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

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO
PROCESSO Nº 08006.001082/2020-13

INTRODUÇÃO

Conforme previsto no Art. 11 da IN 01 SGD/ME nº 2019, a elaboração do 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.

A presente análise tem por objetivo demonstrar a **viabilidade técnica e econômica da contratação** de empresa especializada para o fornecimento de Serviço de Suporte Técnico Especializado em Segurança da Informação e Serviço de Gestão de Vulnerabilidade, por meio da **contratação de empresa especializada para fornecimento e instalação de solução de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo a aquisição de serviços de Consultoria Especializada, suporte 24x7, com garantia (manutenção e suporte técnico)** para o Ministério da Justiça e Segurança Pública (MJSP), incluindo a garantia de atualização das versões, pelo período de 24(vinte e quatro meses), podendo ser prorrogada até o prazo máximo de 48(quarenta e oito) 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. 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. Aliado a isso, o aumento da conectividade dos computadores à rede mundial contribuiu para o crescimento dos incidentes de segurança.

1.2. Conforme apresentado na imagem 1, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), em 2001 houve 12.301 incidentes reportados. Dez anos depois, em 2011 , foi registrado um número 32,48 vezes maior com 399.515 incidentes reportados. No de 2019 houve 875.327 incidentes, número 71,16 vezes maior. Conforme apresentado na Imagem 1.

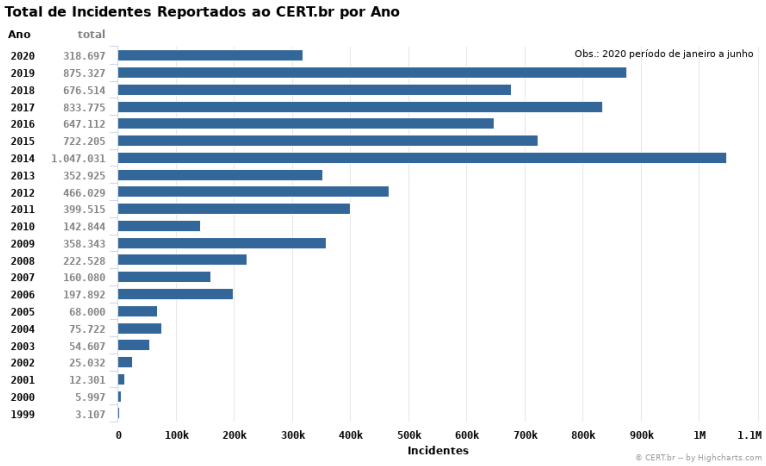


Imagem 1 - Total de incidentes reportados - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/ acesso em 11/01/2021

1.3. O trabalho de manter os ativos de rede seguros vai além do da utilização de antivírus nos computadores. Softwares desatualizados em estações de trabalho e servidores, aliado a más práticas de configurações de serviços criam alvos fáceis para exploradores de vulnerabilidades. A utilização de firewall não é uma solução definitiva, visto que, muitas portas legítimas podem estar vulneráveis, como é o caso da porta 80 que hospeda websites vulneráveis.

1.4. Este Estudo Técnico Preliminar aborda os principais tipos de vulnerabilidades, softwares maliciosos e ataques e procura demonstrar a importância e necessidade da aquisição de uma solução de análise de vulnerabilidade. O intuito da utilização desse tipo de software é automatizar e facilitar a descoberta de vulnerabilidades em uma rede, para correção, antes que as mesmas sejam exploradas por atacantes.

1.5. **Normas e Definições**

1.6. Segurança da Informação é tratada pelo Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21) e pela Comissão de Estudo de Segurança Física em Instalações de Informática através da norma ABNT NBR ISO/IEC 27002:2013.

1.7. Segundo a ISO/IEC 27000:2014, a informação é um ativo que, como outros ativos importantes, é essencial para os negócios de uma organização e, consequentemente precisa ser adequadamente protegido. As informações podem ser armazenadas de várias formas, incluindo: formulário digital (por exemplo, arquivos de dados armazenados em mídia eletrônica ou óptica), formulário material (por exemplo, em papel), bem como informações não representadas na forma de conhecimento dos funcionários.

1.8. Ainda segundo a ISO/IEC 27000:2014, as informações podem ser transmitidas por vários meios, incluindo: correio, comunicação eletrônica ou verbal. Qualquer que seja a forma da informação, ou o meio pelo qual a informação é transmitida, ela sempre precisa de proteção adequada.

1.9. Segundo a Instrução Normativa GSI/PR nº1, de 13 de junho de 2008, entende-se por Segurança da Informação e Comunicações, ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

1.10. A Segurança da Informação tem que ser vista pelas organizações como algo estratégico, pois elas estão muito dependentes dos serviços da Tecnologia da Informação (TI), como por exemplo:

- 1.10.1. Web Site: Como canal de divulgação da organização ou até mesmo para a geração, divulgação ou venda de produtos e serviços.
- 1.10.2. E-mail: Para troca de informações.
- 1.10.3. Videoconferência: Utilizado para realizar reuniões à distância.
- 1.10.4. Telefonia Ip: Fazer ligações entre as unidades de uma organização a um custo reduzido.
- 1.10.5. Sistema de Informação Computadorizado: Para armazenar e gerir informações conforme o modelo de negócio da organização.

1.11. Para o negócio, a proteção da informação, dos serviços e da rede como um todo é muito

importante para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

1.12. São vários casos famosos de falhas de segurança da informação que comprometeram grandes organizações e governos com prejuízos financeiros causados por falhas de Sistemas de Informação devido a indisponibilidade de sistemas. Além da falha em sistemas, a indisponibilidade pode ser causada por malwares. Os danos com malware poderiam ser diminuídos, por exemplo, com a conscientização dos usuários e com a utilização de um controle de proteção e detecção de malwares.

1.13. Os aspectos da Segurança da Informação são formados pela tríade confidencialidade-integridade-disponibilidade, definidos como:

- 1.13.1. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
- 1.13.2. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- 1.13.3. Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

1.14. **Vulnerabilidades**

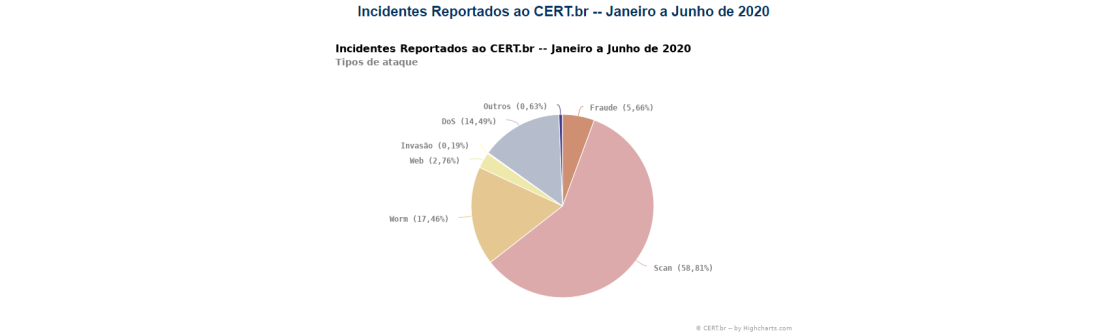
1.15. Vulnerabilidade é um conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação. (NC 04/IN01/DSIC/GSI/PR)

1.16. Já segundo Cert.br, uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança.

1.17. As vulnerabilidades são originadas de falhas na maioria das vezes não intencionais. Estas falhas podem ser:

- 1.17.1. Físicas: Acesso a ativos por pessoas não autorizadas, devido à falta de controle de acesso. Por exemplo, uma empresa terceirizada de limpeza desligar um switch por engano.
- 1.17.2. Hardware: Falhas no Hardware que ocasionam indisponibilidade no sistema ou perda dados. Outro item desta falha é a inclusão de um hardware malicioso como um Keylogger.
- 1.17.3. Naturais: Desastres naturais comprometendo a segurança dos dados armazenados.
- 1.17.4. Humanas: Operador de sistema utilizar erroneamente uma função, prejudicando o funcionamento do mesmo ou ocasionando perda de informações.
- 1.17.5. Software: Falhas de programação, abrindo brechas a serem exploradas.

