorias na infraestrutura de TIC do ministério, com escopo em segurança da informação, indicando os riscos quando não implementadas

Demais requisitos necessários e suficientes à escolha da solução de TIC	
1	Atuar de forma sincronizada com o Network Operations Center - NOC
2	Manter equipe 24 horas por dia e 7 dias por semanas de forma ininterrupta provendo os serviços SOC e **Blue Team** ao Ministério da Justiça e Segurança Pública
3	Prover equipe sob demanda da Coordenação de Riscos e Segurança da informação para atividades de SOC relacionadas a **Red Team.**
4	Prover equipe de **Purple Team** para coordenação das equipes de **Blue Team** e **Red Team**.

2. **ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS**

2.1. O Ministério da Justiça e Segurança Pública possui a necessidade de contratação dos seguintes serviços os quais serão detalhados e motivados separadamente conforme a seguir:

2.1.1. - **Serviço de *Security Operations Center* - SOC** destinado a ser o ente central da estrutura de monitoramento e controle dos incidentes de segurança da informação, operando 24h por dia e 7 dias por semana para suporte de primeiro nível na triagem, investigação e resposta a incidente.

2.1.2. - **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team** responsável por atuar sob o comando do SOC quando da ocorrência de incidentes de segurança da informação ou sempre que solicitado visando contribuir com a melhoria da segurança da informação, sendo

24h por dia e 7 dias por semana para apoio ao suporte de primeiro nível e demais níveis realizado pelo SOC e em horário comercial, sendo 12h por dia 5 dias por semana, para suporte sob demanda.

2.1.3. - **Serviço de Teste de Invasão - Red Team** responsável por realizar testes independentes de penetração e análise de segurança mediante demanda da Coordenação de Riscos e Segurança da Informação - CRS.

2.1.4. Para um melhor entendimento foi definido um diagrama de relacionamento dos serviços e seus respectivos componentes, objeto da presente contratação, com os demais serviços da DTIC adaptado de acordo com o Framework para implementar um SOC de Schinagl, S., Schoon, K., & Paans, R. (2015). A framework for designing a security operations centre (SOC). Proceedings of the Annual Hawaii International Conference on System Sciences, 2015-March, 2253–2262. https://doi.org/10.1109/HICSS.2015.270.

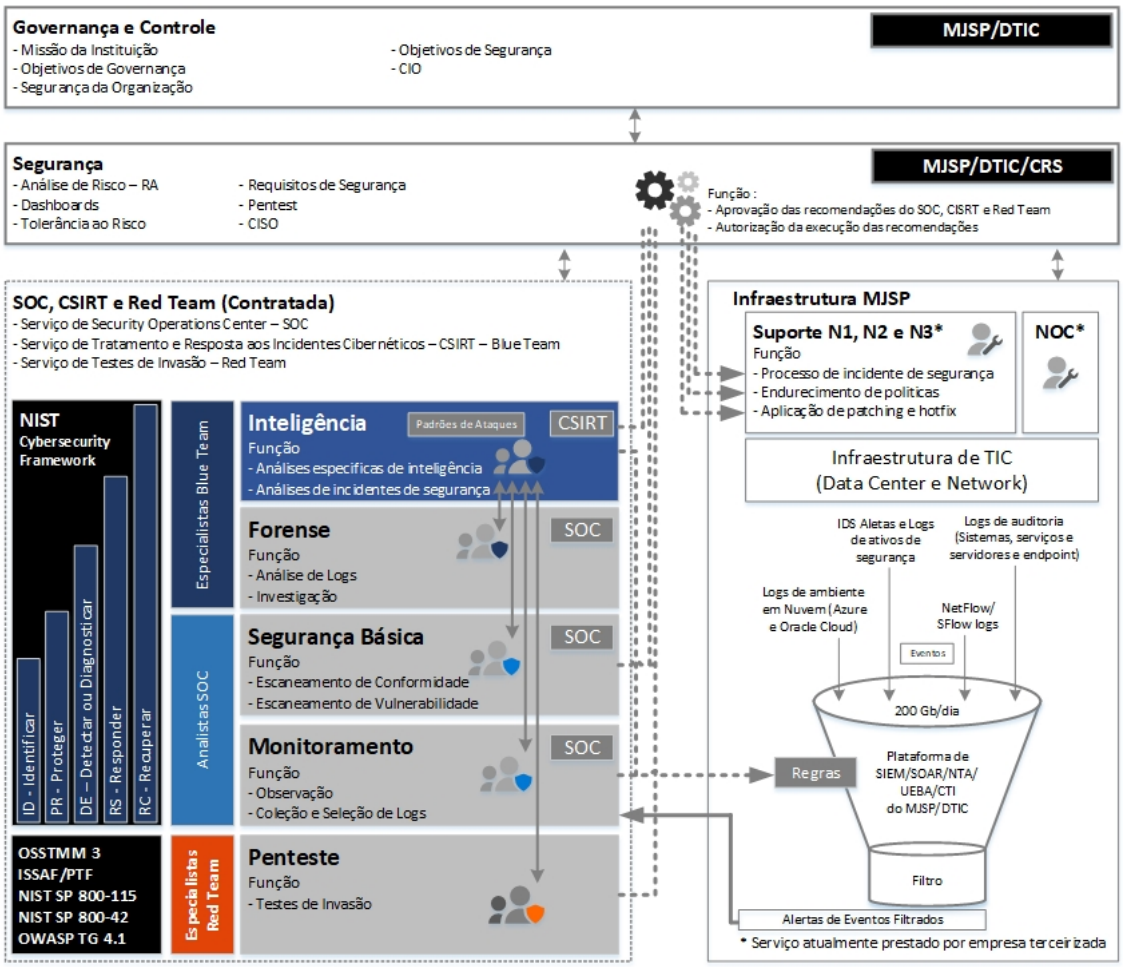

Figura 11 - Diagrama de relacionamento dos serviços e seus respectivos componentes com os demais serviços da DTIC.

2.1.5. Na Figura 11 é apresentado o diagrama de interação, para a presente contração, entre o MJSP representado pela DTIC e a CRS com o papel de gestores estratégicos, táticos e operacionais com a Infraestrutura de TIC do MJSP e os serviços de SOC, de Tratamento e Resposta a Incidentes Cibernéticos e de Testes de Invasão.

2.1.5.1. A DTIC com o papel de Governança e Controle atuando na gestão estratégica realizando a conformidade e função:

2.1.5.1.1. Missão da Instituição;

2.1.5.1.2. Objetivos de Governança;

2.1.5.1.3. Segurança da Organização;

2.1.5.1.4. Objetivos de Segurança;

2.1.5.1.5. CIO (*Chief Information Officer*);

2.1.5.2. A CRS com o papel de Segurança atuando na gestão tática e operacional e realizando conformidade e funções:

2.1.5.2.1. Análise de Risco;

2.1.5.2.2. Dashboards;

2.1.5.2.3. Tolerância ao Risco;

2.1.5.2.4. Requisitos de Segurança;

2.1.5.2.5. Pentest;

2.1.5.2.6. CISO (*Chief Information Security Officer*);

2.1.5.2.7. Intermediando as ações de aprovação e autorizações das requisições entre o CSIRT e SOC com a Infraestrutura de TIC do MJSP;

2.1.5.3. O Serviços de SOC, CSIRT e Red Team executando de forma colaborativa e integrada e conforme o framework de segurança cibernética (CSF) do NIST para CSIRT e SOC, bem como OSSTMM 3, ISSAF/PTF, NIST SP 800-115 e 800-42 e OWASP TB 4.1 para o Red Team, os papeis:

2.1.5.3.1. Inteligência - através da equipe de especialistas Blue Team do CSIRT com as funções de Análise especificas de inteligência e de incidentes de segurança de acordo com os Padrões de Ataques;

2.1.5.3.2. Forense - através da equipe de especialistas Blue Team com as funções de Análise de Logs e Investigação;

2.1.5.3.3. Segurança Básica - através da equipe de analistas do SOC com as funções de Escaneamento de conformidade e vulnerabilidade;

2.1.5.3.4. Monitoramento - através da equipe de analistas do SOC com as funções de Observação e Coleção e Seleção de Logs dos alertas de eventos e realizando a ajustes devidos de regras da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do MJSP.

2.1.5.3.5. Pentest - através da equipe de especialistas Red Team com a função de Testes de invasão.

2.1.5.4. Infraestrutura de TIC do MJSP executando a sustentação do parque computacional com os papeis e componentes:

2.1.5.4.1. Suporte N1, N2 e N3 - através de equipe técnica terceirizada com a realização das funções do processo de incidente de segurança, endurecimento de políticas e aplicação de patching e hotfix, aprovadas pela CRS, de requisições feitas pela CSIRT, SOC e Red Team.

2.1.5.4.2. NOC - através de equipe técnica (atualmente terceirizada) com a monitoramento da infraestrutura de TIC.

2.1.5.4.3. Plataforma de SIEM/SOAR/NTA/UEBA/CTI do MJSP com um consumo aproximado de 200 GB/dia de eventos sendo:

2.1.5.4.3.1. Logs de ambientes em Nuvem (Azure e Oracle Cloud);

2.1.5.4.3.2. IDS Alertas e Logs de ativos de segurança;

2.1.5.4.3.3. NetFlow/ SFlow Logs;

2.1.5.4.3.4. Logs de auditoria (Sistemas, serviços, servidores e endpoint);

2.2. **Serviço de Security Operations Center - SOC**

2.2.1. O SOC funcionará de forma ininterrupta 24 horas por dia e 7 dias por semana realizando as seguintes atividades, não se restringindo somente a elas:

2.2.1.1. Monitoramento continuo e análise, predizendo, prevendo, detectando e respondendo efetivamente as ameaças de todos incidentes de segurança.

2.2.1.2. Gerar painéis dinâmicos e em tempo real da situação atual de segurança do Ministério informando através de um score o nível de segurança.

2.2.1.3. Atuar como suporte de primeiro nível aos incidentes de segurança identificando, classificando, interrompendo, catalogando todas as tentativas de ataque aos sistemas e à infraestrutura do ministério.

2.2.1.4. Demandar ao NOC ou ao Suporte N1, N2 e N3 da infraestrutura de TIC do Ministério medidas a serem tomadas para evitar ou conter incidente.

2.2.1.5. Atuar no sentido de interromper um incidente quando da inoperância do NOC ou suporte N1, N2 e N3, dentro dos serviços autorizados em reunião inicial entre a CONTRATANTE e CONTRATADA, os quais o SOC poderá agir em substituição ao NOC. Todas as ações tomadas devem ser posteriormente repassadas ao NOC ou suporte da infraestrutura e a CRS.

2.2.1.6. Outros serviços os quais o SOC atuará em substituição ao NOC, poderão ser definidos durante a vigência do contrato, por meio de reuniões entre a CONTRATANTE e a CONTRATADA

2.2.1.7. Atuar em harmonia com o NOC do ministério.

2.2.1.8. Prestar o serviço de SOC realizando a **detecção, triagem, investigação e resposta a incidente** de eventos utilizando Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério que possui as seguintes funções:

2.2.1.8.1. Camada de Automação:

2.2.1.8.1.1. Orquestração, Automação e Resposta de Segurança (Security Orchestration, Automation, and Response - SOAR);

2.2.1.8.2. Camada de Análise e Correlacionamento:

2.2.1.8.2.1. Monitoramento de estação de trabalho (Endpoint Detection and Response - EDR);

2.2.1.8.2.2. Análise de Tráfego de Rede (Network Traffic Analysis - NTA);

2.2.1.8.2.3. Análise de Comportamento de Usuário (User Entity and Behavior Analytics - UEBA);

2.2.1.8.2.4. Análise de Inteligência de Ameaças Cibernéticas (Cyber Threat Intelligence - CTI);

2.2.1.8.3. Camada de coleta:

2.2.1.8.3.1. Informações de segurança e gestão de eventos (Security Information and Event Management - SIEM).

2.2.1.9. Configurar, monitorar e operar a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério.

2.2.1.10. Caso as ferramentas de propriedade do Ministério não atendam a completa execução dos serviços objeto da presente contratação a contratada poderá adotar solução tecnológica complementar em termo de hardware e software.

