Guia de Gerenciamento de Vulnerabilidades

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 2.0

Brasília, março de 2023

GUIA DE GERENCIAMENTO DE VULNERABILIDADES

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck

Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PROTEÇÃO DE DADOS

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Proteção de Dados

Equipe Técnica de Elaboração

Francisco Magno Felix Nobre

Ivaldo Jeferson de Santana Castro

Raphael César Estevão

Equipe Revisora

Luiz Henrique do Espírito Santo Andrade

Rogério Vinicius Matos Rocha

Romário César de Almeida

Equipe Técnica de Revisão – Versão 2.0

Francisco Magno Felix Nobre

Julierme Rodrigues da Silva

Rogério Vinícius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
14/06/2022	1.0	Guia de Gerenciamento de Vulnerabilidades	Equipe Técnica de Elaboração
20/06/2022	1.1	Correção de erros ortográficos; inserção dos termos "baselines de segurança" e "controle de compensação" no tópico definições gerais; reestruturação dos riscos do tópico 2.1.5.	Equipe Técnica de Elaboração
31/03/2023	2.0	Atualização para alinhamento com o Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo I.	Equipe Técnica de Atualização

Sumário

Aviso Preliminar e Agradecimentos 4
Introdução 5
Definições Gerais 7
Gerenciamento de Vulnerabilidades 9
1 Ciclo de detecção 10
2 Ciclo de relatórios 15
3 Ciclo de remediação 21
Imagens 26
Referência legal e de boas práticas [Documentos norteadores] 27
ANEXO I 29
ANEXO II 37
ANEXO III 41

Aviso Preliminar e Agradecimentos

O presente Guia, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visa a auxiliar no Gerenciamento de Vulnerabilidades, em atendimento ao previsto no art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve 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 dos dados que estão sob sua custódia. Adicionalmente, o Gerenciamento de Vulnerabilidades visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Este documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do Center for Internet Security (CIS), da International Organization for Standardization (ISO), do National Institute of Standards and Technology (NIST). Com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica da Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST e vice-versa;

b) não se manifesta em nome de autoridades de privacidade e segurança da informação;

c) não é coautora das publicações internacionais abordadas;

d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente guia; e

e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referência legal e de boas práticas” deste documento.

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, às autoridades de proteção de dados referenciadas, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para elaboração deste documento.

Este Guia será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas neste documento.

Introdução

Este Guia tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a realizar seu Gerenciamento de Vulnerabilidades no âmbito institucional.

O Controle 7 do Guia do Framework de Privacidade e Segurança da Informação (p. 45) estabelece que:

__Controle 7: Gestão Contínua de Vulnerabilidades__ - Desenvolver um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos dentro da infraestrutura da organização, a fim de remediar e minimizar a janela de oportunidade para atacantes. Monitorar as fontes públicas e privadas para novas informações sobre ameaças e vulnerabilidades.

O presente documento serve como um modelo prático a ser utilizado para auxiliar na adoção do Controle 7 do Guia do Framework de Privacidade e Segurança da Informação[1] v1 e respectivas evoluções desta versão (1.1, 1.2 etc.) elaborado e publicado pela SGD. As medidas do Controle 7 que estão contempladas por este modelo são: 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7.

Hoje, mais do que em qualquer outro momento da história, o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados.

Nesse contexto, as instituições federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entidades como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

A proteção dessas informações pelo Governo enquanto agente de tratamento está designada no **art. 46 da Lei Geral de Proteção de Dados**, sancionada em 14 de agosto de 2018:

> *"Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de*

[1] < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 03/02/2023.

situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

Importante ressaltar que este Guia não dispensa o órgão de considerar as diretrizes gerais estabelecidas para implementação da Política de Segurança da Informação, conforme prevê o art.12, Inciso IV da Instrução Normativa Nº 01/GSI/PR, bem como os Capítulos III e IV da Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021, a qual dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

Para o preenchimento de lacunas na segurança da informação, o guia foi dividido em ciclos gerenciáveis: detecção, emissão de relatórios e remediação. O guia tem como foco a construção de processos repetitivos em ciclos. Ao implementá-lo, recomenda-se inicialmente realizar uma análise do contexto da instituição para mapear sua maturidade com relação ao gerenciamento de vulnerabilidades, os ativos de informação que devem ser protegidos e os recursos necessários para protegê-los. É importante ressaltar que o propósito do guia apresentado neste documento é elucidar as diversas ações que devem ser avaliadas em cada fase do ciclo de gerenciamento, de forma que os responsáveis pela segurança dos ativos de informação possam aprimorá-lo por meio de melhorias contínuas.

Definições Gerais

Para auxílio na leitura do guia, serão adotadas as seguintes definições no que se refere às instituições da Administração Pública Federal (APF).

Ativo:

Qualquer coisa que tenha valor para a organização

Ativo de Informação:

Os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso

Baseline de segurança:

O conjunto de controles mínimos de segurança definidos para um sistema de informações de baixo impacto, impacto moderado ou alto impacto[2]

Controle de compensação:

Um controle gerencial, operacional ou técnico (ou seja, uma salvaguarda ou contramedida) empregado por uma organização ao invés de um controle de segurança recomendado nas baselines de segurança de impacto baixo, moderado ou alto, e que fornecem proteção equivalente ou comparável para um sistema de informação[3]

Trilha de auditoria:

Logs ou registros que fornecem evidências documentais cronológicas

CVE (Common Vulnerabilities and Exposures):

Vulnerabilidades e Exposições Comuns

ID CVE:

Identificação para um CVE específico

CVSS (Common Vulnerability Scoring System):

O sistema comum de pontuação de vulnerabilidade

FP:

Falso Positivo

KPI:

[2] https://csrc.nist.gov/glossary/term/security_control_baseline
[3] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Indicador de desempenho-chave

KB:

Base de conhecimento

PCI DSS:

Padrão de segurança de dados da indústria de cartões de pagamento

RACI:

Responsável, encarregado, consultado e informado

SCADA:

Controle de supervisão e aquisição de dados

SE:

Engenharia Social

Gerenciamento de Vulnerabilidades

O documento é organizado em três ciclos (triciclo), cada um deles tem um valor numérico e código de cor. As tarefas dentro de cada Ciclo têm as cores e números correspondentes.

1 Detecção	2 Relatórios	3 Remediação

Cada Ciclo é um domínio que compreende quatro tarefas principais. Cada tarefa inclui uma lista de ações a serem realizadas. A ordem dessas listas é lógica, mas pode ser ajustada para se adequar aos objetivos de cada instituição.

Todas as tarefas têm "Entradas" e "Saídas". Por exemplo, a tarefa "Escopo" alimenta-se de vários processos: configuração das ferramentas de segurança para testes de vulnerabilidade, agrupamento dos ativos de informação para varreduras e relatórios, priorização da correção, aplicação de métricas em reports de vulnerabilidade e definição do que é aceitável e o que não é. As "Saídas" do Escopo podem ser impactadas por alterações provenientes das "Entradas", isto é, o Escopo muda à medida que recebe feedback de relatórios e exceções.

A natureza cíclica do gerenciamento de vulnerabilidades implica a melhoria contínua do processo, e é crucial entender como um único processo se alimenta de outros processos e como todas as tarefas são interconectadas em três domínios.

É fundamental que a responsabilidade pelos processos de Segurança da Informação e Comunicações (SIC) seja determinada. De acordo com a IN GSI/PR 03/2019, é disposto no parágrafo único do art. 45, no capítulo que trata das disposições gerais, o seguinte:

> *"Para o cumprimento do previsto no caput, os órgãos e as entidades da administração pública federal devem definir seus próprios planos de ação, com atividades, prazos e* ***responsáveis pela implementação dos processos de gestão de segurança da informação****, conforme descrito nesta Instrução Normativa."*

Portanto, para que a gestão de vulnerabilidades seja realizada de forma efetiva, a instituição deve atribuir as funções e responsabilidades chave para a gestão de vulnerabilidades, incluindo equipe jurídica, TI, segurança da informação, dentre outros, conforme aplicável.

1 Ciclo de detecção

Durante o ciclo de detecção, realizamos as tarefas que suportam testes de vulnerabilidade de maneiras essenciais, definindo: quem, o que, quando, por quê e como **(4W1H)**[4]. As principais ações estão focadas em definir e refinar o escopo após cada rodada do triciclo, preparar as ferramentas e verificar sua integridade, realizar testes e verificar resultados.

É importante ressaltar a necessidade de identificar as vulnerabilidades nos ativos de informação conforme diretriz exposta na IN GSI/PR nº3/2021[5].