1.18. As estatísticas de incidentes do Cert.br reportados de janeiro a junho de 2020, citadas na imagem 2, demonstram que 58,81% de incidentes são do tipo de ataque Scan, onde o atacante faz uma varredura de portas abertas em uma rede para identificar os serviços disponibilizados e suas possíveis vulnerabilidades.



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.

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.

Imagem 2 - Incidentes reportados em 2020, Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html acesso em 11/01/2021

1.19. Muitas vulnerabilidades são exploradas ou criadas a partir de softwares desenvolvidos para este fim conhecidos como Malware. Proveniente do inglês malicious software o Malware é um programa que produz efeitos danosos e indesejados.

1.20. Os principais tipos de Malware encontrados hoje são:

1.20.1. Vírus: Programa capaz de se autoexecutar e infectar outros arquivos com seu próprio código.

1.20.2. Worm: Programa malicioso que se propaga sem a necessidade de infectar outros arquivos, diferentemente do vírus, sua propagação é feita sem intervenção humana utilizando vulnerabilidades em uma rede.

1.20.3. Bot e botnet: Bot é um programa que permite ser controlado remotamente para executar vários comandos maliciosos, como, por exemplo, ataque de negação de serviço a um site. Uma botnet é uma rede com vários bots no qual sua ação maliciosa é amplificada.

1.20.4. Spyware: Os Spywares coletam informações pessoais ou empresariais e as enviam para terceiros. O Keylogger é um tipo de Spyware que captura as teclas digitadas pelo usuário, geralmente utilizado para roubar senhas.

1.20.5. Backdoor: O Backdoor ou Porta do fundo é uma vulnerabilidade que abre uma brecha para o atacante obter acesso indevido.

1.20.6. Cavalo de tróia: Também conhecido como Trojan o Cavalo de Tróia é um programa malicioso que se disfarça por um programa bem intencionado. O usuário executa, sem saber, um código malicioso pensando que está executando apenas um programa legítimo. Eles geralmente são disseminados por e-mails e redes sociais se passando por cartões, álbum de fotos, jogos e etc.

1.20.7. Rootkit: Conjunto de programas utilizado por um atacante para ocultar sua invasão e facilitar um futuro ataque. Os Rootkits podem ser utilizados em outros malwares para dificultar a detecção destes.

1.21. A efetivação de um ataque é o exito na exploração de uma ou mais vulnerabilidades. As motivações para realizar um ataque segundo o Cert.br, podem ser financeiras, por prestígio, demonstração de poder, por ideologia ou comerciais. Com novas tecnologias novos ataques surgem, mas o principais ataques conhecidos atualmente são:

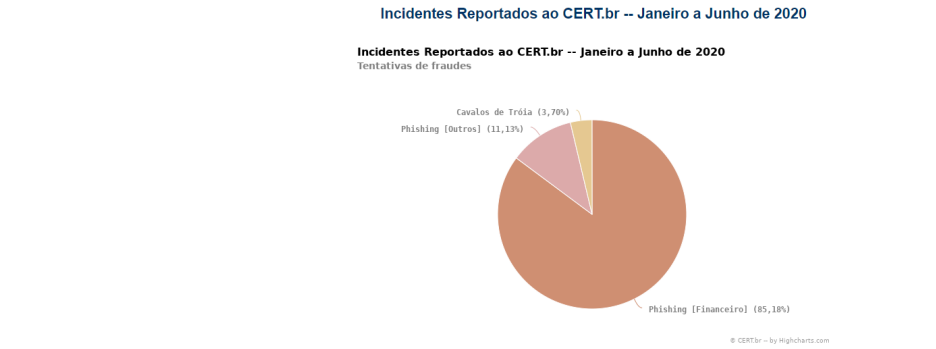
1.21.1. DoS e DDoS: Negação de Serviço do inglês Denial of Service, sigla DoS, ocorre quando um site (ou serviço) fica indisponível por receber uma grande quantidade de tráfego, não podendo atender as requisições legítimas. Os ataques DDoS (Distributed Denial of Service) são vários ataques DoS feitos de maneira distribuída dificultando assim o bloqueio da origem os ataques. Geralmente estes ataques provêm de computadores infectados com Bots participantes de uma rede Botnet.

1.21.2. Buffer Overflow: ou Estouro de Buffer ocorre quando um espaço de memória com tamanho fixo recebe um dado maior que seu tamanho, ocorrendo assim um vazamento

dados na memória sobrescrevendo a memória adjacente.

1.21.3. Spam: são e-mails não solicitados que são enviados em massa gerando tráfego desnecessário nas redes. Geralmente os Spams têm como intuito a divulgação de produtos, mas também são responsáveis por muitos golpes de Internet por disseminarem Malwares.

1.21.4. Phishing Scam: E-mails falsos que se passam por mensagens de instituições confiáveis, como bancos e órgãos governamentais. Seu intuito é induzir o usuário a instalar um programa malicioso ou visitar uma página falsa (cópia de uma verdadeira) para obter dados pessoais, como por exemplo, senhas e números de cartão de crédito. Segundo o Cert.br 87,05% das fraudes de janeiro a dezembro de 2019 eram de páginas falsas, conforme apresentado na imagem 3.



Legenda:

- **Cavalos de Tróia**: Tentativas de fraude com objetivos financeiros envolvendo o uso de cavalos de tróia.
- ***Phishing* [Financeiro]**: Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas. Engloba, por exemplo, páginas falsas de bancos, cartões, boletos e *sites* de comércio eletrônico.
- ***Phishing* [Outros]**: Outras tentativas de fraude envolvendo páginas falsas. Engloba, por exemplo, páginas falsas de serviços de documentos em nuvem, *streaming* de vídeo, *webmail* e redes sociais.

Imagem 3 - Fraudes reportadas ao CERT.BR , Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/fraude.html acesso em 13/01/2021

1.22. **Tipos de incidentes de segurança da informação:**

1.22.1. DNS Poisoning: Envenenamento de DNS é um ataque que forja um endereço falso no servidor de DNS. Assim, o atacante pode capturar senhas e números de cartões de crédito utilizando páginas clones do site original.

1.22.2. Ataque de Força Bruta: Programa que utiliza várias combinações de usuário e senha para conseguir acesso indevido a sistemas ou para descriptografar chaves e arquivos. Além do risco de acesso indevido, o Ataque de Força Bruta gera uma carga excessiva no alvo por ter responder e processar a várias tentativas de logins. Esta técnica é muito utilizada em servidores de SSH mal configurados.