2.2.1.11. A CONTRATADA poderá utilizar soluções de hardware e software proprietárias desde que previamente autorizadas pelo CONTRATANTE, arcando a CONTRATADA com todos os custos diretos e indiretos inerentes a utilização de solução tecnológica e seus licenciamentos necessários.

2.2.1.12. Garantir a implementação do Modelo Adaptativo de Arquitetura de Segurança para Proteção de ataques avançados da Gartner exibido na figura 10.

2.2.2. Prevê-se que o SOC funcionará como o centralizador de todas as informações de segurança da informação e suporte de primeiro nível, por isso, a necessidade de seu funcionamento ser ininterrupto. O dimensionamento da equipe do SOC será a cargo da contratada em quantitativo mínimo que garanta o monitoramento ininterrupto de seu funcionamento, a qualidade das informações prestadas e estar apta a atuar no estado da arte em termos de segurança da informação, assim como cumprir os Acordos de Nível de Serviço determinados.

2.3. **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team**

2.3.1. O **Blue Team** funcionará de forma ininterrupta associado ao SOC para atividades de apoio ao suporte de primeiro nível e contenção de ataques, bem com, para atividades e suporte de segundo nível em diante.

2.3.2. No que diz respeito ao time de primeiro nível, este atuará associado ao SOC de forma ininterrupta uma vez que o nível de qualificação para essas atividades são inferiores aos de segundo nível.

2.3.3. Considerando que a equipe de especialistas de atividades e suporte em segundo nível em diante exige uma qualificação elevada e visando uma redução dos custos na contratação, o Ministério estima que a necessidade por esse tipo de profissional poderá ser utilizada em horário comercial, quando em necessidade urgente devido a um ataque, ou sob demanda fora do horário comercial.

2.3.4. Destacam-se algumas atividades que a equipe de especialistas Blue Team será responsável, não se restringindo somente a estas:

2.3.4.1. Apoiar na atividade de configuração, manutenção e operação a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério, a partir das informações monitoradas pelo SOC realizando a correlação dos eventos e configuração de suas regras de inteligência.

2.3.4.2. Atuar como suporte de segundo nível em diante.

2.3.4.3. Defender o ministério nos incidentes de segurança.

2.3.4.4. Promover a melhoria da segurança da informação do Ministério.

2.3.4.5. Fazer cessar ou interromper os ataques à infraestrutura do Ministério.

2.3.4.6. Atuar em harmonia com o NOC do Ministério.

2.3.4.7. Atuar sob orientação do **CRS** quando de análises realizadas pelo **Red Team**.

2.3.4.8. Sugerir melhorias na segurança da informação do ministério a partir das melhores práticas internacionais.

2.3.4.9. Prover a transferência de conhecimento ao corpo técnico da CRS de sistemas, produtos e soluções utilizados com o fornecimento de perfil de acesso para a supervisão dos serviços prestados.

2.3.4.10. Implantar, configurar e suportar as tecnologias necessárias ao melhoramento da segurança da informação do Ministério.

2.3.4.11. Prover relatórios sob demanda.

2.3.4.12. Manter em funcionamento o painel de segurança da informação com as informações definidas de indicadores de performance e níveis de serviços acordados.

2.3.5. Analisar, remediar, conter e documentar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado obedecendo os frameworks de segurança cibernética do NIST CSF (Cybersecurity Framework) e boas práticas de mercado ou framework definido pelo Ministério.

2.3.6. Monitoramento da rede sociais, Dark Web e Deep Web com ferramentas adequadas para monitoramento de informações sensíveis e de interesse do Ministério a respeito de segurança da cibernética.

2.3.7. Apoiar a CRS na avaliação, elaboração e revisão de relatórios segurança e privacidade.

2.4. **Serviço de Teste de Invasão - Red Team**

2.4.1. O **Red Team** funcionará sob demanda da CRS sem o conhecimento dos outros entes.

2.4.2. Muitas vezes pelo fato de uma equipe estar diretamente associada aos eventos de monitoramento, configuração e suporte, algumas brechas deixam de ser observadas, não por descuido, mas por uma "visão de túnel". Diante disso, torna-se crucial que exista uma equipe que possa ter uma visão externa ao processo e é nesse cenário que o **Red Team** torna-se essencial.

2.4.3. Destacam-se algumas atividades que o **Red Team** será responsável, sob demanda, não se restringindo somente a estas:

2.4.3.1. Infligir ataques a infraestrutura de segurança interna e externa de rede e sistemas do ministério de modo não destrutivo.

2.4.3.2. Realizar tentativas de Data Exfiltration, Internal & External Reconnissance, ShadowMap Scan, Vulnerability Assessment, Social Engineering, Exploitaion, Pivoting / Lateral Movements, entre outros, a rede e aos sistemas do ministério, obedecendo o framework de segurança MITRE ATT&CK que utiliza base global de conhecimento das táticas, técnicas e procedimentos (TTP's) utilizados por atacantes para avaliar a efetividade dos controles de segurança.

2.4.3.3. Gerar relatórios detalhado das tentativas.

2.4.3.4. Sugerir após o ataque melhorias na infraestrutura a serem implementadas pela equipe de Infraestrutura de TIC do Ministério com o apoio da equipe de **Blue Team**, após as devidas aprovações e autorizações da CRS.

2.4.4. O time de Red Team deve ser independente do **Blue Team**. Além disso, os dias de suas incursões não devem ser de conhecimento da equipe de defesa.

2.5. Os serviços citados anteriormente justificam-se devido ao diminuto corpo técnico do Ministério da Justiça e Segurança Pública, visando a não interrupção e o tratamento efetivo das descobertas do Red Team.

3. **ANÁLISE DE SOLUÇÕES**

3.1. **IDENTIFICAÇÃO DAS SOLUÇÕES**

3.1.1. Foram identificadas 4 possíveis soluções, conforme relacionadas na tabela 4.

Tabela 4 - Possíveis soluções

Id	Descrição da Solução
1	Realização dos Serviços de SOC, Blue Team, Red Team e Purple Team pelos servidores lotados na Coordenação de Riscos e Segurança do Ministério da Justiça e Segurança Pública
2	Ampliação da Contratação do Network Operations Center - NOC
3	Aquisição de Equipamentos de Segurança e/ou Softwares
4	Contratação como Serviço

3.2. **ANÁLISE COMPARATIVA DE SOLUÇÕES**

3.2.1. Na tabela 5 é realizada uma análise comparativa de soluções, que foram mapeadas no MJSP.

Tabela 5 - Análise Comparativa de soluções

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3		X	
	Solução 4			X

Requisito	Solução	Sim	Não	Não se Aplica
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3		X	
	Solução 4			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X

4. **REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS**

4.1. **Solução 1**

4.1.1. **Descrição:** A solução um considera a utilização do corpo de servidores lotados na Coordenação de Risco e Segurança - CRS para desempenhar as tarefas de SOC, Blue Team, Red Team e Purple Team.

4.1.2. **Justificativa:** Segundo dados do Portal de Gestão de Pessoas, disponível na intranet em maio de 2021, a força de trabalho do Ministério da Justiça e Segurança Pública é de 1.333 pessoas, sendo que destas apenas 410 são do quadro próprio, ou seja, correspondem ao ativo permanente do órgão, conforme apresentado na figura 12.

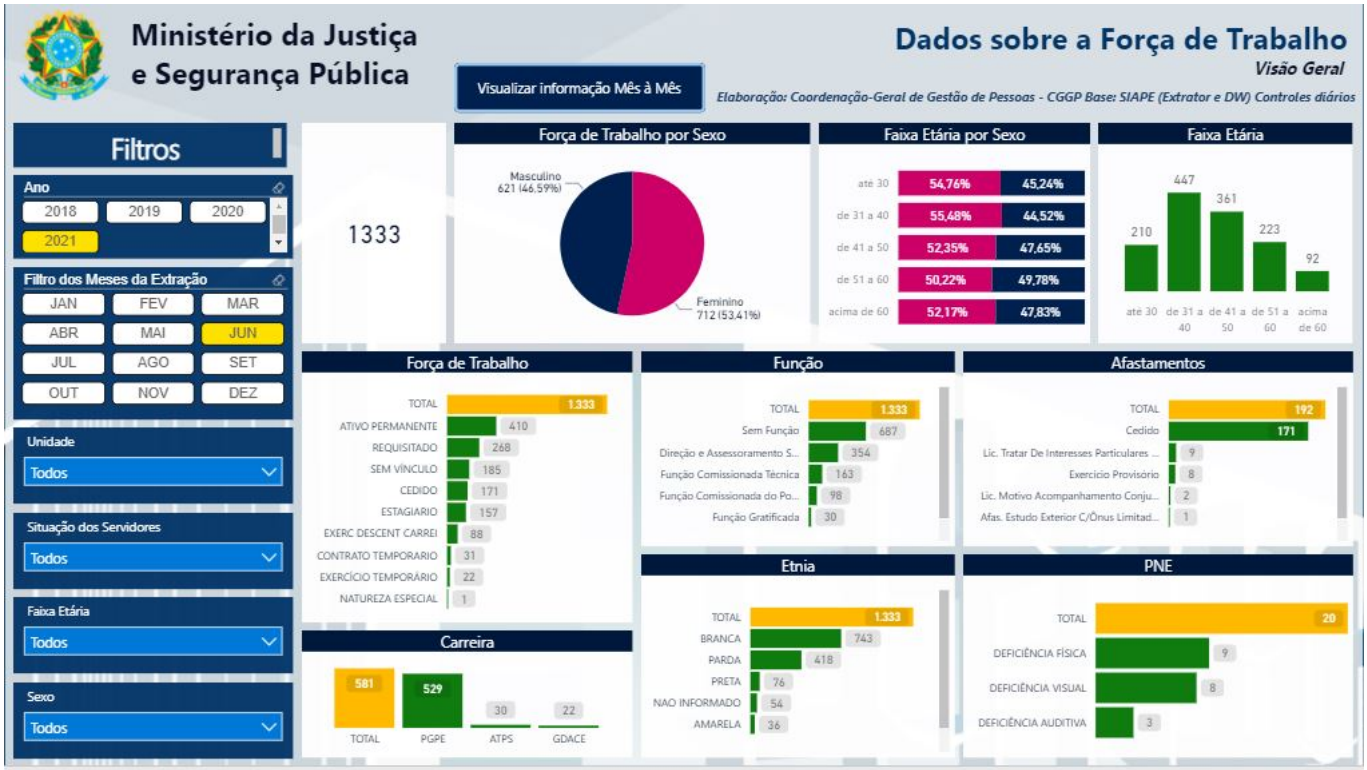

Figura 12 - Força de trabalho do MJSP, Fonte: Portal Gestão de Pessoas, disponível em https://justicagovbr.sharepoint.com/sites/intra-CGGP/SitePages/For%C3%A7a-de-Trabalho.aspx, acesso em 09/06/2021.

4.1.3. Na Diretoria de Tecnologia da Informação e Comunicação são 78 pessoas, sendo que destas apenas 8 são do quadro de ativo permanente, conforme apresentado na figura-13.