1.1 Escopo

1.1 TAREFA	ENTRADA	SAÍDA
Definir/Refinar escopo	2.4 Criar relatórios 3.4 Controlar o processo de exceção da vulnerabilidade	1.2 Otimizar ferramentas 2.1 Criar grupos de ativos de informação 2.2 Definir/Refinar métricas 2.4 Criar relatórios 3.1 Priorizar vulnerabilidades 3.4 Controlar o processo de exceção da vulnerabilidade

#	AÇÃO	POR QUÊ
1.1.1	Conhecer os riscos da instituição	Se a instituição tem ou não um registro de risco, deve compreender quais riscos mais preocupam a gestão e de onde esses riscos estão vindo. Entender a magnitude das perdas e impactos e o que pode comprometer a prestação de serviço da instituição. Estar ciente das possíveis exceções.
1.1.2	Conhecer as restrições operacionais	Entender o que pode comprometer a instituição devido a procedimentos, processos, falhas de sistema, erros humanos, imperícia, atividades fraudulentas ou criminosas. Quais são os requisitos legais, regulatórios e contratuais que a instituição deve atender? Reunir informações relevantes para a política. É necessário criar uma política de gerenciamento de vulnerabilidades ou atualizá-la?
1.1.3	Conhecer as restrições técnicas	Conhecer os limites dos ativos de informação e suas interdependências com tecnologias obsoletas. Por exemplo, algum hardware **SCADA (Supervisory Control and Data Acquisition)**[6] que só funciona no sistema operacional Windows XP.

[4] *Referente ao 5W2H com a subtração de 2 letras (why e how much)*
[5] *https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172*
[6] *Sistema que usa um software para monitorar, supervisionar e controlar as variáveis e os dispositivos de um processo*

1.1.4	Distinguir ativos de informação primários e secundários	Conhecer os ativos de informação essenciais, cuja perda seria prejudicial para a instituição, bem como os ativos de informação de suporte (secundários). Por exemplo, um servidor de produção para os usuários de um sistema que processa a folha de pagamento da instituição. Ao implementar um programa de gerenciamento de vulnerabilidades em todo a instituição, iniciar com os ativos de informação críticos e, em seguida, expandir gradativamente para todos os ativos de informação essenciais ou secundários, e posteriormente para todos os outros ativos de informação.
1.1.5	Distinguir ativos de informação expostos à internet	Conhecer quais os ativos de informação que estão expostos à Internet e considerá-los como ativos de informação críticos. Devido a isso, deve-se avaliar a necessidade de mapeamento do ambiente externo de forma rotineira.
1.1.6	Incorporar processos de gerenciamento de vulnerabilidades em processos corporativos	Promover mudanças gradualmente pode prevenir eventual inércia dentro da instituição. Às vezes é mais rápido construir um novo programa sobre os processos existentes e refinar os processos à medida que avança. Por exemplo, conhecer as datas da janela mensal de correção, pode ajudar o time de desenvolvimento fornecendo análise de vulnerabilidade antes e depois da correção.
1.1.7	Construir apoio gerencial	Adesão gerencial é fundamental no processo, porque o gerenciamento de vulnerabilidades exigirá a atenção de vários departamentos e de várias partes interessadas. Certifique-se de que a liderança entende sua importância e apoia o gerenciamento de vulnerabilidades. Nenhum líder quer incorrer em perdas.
1.1.8	Criar uma política de gerenciamento de vulnerabilidades que seja apropriada à realidade de sua organização	Defina e discuta o processo de gestão de vulnerabilidades com profissionais, gestores e stakeholders. A política de gerenciamento de vulnerabilidades deve estabelecer alguns pontos principais para o gerenciamento de vulnerabilidades da organização.
1.1.9	Comunicar e publicar a política a todos os colaboradores da organização	O modo de estabelecer esta comunicação deve estar alinhado com as diretrizes de governança da organização.

Objetivo final: Obter mapeamento dos ativos mais críticos e canais mais vulneráveis.

Importante: Compreender os limites dos testes de vulnerabilidade e planejar os passos seguintes.

1.2 Ferramentas

1.2 TAREFA	ENTRADA	SAÍDA
Otimizar ferramentas	1.1 Definir/Refinar escopo 1.4 Confirmar descobertas	1.3 Executar testes 1.4 Confirmar descobertas

#	AÇÃO	POR QUÊ
1.2.1	Determinar o tipo de teste/varredura	O escopo define os ativos de informação que serão analisados e determina que tipo de teste de segurança será conduzido. Pode-se optar, por exemplo, pelos seguintes testes e varreduras: • Varreduras de rede: credencial vs. varreduras não credenciadas; Varreduras de aplicativos: Análise de Código Estático (**Static Code Analysis - SAST[7])** vs. Varreduras Dinâmicas (**Dynamic Scans - DAST[8]**); • Testes de segurança de e-mail ou Engenharia Social (Social Engineering- SE). As varreduras de rede são preparadas para detectar correções (patches) não implementadas, erros de configuração e credenciais padrão em servidores web e dispositivos de rede. A varredura credenciada geralmente fornece resultados mais precisos que a não-credenciada. Recomenda-se usar varreduras não-credenciadas para varredura de ativos de informação expostos à Internet. Importante: Quando estiver implantando varreduras pela primeira vez (considerar uma primeira vez para algum grupo de ativos de informação), verificar a "saúde" dos ativos de informação antes e depois. Enquanto o SAST analisa a qualidade do código, o DAST simula ataques reais. Uma estratégia de varredura híbrida que contemple o SAST e o DAST também pode ser utilizada. Testes de segurança de e-mail, ou testes de phishing, são uma maneira de envolver o pensamento crítico dos usuários e evitar perdas. Testes de Engenharia Social (SE), embora não sejam muito comuns, são considerados uma maneira eficaz de conscientizar dos usuários, assim como treinamentos periódicos. **ATENÇÃO: Esteja atento, já que o DAST pode causar danos à aplicação ao servidor Web, e evite a execução do DAST no ambiente de produção.**
1.2.2	Definir a frequência de seus testes de segurança	O escopo deve fornecer a entrada com base nos requisitos legais, regulamentares e contratuais que a instituição deve cumprir. É importante considerar a realização de testes de segurança quando do conhecimento de vulnerabilidades que possam impactar os ativos de informação primários e secundários.
1.2.3	Garantir o feed de vulnerabilidade mais recente	Assine o recebimento de e-mails semanais dos principais fornecedores. Assine o banco de dados de divulgação completa e outros feeds para acompanhar todos os novos **CVEs (Common Vulnerabilities and**

[7] *https://owasp.org/www-community/Source_Code_Analysis_Tools*
[8] *https://owasp.org/www-community/Vulnerability_Scanning_Tools*

		Exposures)[9]. Pergunte ao fornecedor da ferramenta quanto tempo leva para atualizar as definições de vulnerabilidade em seu feed. O prazo máximo razoável é de duas semanas a partir do lançamento do patch.
1.2.4	Verificar se existem exceções de vulnerabilidade	Se a instituição já utilizar uma ferramenta de scanner de vulnerabilidade, é interessante verificar se algumas vulnerabilidades não estão isentas de aparecer no relatório.
1.2.5	Testar a integridade da ferramenta	A instituição pode definir ativos de informação para serem utilizados como laboratório de varreduras. Deve-se cruzar as informações de saída destas varreduras com os demais dispositivos da instituição. É necessário verificar se a ferramenta de escâner varreu corretamente o sistema operacional ou apenas enumera todos os URLs de um aplicativo da Web. Confirme se todos os aplicativos em execução nos dispositivos foram enumerados. Como alternativa, usar os aplicativos vulneráveis do **OWASP (https://owasp.org/www-project-juice-shop/)**.
1.2.6	Ajustar as configurações das ferramentas, preferências e templates	Comece seguro e pequeno, observe os resultados, então incremente e observe novamente. O que está diferente? Acrescenta algum valor? Considerar a ferramenta mais adequada para a varredura com base no escopo definido no primeiro ciclo. Pesquisar a ajuda e os comentários fornecidos pelos fóruns e comunidades das ferramentas de teste de segurança.
Objetivo final: Capacidade de ajustar suas ferramentas para cumprir os objetivos escopo.		

1.3 Testes

1.3 TAREFA	ENTRADA	SAÍDA
Executar testes de vulnerabilidade	1.2 Otimizar ferramentas 3.2 Corrigir Vulnerabilidades	1.4 Confirmar descobertas 2.4 Criar relatórios

#	AÇÃO	POR QUÊ
1.3.1	Escanear endereços IP públicos	Aplique uma varredura não credenciada, verifique se há senhas padrão. O objetivo é ver o que um atacante veria.
1.3.2	Escanear sub-redes privadas	Aplique varreduras credenciadas usando contas de serviço. O uso deste tipo de varredura pode aumentar a taxa de precisão. Considere o gerenciamento seguro de contas de serviço.
1.3.3	Testar/escanear aplicações web	Descubra como uma aplicação web pode ser explorada. Use uma cópia de produção para testes de segurança.