1.22.3. Packet Sniffing: Packet Sniffing ou Farejamento de Pacotes é um método utilizado para capturar pacotes destinados a outras máquinas da mesma rede com objetivo de obter dados pessoais. Ativos de rede que utilizam broadcast de pacotes, como Hub, facilitam o farejamento dos pacotes. Em redes segmentadas por Switches o Packet Sniffing é possível com a utilização de outra técnica conhecida como Man-in-theMiddle (MiTM). Com MiTM o atacante forja a passagem dos pacotes da rede pela sua interface através do envenenamento da tabela ARP dos outros computadores.

1.22.4. Varreduras em Redes – Scan: Técnica onde o atacante descobre máquinas ativas e serviços disponíveis na rede. Em uma rede 192.1 68.0.0/24, por exemplo, o atacante envia ping para todos endereços possíveis para descobrir quais estão ativos. Com os endereços das máquinas ativas é feita uma nova varredura em cada máquina para descobrir suas portas abertas e seus respectivos serviços. Com isso o atacante pode explorar as vulnerabilidades destes serviços e prejudicar o computador alvo. Por exemplo, sabendo que o alvo possui a porta TCP 23 aberta, o atacante irá explorar vulnerabilidades de software ou configuração do serviço para obter acesso ao sistema.

1.22.5. SQL Injection: O ataque de Injeção de SQL consiste em inserir códigos SQL em um software vulnerável para obter ou danificar informações do Banco de dados.

1.22.6. CSS - Cross Site Scripting: XSS ou CSS o Cross Site Scripting é um ataque a um site vulnerável que aceita a inserção de códigos Javascript. Através do CSS o atacante pode inserir uma página externa para capturar logins e senhas.

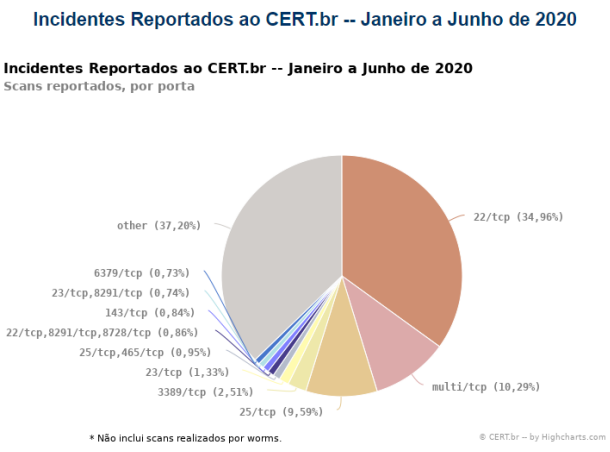


Imagem 4 - Scan reportados por porta - Fonte: CERT.br disponível em https://www.cert.br/stats/incidentes/2020-jan-jun/scan-portas.html acesso em 13/01/2021

2. DEFINIÇÃO DAS NECESSIDADES E REQUISITOS

2.1. **Ministério da Justiça e Segurança Pública**

2.2. O Ministério da Justiça e Segurança Pública possui um ambiente de Tecnologia da Informação e Comunicação (TIC) diversificado com vários recursos tecnológicos, sistemas legados e um grande número de usuários desses recursos, conforme apresentado nos relatórios (Docs SEI Nº 13742791, 13742757 e 13742631) e resumido abaixo:

Categoria	Total
Appliance de Segurança	14
Ativos de Rede	274

Host Físico no Datacenter	84
Sistemas Operacionais de Servidores	917
Armazenamento	21
Estação de Trabalho	4.334
Servidor de Aplicação	187
Sistemas Web	58
Serviços de rede	4
Total	5.893

Tabela 1 - Resumo do Parque de Ativos de TI

Nome	Domínios	Tipo de Domínio
consumidor.gov.br	consumidor.gov.br	Authoritative
defesadoconsumidor.gov.br	defesadoconsumidor.gov.br	Authoritative
infoseg.gov.br	infoseg.gov.br	Authoritative
justica.gov.br	justica.gov.br	Authoritative
justicagovbr.mail.onmicrosoft.com	justicagovbr.mail.onmicrosoft.com	Authoritative
migrantes.gov.br	migrantes.gov.br	Authoritative
mj.gov.br (default domain)	mj.gov.br	Authoritative
seguranca.gov.br	seguranca.gov.br	Authoritative
TOTAL DE DOMÍNIOS		8
TOTAL DE IP's		6.702

Tabela 2 - Domínios e IP's

2.3.

Imagem 5 - 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 14/01/2021.

2.4. Nesse cenário cresce a preocupação relacionada aos problemas com a segurança digital e o monitoramento das vulnerabilidades de segurança no ambiente computacional é absolutamente necessário para se manter a confidencialidade, a disponibilidade e a integridade das informações.

2.5. Em uma rede corporativa, com diversos usuários, manter os ativos livres de vulnerabilidades é um trabalho árduo para os administradores de rede. Alguns dos motivos que contribuem para este problema são:

- 2.6. Dificuldade em implantar uma política contra a instalação de novos softwares pelos usuários. Vários softwares possuem vulnerabilidades conhecidas em algumas de suas versões a exemplo leitores de PDF e navegadores Web;
- 2.7. Desconhecimento dos usuários sobre prevenção contra malwares, pois muitos através de e-mails falsos e mensagens em redes sociais instalam códigos maliciosos;
- 2.8. A diversidade de versões de softwares e sistemas operacionais;
- 2.9. Controle das atualizações dos softwares e sistemas operacionais; e
- 2.10. Impossibilidade dos profissionais de Tecnologia de Informação estarem cientes de todas vulnerabilidades descobertas, principalmente as mais recentes.

2.11. Diante destes fatores a Diretoria de Tecnologia da Informação e Comunicação - DTIC necessita de ferramentas que a auxilie a manter o parque computacional o menos vulnerável possível. É possível atender este requisito da Segurança da Informação com uma solução de gestão vulnerabilidades, a qual é composta, entre outros por um software conhecido como Scanner de Vulnerabilidade.

2.12. Desse modo, busca-se implementar soluções de software capazes de testar os ativos de TI e as aplicações web periodicamente em busca de quaisquer vulnerabilidades, sejam elas relativas a atualização de sistemas operacionais e servidores de aplicação, configurações de serviços ou outras falhas técnicas. Além disso, é preciso que as soluções forneçam relatórios para que seja possível o acompanhamento do trabalho de identificação e mitigação de riscos.

2.13. Segue abaixo a especificação das necessidades de negócio e tecnológicas, e dos requisitos necessários e suficientes à escolha da solução de TIC.

3. IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

Id	Funcionalidades
1.	Aumento da segurança da informação e comunicação no âmbito do Ministério da Justiça e Segurança Pública e o sigilo das informações do cidadão; Gerenciamento de Vulnerabilidades em ativos e Sistemas Operacionais; Gerenciamento de Vulnerabilidades em Sistemas e páginas WEB; Detecção e Correção de falhas de softwares que possam acarretar riscos na segurança, na funcionalidade e no desempenho dos sistemas; Implantação de mecanismos para realizar o bloqueio de ataques constantes; Identificação de novas soluções de segurança e realização de suas alterações; Foco na melhoria constante do sistema de segurança de dados corporativos; Auxílio na implementação de políticas de segurança; Agilidade na identificação de falhas.