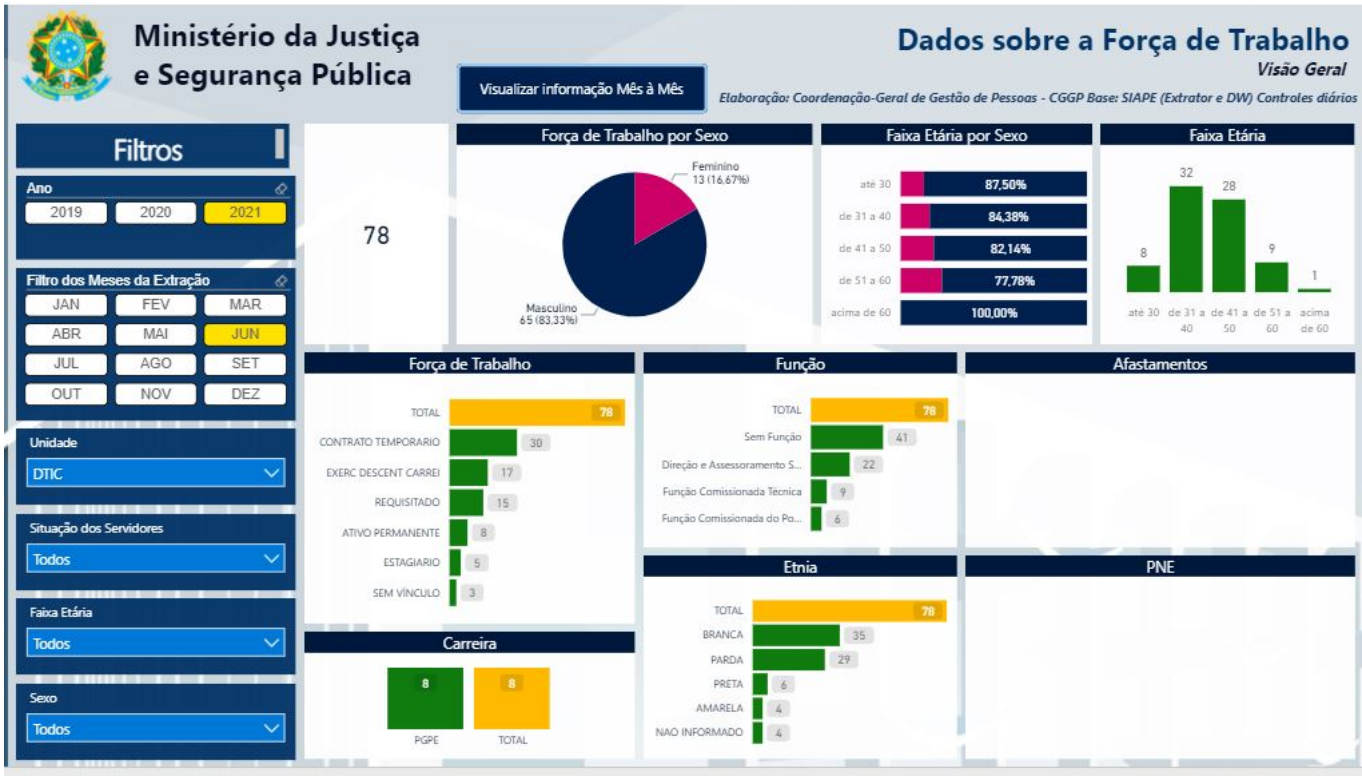

Figura 13 - Força de trabalho da DTIC, Fonte: Portal Gestão de Pessoas, disponível em **https://justicagovbr.sharepoint.com/sites/intra-CGGP/SitePages/For%C3%A7a-de-Trabalho.aspx**, acesso em 09/06/2021.

4.1.4. Baseado nas recomendações da Gartner, o estudo "Como planejar, projetar, operar e evoluir um SOC" publicado em 6 de setembro de 2018 (https://www.gartner.com/document/3889122?ref=cust_reco_sdemail&docType=RESEARCH), um dos pré-requisitos para implantar o SOC:

> *"um SOC 24/7 interno exigirá uma equipe de oito a 12 pessoas no mínimo. Se não houver esses recursos, comece seu planejamento de SOC com uma opção híbrida que depende substancialmente de um ou mais provedores de serviços, em particular para funções que precisam de cobertura 24 horas por dia, 7 dias por semana."*

4.1.5. Baseado nas recomendações da Gartner, considerando o quantitativo de pessoas do quadro de ativo permanente na Diretoria de Tecnologia e Comunicação, conforme item 4.1.3, e considerando o quantitativo de ativos instalados no MJSP, de acordo com Relatório sobre Informações da Infraestrutura do MJSP SEI (14628328), a criação de um SOC com pessoal interno não seria viável.

4.1.6. Verifica-se que o atual modelo de contratações, por meio a compra de produtos e a contratação de serviços de operação, não são suficientes para fazer frente à velocidade com que surgem novos tipos de ameaças, e principalmente, a velocidade com que o mercado de segurança evolui e lança novos produtos. Diante deste cenário, o Gartner desenvolveu o conceito de Managed Security Services - MSS. Neste modelo empresas especialistas de segurança, atuando por meio de Security Operations Center – SOC, ofertam diversas soluções de segurança na modalidade de serviço. As maiores vantagens desta modalidade são:

- Maior flexibilidade com relação à aquisição de produtos;
- Os serviços podem ser contratados sob demanda, conforme a necessidade e disponibilidade financeira do cliente;
- Maior velocidade de inserção de novas tecnologias;
- Utilização de profissionais altamente capacitados e especialistas em cibersegurança, que dificilmente atuariam em um único cliente de pequeno porte;
- Menor custo total de propriedade (Total Cost of Ownership – TCO), tendo em vista os custos de compra, operação e capacitação contínua a longo prazo.

4.1.7. É importante destacar que no caso específico do segmento de informática, o processo de execução indireta tem se consolidado nos últimos anos, em decorrência das normas legais, de orientações do TCU e do seu comprovado sucesso. Ele desonera as organizações dos altos custos de operação e manutenção da infraestrutura do ambiente de tecnologia da informação, especialmente quanto aos esforços diretos e indiretos de manutenção e para aperfeiçoamento de quadro de profissionais especializados nestas atividades. Ainda, possibilita ao quadro técnico interno dedicar-se às principais tarefas definidas em seu Regimento Interno do Ministério da Justiça e Segurança Pública:

I - elaborar, estabelecer, manter e propor mudanças nas políticas, normas, controles e metodologias de Gerenciamento de Riscos e de Segurança da Informação de TIC do Ministério;

II - coordenar a elaboração da Política de Segurança da Informação e Comunicações – POSIC e demais planos ou normas relacionados à segurança da informação da TIC;

III - promover e disseminar a cultura de Gerenciamento de Segurança de TIC;

IV - assessorar o Comitê de Segurança da Informação nas questões que envolvem tecnologias em segurança da informação e comunicações;

V - planejar, coordenar e controlar as ações associadas à Segurança da Informação e Comunicações de TIC;

VI - prospectar e propor a adoção de mecanismos, equipamentos e recursos para melhoria da segurança de TIC;

VII - acompanhar e monitorar as atividades, operações e incidentes de segurança de TIC, atuando quando necessário em seu bloqueio em última instância;

VIII - identificar as necessidades de qualificação técnica de sua equipe;

IX - gerenciar as divisões vinculadas à área de atuação da coordenadoria;

X - atuar de forma integrada e sistêmica com as coordenações e divisões da DTIC;

XI - realizar análises, varreduras, inspeções, prospecções, testes e auditorias de segurança no âmbito do ministério; e

XII - desempenhar outras competências típicas da unidade, delegadas pela autoridade superior ou conforme determinação legal.

4.1.8. Diante do exposto acima, é necessária a terceirização de parte dos serviços operacionais, permanecendo sob responsabilidade do quadro de servidores, as funções de gestão e de planejamento, intransferíveis para empresas terceirizadas.

4.1.9. Apesar de ter sido realizando um concurso para servidores temporários no Ministério da Justiça e Segurança Pública esse concurso não previu vagas para a especialidade de segurança da informação. Ainda que houvesse vagas nesse concurso, seria necessário também viabilizar, do ponto de vista normativo e operacional, a utilização de servidores do órgão em regime de escala de trabalho e/ou de plantão 24x7, considerando que os incidentes de segurança da informação não possuem hora específica para ocorrer. Atualmente não é permitido no âmbito do Ministério o regimento de escala de trabalho e/ou de plantão 24x7 para os seus servidores. Desta forma, essa solução é considerada inviável.

4.2. **Solução 2**

4.2.1. **Descrição:** A solução dois considera a ampliação da Contratação do Network Operations Center - NOC para desempenhar as tarefas de SOC, Blue Team, Red Team e Purple Team.

4.2.2. **Justificativa:** O Ministério da Justiça e Segurança Pública possui o Contrato nº 40/2019 (10267604), o qual tem por objeto a prestação de serviço de *service desk* e sustentação de infraestrutura de tecnologia para organização, desenvolvimento, implantação e execução continuada de tarefas de suporte, rotina e demanda, compreendendo atividades de suporte técnico de 1º, 2º e 3º níveis, a usuários de tecnologia da informação do MJSP, abrangendo a execução de rotinas periódicas orientação e esclarecimento de dúvidas e recebimento, registro, análise, diagnóstico e atendimento de solicitações de usuários, sustentação e projetos de evolução do ambiente de infraestrutura tecnológica e gerenciamento de processos de Tecnologia da Informação e Comunicações - TIC.

4.2.3. Dentre os vários serviços incluídos no contrato supracitado está o NOC, responsável pela monitoração da infraestrutura de TIC, conforme definido no Termo de Referência (9629880), referente a contratação de empresa especializada na prestação de serviço de *service desk* e sustentação de infraestrutura de tecnologia para organização.

4.2.4. Um *Network Operations Center* - NOC, "é responsável por lidar com incidentes que afetem a performance ou disponibilidade, enquanto o SOC lida com incidentes de segurança que afetam os ativos de segurança"[1].

4.2.5. O NOC lida com problemas relacionados ao gerenciamento, monitoramento e controle das redes dentro da infraestrutura. Isso inclui servidores, máquinas virtuais e bancos de dados. Esses itens mantêm o fluxo de dados para os aplicativos e sistemas usados pelo órgão. Quando a rede, site, servidores ou aplicativos caem, o NOC é responsável por encontrar a origem do problema e fazer tudo funcionar novamente. Eles estão garantindo que a infraestrutura de TI permaneça em funcionamento.

4.2.6. Outras funções do NOC incluem relatórios de desempenho e recomendações de melhoria, resposta à interrupção, planejamento de capacidade, alerta de acordo com procedimentos de escalação definidos e garantir a coordenação entre redes díspares.

4.2.7. Ter uma equipe NOC pronta para monitorar e resolver os problemas antes que eles se manifestem aos usuários funciona melhor para minimizar o tempo de inatividade do órgão. Os NOCs geralmente têm uma sala de controle central configurada para vigiá-los e alertá-los sobre possíveis complicações que ameaçam a infraestrutura de uma organização.

4.2.8. Enquanto um NOC trabalha para manter as redes, aplicativos e outros equipamentos em funcionamento, um SOC (Security Operations Center) rastreia ameaças inteligentes que fazem tentativas hostis de entrar na infraestrutura de uma organização. Esses esforços podem vir de dentro ou de fora da organização, incluindo malwares e outros softwares suspeitos projetados para roubar dados ou causar interrupção na rede.

4.2.9. Cabe a um SOC proteger as organizações contra e-mails contendo vírus e outras ameaças acessadas acidentalmente pelos funcionários. Eles rastreiam tentativas não autorizadas de entrar na rede de uma organização, usando ferramentas de monitoramento de segurança e outros recursos para aprender os padrões e se adaptar às táticas usadas.

4.2.10. Outras funções SOC incluem, mas não se limitam a, monitorar e impedir o vazamento de dados, avaliar novos softwares para vulnerabilidades, manter as ferramentas de segurança e patches atualizados, acompanhar tendências relacionadas a diferentes ameaças cibernéticas, implementar medidas anti-DDOS e executar testes de intrusão. A tabela 6 apresenta as principais diferencias entre os conceitos de NOC e SOC.