[9] *https://www.cve.org/*

1.3.4	Testar/escanear Aplicativos móveis	Descubra como os usuários podem explorar uma aplicação de produção.
1.3.5	Testar Usuários (phishing, treinamento em Engenharia Social)	Os usuários são os ativos de informação mais valiosos, porém propensos à Engenharia Social. Use o teste de segurança para descobrir quem provavelmente clicará no link malicioso ou executará um arquivo malicioso. Vincule os resultados para treinar novamente os usuários.
1.3.6	Testar ativos de informação com o Sistema Operacional Windows	Aplique varreduras em laptops, workstations e servidores que utilizem o Sistema Operacional Windows.
Objetivo final: Ser capaz de executar testes de vulnerabilidade como planejado.		

1.4 Descobertas

1.4 TAREFA	ENTRADA	SAÍDA
Confirmar descobertas	1.2 Otimizar ferramentas 1.3 Executar testes de vulnerabilidades	2.4 Criar relatórios 1.2 Otimizar ferramentas

#	AÇÃO	POR QUÊ
1.4.1	Verificar se os resultados do teste têm dados que agregam valor	Os resultados da varredura podem ser incompletos, inconclusivos ou contraditórios. Pode ser necessário alguns ajustes para encontrar o resultado mais adequado para cada ambiente. Certifique-se de colocar na white-list do firewall o IP associado ao scanner. Caso contrário, o firewall pode filtrar qualquer tentativa de conexão a várias portas, o que significa que a ferramenta verá todas as portas fechadas e nenhuma vulnerabilidade. É fundamental garantir a integridade de seus resultados antes de compartilhá-los com o gestor e demais integrantes da equipe de segurança.
1.4.2	Verificar através dos testes se as impressões digitais do sistema/dispositivo estão em conformidade	Leve o tempo que for necessário para analisar os resultados, garantindo que a impressão digital do dispositivo seja representativa no seu ambiente e bem definida. Pode ser necessário executar as verificações de descoberta antes de começar a executar os testes de vulnerabilidade. Execute novamente os testes de segurança se achar necessário.
1.4.3	Confirmar que os serviços em execução, são o que deveriam ser	É plausível que a ferramenta possa detectar uma vulnerabilidade de software que não está mais no sistema. Deve-se ajustar as configurações da ferramenta para se certificar que ela seja uma fonte confiável de descoberta de vulnerabilidades.
1.4.4	Encontrar algo fora do padrão e investigar a causa	A instituição deve ser capaz de identificar e compreender algo que foge do padrão. Tal identificação deve ser baseada em evidências. Dessa forma ficará mais fácil de utilizar e melhorar as ferramentas de segurança.

1.4.5	Selecionar aleatoriamente vulnerabilidades e confirmá-las manualmente ou com uma ferramenta diferente	Cada vulnerabilidade pode ter um nível de certeza e risco. Algumas vulnerabilidades são mais difíceis de replicar ou provar, e algumas são mais difíceis de explorar. No final deste exercício, a instituição pode adquirir e/ou melhorar suas habilidades de pentester e aprender algo novo sobre uma vulnerabilidade que pode ajudar a dar-lhe uma prioridade maior ou menor e melhorar seus relatórios. Ao empregar uma ferramenta diferente, caso vulnerabilidades não apontadas pela ferramenta principal sejam identificadas, esta deverá ser ajustada.
Objetivo final: Compreender os resultados dos testes de segurança; usar os dados coletados para ajustar a ferramenta de varredura de vulnerabilidade para aperfeiçoar a precisão.		

2 Ciclo de relatórios

Este ciclo visa tarefas que ajudam a organização a entender e mensurar as vulnerabilidades. As principais tarefas são focadas na aprendizagem e categorização organizacional, e na criação de métricas significativas que se tornarão o alicerce para os principais relatórios de gerenciamento de vulnerabilidades. Essas tarefas devem ser seguidas pela atribuição de equipes de trabalho para remediação e mitigação de vulnerabilidades.

É conveniente que a instituição empregue métricas julgadas relevantes ou úteis para a sua realidade e mais aderente à sua maturidade. Dessa forma, nem todas as métricas apresentadas neste documento devem ser obrigatoriamente utilizadas, podendo a instituição optar por utilizar somente um subconjunto delas.

2.1 Grupos de Ativos de Informação

1.1 TAREFA	ENTRADA	SAÍDA
Criar grupos de ativos de informação	1.1 Definir/Refinar escopo 2.3 Criar trilha de auditoria	1.3 Executar testes de vulnerabilidade 2.4 Criar relatórios 3.1 Priorizar vulnerabilidades

#	AÇÃO	POR QUÊ
2.1.1	Determinar grupos de ativos de informação funcionais	Através do mapeamento de ativos de informação[10],defina quais ativos de informação são de missão crítica e o quais não são. Se a ferramenta de gestão de ativos de informação não estiver disponível, reúna informações conversando com colegas de trabalho de vários níveis hierárquicos. Defina quanto tempo os ativos de informação podem ficar indisponíveis sem causar prejuízos ao negócio. Dentro de um grupo mais amplo de ativos de informação, os servidores web, por exemplo, crie subgrupos de ativos de informação significativos que poderiam ser usados em relatórios de vulnerabilidade. Exemplos podem incluir, mas não se limitando à localização, departamento e tipo de ativo de informação (virtual vs. HD, cloud vs. data center, por exemplo). Os critérios de organização dos grupos e subgrupos devem fazer sentido e serem claros para quem vai ler e analisar os relatórios.

[10] *Instrução normativa GSI/PR Nº 3, de maio de 2021, Capitulo II.*

2.1.2	Determinar grupos de ativos de informação por tipo de ambiente	Teste seus ambientes de produção, homologação e desenvolvimento para comparar os dados de vulnerabilidade em cada ambiente. Os dados gerados pelos testes são idênticos ou não? As diferenças podem indicar problemas de governança. Agrupar ativos de informação pelo tipo de ambiente pode ser benéfico para a priorização de atividades.
2.1.3	Determinar grupos de ativos de informação por tipo de sistema	Qual o SO tem mais vulnerabilidades de alta gravidade? Onde estão concentrados os problemas? Se uma instituição possui uma página na web, e os resultados da varredura indicam vulnerabilidades críticas em servidores Apache, isso significaria inconformidade ou falta de gerenciamento de mudança.
2.1.4	Determinar grupos por ID CVE	Entenda quais vulnerabilidades são inaceitáveis para a instituição. Por exemplo, agrupar as **CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147** e **CVE-2017-0148** em um Grupo de vulnerabilidade "**EternalBlue/Petya**[11]" e rastreá-lo.
2.1.5	Determinar grupos por tipo de vulnerabilidade	Agrupe os riscos de acordo com, no mínimo, os seguintes grupos indicados no **OWASP Top 10 Web Application Security Risk**[12]. • Controle de acesso insatisfatório ou falho • Falhas criptográficas • Projeto inseguro • Configuração de segurança insatisfatória ou falha • Componentes vulneráveis e obsoletos • Falhas de identificação e autenticação • Falhas de integridade de software e dados • Falhas no monitoramento e no registro de log de segurança • Falsificação de requisições do lado do servidor (server-sided) Quando necessário, identificar outras categorizações que sejam aplicáveis.
Objetivo final: Conhecer plenamente o ambiente para criar as categorias para os ativos de informação da instituição.		

2.2 Métricas

2.2 TAREFA	ENTRADA	SAÍDA
Definir/Refinar Métricas	1.1 Definir/Refinar escopo 2.4 Criar relatórios	2.4 Criar relatórios
#	**AÇÃO**	**POR QUÊ**
2.2.1	Determinar a quantidade e porcentagem de ativos de informação	Distribua a quantidade e porcentagem de vulnerabilidades identificadas em todos os grupos funcionais. É importante apresentar nos relatórios que alguns grupos funcionais são mais vulneráveis do que outros.