3.1. Identificação das necessidades tecnológicas

Id	Necessidades Tecnológicas
1	Fornecimento de solução de segurança para proteção de aplicações, servidores físicos, virtuais e container com serviços de implementação e capacitação; Solução de análise de vulnerabilidades e Serviços técnicos especializados na área de Segurança da Informação; Análise de Vulnerabilidades; Gerenciamento de patches; Gerenciamento da configuração de segurança; Auditoria de software de alto risco; Detecção e mitigação de vulnerabilidades de dia zero; Aprimoramento da segurança dos servidores web.

3.2. Demais requisitos necessários e suficientes à escolha da solução de TIC

Id	Demais necessidades

1	Integração e Customização dos Sistemas de Informação existentes; Otimização dos processos de infraestrutura da TIC conforme as melhores práticas; Testar os hosts (físicos e virtuais), comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de software; Testar as aplicações e páginas web, internas e externas, comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de software; Emitir relatórios de acompanhamento dos testes e das vulnerabilidades encontradas, apontando quando forem solucionadas. Aumento da proteção dos ativos de informação do Ministério da Justiça e Segurança Pública

4. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

4.1. Para estimar a quantidade de bens e serviços necessários para a composição da solução a ser contratada é importante entender como funciona as ferramentas de gestão de vulnerabilidades, seu modelo de licenciamento e a estratégia de segurança da informação da Diretoria de Tecnologia da Informação e Comunicação - DTIC.

4.2. Um dos principais componentes das soluções de gestão de vulnerabilidades é o scan de vulnerabilidade, que tem por objetivo identificar os riscos e vulnerabilidades externas e internas de uma rede. O scan de vulnerabilidades é uma ferramenta que faz uma varredura em IP's externos ou ativos na rede interna, tipificando as vulnerabilidades por riscos, identificando e classificando as possíveis brechas de segurança presentes na rede.

4.3. O scan de vulnerabilidades é uma ferramenta muito eficaz, pois opera de maneira constante, detectando qualquer alteração que acontece dentro do período que foi configurado na ferramenta. Basicamente, o scan atua com duas estratégias: varreduras internas e externas da rede. Isso porque, ele realiza a varredura nos IP's, classificando vulnerabilidades e, assim, identificando as brechas de segurança da rede.

4.4. No caso das verificações externas de vulnerabilidades, eles identificam as maiores ameaças imediatas à rede, conferem as atualizações de softwares e firmwares necessárias para manutenção, portas e protocolos, ou seja, os pontos de entrada da rede e buracos no firewall de rede.

4.5. Já a varredura da vulnerabilidade interna, como o nome indica, tem como objetivo a rede interna. Elas podem ser aprimoradas com credenciais para efetuar login no dispositivo e executar verificações de conformidade e vulnerabilidades.

4.6. Além dessas estratégias, o scan utiliza a aquisição ativa e passiva de informações. A aquisição ativa compreende em enviar um grande número de pacotes, possuindo pontos característicos, que, na maior parte do tempo, não seguem as recomendações, analisando as respostas para determinar a versão da aplicação utilizada. Com efeito, cada aplicação utiliza os protocolos de uma maneira ligeiramente diferente, que permite distingui-los.

4.7. No caso, a aquisição passiva é menos intrusiva, correndo menos risco de ser detectada por um sistema de detecção de intrusos, o IDS. Ele funciona analisando os campos dos datagramas IP que circulam sobre uma rede, com a ajuda de um sniffer. A caracterização, na versão passiva, analisa a evolução dos valores dos campos sobre séries de fragmentos, o que implica um tempo de análise muito mais longo. Este tipo de análise é muito difícil, ou mesmo impossível de detectar.

4.8. **Plataforma de Gestão de Vulnerabilidades e Auditoria de Configurações de Ativos de Rede**

4.9. Uma vez entendido o funcionamento desse componente das ferramentas de gestão de vulnerabilidades fica fácil o entendimento do porquê o modelo de licenciamento atual de mercado para a plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, baseia-se na quantidade de endereços IP's escaneados.

4.10. Como visto, a análise de vulnerabilidade objetiva detectar falhas em diversos componentes como: aplicações, softwares, equipamentos, sistemas operacionais, dentre outros. Deve-se fazer continuamente o processo de verificação e análise da rede, para que a mesma fique sempre atualizada e livre de acessos não permitidos e indesejáveis. Essa análise pode ser feita local e/ou remota.

4.11. Após tal análise são oferecidos relatórios com as respectivas soluções propostas. Nesses relatórios podem constar também itens dos quais objetiva-se melhorar a segurança do ambiente, não necessariamente relacionados às falhas encontradas. Divide-se em dois tipos: Ativa - Encontra-se e corrige-se as falhas, emitindo relatórios apenas do que foi feito. Passiva - Encontra-se as falhas e emite-se relatórios para que o cliente se encarregue de corrigir.

4.12. O relatório de análise de vulnerabilidades é constituído de informações essenciais que indicam a melhor estratégia para manter o ambiente da Organização protegido de falhas, ataques e invasões, através de uma avaliação completa, auxiliando de uma forma mais fácil e assertiva a tomada de decisão em relação à segurança da informação.

4.13. Conforme relatório técnico (Doc Sei nº 13742631) da Central IT, empresa contratada para 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 remoto e/ou presencial de 1º, 2º e 3º Níveis, a usuários de soluções 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 Comunicação - TIC, para o Ministério da Justiça e Segurança Pública e suas unidades regionais, o Ministério possui um total de 6.702 IP's e 8 domínios.

4.14. Segundo a Norma Complementar 04/IN1/DSIC/GSI/PR, ativos de informação são os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

4.15. Dada a grande quantidade de endereços IP's e de ativos de informação do Ministério da Justiça e Segurança Pública, conforme mencionado neste e em tópicos anteriores, a estratégia de segurança da informação da DTIC, visa priorizar num primeiro momento a proteção dos ativos estratégicos do Ministério. Deve-se ter em mente que os ativos estratégicos de uma organização são os ativos que permitem a sua diferenciação face às demais organizações e a sustentação do negócio no longo prazo.

4.16. Considerando que o modelo de licenciamento atual de mercado para a plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, baseia-se na quantidade de endereços IP's escaneados e considerando o total 6.702 endereços de IP's atuais, acrescidos de uma **previsão de crescimento de 30%**(trinta) porcento, estima-se a necessidade de uma quantidade de licenças necessárias para **9.000** IP's, número arredondado para fins de cálculo.

4.17. A previsão de crescimento é baseada na quantidade de aquisições de equipamentos previstas no PDTIC 2021-2023 (13743301), sobretudo nas necessidades vinculadas as ações A0002, A0007, A0009, A0010, A0040, A0042, A0053, A0062, como também na implantação de novos sistemas Web, aplicações e soluções que requerem a instalação de novas máquinas virtuais.