Tabela 6 - Diferença entre NOC E SOC

DIFERENÇAS	NOC	SOC
Significado da sigla	Centro de Operações de Rede (Network Operations Center).	Centro de Operações de Segurança (Security Operations Center).
Terminologia	Usado para lidar com desafios relacionados ao gerenciamento, monitoramento e controle das redes no ecossistema de TI do cliente.	Rastreia ameaças à infraestrutura, fazendo tentativas de usar a vulnerabilidade e entrar em uma rede.
Papel fundamental	Para cumprir acordos de nível de serviço e gerenciar incidentes relacionados a disponibilidade para atingir o tempo de atividade máximo.	Para proteger a propriedade intelectual, proteger as informações confidenciais do cliente e gerenciar incidentes relacionados a disponibilidade, integridade e confidencialidade.
Objetivos	Para monitorar o desempenho.	Para monitorar a segurança.
Tecnologia	Acesso a dados em tempo real.	Acesso a dados em tempo real e históricos.
Ferramentas	Software de monitoramento de falhas, problemas e desempenho.	Qualidade de serviço, experiência do cliente e software de marketing.
Habilidades	* Infraestrutura de rede * Análise de dados, * Solução de problemas e * Conhecimento de tecnologia.	* Infraestrutura de segurança * Modelagem de serviço * Interpretação de dados * Comunicação.
Métricas	Abordagem reativa.	Abordagem reativa e proativa.

DIFERENÇAS	NOC	SOC
Impacto nos negócios	Operacional.	Estratégico.

Fonte: adaptado de https://ipwithease.com/noc-vs-soc/

Nota: 1 - SOC vs NOC, qual a diferença?. <https://realprotect.net/blog/qual-diferenca-security-operations-center-soc-vs-network-operations-center-noc/> Página da internet. Acesso em 13/05/2021.

4.2.11. Percebe-se que as atividades desempenhadas por ambos os centros de operação são diferentes, um destinado a segurança da informação enquanto o outro a infraestrutura de redes.

4.2.12. Isso posto, a possível solução de ampliar o Contrato nº 40/2019 (10267604) para desempenhar as tarefas de SOC, Blue Team, Red Team e Purple Team torna-se inviável, pois poderia ser considerado como uma alteração do objeto licitatório, uma vez que incluiria serviços não previstos originalmente na licitação.

4.2.13. Além disso, não é recomendável que quem proveja os serviços de rede verifique se ela é efetivamente segura uma vez que, muitas vezes, falhas na verificação do próprio trabalho podem acontecer. A norma ISO 27001 considera a segregação de funções no Sistema de Gestão de Segurança da Informação (SGSI) para minimizar o risco de uma única posição possa ter a oportunidade de comprometer as atividades de uma organização.

4.2.14. A principal razão de se aplicar a segregação de funções é prevenir a realização e ocultação de fraude e erro no curso normal das atividades, uma vez que havendo mais de uma pessoa para realizar uma atividade se minimiza a oportunidade de transgressões e aumenta as chances de se detectá-la, assim como de se detectar erros não intencionais.

4.3. **Solução 3**

4.3.1. **Descrição:** A solução três considera a aquisição de Equipamentos de Segurança e/ou Softwares para desempenhar as tarefas de SOC, Blue Team, Red Team e Purple Team.

4.3.2. **Justificativa:** A simples aquisição de equipamentos ou softwares de segurança não exime a necessidade de pessoas para operá-los. Não adianta ter diversos alarmes, indicadores, sugestão ou inteligência artificial sem que se tenha o ente humano para tratar os alarmes, observar os indicadores, implementar as sugestões ou programar e manter a inteligência artificial.

4.3.3. Atualmente o Ministério da Justiça e Segurança Pública possui, como é possível observar no no **relatório de informações sobre a infraestrutura** (14628328), um vasto *pool* de Tecnologias, sendo o elo mais fraco dessa corrente de segurança da informação a quantidade de pessoas dedicadas a análise, monitoramento, controle e gestão dessas tecnologias.

4.3.4. Por isso, a simples aquisição de mais tecnologia apenas irá aumentar esse *pool*, não aumentando a segurança da informação do Ministério.

5. **ANÁLISE COMPARATIVA DE CUSTOS (TCO)**

5.1. **CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE**

5.1.1. **Solução Viável 4**

5.1.2. **Descrição: Contratação de um SOC, Blue Team, Purple Team e Red Team como serviço**

5.1.3. De acordo com o curso PCTI - Planejamento da Contratação de TI da Escola Nacional de Administração Pública - ENAP, em seu Módulo 2 - Análise de Viabilidade da Contratação e Plano de Sustentação (figura-13), temos que:

Total Cost of Ownership - TCO

O *Total Cost of Ownership* ou Custo Total de Propriedade é um critério de escolha entre alternativas tecnológicas muito utilizado no setor privado. Este conceito defende que, ao se comparar duas ou mais Soluções de Tecnologia da Informação, não se deve considerar apenas o custo de aquisição (ou de desenvolvimento) de cada uma delas. Deve-se considerar o custo total que a aquisição e consequente propriedade daquele ativo trará ao contratante. Engloba, assim, custos de aquisição/desenvolvimento, instalação, treinamento, operação e manutenção.

Figura 14 - TCO - Total Cost of Ownership. Disponível em: https://repositorio.enap.gov.br/bitstream/1/1131/1/M%C3%B3dulo_2.pdf, atualizado em: dezembro de 2013. Acesso em 13/05/2021.

5.1.4. Das soluções apresentadas na tabela 4, apenas a solução 4, item 5.1.1, ou seja, a contratação da solução como serviço se mostra viável devido as características e especificidades do Ministério. Além disso, a contratação do serviço de SOC não envolverá aquisição por parte do Ministério da Justiça e Segurança Pública de qualquer bem, software ou sistema. Apenas o serviço prestado de SOC, Blue Team, Purple Team e Red Team será contratado. Os ativos, bens, sistemas, insumos necessários a execução do serviços que forem providos pela contratada, em complemento aos disponibilizados pelo Ministério, serão devolvidos ao final do contrato, exceto as informações produzidas durante a prestação do serviço.

5.1.5. Diante disso, para estimar o custo total de propriedade, utilizaremos uma contratação similar, realizada pelo Conselho da Justiça Federal do DF, Pregão Eletrônico nº 1 de 2020, ocorrida no dia 05 de fevereiro de 2020.

5.1.6. Devido as características e especificidades tanto do Conselho da Justiça Federal do DF quanto do Ministério da Justiça e Segurança Pública, adaptações serão realizadas e justificadas.

5.1.7. O pregão do CJF considerou a contratação dos seguintes itens:

1. **Item 1 do pregão- Serviço de operação e atendimento a requisições**: para sustentar e operar todas as soluções e produtos de segurança do CJF, bem como a realização permanente de ações proativas (gap analysis) voltadas para a segurança do parque computacional do CJF com o objetivo de mantê-lo estável, disponível e integro.
2. **Item 2 do pregão - Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)**: para analisar, remediar, conter e documentar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação, obedecendo os principais frameworks de gestão de incidentes de segurança da informação e boas práticas de mercado.

3. **Item 3 do pregão - Serviço de gestão de vulnerabilidades**: que tem por objetivo, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação no ambiente a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas.
4. **Item 4 do pregão - Serviço de monitoramento e visibilidade de ataques cibernéticos**: visando o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao CJF, através de correlacionamento de logs, análise de pacotes de rede, comportamento anômalo de usuários, aplicações, serviços e infraestrutura que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação.
5. **Item 5 do pregão - Serviço de orquestração, automação e resposta de segurança (SOAR)**: serviços e infraestrutura que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação.
6. **Item 6 do pregão - Serviço de testes de invasão (Red Team)**: tem como objetivo principal identificar, mapear e documentar possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações, bem como a indicação de soluções para a correção das vulnerabilidades encontradas.

5.1.8. O presente Estudo Técnico Preliminar visa a contratação, conforme expresso alhures, dos seguintes itens:

5.1.8.1. **Serviço de Security Operations Center - SOC**: conforme item 2.2 deste estudo.

5.1.8.2. **Serviço de Blue Team**: conforme item 2.3 deste estudo.

5.1.8.3. **Serviço de Red Team**: conforme item 2.4 deste estudo.

5.1.9. A tabela 7 apresenta a comparação dos serviços contratados pelo CJF com os serviço almejados pelo Ministérios da Justiça e Segurança Pública chegamos as seguintes conclusões de equivalência, quando possível.

5.1.10. Cabe registrar que a ata do pregão do Conselho da Justiça Federal - CJF foi inserido no presente processo sob o numero de documento (13624102). Foi inserido no presente processo o Edital do Conselho da Justiça Federal, sob o número de documento (13624084).

Tabela 7 - Equivalência dos serviços contratados pelo CJF e os almejados pelo MJSP.

MJSP	CJF
Serviço de Security Operations Center - SOC	Serviço de operação e atendimento a requisições
Serviço de Blue Team	Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)
Serviço de Red Team	Serviço de testes de invasão (Red Team)

5.1.11. Além da equivalência devemos comparar o tempo de prestação dos serviços no CJF com os desejados pelo MJSP. Visando comparar os serviços para ambos os órgãos criamos a tabela 8.

Tabela 8 - Método de comparação utilizado para estimar o valor.

MJSP	Prestação	CJF	Prestação		Forma de Comparação
Serviço de Security Operations Center - SOC	24h x 7 dias	Serviço de operação e atendimento a requisições	Segunda-feira até Sexta-feira		Será dividido o valor dos itens pelas quantidades de horas contratadas e multiplicado pela necessidade do MJSP
			Remoto	Presencial	
			9h até 20h = 11 horas	13h até 21h = 8h	
Serviço de Blue Team	Horário Comercial	Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)	24h x 7 dias 1 vez por mês		Será dividido o valor dos itens pelas quantidades de horas contratadas e multiplicado pela necessidade do MJSP
Serviço de Red Team	Sob demanda	Serviço de testes de invasão (Red Team)	Sob demanda por sistema (15 Sistemas)		Será utilizado valor integral devido aos itens serem equivalentes
Serviço de Purple Team	Não comparado por estar incluído nos outros serviços ou não estar relacionado com prestação em horas.				

5.1.12. Considerando as tabelas 7 e 8 chegamos aos custos por hora e serviço para o CJF, apresentados na tabela 9:

Tabela 9 - Custo final por hora ou serviço

Serviço CJF	Custo do Item de Serviço e Quantidade de Horas	Total final por hora ou serviço [2]
Serviço de operação e atendimento a requisições	Horas por mês de 22 dias úteis com 11 horas remotas por dia: 242 horas Valor [1] do item 1 por mês: R$ 56.520,00	R$ 233,55 por hora
Serviço de monitoramento e visibilidade de ataques cibernéticos	15GB/dia ou 440 EPS R$ 8.705,62	R$ 580,37 por GB/dia
	1000 ativos R$ 4.249,97	R$ 4,24 por ativo
	1 Gbps	R$ 13.261,75 por 1 Gbps

	R$ 13.261,75	
Serviço de orquestração, automação e resposta de segurança (SOAR)	24h x 7 dias R$ 24.670,00	R$34,26 por hora
Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)	24h x 7 dias R$ 18.443,65	R$ 25,62 por hora
Serviço de testes de invasão (Red Team)	Para 1 sistemas que geralmente possui 10 alvos em média R$ 11.508,40	R$ 11.508,40 por sistema ou R$ 1.150,84 por alvo
Serviço de gestão de vulnerabilidades	Uma vez por mês independente do tempo que levar para conclusão R$ 17.040,65	R$ 17.040,65

1 Ata do pregão publicado no comprasnet (http://comprasnet.gov.br/livre/pregao/ata2.asp?co_no_uasg=90026&numprp=000012020&f_lstSrp=T&f_Uf=DF&f_numPrp=12020&f_coduasg=&f_tpPregao=E&f_lstICMS=T&f_dtAberturaIni=&f_dtAberturaFi
2 Considerado um mês de 30 dias.