[11] *http://tracker.h3x.eu/info/470*
[12] *https://owasp.org/Top10/*

	vulneráveis	
2.2.2	Determinar o valor e percentual dos ativos de informação vulneráveis por gravidade e CVSS	Repita o passo acima e defina por gravidade ou pontuação **CVSS**[13]. A classificação por gravidade depende da ferramenta de scanner de vulnerabilidade, mas geralmente corresponde ao CVSS. No final, deve-se ter gráficos onde os eixos Y são grupos funcionais A, B, C, D e os eixos X são classificações de gravidade.
2.2.3	Determine a quantidade e porcentagem de novas vulnerabilidades:	Durante esta etapa, usando os resultados de teste mais recentes e verificados, tabelas e gráficos podem ser elaborados para o seu relatório, aplicando as subcategorias de ações da coluna esquerda (2.2.3.1 a 2.2.3.6).
2.2.3.1	- por severidade	A classificação de gravidade/severidade depende do fornecedor do scanner, mas corresponde à CVSS para scanners de rede. Para aplicações web, tal classificação pode ser alto, médio e baixo.
2.2.3.2	- por grupos funcionais	Aplique seus resultados a partir do item 2.1 e/ou crie subgrupos mais detalhados. Por exemplo, grupos funcionais podem ser: • Predefinidos por equipes que suportam esses ativos de informação: rede, hospedagem de clientes. • Predefinidos pelo tipo de dispositivos: webservers, ICS, estações de trabalho, IoT. • Predefinido pela localização dos ativos de informação.
2.2.3.3	- por tipo de ambiente	Por exemplo: produção, desenvolvimento, testes, rede corporativa, IPs públicos, aplicativos hospedados.
2.2.3.4	- por tipo de sistema	Aplique os resultados a partir do item 2.1. e utilize dados consolidados por um sistema operacional.
2.2.3.5	- pela autoridade de numeração CVE	Aplique os resultados a partir do item 2.1. e utilize dados consolidados pelo número CVE.
2.2.3.6	- por tipo de vulnerabilidade	Observar o item 2.1.5.
2.2.4	Comparar e analisar os dados de envelhecimento pela severidade das vulnerabilidades e seu peso/ importância:	Existem dois aspectos do envelhecimento da vulnerabilidade: a data de publicação de uma vulnerabilidade (refletida no número CVE) e o tempo de descoberta. A análise de dados do envelhecimento da vulnerabilidade impactará a prioridade para o trabalho de remediação.
2.2.4.1	-em toda a instituição	Reflita e pondere sobre o uso de ativos de informação corporativos que tenham as vulnerabilidades mais antigas.
2.2.4.2	-entre todos os outros ativos de informação vulneráveis	Um ativo pode ser mais suscetível à exploração se as vulnerabilidades já conhecidas não foram corrigidas. Quanto a varredura, se o relatório mostrar que a vulnerabilidade foi descoberta há 180 dias, isso pode significar que um processo de resolução específico não foi totalmente adotado ou a instituição não possui controle de qualidade.

[13] *https://nvd.nist.gov/vuln-metrics/cvss*

2.2.4.3	-por grupos funcionais	Agregar esses dados por grupos funcionais e nomear os responsáveis pela remediação e correção de determinados grupos de ativos de informação. Isso agrega transparência, responsabilização e prestação de contas em seu relatório.
2.2.4.4	-por tipo de ambiente	Por exemplo: uma infraestrutura pública versus infraestrutura privada, produção versus desenvolvimento. Defina quais comparações são essenciais para sua organização.
2.2.4.5	-por tipo de sistema	Por exemplo, servidores de extranet e DMZ, servidores internos, pontos de acesso à rede, estações de trabalho, sistemas IoT, sistemas SCADA. Pode ser mais específico para distinguir servidores DNS de servidores de e-mail, por exemplo, ou interface de firewall de outros dispositivos de rede, bem como identificar a vulnerabilidade pelo tipo de sistema operacional.
2.2.4.6	-pelo ID CVE	Analisar os dados e avaliar se há alguma diferença da classificação de score desproporcional entre a gravidade das vulnerabilidades encontradas e a gravidade específica já estabelecidas pela CVE.
2.2.4.7	-por tipo de vulnerabilidade	Consulte o item 2.1.5 e cruze os resultados dos testes entre grupos funcionais. Com isso, é possível mapear certos tipos de riscos transversais que devem ser mitigados ou aceitos organizacionalmente.
2.2.5	Projetar tendências por contagem e porcentagem utilizando indicadores-chave de desempenho (KPIs) que importam para os riscos e conformidade da sua instituição	Ao repetir o Ciclo de Gerenciamento de Vulnerabilidades, será possível observar uma mudança, por meio dos indicadores, que coloca tudo em perspectiva. Note que uma tendência de queda pode significar que a organização está fazendo um bom trabalho remediando vulnerabilidades ou que estas não foram detectadas corretamente. Se isso é uma preocupação, consulte 1.4 Confirme os resultados. Alguns indicadores que podem ser utilizados são: Tempo de descoberta da vulnerabilidade até sua escalação e correção; • Idade média das vulnerabilidades que estão em aberto (descobertas, mas não corrigidas ainda); • Cobertura ou percentual de ativos e vulnerabilidades descobertos em cada tipo de scanning; • Percentual de vulnerabilidades remediadas conforme exigências de compliance; • Quantidade de exceções de vulnerabilidade aprovadas pela liderança ou em processo de aprovação; • Quantidade de falhas em remediações; • Quantidade de remediações atendidas fora dos padrões estabelecidos no NMS (Níveis Mínimos de Serviço).[14]
2.2.6	Determinar a explorabilidade de ativos de informação vulneráveis por gravidade; especificar contagem, porcentagem, diminuição ou aumento	Use fontes reconhecidas para exploração e não utilize apenas uma fonte, como, por exemplo, uma base de conhecimento de referência. Alguns fabricantes de software podem ser menos transparentes do que outras.

[14] "A Guidance Framework for Developing and Implementing Vulnerability Management", Abril/2021

Objetivo final: Deve-se criar (e revisar posteriormente) métricas para relatórios de vulnerabilidade. Essas métricas devem ser consistentes e fazer sentido para o público-alvo dos relatórios (gestores e equipes designadas para fazer o trabalho de remediação).

2.3 Trilha de Auditoria

2.3 TAREFA	ENTRADA	SAÍDA
Criar trilha de auditoria	3.4 Controlar o processo de exceção da vulnerabilidade 2.4 Criar relatórios 3.3 Investigar falsos positivos	2.1 Criar grupos de ativos de informação 2.4 Criar relatórios

#	AÇÃO	POR QUÊ
2.3.1	Usar o sistema de ticket da instituição	A remediação é essencialmente uma solicitação de trabalho. A instituição deve ser capaz de cumprir com o processo de solicitação de trabalho existente em uso e rastrear quanto tempo leva para fazer o trabalho. Importante: algumas instituições têm processos automatizados de patches; isso não significa que eles estão livres de vulnerabilidades. Assim, pode-se argumentar que a coordenação/departamento de segurança da informação atua como garantia independente de qualidade, estabelecendo um programa de gestão de vulnerabilidades.
2.3.2	Fornecer um resumo da demanda	Seja conciso, vá direto ao ponto e evite adjetivos que não sejam relevantes para a classificação de severidade: crítico, alto, grave, médio, moderado ou baixo.
2.3.3	Fornecer saídas interoperáveis com as ferramentas	Isso ajuda a eliminar os falsos positivos ou outros erros.
2.3.4	Notificar/atribuir a demanda/ticket às equipes ou indivíduos responsáveis	É imprescindível criar uma cultura de responsabilização em torno do trabalho de remediação. Atribuir uma pessoa a uma questão de segurança pode provocar algumas repercussões políticas dentro de uma instituição; é importante que problemas potenciais sejam resolvidos de antemão, por meio de uma comunicação eficiente.
2.3.5	Garantir que o responsável pela Segurança da Informação esteja ciente	Portanto, é fundamental ter sua gestão apoiando suas ações.

Objetivo final: criar uma trilha de auditoria para o trabalho de remediação. Atribuir trabalho ou treinamento a indivíduos responsáveis pela remediação de vulnerabilidades (uma reescrita de código, uma correção de configuração, por exemplo).