4.18. Desta forma, **a aquisição deverá ocorrer por meio de 9 licenças contemplando 1.000 IP's cada uma, por ano**. Com as primeiras licenças adquiridas, serão analisados os Appliance de Segurança(14), os Ativos de rede(274), os Hosts físicos no Datacenter(84), os sistemas operacionais de servidores(917), os dispositivos de armazenamento (21), os servidores de aplicação(187) e as estações de trabalho da alta administração e colaboradores diretos. com as demais licenças adquiridas no período de um ano, será possível cobrir todo o parque computacional do Ministério.

4.19. Com essa estratégia procura-se evitar o que ocorre na maioria das vezes em outras organizações, quando os projetos de análise de vulnerabilidades terminam apenas com a entrega de diversos relatórios, e com poucas ações realizadas, o famoso projeto de relatório de gaveta. Além disso, os períodos entre as aquisições das licenças possibilitará a execução dos planos de ação, ao mesmo tempo em que trará economia de recursos. A Gestão de Vulnerabilidades compreende todo o ciclo de vida necessário para que as vulnerabilidades sejam tratadas, priorizadas, tendo acompanhamentos por períodos através de relatórios gerenciais e planos de ações factíveis.

4.20. **Solução de Análise em Aplicações Web**

4.21. Para compreender a necessidade dessa solução é importante entender como uma ferramenta de análise funciona e a importância de realizar verificações de segurança em bibliotecas.

4.22. Os testes por análise dinâmica para aplicações web funcionam basicamente em dois passos:

1. 4.23. É executada uma varredura completa na aplicação, identificado as páginas e recursos por meio de navegação nas URLs, processo conhecido pelo termo em inglês *crawling*.
2. 4.24. Baseado no resultado na navegação, é inferido possíveis vulnerabilidades que o recurso possa ter. Então é realizado a tentativa de exploração da falha, desde a manipulação de cookies à injeção de SQL. Baseado na resposta do servidor, é possível identificar se a vulnerabilidade é explorável ou não.

4.25. Hoje a maior parte do código de uma aplicação é originado de bibliotecas de fonte aberto ou código proprietário. As bibliotecas são geralmente módulos de software de terceiros projetados para executar funções frequentemente necessárias. Elas fornecem mecanismos como suporte para acesso a dados, gerenciamento de recursos, comunicações e criação de interface com o usuário. Por isso, muitas vezes, as aplicações contém fragilidades que um atacante sem muito esforço possa explorar, sem necessitar um conhecimento prévio da aplicação.

4.26. Os pesquisadores de segurança periodicamente identificam vulnerabilidades em bibliotecas e disponibilizam os detalhes da descoberta através de um processo de divulgação de sua própria escolha. Algumas dessas divulgações são coordenadas com o CVE - Common Vulnerabilities and Exposures ou com o Open Source Vulnerability Database (OSVDB). Porém uma boa parte simplesmente são publicadas em posts de blogs ou e-mails para listas de discussão.

4.27. As vulnerabilidades que as bibliotecas podem conter colocam em risco a segurança da aplicação como um todo. O Ministério da Justiça e Segurança Pública, possui, pelo menos, 58 (cinquenta e oito) serviços críticos e essenciais, a maioria disponibilizado por meio de aplicações web, conforme relatório(13742757).

4.28. Demonstra-se dessa forma, a importância de identificar e tratar as vulnerabilidades desses sistemas, pois eles contém além de informações de segurança pública, informações de inteligência e dados pessoais que precisam ser protegidos.

4.29. **Consultoria Especializada**

4.30. Segundo dados do Portal de Gestão de Pessoas, disponível na intranet em janeiro de 2021, na Diretoria de Tecnologia da Informação e Comunicação trabalham 70 pessoas, sendo que destas apenas 8 são do quadro de ativo permanente, o que equivale a 11,42% do total. Já a Coordenação de Riscos e Segurança da Informação - CRS, responsável pela gestão e fiscalização da presente contratação, possui apenas 8 pessoas, sendo destas 4 contratos temporário, 1 Exercício Descentralizado e 3 requisitados, ou seja, não possui servidor do próprio quadro.

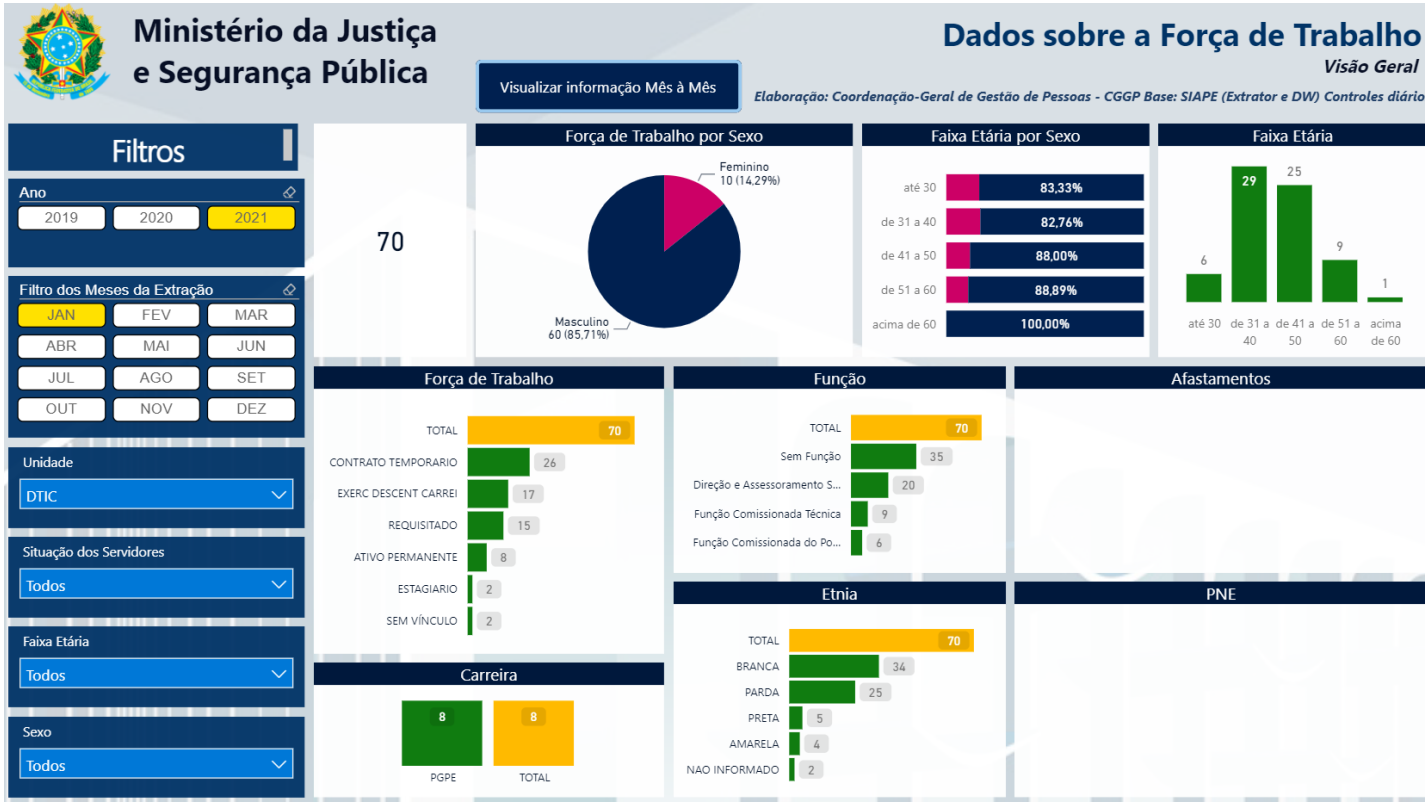


Imagem 6 - Força de trabalho do MJSP, Fonte: Portal Gestão de Pessoas, disponível em https://justicagovbr.sharepoint.com/sites/intra-CGGP/SitePages/For%C3%A7a-de-Trabalho.aspx, acesso em 19/01/2021.