5.1.13. Diante das equivalências demonstradas pela Tabela 7, 8 e 9, podemos estimar o custo total de propriedade para a contratação dos serviços no MJSP. Conforme tabela 10. Os serviços "Serviço de monitoramento e visibilidade de ataques cibernéticos", "Serviço de orquestração, automação e resposta de segurança (SOAR)" e "Serviço de gestão de vulnerabilidades" não foram considerados por tratarem de serviços relacionados a contratação de software, que não são objeto da contratação sendo realizada pelo MJSP.

Tabela 10 - Custo estimado para o MJSP.

Custo Total de Propriedade – Memória de Cálculo

Com o auxílio das tabelas 7, 8 e 9 chegamos a uma estimativa para o custo de uma possível contratação para o Ministério da Justiça e Segurança Pública, que é apresentado na tabela 10:

Serviço MJSP	**Serviço CJF associado**	**Valor por hora ou Serviço**	**Quantidade horas ou serviço MJSP**	**Total**
Serviço de Security Operations Center - SOC + Blue Team Suporte Nivel 1	Serviço de operação e atendimento a requisições	R$ 233,55 por hora	24h x 7 dias = 720 horas 720 x 24 meses = 17.280	17.280 x R$ 233,55 =**168.156,00 por mês e R$ 4.035.744,00 por 24 meses**
Serviço de Blue Team Suporte Nível 2 em diante	Serviço de gestão de incidentes de segurança (CSIRT - Blue Team)	R$ 25,62 por hora	24h x 7 dias = 720 horas 720 x 24 meses = 17.280	720 horas x R$ 25,62 = **R$ 18.446,40 por mês e R$ 442.713,60 por 24 meses**
Total Mensal (Continuo):				**R$186.602,40**
Serviço de Red Team	Serviço de testes de invasão (Red Team)	R$ 1.150,84 por alvo	Sob demanda 217 Sistemas + 14 Appliance de Segurança + 110 Ativos de Rede + 68 Host Físico no Datacenter + 400 Sistemas Operacionais de Servidores + 18 Sistemas de Armazenamento = 827 alvos Considerando que um sistema possui em média 10 ativos (Gateway de Rede, Firewall, DNS, Balanceador de Carga, Firewall de APP, 2x Servidores de App, 2x Servidores de Transação, Servidor de Banco de Dados - Clusterizado dentre outros ativos)	827 alvos x R$ 1.150,84 = R$ 951.744,68 / 24 meses **= 39.656,02 por mês**
Total (sob demanda):				**R$ 951.744,68**
Total 24 meses				R$ 5.430.202,28

5.1.14. Cabe o registro de que equipe de planejamento buscou junto a contratações similares, mas não encontrou uma métrica precisa e comum de mercado para definir o quantitativo e variação dos serviços de SOC sem considerar a contratação de software. Nesse sentido o dimensionamento da equipe para execução adequada dos serviços será de responsabilidade da CONTRATADA, devendo ser suficiente para o cumprimento integral dos níveis mínimos de serviço exigidos.

5.1.15. Considerando o valor mensal de **R$ 186.602,40** referente aos serviços contínuos, foi multiplicado por 12 meses, para chegar ao valor anual de **R$ 2.239.228,80** e somado a metade do valor estimado referente ao serviço de testes de invasão (Red Team) de 24 meses que é de R$ **475.872,34**, chega-se ao total de **R$ 2.715.101,14** para 12 meses, conforme valores unitários e totais da tabela 10**.**

5.2. **MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)**

5.2.1. A tabela 11 apresenta a estimativa dos cálculos totais de propriedade para os próximos 5 anos, conforme memória de cálculo explicada no item 5.1.14. Não foram identificadas métricas de variação para a contratação que não esteja relacionada ao ICTI (índice de custo da tecnologia da informação) ou a valores de repactuação que poderão ocorrer. O valor pago por hora para a contratação de serviço não envolve software ou log em sua formação e não foi identificada relação adotada pelos fornecedores na variação de pessoas em uma equipe de SOC que pudesse compor a variação dos valores abaixo.

Tabela 11 - Estimativa dos cálculos totais de propriedade para os próximos 5 anos

Descrição da solução	Estimativa de TCO ao longo dos anos					Total para 5 anos de Contratação
	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5	
Solução Viável 4	**R$ 2.715.101,14**	R$ **2.715.101,14**	R$ **2.715.101,14**	R$ **2.715.101,14**	R$ **2.715.101,14**	**R$13.575.505,70**

DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

5.3. A solução de contratação de um SOC, Blue Team e Red Team terá o seu detalhamento realizado junto ao Termo de Referência, porém, podemos descrever essa solução com menos detalhes visando obter junto a fornecedores no mercado uma estimativa de custos dessa contratação. Dessa forma, passamos a descrever em mais detalhes, mas ainda superficialmente as características da solução.

5.4. Após análise de uma contratação similar junto ao Conselho de Justiça Federal, chegou-se a conclusão que contratar em itens separados um Purple Team não traria benefícios concretos a essa contratação e dessa forma, optou-se por inserir esses serviços nos demais itens sendo seus detalhes explicitados no Termo de Referência. Devido a essa opção, optou-se também por estender o serviço de Blue Team de suporte em segundo nível também de forma ininterrupta atuando em sincronia com o SOC.

5.4.1. A solução será composta por 3 (três) itens de serviço integrados, não se limitando aos descritos abaixo, os quais serão detalhados no Termo de Referência:

5.4.1.1. **Serviço de Security Operations Center - SOC;**

5.4.1.2. **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team;**

5.4.1.3. **Serviço de Testes de Invasão - Red Team;**

5.4.1.4. **O Serviço de Security Operations Center - SOC** e o **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team** atuarão em conjunto e envolve os seguintes serviços, conforme *Information Technology Infraestructure Library* – ITIL e com as atividades dos processos do volume de **Transição de Serviços e Operação de Serviços**;

5.4.1.4.1. Gerenciamento de Configurações e de Ativo de Serviços;

5.4.1.4.2. Gerenciamento de Mudanças;

5.4.1.4.3. Gerenciamento de Liberações e Implantação;

5.4.1.4.4. Gerenciamento do Conhecimento;

5.4.1.4.5. Gerenciamento de Evento;

5.4.1.4.6. Gerenciamento de Incidente;

5.4.1.4.7. Gerenciamento de Problema;

5.4.1.4.8. Gerenciamento de Requisição;

5.4.1.4.9. Gerenciamento de Acesso;

5.4.1.4.10. Desempenhar atividades de 3º nível de **Operação de Serviços** das funções:

5.4.1.4.10.1. Central de Serviços;

5.4.1.4.10.2. Gerenciamento de Operações de TI (Controle de Operações de Segurança da Informação);

5.4.1.4.10.3. Gerenciamento Técnico;

5.4.1.4.10.4. Gerenciamento de Aplicação;

5.4.1.4.11. Ambos os serviços desempenharão os seguintes objetivos e propósitos:

5.4.1.4.11.1. Gerenciar a capacidade e recursos requeridos para empacotar, construir, testar e implementar as liberações no ambiente de produção.

5.4.1.4.11.2. Estabelecer e manter a integridade dos ativos de serviços e suas configurações.

5.4.1.4.11.3. Prover conhecimento de qualidade para a organização.

5.4.1.4.11.4. Prover mecanismos de implementação eficientes e padronizados.

5.4.1.4.11.5. Garantir que os serviços possam ser gerenciados, operados e suportados conforme os requisitos definidos.

5.4.1.4.11.6. Realizar as atividades e processos necessários para garantir o gerenciamento e a entrega dos serviços conforme níveis de serviços aqui definidos.

5.4.1.4.11.7. Gerenciar continuamente a tecnologia em uso para entregar e suportar os serviços.

5.4.1.4.11.8. Melhorar a percepção de qualidade e a satisfação de usuários e clientes quanto ao uso dos serviços do MJSP.

5.4.1.4.11.9. Prover mecanismos eficientes para tratamento das questões relativas ao dia-a-dia dos serviços.

5.4.1.4.11.10. Monitoramento e Análise remota de toda a infraestrutura do Ministério, utilizando-se de análise dos logs disponibilizados em tempo real através da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério. Para o devido dimensionamento do esforço de trabalho necessário a Contratada deverá estimar um quantitativo mínimo de pessoal capaz de monitorar, analisar, operar e acompanhar a Plataforma de SIEM/SOAR/NTA/UEBA/CTI para um volume de no mínimo 200 GB/dia e 5000 EPS (Despacho nº 333, nº SEI 14781049). O cálculo do valor de EPS foi estimado utilizando a ferramenta LogPoint e distribuição realizada no Despacho 80 (nº SEI 14612910) com alteração nas quantidades existentes.

5.4.1.4.11.11. Configuração, manutenção, monitoramento e operação da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério. sendo responsável pela solicitação da coleta dos logs ao Ministério.

5.4.1.4.11.12. Realização de atividades de preparação do processo de coleta de logs, incluindo a normalização, filtragem, redução, agregação e priorização. O processamento, normalização, armazenamento, e demais atividades de correlacionamento de logs que serão realizadas nas ferramentas da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério, a partir dos dados disponibilizados pelo Ministério.

5.4.1.4.11.13. A CONTRATADA deverá disponibilizar uma ferramenta de ITSM (Information Technology Service Management) para registro, acompanhamento e controle dos Incidentes e Requisições de Segurança e gerir todo o ciclo de vida dos chamados de SOC. Ao final do contrato, as bases de dados das ferramentas utilizadas, com todos os dados, inclusive históricos das demandas, solicitações, atendimentos e demais informações relativas à prestação de serviços deverão ser entregues e permanecerão sob custódia exclusiva do Ministério;

5.4.1.4.11.14. Resposta aos incidentes por meio de monitoramento, análise e despacho, operando de forma sincronizada ao NOC do Ministério e, em caso de inoperância do NOC, atuar em substituição ao NOC dentro dos serviços autorizados em reunião inicial entre a CONTRATANTE e CONTRATADA, visando minimizar as consequências e proteger as informações e ativos do ministério. Todas ações tomadas devem ser posteriormente repassadas ao NOC ou suporte da infraestrutura e a CRS.

5.4.1.4.11.15. Sugestão de ajustes de configuração dos dispositivos visando reduzir a probabilidade de ataques, sendo a execução desses ajustes de responsabilidade do NOC do ministério.

5.4.1.4.11.16. Realização de transferência de conhecimento para equipe técnica do ministério em todas as tecnologias instaladas e/ou utilizadas, sistemas, produtos e soluções instaladas pela CONTRATADA com o fornecimento de perfil de acesso para a supervisão dos serviços prestados, assim como, atualização rotineira no estado da arte em termos de segurança da informação.

5.4.1.4.11.17. Execução de serviços técnicos especializados, sob demanda e de maneira eventual.

5.4.1.4.11.18. Prestação remota dos serviços, sendo a presença física somente quando necessário ou mediante justificativa.

5.4.1.4.11.19. Utilização das ferramentas, soluções e equipamentos de segurança instalados no ministério.

5.4.1.4.11.20. Alocação de equipamentos e softwares quando necessários à consecução das atividades de segurança da informação e ao atendimento das especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

5.4.1.4.11.21. Prestação de informações e realização de demandas através de chamados técnicos do ministério, sob autorização e controle da Coordenação de Riscos e Segurança da Informação.

5.4.1.4.11.22. Disponibilização de pessoal técnico qualificado mediante certificação oficial e experiência profissional em todos os itens da possível contratação.

5.4.1.4.11.23. Análise fim a fim dos incidentes e ataques.

5.4.1.4.11.24. Apoiar a CRS na elaboração de minuta de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) quanto ao registro de incidentes junto ao Ministério, de acordo com o Art. 48 da LGPD .

5.4.1.4.11.25. Apoiar a CRS na elaboração de minuta de comunicação à Autoridade Policial quanto ao registro de incidentes com classificação de crimes cibernético junto ao Ministério.