2.4 Relatórios

2.4 TAREFA	ENTRADA	SAÍDA
Criar relatórios	1.1 Definir/Refinar escopo 1.3 Executar testes de vulnerabilidade 1.4 Confirmar descobertas 2.1 Criar grupos de ativos de informação 2.2 Definir/Refinar métricas 2.3 Criar trilha de auditoria	1.1 Definir/Refinar escopo 3.1 Priorizar vulnerabilidades 3.2 Corrigir Vulnerabilidades 3.3 Investigar falsos positivos 3.4 Controlar o processo de exceção da vulnerabilidade

	3.2 Corrigir Vulnerabilidades 3.3 Investigar falsos positivos	

#	AÇÃO	POR QUÊ
2.4.1	Manter uma frequência consistente de relatórios e utilizá-los para rastrear alterações	Esse passo é vital para se tornar uma fonte transparente e confiável de informações para o público-alvo de relatórios de vulnerabilidade.
2.4.2	Coletar e agregar dados de processos	Use os dados originais sem alterá-los e aplique métricas úteis ao público-alvo. Certifique-se de documentar seu processo ao longo de sua execução para evitar erros acidentais. Cruze dados de forma que se possa comparar os resultados para ter certeza de que eles estão corretos. Os dados obtidos podem ser usados para identificar áreas problemáticas ou gargalos de correção, além de fornecer a base para obtenção de recursos adicionais para melhoria e aperfeiçoamento do desempenho do processo.
2.4.3	Usando o CVSS, aplique traços ambientais únicos à sua análise de vulnerabilidade	Embora a pontuação CVSS seja seu denominador comum, é plausível que uma pontuação de baixo risco possa ser maior no ambiente da instituição devido a fatores de exposição ou sistemas legados.
2.4.4	Analisar as tendências do status das vulnerabilidades	Compare as vulnerabilidades do último mês, semana, trimestre, ano? Se é melhor, pior, continua igual, enfim, qual a tendência?
2.4.5	Estabelecer as hipóteses sobre essas tendências em uma frase	Se houver uma tendência de queda devido à falha do scanner, deve ser declarada no relatório. Se vemos uma tendência ascendente, provavelmente nenhum trabalho de correção foi realizado, e este é o momento certo para comunicar isso.
2.4.6	Adicionar recomendações de forma resumida	Adicionar recomendações práticas sobre como transformar um ambiente (sub-redes/sistemas/aplicativos) de alto risco em um ambiente de menor risco possível, eliminando as vulnerabilidades. Nota: As recomendações devem ser expostas de forma concisa, pragmática e orientada para a missão da organização.
2.4.7	Aplicar classificação de confidencialidade ao seu relatório	O relatório pode conter informações e dados sensíveis da instituição, e agentes maliciosos podem ter interesses duvidosos quanto ao acesso dessas informações. Neste sentido, classifique tais informações como ao menos “confidenciais”, e reitere a sensibilidade da informação em cada página do relatório.
2.4.8	Elaborar uma versão resumida (1-2 páginas) do relatório	Sacrificar a granularidade para demonstrar o quadro mais amplo: o que essas vulnerabilidades significam para a continuidade operacional da organização e onde estão os problemas concentrados. Torná-lo mais ilustrativo do que textual. Evite usar jargões técnicos ou números CVE: “EternalBlue” pode soar mais familiar do que o CVE-2017-0143.
2.4.9	Enviar todas as versões do relatório para a o gestor de segurança da informação.	Usar a comunicação eletrônica e verbal. É interessante armazenar seus relatórios em uma unidade criptografada compartilhada e compartilhar apenas a URL do relatório.

2.4.10	Criar e manter o repositório de gerenciamento de vulnerabilidades para auditoria interna ou externa	Certifique-se de estar aderente com os requisitos exigidos em uma auditoria. Crie um local de armazenamento seguro para os dados coletados e relatórios finais. Certifique-se de documentar seu processo ao longo do caminho para evitar erros acidentais. Convém que, no mínimo, as seguintes informações sobre as vulnerabilidades estejam presentes no repositório: sua "prevalência" (ativos onde ela foi encontrada), grau de envelhecimento (de descoberta na comunidade e dentro da organização), norma (compliance) que torne sua remediação prioritária, plano de correção e responsáveis pela sua execução. Disponibilize estes repositórios para auditores internos e externos da organização durante auditorias de segurança.
2.4.11	Conseguir explicar os detalhes da detecção de vulnerabilidade e do processo de elaboração de relatórios	Ser transparente com a gestão e com os colegas sobre coleta de dados e sobre o tratamento de dados. Transparência mais consistência torna o processo mais confiável.
Objetivo final: resumir os resultados de varredura de segurança de forma concisa que seja fácil de entender. Compartilhe seus relatórios com todos que precisam saber. Mantenha os relatórios de vulnerabilidade consistentes em formato e entrega.		

3 Ciclo de remediação

O ciclo de remediação visa tarefas que reduzem ou eliminam vulnerabilidades, além de fornecer evidências sobre porque uma determinada vulnerabilidade não é considerada uma ameaça.

As principais tarefas do ciclo estão focadas na definição de prioridades, termos de trabalho de correção, discussão e documentação de falsos positivos além de lidar com exceções. Essas tarefas devem permitir que uma organização maximize o uso da capacidade de remediação e mitigação disponível e alcance a máxima redução de risco possível.

Além disso, a remediação ou correção deve ser implementada com risco mínimo para a disponibilidade dos sistemas e sem processos frustrantes do tipo 'back-and-forth' (ex.: patchs instalados e, na sequência, desinstalados por motivos diversos)".[15]

É uma boa prática integrar as ferramentas de análise de vulnerabilidades aos sistemas de ticket da instituição e outras ferramentas de gestão de fluxo de processos (workflow), visando acelerar a troca/intercâmbio de informações entre equipes de segurança, de operação de infraestrutura e outros stakeholders.

3.1 Priorização

3.1 TAREFA	ENTRADA	SAÍDA
Priorizar vulnerabilidades	1.1 Definir/Refinar escopo 2.1 Criar grupos de ativos de informação 2.4 Criar relatórios	3.2 Corrigir vulnerabilidades

[15] Guidance Framework for Developing and Implementing Vulnerability Management, April/2021

#	AÇÃO	POR QUÊ
3.1.1	Fazer uso dos relatórios	Para priorizar o trabalho de correção, é necessário usar métricas de relatórios com base na criticidade dos ativos de informação da organização. A maneira ideal de priorizar vulnerabilidades para correção e mitigação é se basear no risco de segurança associado à organização. Alguns aspectos devem ser considerados, como: a gravidade da vulnerabilidade (normalmente representada por CVSS); o contexto da ameaça; o nível de exposição do ativo; e o impacto potencial nos negócios. Além da severidade das vulnerabilidades, outros fatores também devem ser considerados, como: • vulnerabilidades mais presentes em ativos (prevalência); • seu envelhecimento (corrigir antes as vulnerabilidades mais antigas, em termos de disseminação na comunidade e na sua descoberta dentro da organização); • vulnerabilidades cuja prioridade na correção é definida em compliance; • papel do ativo dentro da organização; • seu valor comercial e monetário; • sua localização na rede.
3.1.2	Fazer uso das análises de tendências	Quais são as áreas onde a tendências de exposição a vulnerabilidades está crescendo ao nível maior que o pré-estipulado e como normalizá-las? Essas áreas devem ter prioridade na correção de vulnerabilidades.
3.1.3	Fazer uso das informações de fontes adicionais	É importante que a organização se atualize de notícias de segurança cibernética: vulnerabilidade *Zero Day*, explorações significativas de ransomware etc. Estas informações podem mudar as prioridades da equipe que realizara a correção.
3.1.4	Aplicar outros fatores ambientais	A organização tem prioridades diárias, semanais, mensais e trimestrais. Com base na função de cada equipe, essas prioridades podem ser primárias ou secundárias. Pense em como o gerenciamento de vulnerabilidades pode se encaixar aos objetivos de outras equipes.
3.1.5	Comunicar às partes interessadas (stakeholders) que são responsáveis pela gestão e às partes responsáveis pela prestação de contas	No item 2.3.1, discutimos o uso do sistema de ticket. Utilize também a comunicação escrita e verbal. É de suma importância obter apoio das equipes e pessoas da organização.
Objetivo final: criar argumentos baseado em dados para priorização de vulnerabilidades.		

3.2 Remediação

3.1 TAREFA	ENTRADA	SAÍDA
Corrigir Vulnerabilidades	1.1 Definir/Refinar escopo 2.4 Relatórios 3.1 Priorizar vulnerabilidades	2.4 Criar relatórios 3.3 Investigar falsos positivos 3.4 Controlar o processo de exceção da vulnerabilidade 1.3 Executar testes de vulnerabilidade