4.31. A consultoria especializada será realizada sob demanda e tem como objetivos realizar as seguintes tarefas:

- 4.31.1. Esclarecer dúvidas de usuários em relação à operação do sistema;
- 4.31.2. Acompanhar, quando solicitado, todas as operações realizadas no sistema;
- 4.31.3. Prestar serviços de suporte técnico para a solução de problemas que impeçam o perfeito funcionamento do sistema;
- 4.31.4. Identificar problemas inerentes ao software e ao ambiente onde este se encontra instalado;
- 4.31.5. Discutir implementações de melhorias, visando possíveis adequações;
- 4.31.6. Produzir relatórios personalizados em diversos formatos;
- 4.31.7. Documentação e transferência de conhecimento das atividades técnicas realizadas;
- 4.31.8. Apoio no desenvolvimento de dashboard´s e solução de problemas internos, relativos às licenças adquiridas; e
- 4.31.9. Integração da solução com a ferramenta de ITSM utilizada pelo órgão.

4.32. Na prestação dos serviços de consultoria especializada, deverão ser utilizados profissionais com qualificação e treinamento adequados para o desenvolvimento das tarefas relacionadas anteriormente. Para a consultoria especializada foi estimado **480 horas por ano**, para cada solução, essa estimativa foi obtida considerando a média do tempo da análise de duas PoC's (*Proof of Concept),* prova de de conceito, de ferramentas de vulnerabilidades, considerando o tempo de varredura e o tempo de análise e também com base na análise de outras contratações de TIC do Ministério.

4.33. Portanto sugere-se que os itens a serem contratados , sejam os itens relacionados na tabela 1 - Relação de itens da contratação.

Objeto	Unidade	Quantidade

Licenciamento de plataforma de gestão de vulnerabilidades e auditoria de configurações de ativos de rede, contemplando no mínimo 1.000 endereços IP, por ano de uso, com garantia e atualização upgrade/update por até 24(vinte e quatro) meses	Licença	9
Consultoria Especializada	horas/ano	480
Licenciamento para solução de análise em aplicações Web, pacote para 8 (oito) domínios (FQDN), por ano de uso, com garantia e atualização upgrade/update por até 24(vinte e quatro) meses	Licença	1
Consultoria Especializada	horas/ano	480

Tabela 3 - Relação de itens da contratação

5. ANÁLISE DE SOLUÇÕES

5.1. Conforme inciso II do art. 11, deve-se verificar para composição da análise comparativa:

5.1.1. – A disponibilidade de solução similar em outro órgão ou entidade da Administração Pública;

5.1.2. – As alternativas do mercado;

5.1.3. – A existência de software público brasileiro;

5.1.4. – As políticas, os modelos e os padrões de governo, a exemplo do ePing, eMag, ePwg, ICP-Brasil e e-ARQ Brasil, quando aplicáveis;

5.1.5. – As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc);

5.1.6. – A possibilidade de aquisição na forma de bens ou contratação como serviço;

5.1.7. – Os diferentes modelos de prestação do serviço;

5.1.8. – Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;

5.1.9. – A ampliação ou substituição da solução implantada.

5.1.10. Com base neste levantamento, cenários ou arranjos poderão ser formados para compor as soluções possíveis para atendimento da necessidade.

6. IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Cenário 1
Solução	Utilização de solução do Portal do Software Público Brasileiro
Descrição	O Software Público Brasileiro é um tipo específico de software livre que atende às necessidades de modernização da administração pública de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e é compartilhado sem ônus no Portal do Software Público Brasileiro, resultando na economia de recursos públicos e constituindo um recurso benéfico para a administração pública e para a sociedade.
Fornecedor	Portal do Software Público Brasileiro
Análise da Solução	O presente cenário tem o objetivo de analisar a adquisição junto ao Portal do Software Público Brasileiro para atender às necessidades do MJSP. O principal objetivo do Portal é promover o desenvolvimento de um "ambiente colaborativo que não só reduz os custos do governo, mas também permite o desenvolvimento de artefatos tecnológicos" (Santanna, 2007). De acordo com Santanna, "o conceito de utilização livre de código fonte - que deve sustentar as sociedades modernas - é central para o Portal do Software Público Brasileiro. A Administração Pública brasileira precisava de um ambiente no qual diversos atores sociais fossem capazes de compartilhar suas soluções já testadas e aprovadas a fim de evitar, entre outros fatores, a sobreposição de custos com outras soluções que são similares às que já existem" (Santanna, 2007). Além disso, o Portal colabora para a geração de emprego e renda, facilitando o contato entre pessoas que pretendem utilizar soluções informatizadas e aqueles que fornecem serviços. A rede estabelecida cria um complexo sistema de garantias econômicas, políticas e relações sociais que envolvem diversas esferas da sociedade. O software, neste contexto, não é apenas um produto, mas também um artefato por meio do qual seus criadores proporcionam novos referenciais de produção. Os atores neste cenário são simultaneamente produtores e consumidores, o que Tapscott & williams definem como os prosumers" (Tapscott & williams, 2007). Sempre que possível são utilizados softwares desenvolvidos na plataforma de Software público no ambiente de processamento central do MJSP, como por exemplo, os Sistema de Informação Eletrônica - SEI. Conforme pesquisa no portal de software público Brasileiro, registrada no documento SEI (13709507), Constam 81 softwares disponíveis no portal na data pesquisada, no entanto **não encontra-se disponível nenhuma solução de gestão de vulnerabilidades**. Conclui-se pelos fatos expostos que não é possível adotar os softwares disponíveis no Portal de Software Público Brasileiro para atender às necessidades do MJSP

Id	Cenário 2
Solução	Utilização de softwares livres
Descrição	Utilização de ferramentas livres ou gratuitas, como os softwares Wireshark, Nmap, Metasploit, OpenVas...
Fornecedor	Comunidades *Open Source* e páginas específicas dos projetos.
Análise da Solução	A solução proposta atende apenas parte da necessidade, pois a utilização desse cenário implica em não contar com suporte técnico especializado, ademais a atualização da base de vulnerabilidades e falhas não possui a mesma frequência de cenários com softwares pagos. Além disso, a adoção da solução proposta, por não possuir uma equipe dedicada de pesquisadores para avaliar e atualizar a ferramenta quando da descoberta de vulnerabilidades de dia zero não provê uma atualização tempestiva, não atendendo às necessidade do Ministério. A vulnerabilidade de dia zero é uma vulnerabilidade encontrada em um sistema, um hardware ou um software e pode ser uma porta para ameaças, como um ataque de malware. Em outras palavras, vulnerabilidade de dia zero é uma falha que precisa ser corrigida o mais rápido possível por causa dos riscos que ela gera para as organizações. Ela pode ocasionar uma exploração de dia zero, um ataque digital que faz uso das vulnerabilidades de dia zero para instalar softwares maliciosos em um dispositivo. Outro ponto desfavorável ao cenário apresentado é que os relatórios fornecidos pelas ferramentas não apresentariam rastreabilidade das atividades já realizadas nos ativos e sistemas, pois seriam utilizadas ferramentas de diferentes fabricantes para realização de diferentes atividades complementares. Seriam utilizadas, por exemplo, ferramentas específicas para detectar dispositivos remotos, como firewalls e roteadores com suas marcas e modelos, além da verificação de conexões e pacotes de rede como é o caso do Nmap e Wireshark. Outras ferramentas como o Metasploit e OpenVas para realizar exames rigorosos contra um conjunto de endereços IP e outras ferramentas de scanners para segurança de rede sem fio como Aircrack. Assim, como se vê a solução proposta não atende grande parte das necessidades tecnológicas e de negócio requeridas pelo Ministério.