5.4.1.4.11.26. Apoiar o Ministério na retenção de informações de acordo com os mecanismos de retenção e guarda de registros de conexão, nos termos da Lei 12.965/2014 que estabeleceu os princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

5.4.1.4.11.27. Para divulgação de ações de segurança da informação (Alertas, Conscientização e Recomendações) aos usuários finais, equipes de TIC e aos gestores com o objetivo de fortalecer uma estrutura para projetar, implementar, monitorar, manter e melhorar a segurança da informação consistente com a cultura organizacional, conforme preceitua a ABNT NBR ISO/IEC 27000, bem como para acompanhamento e avaliação dos indicadores de performance e serviços de SOC e CSIRT pelos gestores de TIC do Ministério a CONTRATADA deverá desenvolver e manter um **Portal WEB de CSIRT do Ministério** hospedado na infraestrutura da CONTRATANTE, para a disponibilização de tais informações, como também informações para registro de notificações por usuários externos ao Ministério com uso de tecnologias seguras, definidas pela CRS, para comunicações através de canal seguro.

5.4.1.4.11.28. Disponibilização de painel para acompanhamento em tempo real do status de segurança do ministério, dos alertas gerados pelas ferramentas que compõem o SOC, dos incidentes reportados, dos ataques em andamento ou contidos, das vulnerabilidades descobertas, enfim, de todas as informações de segurança da informação.

5.4.1.4.11.29. A Contratada deverá disponibilizar a Contratante acesso aos sistemas que utilize na prestação do serviço e que não sejam do MJSP.

5.4.1.4.12. O **Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team** deverá ser observadas as orientações e técnicas emanadas pelos padrões internacionais, além de outros apresentados pela CONTRATADA, caso haja em seu portfólio normativos que comprovadamente complementem os demonstrados abaixo:

5.4.1.4.12.1. NIST Cybersecurity Framework, Version 1.1 ou mais recente;

5.4.1.4.12.2. NIST Privacy Framework, Version 1.0 ou mais recente;

5.4.1.4.12.3. NIST Special Publication 800-61 Revision 2 (Computer Security Incident Handling Guide);

5.4.1.4.12.4. NIST Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment);

5.4.1.4.12.5. SANS Incident Handler's Handbook;

5.4.1.4.12.6. CIS Control, Version 7.1 ou mais recente;

5.4.1.4.12.7. ISO/IEC 27035-1:2016 - Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management;

5.4.1.4.12.8. ISO/IEC 27035-2:2016 - Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response;

5.4.1.4.12.9. ISO/IEC 27035-3:2020 - Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations;

5.4.1.4.13. Monitoramento e Análise de Logs e Eventos com capacidade, atualmente em aproximadamente 200GB/dia ou 5.000 EPS. O cálculo do valor de EPS foi estimado utilizando a ferramenta LogPoint e distribuição realizada no Despacho 80 (nº SEI 14612910) com alteração nas quantidades existentes.

5.4.1.4.14. Monitoramento da rede sociais, Dark Web e Deep Web com ferramentas adequadas para monitoramento de informações sensíveis e de interesse do Ministério a respeito de segurança da cibernética.

5.4.1.4.15. Para fins de execução do contrato, a CONTRATADA deverá atender os requisitos técnicos especificados deste ETP. Todos os processos poderão ser amadurecidos conforme evolução da operação no ambiente de infraestrutura durante a execução do contrato.

5.4.1.5. O **Serviço de Teste de Invasão - Red Team** envolve os seguintes serviços, conforme *Information Technology Infraestructure Library* – ITIL e com das atividades dos processos do volume de **Transição de Serviços e Operação de Serviços**;

5.4.1.5.1. Gerenciamento do Conhecimento;

5.4.1.5.2. Gerenciamento de Incidente;

5.4.1.5.3. Gerenciamento de Problema;

5.4.1.5.4. Gerenciamento de Requisição;

5.4.1.5.5. Desempenhar atividades de 2º e 3º nível de **Operação de Serviços** das funções:

5.4.1.5.5.1. Central de Serviços;

5.4.1.6. Serviços de Red Team desempenhará os seguintes objetivos e propósitos:

5.4.1.6.0.1. Estabelecer e manter a integridade dos ativos de serviços e suas configurações.

5.4.1.6.0.2. Prover conhecimento de qualidade para a organização.

5.4.1.6.0.3. Garantir que os serviços possam ser gerenciados, operados e suportados conforme os requisitos definidos.

5.4.1.6.0.4. Realizar as atividades e processos necessários para garantir o gerenciamento e a entrega dos serviços conforme níveis de serviços aqui definidos.

5.4.1.6.0.5. Gerenciar continuamente a tecnologia em uso para entregar e suportar os serviços.

5.4.1.6.0.6. Prover mecanismos eficientes para tratamento das questões relativas ao dia-a-dia dos serviços.

5.4.1.6.1. Realização de testes de penetração.

5.4.1.6.2. Identificar, mapear e documentar possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos e informações, bem como a indicação de soluções para a correção das vulnerabilidades encontradas.

5.4.1.6.3. A CONTRATADA deverá disponibilizar ferramenta de ITSM (Information Technology Service Management) para registro, acompanhamento e controle dos Incidentes e Requisições de Segurança e gerir todo o ciclo de vida dos chamados de RED TEAM. Ao final do contrato, as bases de dados das ferramentas utilizadas, com todos os dados, inclusive históricos das demandas, solicitações, atendimentos e demais informações relativas à prestação de serviços deversão ser entregues e permanecerão sob custódia exclusiva do Ministério;

5.4.1.6.4. O Serviço de Testes de Invasão será do tipo externo e interno e terá como objetivo principal identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Para a realização dos testes de invasão deverão ser observadas as orientações e técnicas emanadas pelos padrões internacionais, além de outros apresentados pela CONTRATADA, caso haja em seu portfólio normativos que comprovadamente complementem os demonstrados abaixo:

5.4.1.6.4.1. OSSTMM 3 (The Open Source Security Testing Methodology Manual) ;

5.4.1.6.4.2. ISSAF/PTF (Information Systems Security Assessment Framework);

5.4.1.6.4.3. NIST Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment);

5.4.1.6.4.4. NIST Special Publication 800-42 (Guideline on Network Security Testing);

5.4.1.6.4.5. OWASP TESTING GUIDE 4.1 The Open Web Application Security Project.

5.4.1.6.5. Neste documento os termos “pentest”, teste de penetração, teste de intrusão e testes de invasão, são considerados sinônimos;

5.4.1.6.6. Os alvos dos “Testes de Invasão” bem como as premissas e condições para realização destes serão, necessariamente, definidos e aprovados através de demanda por parte do Ministério;

5.4.1.6.7. A Contratada deverá observar que os testes de invasão serão executados internamente (qualquer ponto da rede corporativa do Ministério) e externamente (através da Internet);

5.4.1.6.8. Todas as fases dos “Testes de Invasão” serão acompanhadas e supervisionadas a critério do Ministério;

5.4.1.6.9. Quaisquer atividades que possa comprometer ou prejudicar algum ambiente ou ativo deverá ser imediatamente reportada, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos;

5.4.1.6.10. O teste de invasão deverá obedecer às seguintes fases:

5.4.1.6.10.1. Planejamento;

5.4.1.6.10.2. Descoberta;

5.4.1.6.10.3. Ataque;

5.4.1.6.10.4. Relatório Teste de Invasão;

5.4.1.6.10.5. Reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o teste;

5.4.1.6.10.6. Reavaliação, novo teste pós remediação;

5.4.1.6.10.7. Relatório Final do Teste de Invasão.

5.4.1.7. Para fins de execução do contrato, a CONTRATADA deverá atender os requisitos técnicos especificados deste ETP. Todos os processos poderão ser amadurecidos conforme evolução da operação no ambiente de infraestrutura durante a execução do contrato.

5.5. **Matriz de Responsabilidade R.A.C.I**

5.5.1. Para um melhor entendimento das responsabilidades a serem executadas pelos serviços objeto da presente contratação, foi definido uma Matriz de Responsabilidade R.A.C.I apresentado a seguir, a qual esta alinhada com a Figura 11 - Diagrama de relacionamento dos serviços e seus respectivos componentes com os demais serviços da DTIC e envolve todos os atores com participação no SOC e na Área de Segurança Cibernética ;

Tabela 12 - Matriz de Responsabilidade R.A.C.I - Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério e Área de Segurança da Cibernética

Matriz de Responsabilidade R.A.C.I - Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério e Área de Segurança da Cibernética														
Serviços		Transição de Serviços				Operação de Serviços								
		Processos				Processos					Funções			
Situação	Descrição	Ger. de Configurações e de Ativo de Serviços	Ger. de Mudanças	Ger. de Liberações e Implantação	Ger. do Conhecimento	Ger. de Evento	Ger. de Incidente	Ger. de Problema	Ger. de Requisição	Ger. de Acesso	Central de Serviços	Ger. de Operações de TI	Ger. Técnico	Ger. de Aplicação

Nova contratação	Solução de SOC	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I
	Serviços de CSIRT Blue Team	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I
	Serviços de Red Team	-	-	-	R/C	-	R/C	R/C	R/C/I	-	R/C/I	-	-	-
Contratação existente	Serviço de NOC	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I	C/I
	Serviços de Infraestrutura	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I	R/C/I
Contratante	**MJSP\DTIC\CRS**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**	**A/C/I**

Legenda:
R: Responsável por executar uma atividade;
A: Autoridade, quem responde pela atividade, o dono
C: Consultado, quem deve ser consultado e participar da decisão ou atividade no momento que for executada;
I: Informado, quem deve receber a informação de que uma atividade foi executada;
Obs.: As atividades da nova contratação são junto a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério e não conflitará com as atividades da contratação existente, pois a mesma, atuará de forma subsidiária ao contrato existente quando da necessidade de ações junto a Área de Segurança Cibernética, conforme definido no item 2.2.1.5 desse Estudo Técnico Preliminar.

5.6. **Indicadores de performance do Serviço de Security Operation Center - SOC**

5.6.1. A frequência de aferição dos indicadores de performance será mensal, porém com registros diários quando aplicável, devendo a contratada elaborar Relatório Mensal de Atividades, apresentando-o ao Ministério até o quinto dia útil do mês subsequente ao da prestação do serviço.

5.6.2. Devem constar desse relatório, entre outras informações, os indicadores de performance, metas de níveis de serviço alcançados, recomendações técnicas, administrativas e gerenciais para o próximo período e demais informações relevantes para a gestão contratual. O conteúdo detalhado e a forma do relatório gerencial serão definidos pelas partes.

5.6.3. Caberá à Comissão de Fiscalização do contrato analisar mensalmente o Relatório Mensal de Atividades executados pela Contratada, observando os indicadores e os níveis de serviço alcançados.