#	AÇÃO	POR QUÊ

3.2.1	Encontrar os stakeholders e responsáveis pelo trabalho/tarefas de correção	Identificar se o profissional ou equipe designada tem os conhecimentos e capacidades necessárias para poder atuar na atividade.
3.2.2	Comunicar os achados por meio de ferramentas e processos já utilizados comunicação	Se a equipe designada estiver vinculada aos procedimentos internos da instituição e ao processo de compartilhamento de conhecimento já estabelecido, ela deverá se adequar a eles.
3.2.3	Estabelecer uma frequência e escopo de patching, reescrita de código e retreinamento de pessoas	Idealmente, a frequência de remediação deve estar alinhada com a frequência de teste de vulnerabilidade (item 1.3). A instituição tem que estar pronta para concessões (renunciar a certas tarefas) nos estágios iniciais da implementação de um programa de gerenciamento de vulnerabilidades e se esforçar por melhorias à medida que repete esses ciclos mensalmente.
3.2.4	Estabelecer um grupo de ativos de informação dedicados aos testes de remediação	Por exemplo, caso seja realizada uma correção de configuração em massa, teste tal correção **imediatamente e não espere até outro ciclo mensal de detecção.**
3.2.5	Informar os resultados dos testes aos stakeholders e gestores.	Para a trilha de auditoria, é importante armazenar os resultados dos testes em uma unidade compartilhada e/ou inseri-los no sistema de ticket.
3.2.6	Usar o sistema de ticket ou mudar o sistema de gerenciamento para resolver os problemas de gerenciamento de correção	É possível que em determinada situação a execução esteja adiantada com relação ao planejamento. Independentemente se é o caso ou não, deve-se buscar uma forma de utilizar o sistema de tickets ou mudar o sistema de gestão para que ele possa ser utilizado nas trilhas de auditoria. Se as ações de remediação ou correção forem executadas por equipes terceirizadas, convém que sejam realizadas em conformidade com os Níveis Mínimos de Serviços (NMS) estabelecidos previamente.
3.2.7	Sempre atribuir a um responsável a realização de uma tarefa de correção	Não ter um responsável pela realização de uma tarefa de correção ou não ter um prazo para sua realização significa que a trilha de auditoria está incompleta.
3.2.8	Envolver os stakeholders responsáveis, os stakeholders que prestam contas e demais colaboradores que precisam ser informados nos problemas não resolvidos	Consultar a matriz RACI da instituição, ou considerar, de acordo com o conhecimento da instuição, o seguinte: equipe responsável por tarefas de correção; gestores que aprovam tarefas de correção; profissionais que precisam estar cientes se a correção foi realizada ou não; equipes que podem ser impactadas pela próxima janela de correção e precisam ser informadas.
3.2.9	Utilizar a frequência do ciclo de relatórios para acompanhar vulnerabilidades ainda não corrigidas	Pode-se atualizar os relatórios com estatísticas de remediação; quantificar a as vulnerabilidades recorrentes; utilizar o histórico de estatísticas para os grupos de ativos de informação.
Objetivo final: completar o trabalho de correção de vulnerabilidades. Não se pode assumir que a correção esteja finalizada até que seja feito o reteste (item 1.3 Executar testes de vulnerabilidade). Todas as vulnerabilidades que não puderam ser corrigidas devem ser identificadas e documentadas.		

3.3 Falsos Positivos (FP)

3.3 TAREFA	ENTRADA	SAÍDA
Investigar Falsos Positivos (FP)	2.4 Criar relatórios 3.2 Corrigir vulnerabilidades	1.2 Otimizar ferramentas 2.4 Criar relatórios

#	AÇÃO	POR QUÊ
3.3.1	Garantir a integridade da identificação do falso positivo	Obter evidências da fonte de informação: uma captura de tela, uma saída de código etc.
3.3.2	Construir um processo de negócios repetível	Com base no que é aceitável dentro da cultura organizacional, crie um processo repetível e que seja considerado adequado pelos colaboradores.
3.3.3	Documentar todas as identificações de FP	Documentar falsos positivos deve fazer parte do processo. Pode-se utilizar um sistema de ticket, uma ferramenta de testes, ou ambas ao mesmo tempo, desde que se mantenha um histórico que possa ser utilizado em uma possível auditoria. Mantenha o equilíbrio entre transparência e da confidencialidade.
3.3.4	Submeta a identificação de um falso positivo à análise de uma terceira parte	Encontre um terceiro que possa confirmar ou refutar um possível falso positivo. Encontre um especialista fora da organização e solicite que comente sobre o assunto sem revelar os detalhes sensíveis.
3.3.5	Definir um prazo em que a falso positivo deve ser reavaliado	Pode ser três meses, seis meses ou um ano. Usar diretrizes normativas e de conformidade para estabelecer tal prazo.
3.3.6	Documentar cada falso positivo e armazene-os em um repositório auditável	Pode-se armazenar a base de dados em uma unidade compartilhada, desde que ela permaneça confidencial. Estabeleça controles de modificação e versão da base de dados.

Objetivo final: Estabelecer regras básicas de como uma vulnerabilidade será categorizada como falso positivo. Revise as evidências caso a caso. Revisite e revise periodicamente alertas de falsos positivos. O processo deve ser transparente e não deve ser desrespeitado.

3.4 Exceções

3.4 TAREFA	ENTRADA	SAÍDA
Controlar o processo de exceção da vulnerabilidade	1.1 Definir/Refinar escopo 3.2 Corrigir vulnerabilidades	1.1 Definir/Refinar escopo 2.3 Criar trilha de auditoria

#	AÇÃO	POR QUÊ
3.4.1	Estabelecer um gestor que seja o responsável por uma exceção à segurança cibernética	Exceções de vulnerabilidade implicam que vulnerabilidades específicas podem não ser corrigidas por algum tempo. Dever haver alguma justificativa para essa decisão. Por isso, é importante definir quem tem autoridade final para aprovar uma exceção de vulnerabilidade. Em muitos casos, o responsável por esta aprovação é o Gestor de Segurança da Informação da instituição, em alguns casos, pode ser o

		mesmo gestor da área de Tecnologia da Informação. Isso dependerá da legislação aplicável a cada caso.
3.4.2	Estabelecer regras básicas para exceções de vulnerabilidade	É importante que as exceções só sejam concedidas caso haja uma forte justificativa de negócios. Por exemplo, storage antigos que são caros ou impossíveis de substituir, que funcionam relativamente bem mesmo após o encerramento do suporte de fabricação.
3.4.3	Estabelecer revisões periódicas de exceções de vulnerabilidade	As revisões periódicas devem ser estabelecidas de acordo com a normatização e melhores práticas aplicáveis.
3.4.4	Estabelecer controles de compensação aceitáveis	Estabeleça controles para evitar que a vulnerabilidade seja explorada. Estes controles devem ser periodicamente revistos. A frequência das revisões devem estar em conformidade com leis e normas, além de estar alinhado com a política de gerenciamento de vulnerabilidades.
3.4.5	Documentar cada exceção e armazenar no sistema de auditoria da instituição	O sistema de ticket também pode ser usado para isso. **ATENÇÃO: É importante estar atento à sensibilidade dessas informações e categorizá-las adequadamente.**
3.4.6	Criar uma política adequada para o gerenciamento de exceções de vulnerabilidades	Pode-se adicionar exceções de vulnerabilidade à sua política de gerenciamento de vulnerabilidades ou criar uma nova política.
3.4.7	Comunicar e publicar essa política a todos os funcionários	O modo de estabelecer esta comunicação deve estar alinhado com as diretrizes de governança da organização.
3.4.8	Ter pessoal adequado para solicitar possíveis exceções de vulnerabilidade pedindo à autoridade máxima uma aprovação de cada vez	Se o processo de exceções de vulnerabilidade for muito fácil – pode se tornar uma pretexto para que as vulnerabilidades não sejam corrigidas. Quem busca uma exceção deve solicitar que um gestor aprove e seja responsável por tal exceção.
Objetivo final: garantir que toda não conformidade seja aprovada pela alta administração e documentada no repositório de toda a instituição. As exceções de vulnerabilidade devem ter uma data de validade e, vencendo esta data, elas devem ser revistas. As exceções de vulnerabilidade devem incluir controles compensatórios que impeçam a exploração de vulnerabilidades.		