Id	Cenário 3
Solução	Contratação de empresa especializada para fornecimento e instalação de solução de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo a aquisição de serviços de Consultoria Especializada, suporte 24x7, com garantia (manutenção e suporte técnico)
Descrição	Aquisição de software de gerenciamento de vulnerabilidades em Ativos e web applications, com modelo de licenciamento anual
Fornecedores*	Brinqa, Digital Defense, Expanse, Kenna Security, NopSec, Outpost24, Qualys, Rapid7, RedSeal, RiskIQ, RiskSense, Skybox Security e Tenable
Fornecedores**	Synopsys, CheckMarx, Veracode, MicroFocus, Whitehat Security, Constrast Security, HCL Software, Rapid7, Onapsis, GitLab e CAST
Análise da Solução	Nesse cenário é contemplado a aquisição de solução baseada em nuvem (*cloud computing*). Essa solução apresenta facilidade de gerenciamento, valor de aquisição adequado e atualização automática da plataforma. No modelo de contratação em nuvem, todo o faturamento será na forma de custeio. Todas os requisitos de funcionalidades do projeto são atendidos por esse cenário. As soluções analisadas Qualys (VM e WAS) e Tenable.io conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. Ambas foram testadas com versão de avaliação e os resultados e relatórios se mostraram adequados.

* Fonte: Relatório The Forrester Wave™: Vulnerability Risk Management, Q4 2019. The 13 providers that matter most and How they Stack Up. (Fornecedores de ferramentas de vulnerabilidades em ativos)

** Fonte Gartner (April 2020) (Fornecedores de ferramentas de vulnerabilidades em Aplicações)

7. ANÁLISE COMPARATIVA DE SOLUÇÕES

7.1. Consiste em uma análise crítica entre as diferentes soluções, considerando o aspecto econômico (TCO) entre as Soluções e os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

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		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2	X		
	Solução 3		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
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			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

8. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

8.1. Conforme § 1º do art. 11, as soluções identificadas e consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação (breve descrição e justificativa), dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

CENÁRIO 1	
Análise da Solução	Não existe solução disponível no Portal do Software Público Brasileiro.
CENÁRIO 2	
Análise da Solução	A solução proposta atende apenas parte da necessidade, pois a utilização desse cenário implica em não contar com suporte técnico especializado, além disso a atualização da base de vulnerabilidades e falhas não possui a mesma frequência de cenários com softwares pagos.

9. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

9.1. <Conforme inciso III do art. 11, deve-se proceder a comparação de custos totais de propriedade para as soluções técnica e funcionalmente viáveis>.

Cenário	Estimativa (R$)
1.	R$ 0,00
2.	R$ 0,00
3.	R$ 3.982.447,80

10. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

Solução Viável 1
Custo Total de Propriedade – Memória de Cálculo
Cálculo do Custo Total de Propriedade da Solução 3, considerando os custos inerentes ao ciclo de vida dos bens e serviços da solução, incluindo custos direitos e indiretos, a exemplo dos valores de aquisição dos ativos, insumos, garantia, manutenção, etc. Será disponibilizado na fase de Pesquisa de Preço.

11. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Descrição da solução	Estimativa de TCO ao longo dos anos					Total
	Ano 2021	Ano 2022	Ano 2023	Ano 2024	Ano 2025	
Contratação de empresa especializada para fornecimento e instalação de solução unificada de gestão de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo a aquisição de serviços de operação assistida e Consultoria Especializada , suporte 24x7, com garantia (manutenção e	**R$ 2.532.748,47**	**R$ 1.355.134,53**	**R$ 2.627.313,27**	**R$ 1.355.134,53**	**R$ 1.408.221,43**	**R$ 9.278.552,23**

suporte técnico)						

12. **DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA**

12.1. **Contratação de empresa especializada para fornecimento e instalação, por meio de subscrição de licenças de software, de solução de avaliação de vulnerabilidades em ativos de tecnologia da informação e aplicações web, compreendendo a aquisição de serviços de consultoria especializada, suporte 24x7, com garantia (manutenção e suporte técnico) para o Ministério da Justiça e Segurança Pública (MJSP), incluindo a garantia de atualização das versões, pelo período de 24(vinte e quatro) meses, podendo ser prorrogada até o prazo máximo de 48(quarenta e oito) meses.**

12.2. A presente aquisição visa suprir o Ministério da Justiça e Segurança Pública com o aparato tecnológico necessário para o efetivo cumprimento da sua missão de trabalhar para a consolidação do Estado Democrático de Direito e de sua visão em ser reconhecido pela sociedade como protagonista na defesa da cidadania, na proteção de direitos, na integração da política de segurança pública, na cooperação jurídica internacional e no combate à corrupção, ao crime organizado e ao crime violento.

12.3. Nesse sentido, o fortalecimento e ampliação da estrutura e dos serviços de tecnologia da informação e comunicação contribuem, invariavelmente, para o aumento de desempenho dos servidores que atuam diretamente nas áreas finalísticas. Desta forma, a presente aquisição busca o alinhamento estratégico entre a área de Tecnologia da Informação e as áreas de negócio do Ministério da Justiça e Segurança Pública.

12.4. Na sociedade contemporânea, ao mesmo tempo em que as informações são consideradas os principais ativos de uma organização, as mesmas estão também sob o constante risco. por isso, sua perda ou vazamento constitui um enorme prejuízo para as organizações. Principalmente, para um órgão como o Ministério da Justiça e segurança pública que atua, dentre outras, em áreas que envolvem Segurança Pública, combate à corrupção e lavagem de dinheiro, proteção e defesa do consumidor, repressão ao tráfico ilícito de drogas, operações policiais e atividades de inteligência, a ocorrência de tais eventos deve ser salvaguardada.

12.5. A adoção de um processo de gestão de vulnerabilidades com o objetivo de reduzir drasticamente problemas como malwares, contas inativas, senhas ruins ou sistemas desatualizados, bem como a mitigação de riscos e a proteção de dados, é o que se espera com a utilização de uma ferramenta como a solução a ser contratada.