5.6.4. Os indicadores de performance são flexíveis em quantidade e qualidade e estão descritos na tabela a seguir:

Tabela 13 - Indicadores de Performance do Serviço SOC

Categoria	Subcategoria	Métrica	Unidade de medida
Governança	Conformidade	Quantidade de violações de políticas	número
		Porcentagem de sistemas com controles de segurança testados	percentual
	Privacidade	Quantidades de incidentes notificados a ANPD	número
	CSIRT	Avaliação da Maturidade do CSIRT de acordo com o "ENISA CSIRT maturity assessment model versão 2.0 - 30 de abril de 2019"	Nível e percentual de evolução
	Orquestração	Automação/Orquestração dos processos continuidade de negocio e resposta a incidentes cibernéticos	Nível e percentual de evolução
Técnico	Ameaças	Nível de segurança	Classificação de cores
		Atribuição de ameaças a atores (usando inteligência de ameaças)	a definir
	Vulnerabilidade	Tempo para remediação da vulnerabilidade	tempo
		Gravidade da vulnerabilidade	escala
		Incidentes de vulnerabilidade conhecida vs. desconhecida	número/escala
		Exposição à vulnerabilidade	escala
	Risco	Posição de risco	escala
		Risco por sistema/serviço	escala
		Principais riscos	texto
		Tipos de casos (MITRE ATT&CK)	número
	Alerta	Tempo por investigação de alerta	tempo
		Índice de geração de alerta	número/escala
		Número de alertas que permanecem por analisar (em aberto)	número
		Criticidade de um alerta	escala
	Incidente	Prioridade de incidentes	texto
		Total de incidentes por mês	número
		Número de ataques bem sucedidos	número/percentual
		Tempo médio de detecção (MTTD)	tempo
		Tempo médio para resolução/recuperação (MTTR)	tempo
		Custo por incidente	valor/texto
		Sucesso na mitigação	número/percentual
	Resiliência	Tempo médio gasto por ataque (MTTA)	tempo
		Eficiência defensiva	escala
		Repercussão do ataque	texto
		Quantidade de interrupções	número e percentual
		Tempo de interrupções	tempo
Pessoas	Performance	Número de incidentes encerrados em um turno	número
		Produtividade do analista	número
		Análise de escalação de caso	número
Gerais	Performance	Taxa de falso positivo	percentual
		Tempo médio de analise	tempo
		Nível de disponibilidade	percentual
	Cobertura	Quantidade de ativos monitorados	número
		Quantidade de ativos monitorados vs. Quantidade total de ativos	número e percentual

5.7. **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério**

5.7.1. Como forma de avaliar os recursos da **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério, Microsoft Azure Sentinel,** foi realizado um estudo comparativo entre os principais fornecedores de produtos que compõem a solução incluindo serviços de Plataforma como Serviço (PaaS), os

quais são apresentados na tabela a seguir:

Tabela 14 - Benchmark SIEM + SOAR + UEBA

Benchmark SIEM + SOAR + UEBA versão 15/03/2021				
Funcionalidades\Players	**Microsoft**	**Exabeam**	**LogRhythm**	**Splunk**
SaaS (1)	Azure Sentinel	EXABEAM CLOUD PLATFORM (19)	LogRhythm Cloud	Splunk Cloud
SaaS no Brasil (1)	Sim	Sim (20)		Não (AWS e GCP) (14)
SIEM (2)	Azure Sentinel	Exabeam Security Management Platform	LogRhythm NextGen SIEM Platform	Splunk Enterprise Security
SOAR (2)	Azure Sentinel	Exabeam Security Management Platform	LogRhythm's SmartResponse™	Splunk Phantom
UEBA (Monitoramento de Usuários)	Azure Sentinel UEBA	Exabeam Security Management Platform	LogRhythm UserXDR	Splunk UBA
Recursos de ML e AI	Sim	Sim (23)	Sim (36)	Sim (MLTK)
Integração Exchange	Sim	Sim (25)	Sim com solução de terceiro (37)	Sim
Certificações externas que a solução possui		SOC 2 Tipo II (20)	SOC 2 Type I e GDPR (39)	SOC 2 Tier II / ISO/IEC 27001:2013 (3)
Ferramenta de compliance de implantação do cliente (Cybersecurity Posture Score and Compliance)	CMMC 4 e MITRE ATT&CK	GDPR, GPG, HIPAA, FISMA, PCI DSS, SOX (26)	CCF, GDPR, ISSO 27001, NIST (38)	FISMA, HIPAA, PCI
Tipo de licenciamento	Ingestão de dados GB (Logs)	Eventos de Segurança por segundo (27)	Ingestão de dados GB (Logs) (35)	Baseado em infraestrutura sem limites de dados ou por GB/dia (8)
Tipos de Retenção	90 dias de retenção incluso (6)	Retenção ilimitada (22)	90 dias de retenção incluso (40)	90 dias de retenção incluso (8)
Suporte a integração com nuvens	AWS, GCP e Oracle Cloud (OCI) (5 e 7)	AZURE, AWS e GCP (25)	Azure e AWS (41)	Azure, AWS e GCP (15 e 28)
Node Forward	Sim (5)	Sim (29)	Sim (44)	Sim (17)
Agent Forward	Sim (5)	Sim (29)	Sim (44)	Sim (18)
Suporte protocolos	Common Event Format (CEF), Syslog or REST-API (5)	Syslog e API (30)	UDP Syslog Device, TCP Syslog Device, NetFlow v1, v5 or v9 Device, IPFIX Device, J-Flow Device, sFlow Device e SNMP Trap Device (44)	HTTP Event Collector (HEC), Syslog e SNMP
Network Logs - Suporte a protocolos de flow (Netflow ou sFlow) - visão norte/sul e leste/oeste	Não (utiliza o logstash)	Sim (31)	Sim (43)	Sim (NetFlow ou IPFIX, Sflow e JFlow) (11)
Suporte a conectores	Sim (5)	Sim (24)		Sim (16)
Formas de Transferência de dados				VPN limitado a 1000 GB dia (14)
Arquitetura	Cloud | Local	MSSP | Hibrido | Local (21)		Cloud | Local
Suporte a Detecção e resposta de endpoint (EDR) Nativo	Sim - Windows Defender ATP + MS Defender Security Center (13)	Não (Integração com ferramentas de terceiros) (25)	Sim. (LogRhythm's Endpoint Monitoring and Forensics) (42 e 43)	Não (Integração com ferramentas de terceiros (Ex. Cisco Security Platforms) (12)
Processo de Gestão de Incidente e Problema (ITSM) Nativo	Não (Suporta com o uso de conector ServiceNow, System Center, Provance e Cherwell	Não (Suporte Atlassian JIRA e ServiceNow) (25)	LogRhythm Incident Management (40)	

Suporte a Inteligência Contra Ameaças Cibernetícas Nativo (CTI)	Não (Integração com ferramentas de terceiros) (34)	Não (Integração com ferramentas de terceiros) (25)	Sim (LogRhythm Threat Intelligence Services (TIS)) (46)	Sim (47)
Normalização de Dados (Parser Normalization)	OSSEM (9)	Exabeam Auto Parser Generator (APG) (32)	MDI Fabric (45)	CIM (10)

Obs.: Os campos que estão em branco ainda não foram possíveis identificar a informação pública no site do fabricante.

Fontes:
1 https://marketplace.fedramp.gov/#!/products
2 http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm
3 https://www.splunk.com/pdfs/legal/splunk-ISO-27001-certificate.pdf
4 https://techcommunity.microsoft.com/t5/azure-sentinel/what-s-new-cybersecurity-maturity-model-certification-cmmc/ba-p/2111184
5 https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources
6 https://azure.microsoft.com/en-us/pricing/details/monitor/
7 https://techcommunity.microsoft.com/t5/azure-sentinel/azure-sentinel-the-connectors-grand-cef-syslog-direct-agent/ba-p/803891
8 https://www.splunk.com/en_us/software/pricing.html
9 https://ossemproject.com/intro.html
10 https://docs.splunk.com/Documentation/CIM/4.18.0/User/UsetheCIMtonormalizedataatsearchtime
11 https://docs.splunk.com/Documentation/StreamApp/7.3.0/DeployStreamApp/UseStreamtoingestNetflowandIPFIXdata
12 https://conf.splunk.com/files/2019/slides/SECS2899.pdf
13 https://docs.microsoft.com/en-us/azure/sentinel/microsoft-365-defender-sentinel-integration
14 https://docs.splunk.com/Documentation/SplunkCloud/8.1.2101/Service/SplunkCloudservice
15 https://www.splunk.com/en_us/blog/tips-and-tricks/getting-microsoft-azure-data-into-splunk.html
16 https://splunkbase.splunk.com/
17 https://docs.splunk.com/Documentation/Splunk/8.1.2/Indexer/forwardersdirecttopeers
18 https://www.splunk.com/en_us/download/universal-forwarder.html
19 https://www.exabeam.com/wp-content/uploads/2020/02/EXA_Data-Sheet_Cloud-Platform.pdf
20 https://www.exabeam.com/newsroom/exabeam-expands-international-availability-of-cloud-based-siem-to-help-organizations-modernize-security-operations/
21 https://www.exabeam.com/siem-guide/siem-architecture/
22 https://www.exabeam.com/siem-guide/siem-buyers-guide/
23 https://www.exabeam.com/information-security/machine-learning-for-cybersecurity/
24 https://www.exabeam.com/product/cloud-connectors/
25 https://www.exabeam.com/wp-content/uploads/2020/03/Data-Integrations-WP-Mar20.pdf
26 https://docs.exabeam.com/en/data-lake/i35/data-lake-user-guide/111941-exabeam-data-lake-reports.html#UUID-486e3195-13c5-8e7d-3569-2de7f762228e
27 https://www.exabeam.com/siem-guide/siem-architecture/#sizing
28 https://www.splunk.com/en_us/app-integrations.html
29 https://docs.exabeam.com/en/data-lake/i36/exabeam-data-lake-collector-guide/119236-exabeam-data-lake-agent-log-collectors.html
30 https://docs.exabeam.com/en/aws/all/amazon-web-services-setup-guide/UUID-d5c8b4f7-e188-c622-9722-16408f646425.html
31 https://docs.exabeam.com/en/content/all/how-content-works-guide/53754-event-types-and-required-fields.html
32 https://www.exabeam.com/siem/auto-parser-generator-now-available-for-customers/
33 https://docs.microsoft.com/en-us/learn/modules/incident-management-sentinel/
34 https://docs.microsoft.com/pt-br/azure/sentinel/import-threat-intelligence
35 https://logrhythm.com/wp-content/uploads/2020/03/logrhythm-cloud-data-sheet-1.pdf
36 https://logrhythm.com/products/logrhythm-user-xdr/
37 https://gallery.logrhythm.com/joint-solution-briefs/logbinder-for-exchange-joint-solution-brief.pdf
38 https://gallery.logrhythm.com/data-sheets/logrhythm-for-compliance-data-sheet.pdf
39 https://gallery.logrhythm.com/terms-and-conditions/logrhythm-cloud-security-overview-final-2019-05.pdf
40 https://gallery.logrhythm.com/terms-and-conditions/logrhythm-cloud-security-overview-final-2019-05.pdf
41 https://logrhythm.com/solutions/security/cloud-security/
42 https://gallery.logrhythm.com/data-sheets/endpoint-monitoring-and-forensics-data-sheet.pdf
43 https://gallery.logrhythm.com/data-sheets/na-data-sheet-sysmon.pdf
44 https://docs.logrhythm.com/docs/sysmon/system-monitor-installation-guide/networking-and-communication
45 https://gallery.logrhythm.com/data-sheets/data-processing-and-indexing-tiers-data-sheet.pdf
46 https://logrhythm.com/blog/logrhythm-threat-intelligence-services-stix-via-taxii/
47 https://www.splunk.com/en_us/resources/videos/splunk-threat-intelligence-demo.html

5.7.2. Observa-se conforme Tabela acima que a Plataforma da Microsoft - Azure Sentinel é um produto o qual possui todos os requisitos e funcionalidades comuns para o segmento.

5.7.3. Após a avaliação técnica, essa equipe de planejamento da contratação realizou uma comparação de preços entre as soluções comercializada no pais e com objetivo de avaliar custos entre as opções de solução disponíveis no mercado nacional como serviço que compõe (software e hardware), foi realizado uma pesquisa entre as tecnologias que possuem preços públicos na internet bem como preços público presente na ATA do Pregão 01/2020 do Conselho da Justiça Federal, apresentados na tabela a seguir.