Imagens

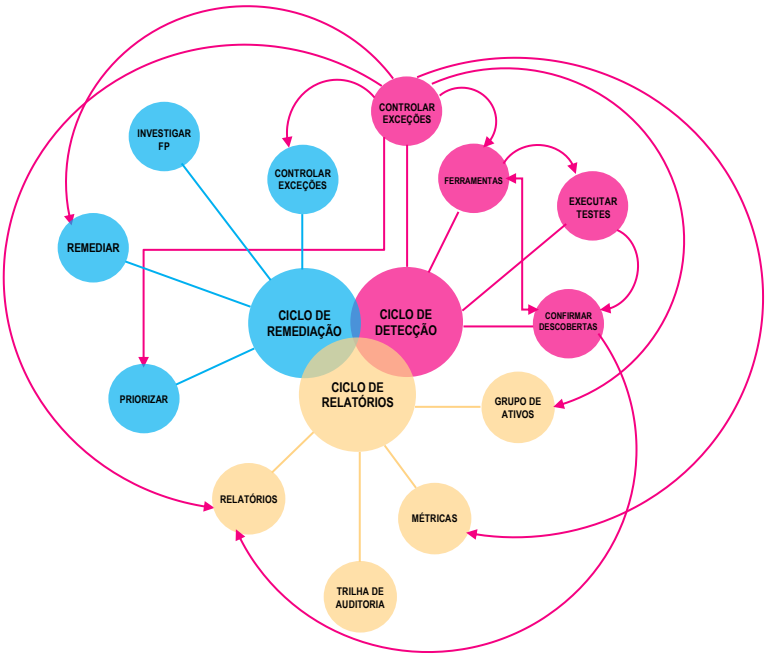

Figura 1 - Entradas do Ciclo de Detecção

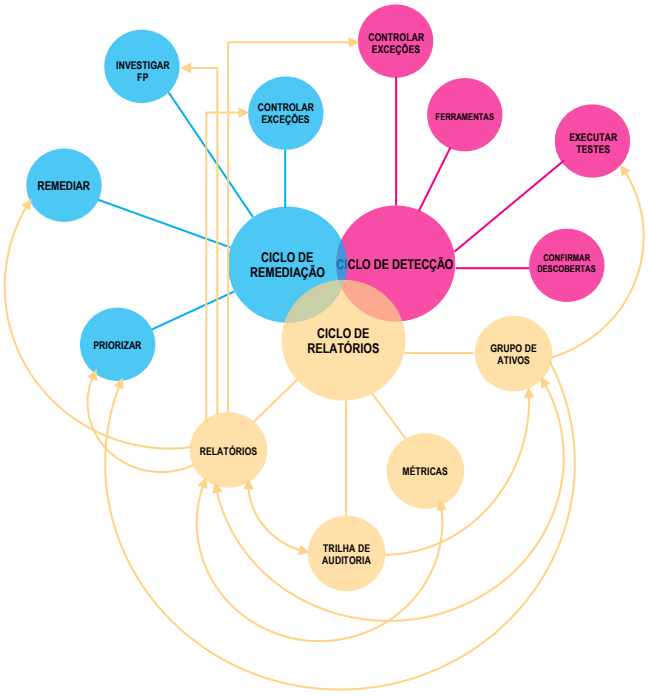

Figura 2 - Entradas do Ciclo de Relatórios

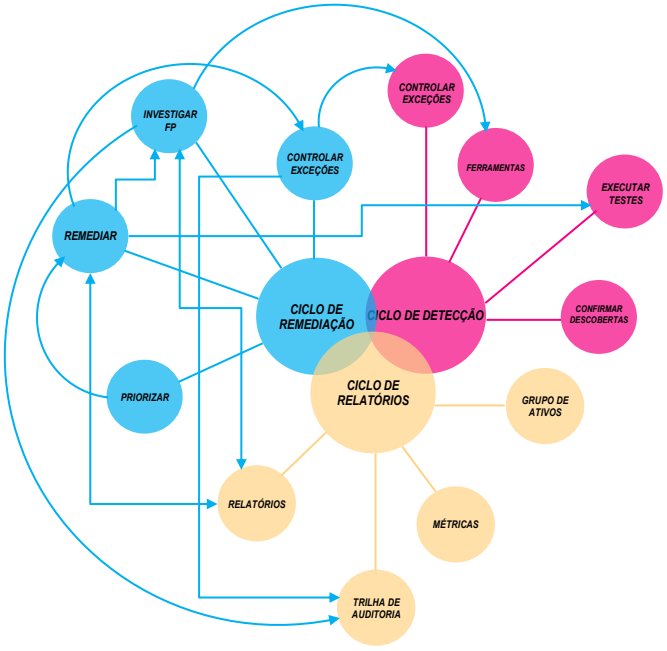

Figura 3 - Entradas do Ciclo de Remediação

Referência legal e de boas práticas [Documentos norteadores]

Se for aplicável, liste quaisquer leis, regulamentos ou guias de boas práticas que regem a gestão de vulnerabilidades ou com as quais o guia deve estar em conformidade ou ser cumprido. Confirme com a consultoria jurídica que a lista é completa e precisa.

Orientação	Seção
Decreto 10.332/2020 – Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 – Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 – Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto N° 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	Art. 15.
Decreto Nº 9.573/2018 – Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo, art.3, Inciso I, II e V
Decreto N° 10.569/2020 - Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC)	Em sua íntegra
OWASP Vulnerability Management Guide (OVMG)	https://owasp.org/www-project-vulnerability-management-guide/OWASP-Vuln-Mgm-Guide-Jun05-2020.pdf
OWASP Top 10	https://owasp.org/www-project-top-ten/ OWASP
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;	Gestão da Segurança da Informação
Guias Operacionais SGD	Todos
Guia de Framework de Privacidade e Segurança da Informação (PPSI)	Controle 7
Instrução Normativa 01/GSI/PR, de 27 de maio de 2020	Art.12, Inciso IV
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)	CAPÍTULO VII – Seção I – Art. 46, Seção II - Art. 50
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos;	A.12.3 Cópias de segurança
Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;	12.3 Cópias de segurança
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
A Guidance Framework for Developing and Implementing Vulnerability Management, Abril/2021, Gartner.	Em sua íntegra
A Guidance Framework for Establishing and Maturing an Application	Em sua íntegra

Security Program”, September/2021, Gartner.	

ANEXO I

Relatório de Avaliação de Vulnerabilidades

O relatório de vulnerabilidades, é um documento que detalha as vulnerabilidades encontradas em um ou mais ativos de informação. Essas vulnerabilidades são classificadas de acordo com sua gravidade/criticidade, o que ajuda a priorizar quais delas devem ser corrigidas primeiro.

No caso de aplicativos de missão crítica, esses relatórios são especialmente importantes, pois qualquer falha ou exploração de vulnerabilidade pode ter um impacto significativo nas operações diárias do órgão ou entidade. Por exemplo, uma vulnerabilidade em um sistema bancário pode permitir que um atacante roube informações confidenciais ou execute transações não autorizadas, o que pode causar danos financeiros significativos e abalar a confiança do cliente.

Ao receber um relatório de vulnerabilidades, é importante que a equipe de segurança da informação responsável revise cuidadosamente as vulnerabilidades identificadas e desenvolva um plano de ação para corrigir as mais críticas o mais rápido possível. Isso pode envolver a instalação de patches de segurança, atualizações de software, mudanças de configuração ou outras medidas para mitigar as vulnerabilidades identificadas.

Conforme orientações da **IN GSI/PR nº3/2021**[16], a instituição deve consolidar informações resultantes da análise do nível de segurança de cada ativo de informação ou de grupos de ativos em um relatório, podendo ainda conter dados de identificação, análise e avaliação de riscos de segurança da informação que deverá ser atualizado anualmente ou quando houver alteração em algum dos fatores de risco. Com o objetivo de cumprir estas orientações, a SGD elaborou este modelo de relatório de avaliação de vulnerabilidade que pode ser adaptado à realidade operacional de cada instituição.

Para usar este modelo, basta substituir o texto em cinza por informações personalizadas do seu órgão ou entidade. Quando estiver concluído, exclua todos os textos introdutórios ou de exemplo e converta todo o texto restante em preto antes do processo de aprovação.

1. Sumário executivo:

Descreva aqui o resumo das informações mais importantes dos tópicos do documento.

O objetivo desta verificação de vulnerabilidade é coletar dados e níveis de patch de software de terceiros nos ativos de informação do domínio [nome do domínio da instituição] na sub-rede [99.99.99.99/20]. A auditoria foi realizada em [data] usando a ferramenta de análise de vulnerabilidades [nome da ferramenta e versão].

Dos 35 ativos de informação identificados, 32 sistemas possibilitaram a verificação. Um total de 247 vulnerabilidades de gravidade crítica, alta, média e baixa foram encontradas em todos os 32 sistemas durante esta verificação.

[16] *https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172*

Crítica	Alta	Média	Baixa
44	*109*	*84*	*10*

As vulnerabilidades encontradas nos Servidores Windows consistem em patches desatualizados do sistema operacional e software de terceiros, incluindo Google Chrome e Adobe Flash. Os sistemas também foram encontrados sem patches desde 2014. Vulnerabilidades mais antigas apresentam um risco mais significativo, pois os agentes mal-intencionados geralmente automatizam a exploração de vulnerabilidades conhecidas para obter êxito de forma mais fácil. Portanto, é altamente recomendável aplicar o patch mais recente ao software desatualizado o mais rápido possível.

As vulnerabilidades encontradas nos switches consistem em certificados TLS/SSL e lidam principalmente com o uso de conjuntos de criptografia desatualizados. Embora os certificados desatualizados/autoassinados em dispositivos internos não sejam tão arriscados quanto os mesmos em dispositivos externos, certificados SSL adequados e atualizados devem ser instalados para atender às práticas recomendadas. Além disso, os switches estavam executando variações de 3 versões de firmware desatualizados.

Recomenda-se, por fim, que as seguintes ações sejam implementadas: atualizar o Adobe Flash Player e o Chrome nos ativos avaliados; instalar mecanismo contra proteção de malware; atualizar os firmwares dos switches para a versão mais recente suportada pelo fornecedor; aplicar os patches de segurança para o ambiente Windows.