12.6. Tem-se a clareza de que um processo de gestão de vulnerabilidades é muito maior e mais complexo que apenas a execução de uma ferramenta e que de forma básica todo processo de gestão de vulnerabilidades deve apresentar no mínimos as etapas de **Identificação de vulnerabilidades; Verificação da vulnerabilidade; Mitigação de Vulnerabilidades e Remediação de Vulnerabilidades**. No entanto, a escolha de uma ferramenta de avaliação de vulnerabilidades é um pré requisito conforme demonstra a imagem 7, nova estrutura de orientação para gerenciamento de vulnerabilidades (disponível em https://blogs.gartner.com/augusto-barros/2019/10/25/new-vulnerability-management-guidance-framework/ acesso 15/04/2021).

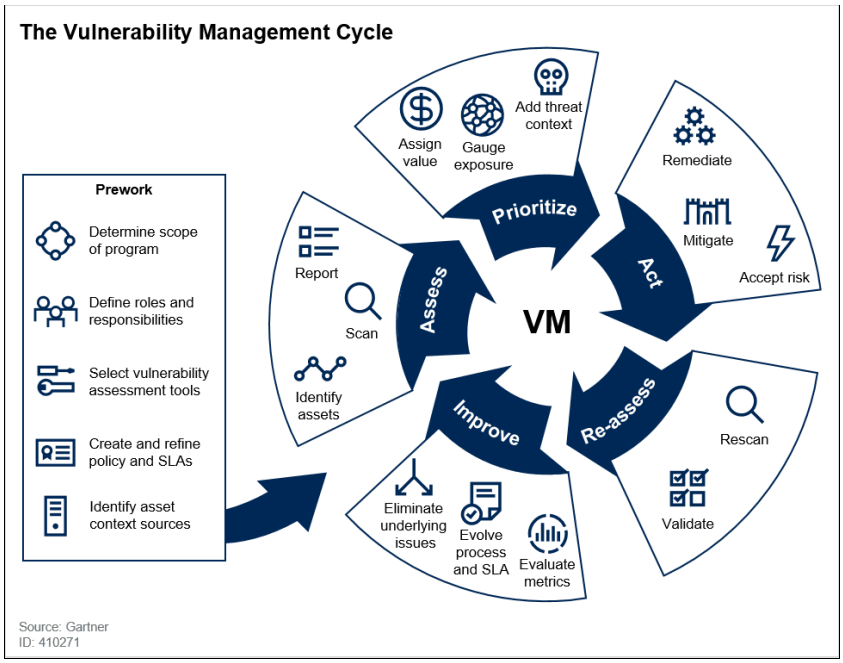


Imagem 7 - Nova estrutura de orientação para gerenciamento de vulnerabilidades (disponível em https://blogs.gartner.com/augusto-barros/2019/10/25/new-vulnerability-management-guidance-framework/ acesso 15/04/2021)

12.7. Ressalta-se que a contratação está alinhada com as boas práticas e aos normativos e padrões de segurança da informação, como por exemplo, a norma ABNT NBR ISO/IEC 27002 que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

12.8. A gestão de vulnerabilidades técnicas, a qual tem por objetivo prevenir a exploração de vulnerabilidades técnicas, é um dos controles comumente aceitos e necessário dentro do processo de implementação de um sistema de gestão da segurança da informação baseado na ABNT NBR ISO/IEC 27001 descrita no item 12.6.

12.9. A contratação está alinhada, também, a Lei Geral de Proteção de Dados Pessoais (LGPD), a qual no Capítulo VII que trata da segurança e das boas práticas, dispõe no artigo 46 que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

12.10. **Benefícios esperados com a contratação**

12.10.1. **Maior controle de segurança da informação e proteção de dados no âmbito do Ministério da Justiça e Segurança Pública** através da redução de malwares, sistemas desatualizados, dentre outros problemas;

12.10.2. **Aumento dos esforços de correção e testes de eficácia**: as análises de vulnerabilidades de rede permitem não só a identificação de problemas de rede, mas também ajuda na sua priorização e no desenvolvimento de uma estratégia para lidar com aqueles mais críticos;

12.10.3. **Melhoria na gestão de mudanças e no gerenciamento de patches**: faz parte da gestão de vulnerabilidades centralizar e gerar todos os feedbacks sobre os problemas, as suas correções e as próximas ações;

12.10.4. **Fortalecimento da atuação da Equipes de Tratamento de Incidentes de Segurança nas Redes de computadores**: A identificação e o tratamento das vulnerabilidades auxiliarão a ETIR na execução de suas responsabilidades de análise e respostas às notificações e atividades relacionadas a incidentes de segurança em redes de computadores além da redução desses incidentes;

12.10.5. **Apoio nas auditorias de Segurança da Informação e Comunicações** a obtenção de relatórios detalhados permitirá a devida diligência durante as auditorias;

12.10.6. **Atualização da Política de Segurança da Informação e Comunicações**: O gerenciamento de vulnerabilidades possibilitará aplicar melhorias na segurança da informação e na revisão da POSIC e suas normas complementares.

12.10.7. **Auxílio nos requisitos regulamentares**: A identificação e o tratamento das vulnerabilidades contribuirá para que o Ministério mantenha-se em conformidade com:

12.10.8. os normativos emanados pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República;

12.10.9. os princípios e controles de segurança definidos nos padrões ABNT NBR ISO/IEC 27001, 27002, 27005, 27011 e 27014;

12.10.10. a Lei Nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

12.10.11. os frameworks de processos de governança e boas práticas como o ITIL e COBIT.

12.11. Nesta fase de planejamento da contratação, a equipe estimou o valor para a presente contratação para o período de 24 meses em **R$ 3.982.447,80 (três milhões, novecentos e oitenta e dois mil quatrocentos e quarenta e sete reais e oitenta centavos)**, valor este oriundo de levantamento prévio com várias empresas, entretanto será feito o levantamento da pesquisa de mercado por área competente dentro da Sede do Ministério da Justiça e Segurança Pública junto aos *players* do mercado de Tecnologia da Informação com, posterior, juntada ao Termo de Referência, para posterior análise desta equipe técnica.

13. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO PARA O MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

13.1. Estima-se um custo total da contratação, para os cinco anos, o valor de R$ 9.278.552,23 (nove milhões, duzentos e setenta e oito mil quinhentos e cinquenta e dois reais e vinte e três centavos) .

14. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

14.1. 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), sendo descritas e tratadas como macro requisitos e necessidades de negócio como serviço para tal finalidade.

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

14.3. 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.

15. APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi atualizada pela PORTARIA SAA Nº 64, DE 9 DE JULHO DE 2021 (15257536).

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	
Nome	LUCAS REINEHR DE ANDRADE
Matrícula/SIAPE	3223177
Integrante Requisitante	
Nome	IVANILDO DE OLIVEIRA DA SILVA JR
Matrícula/SIAPE	1535600
Integrante Requisitante Substituto	
Nome	JOÉDES CARDOSO DA SILVA
Matrícula/SIAPE	3730955
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 **Joedes Cardoso da Silva**, **Integrante Requisitante - Substituto(a)**, em 28/07/2021, às 15:25, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Lucas Reinehr de Andrade**, **Integrante Técnico(a)**, em 28/07/2021, às 17:44, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Leonardo Bueno de Melo**, **Diretor(a) da Tecnologia da Informação e Comunicação - Substituto(a)**, em 10/08/2021, às 20:28, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **15356773** e o código CRC **0C7681D5**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.