Tabela 15 - Comparação de Preços Públicos entre os softwares de SOC

Comparação de Preços Públicos entre os softwares de SOC										
		Microsoft			**RSA - Empresa ISH (Pregão 01/2020 - CJF)**		**Logrhythm - Empresa APURA (Pregão 01/2020 - CJF)**		**ELK - Empresa NCT (Pregão 02/2020 - CJF)**	
Produtos Cloud envolvidos	**SOAR**	**1 - Azure Sentinel 2 - Log Analytics do Azure Monitor**			**Item 5 - RSA Netwitness Orchestrator**		**Item 5 - LogRhythm**		**Item 5 - ServiceNow**	
	Endpoint Análise				**Item 3 - TENABLE NESSUS, ACUNETIX e RSA Archer VM**		**Item 3 - Tenable**		**Item 3 - Qualys**	
	Network Análise				**Item 4.3 - NTA RSA Netwitness Packets**		**Item 4.3 - LogRhythm**		**Item 4.3 - ELK/IXIA/VIAVI**	
	UEBA				**Item 4.2 - UBA - RSA UEBA Essentials + Analytics**		**Item 4.2 - LogRhythm**		**Item 4.2 - ELK**	
	Inteligência de Ameaça				**Item 2 - CTI RSA ARCHER ISSUE**		**Não informado**		**Item 2 - Recorder Future**	
	SIEM				**item 4.1 - RSA Netwitness Logs**		**Item 4.1 0 LogRhythm**		**Item 4.1 - ELK**	
Referência		**Reservado***			**Ata do Pregão (6)**		**Ata do Pregão (6)**		**Ata do Pregão (6)**	
		Item	**Unitário**	**Total (Mensal)**	**Unitário**	**Total (Mensal)**	**Unitário**	**Total (Mensal)**	**Unitário**	**Total (Mensal)**
Logs	**100 GB/dia de logs**	1	R$ 979,78 por dia	R$ 29.393,40	R$ 580,03 por GB ingerido (2)	R$ 58.037,46	R$ 507,05	R$ 50.705,07	R$ 950,71	R$ 95.071,33
		2	R$ 1920,37 por dia	R$ 57.611,10	R$ 4,24 por ativo (3)	R$ 16.960,00	R$ 3,71	R$ 14.851,84	R$ 6,96	R$ 27.847,56
	Processamento de 1 Gbps de volume de rede	N/A	R$ 0,00 incluído (1)	R$ 0,00 incluído (1)	R$ 13261,75 para 1Gbps (4)	R$ 13.261,75	R$ 4.681,28	R$ 4.681,28	R$ 8.777,42	R$ 8.777,42
Endpoits	**4000**	N/A	R$ 0,00 incluído (1)	R$ 0,00 incluído (1)	R$ 11,36 por endpoint (5)	R$ 45.440,00	R$ 4,73	R$ 18.920,00	R$ 10,33	R$ 41.333,33
Total Mês				**R$ 87.004,50**		**R$ 133.699,21**		**R$ 89.158,19**		**R$ 173.029,65**

Total Ano		**R$ 1.044.054,00**		**R$ 1.604.390,52**		**R$ 1.069.898,24**	**R$ 2.076.355,76**

Obs.: Foram considerando apenas os itens de software do Pregão do CJF e os valores constante na Ata do Pregão 01/2020 (http://comprasnet.gov.br/livre/pregao/ata2.asp?co_no_uasg=90026&numprp=000012020&f_lstSrp=T&f_Uf=DF&f_numPrp=12020&f_coduasg=&f_tpPregao=E&f_lstICMS=T&f_dtAberturaIni=&f_dtAberturaFim=)
* Retenção gratuita por 90 dias
https://azure.microsoft.com/pt-pt/pricing/details/azure-sentinel/
https://azure.microsoft.com/pt-pt/pricing/details/monitor/
1 - Azure Activity Logs, Office 365 Audit Logs (all SharePoint activity and Exchange admin activity) and alerts from Microsoft Defender products (Azure Defender, Microsoft 365 Defender, Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Endpoint), Azure Security Center, Microsoft Cloud App Security, and Azure Information Protection can be ingested at no additional cost into both Azure Sentinel, and Azure Monitor Log Analytics. não faz parte do os logs do Azure Active Directory conforme link https://azure.microsoft.com/pt-pt/pricing/details/azure-sentinel/ na aba de FAQ.
2 - Item 4.1 do edital do CJF ao custo mensal de R$ 8.705,62 para 15GB/dia.
3 - Item 4.2 do edital do CJF ao custo mensal de 4.249.97 para 1000 ativos.
4 - Item 4.3 do edital do CJF ao custo mental de 13.261,75 para processar no mínimo 1 Gbps.
5 - Item 3 do edital do CJF ao custo mensal dividido por 1500 endpoint.
6 - Para chegar ao valor dos itens 4.1, 4.2 e 4.3 foram identificados na proposta original da empresa o percentual correspondente ao item 4 e assim utilizado.

5.7.4. Na realização da pesquisa e sua comparação identificou-se que o produto da Microsoft Azure Sentinel frente aos demais produtos (RSA, Logrhythm e ELK) não cobra pelo processamento de tráfego de rede e monitoramento de dispositivos endpoint, cujo os produtos são Microsoft, diferente dos demais, o que apresenta ser uma estratégia de mercado adotado pelos fabricantes na comercialização de seus produtos, pois o somatório de todos os produtos/serviços se mostra mais vantajoso quando do produto da Microsoft Azure Sentinel é comparado.

5.7.5. Diante dos preços mensais e totais constantes na tabela acima é possível identificar que a média mensal de preço das soluções pesquisada foi de R$ 111.428,70 e o melhor valor foi da Plataforma da Microsoft Azure Sentinel, o que demonstra que a permanência da **Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério, Microsoft Azure Sentinel,** representa o melhor custo beneficio para a administração bem como, a melhor estratégia da presente contratação.

5.8. **Dimensionamento da força de trabalho pela CONTRATADA.**

5.8.1. Para o dimensionamento da força de trabalho da CONTRATADA, o fluxo de dados do Ministério a ser considerado de forma escalável, sob demanda e de acordo com o item 6.2.1.1.12, será conforme segue;

Tabela 16 - Fluxo de dados do Ministério coletado pela Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério

Descrição	Estimativa adicionais a serem dimensionados de acordo com a demanda e utilização	Quantidade Estimada inicial (GB/dia e EPS)	Retenção Hot e Warm (Tipo 1)	Retenção Cold (Tipo 2)	Retenção Frozen (Tipo 3)
Logs de ambiente em Nuvem (Azure e Oracle Cloud)	5 x 100GB/dia | 2.000 EPS	5 GB/dia | 100 EPS	1 mês	6 meses	12 meses
IDS Aletas e Logs de ativos de segurança		30 GB/dia | 1000 EPS	15 dias	6 meses	12 meses
NetFlow/SFlow logs		10 GB/dia | 300 EPS	1 mês	6 meses	12 meses
Logs de auditoria (Sistemas, serviços e servidores e endpoint)		55 GB/dia | 600 EPS	72 horas	6 meses	12 meses
Quantitativo máximo	**500GB/dia | 12.000 EPS**	**100GB/dia | 2.000 EPS**	-	-	-

5.9. **Itens que compõe a pretensa contração**

5.9.1. A tabela 17 apresenta os itens a serem contratados, para o período de dois anos (24 meses).

Tabela 17 - Itens a serem contratados

Grupo	Item	Descrição do item	Quantidade	Métrica ou Unidade	Forma
1	1	Serviço de Security Operations Center - SOC	24	Unidade (Mensal)	Contínuo
	2	Serviço de Tratamento e Resposta aos Incidentes Cibernéticos - CSIRT - Blue Team	24	Unidade (Mensal)	Contínuo
2	3	Serviço de Teste de Invasão - Red Team	827	Unidade (Alvos)	Sob demanda

6. **ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO**

6.1. A estimativa de custo total da contratação é apresentada na tabela 18.

Tabela 18 - Estimativa de quantidades e custos

Grupo	Item	Descrição do item	Quantidade	Unidade	Valor Unitário	Valor Mensal máximo (R$)	Valor Total máximo (24 meses) (R$)
1	1	Serviço de Security Operations Center - SOC	24 meses	Unidade (Mensal)	R$ 168.156,00	R$ 168.156,00	R$ 4.035.744,00
	2	Serviço de Tratamento e Resposta aos Incidentes Cibernéticos	24 meses	Unidade (Mensal)	R$ 18.446,40	R$ 18.446,40	R$ 442.713,60

		- CSIRT - Blue Team					
2	3	Serviço de Teste de Invasão - Red Team	827	Unidade (Alvos)	R$ 1.150,84	N/A	R$951.744,68
	Total					**R$ 186.602,40**	**R$ 5.430.202,28**

As valores de referência utilizados para compor a estimativa de custo são os mesmos presentes na tabela 10 - Custo estimado para o MJSP, baseadas no preço final homologado do Pregão 01/2020 do Conselho de Justiça Federal (CJF) que possui objeto similar a essa pretensa contratação.

6.2. A estimativa total da contratação para 24 meses é de R$ 5.430.202,28 (cinco milhões, quatrocentos e trinta mil duzentos e dois reais e vinte e oito centavos) e de R$ 13.575.505,70 (treze milhões, quinhentos e setenta e cinco mil quinhentos e cinco reais e setenta centavos) para cinco anos.

7. **AVALIAÇÃO DAS NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO**

7.1. **Não** é necessário adequar o ambiente da infraestrutura física das instalações do Ministério para viabilizar a entrega ou a execução contratual.

7.2. **Não** é necessário adequar o ambiente da infraestrutura elétrica para viabilizar a entrega ou a execução contratual.

8. **RECURSOS HUMANOS**

8.1. Gestor do contrato– responsável pela gestão do contrato, no âmbito do Ministério;

8.2. Fiscal Técnico do contrato– responsável pela fiscalização do contrato, no âmbito da DTIC;

8.3. Fiscal Administrativo do contrato – responsável pela fiscalização do contrato, no âmbito da CGL;

8.4. Fiscal Requisitante do contrato - responsável pela fiscalização do contrato, no âmbito da Unidade Requisitante;

8.5. Equipe técnica– formada por servidores da equipe de CRS da DTIC responsáveis pelo acompanhamento de chamados técnicos, de execução de configurações e dos serviços contratado.

9. **RECURSOS MATERIAIS**

9.1. Será necessário disponibilizar mobiliário e computadores nas dependências do MJSP para prestação de serviços, quando a CONTRATA informar necessidade.

10. **DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO**

10.1. De acordo com este estudo técnico preliminar da contratação, conclui-se que esta contratação está alinhada com as necessidades estratégicas elencadas no Plano Diretor de Tecnologia da Informação e Comunicação do Ministério da Justiça e Segurança Pública (2021-2023) (14424141), sendo descritas e tratadas como macro requisitos e necessidades de negócio como serviço para tal finalidade.

10.2. Foram avaliadas as soluções disponíveis no mercado quanto à viabilidade técnica e econômica para o atendimento das necessidades deste órgão.

10.3. Após análise das soluções, suas vantagens, desvantagens, avaliação das necessidades de adequação e demais itens cabíveis, os Integrantes Técnico e Requisitante declaram que a contratação da solução é viável.

11. **APROVAÇÃO E ASSINATURA**

11.1. A Equipe de Planejamento da Contratação foi instituída pela PORTARIA DE PESSOAL SAA/SE/MJSP Nº 1, DE 08 DE JANEIRO DE 2021 (13636809), alterado pela PORTARIA SAA/SE/MJSP Nº 57, DE 11 DE MAIO DE 2021 (14627967).

11.2. Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC.

INTEGRANTE TÉCNICO	**INTEGRANTE REQUISITANTE**
Cintia Mye Yonekawa Yamaguti **Matrícula/SIAPE:** 3201981	Ivanildo de Oliveira da Silva JR **Matrícula/SIAPE:** 2535600

AUTORIDADE MÁXIMA DA ÁREA DE TIC (*OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11*)	
Nome	Rodrigo Lange
Matrícula/SIAPE	1558579

Documento assinado eletronicamente por **Cintia Mye Yonekawa Yamaguti**, **Integrante Técnico(a)**, em 14/10/2021, às 16:26, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **IVANILDO DE OLIVEIRA DA SILVA JUNIOR**, **Integrante Requisitante**, em 14/10/2021, às 17:03, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Rodrigo Lange**, **Diretor(a) de Tecnologia da Informação e Comunicação**, em 15/10/2021, às 11:38, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.