2. Escopo da varredura

Defina os ativos de informação que foram avaliados para a elaboração do relatório.
A varredura foi realizada nos ativos de informação do domínio [nome do domínio da instituição] na sub-rede [99.99.99.99/20], totalizando um total de 35 ativos de informação analisados.

3. Metodologia

Descreva o método utilizado para categorização das vulnerabilidades e a ferramenta utilizada para realizar a varredura.
A verificação foi realizada usando a plataforma de verificação de vulnerabilidades [nome da ferramenta de análise de vulnerabilidades].

A verificação de vulnerabilidade ocorreu em duas fases:

1. *Descoberta de Rede*
2. *Avaliação de vulnerabilidade*

A fase de descoberta de rede foi conduzida através de vários métodos para identificar ativos de informação online na rede de destino, como pings ICMP, pings ARP e conexões TCP para portas conhecidas.

Foi utilizado o Common Vulnerability Scoring System (CVSS)[17] para avaliação da severidade das vulnerabilidades encontradas,

4. Resultados

Apresente as informações de vulnerabilidades encontradas durante a varredura.

Os resultados da auditoria de credentialed patch estão listados abaixo. É importante notar que nem todos os ativos de informação identificados puderam ser verificados durante esta avaliação – do total de 35 ativos de informação pertencentes ao domínio [nome do domínio da instituição], apenas 32 foram verificados com sucesso. Além disso, alguns dos ativos de informação verificados não foram incluídos na lista inicial de ativos de informação mapeados.

O restante dos ativos de informação estavam offline durante as verificações ou as credenciais fornecidas falharam durante a autenticação. Embora nem todos os ativos de informação possam ser verificados, as descobertas devem ser representativas do status atual geral de vulnerabilidade da rede.

A ferramenta contabilizou o total de [inserir quantidade], de falso positivo, são considerados falsos positivos pois o plugin vulnerável não é utilizado pela instituição.

Os seguintes resultados foram encontrados:

- ***Níveis de patch do Windows desatualizados**: muitos sistemas relataram a necessidade de patches e atualizações que foram publicados por pelo menos trinta dias.*
- ***Softwares de terceiros desatualizados**: muitos sistemas relataram a falta de atualizações de segurança necessárias para pacotes de software de terceiros populares, como Google Chrome e Adobe Flash.*

A figura abaixo apresenta em forma de um gráfico as vulnerabilidades encontradas na análise. Para informações detalhadas, verificar documento [citar documento completo, por exemplo, vulnerabilidades_detalhadas.docx].

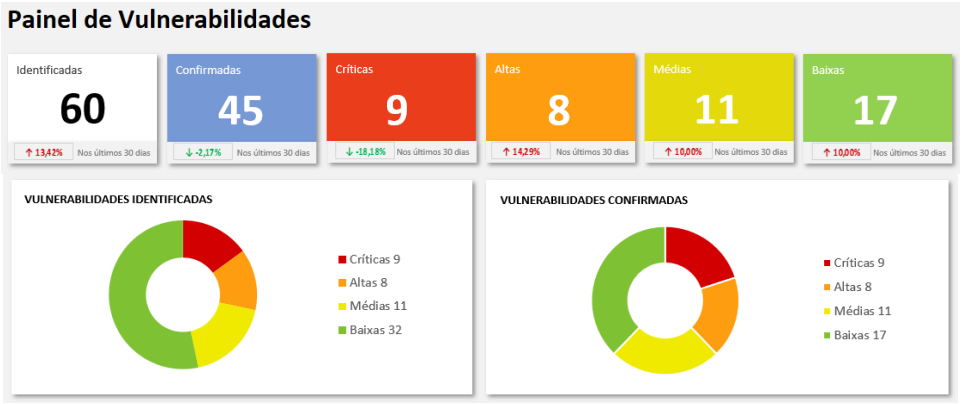

Figura 4 Exemplo de painel vulnerabilidades

[17] *https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator*

5. Correções Necessárias

Apresente as correções necessárias para as vulnerabilidades encontradas ou as soluções de contorno, caso não haja nenhuma correção disponível pelo fabricante no momento da elaboração do relatório (exemplo: vulnerabilidades zero-day).

Este relatório demonstra as vulnerabilidades identificadas que podem ter um impacto significativo em aplicativos de missão crítica usados nas operações diárias. Dos 32 ativos de informação verificados, um total de 247 vulnerabilidades foram encontradas.

***Vulnerabilidade de severidade crítica:** 44 vulnerabilidades críticas requerem atenção imediata. Elas são relativamente fáceis de serem explorados por invasores e podem fornecer a eles controle total dos sistemas afetados.*

A lista das vulnerabilidades de severidade crítica mais frequentes é fornecida abaixo:

Plugin	Descrição	Remediação	Ativos
KB4022715: Windows 10 versão 1607 e Windows Server 2016 junho de 2017 atualização cumulativa	*O Windows não tem a atualização de segurança KB4022715. Portanto, é afetado por várias vulnerabilidades. Um invasor local pode explorá-los por meio de um script especialmente criado para ignorar a política de integridade de código do Device Guard e injetar código arbitrário em um processo confiável do PowerShell.*	*Aplicar a atualização de segurança KB4022715 e consulte o artigo da base de conhecimento para obter informações adicionais.*	*5*
Atualizações de segurança para o Microsoft .NET Framework (fevereiro de 2019)	*A instalação do Microsoft .NET Framework no ativo não possui atualizações de segurança. Existe uma vulnerabilidade de execução remota de código no software .NET Framework e Visual Studio quando o software não verifica a marcação de origem de um arquivo. Um invasor que explorou com êxito a vulnerabilidade pode executar código arbitrário no contexto do usuário atual.*	*A Microsoft lançou atualizações de segurança para o Microsoft .NET Framework.*	*4*
Atualizações de segurança para o Microsoft .NET Framework (dezembro de 2018)	*A instalação do Microsoft .NET Framework no ativo não possui atualizações de segurança. Existe uma vulnerabilidade de execução remota de código quando o Microsoft .NET Framework falha ao validar a entrada corretamente. Um invasor que explorar com êxito essa vulnerabilidade pode assumir o controle de um sistema afetado. Um invasor pode instalar programas, visualizar, alterar ou excluir dados; ou criar novas contas com direitos totais de usuário.*	*A Microsoft lançou atualizações de segurança para o Microsoft .NET Framework.*	*4*
Detecção de versão não suportada do Microsoft SQL Server	*De acordo com seu número de versão informado, a instalação do Microsoft SQL Server no host remoto não é mais suportada. A falta de suporte implica que nenhum novo patch de segurança para o produto será lançado pelo fornecedor. Como resultado, é provável que contenha vulnerabilidades de segurança.*	*Atualizar para uma versão do Microsoft SQL Server com suporte no momento.*	*3*
MS16-077: Atualização de segurança para	*O Windows não tem uma atualização de segurança. Existe uma vulnerabilidade de elevação de privilégio no protocolo Web Proxy Auto Discovery (WPAD)*	*A Microsoft lançou um conjunto de patches para Windows Vista, 2008, 7,*	*3*

WPAD (3165191)	*devido ao manuseio inadequado do processo de descoberta de proxy. Um invasor remoto pode explorar isso respondendo a solicitações de nome NetBIOS para WPAD ignorar as restrições de segurança e obter privilégios elevados.*	*2008 R2, 8, 2012, 8.1, RT 8.1, 2012 R2 e 10. Observar que a atualização cumulativa 3160005 no MS16-063 também deve ser instalada para resolver CVE-2016-3213.*	

Vulnerabilidade de severidade alta: *109 vulnerabilidades de severidade alta geralmente são mais difíceis de explorar e podem não fornecer o mesmo acesso aos sistemas afetados.*

A lista das vulnerabilidades de alta severidade mais frequentes é fornecida abaixo:

Plugin	Descrição	Remediação	Ativos
MS15-011: Vulnerabilidade na Diretiva de Grupo pode permitir a execução remota de código (3000483)	*O Windows é afetado por uma vulnerabilidade de execução remota de código devido à forma como o serviço de Diretiva de Grupo gerencia os dados de diretiva quando um sistema ingressado no domínio se conecta a um controlador de domínio. Um invasor usando uma rede controlada pode explorar isso para obter controle total do host. Observe que a Microsoft não tem planos de lançar uma atualização para o Windows 2003, mesmo que seja afetada por essa vulnerabilidade.*	*A Microsoft lançou um conjunto de patches para o Windows Vista, 2008, 7, 2008 R2, 8, 2012, 8.1 e 2012 R2.*	*18*
Atualizações de segurança para o Internet Explorer (junho de 2017)	*A instalação do Internet Explorer no ativo não possui atualizações de segurança. Existe uma vulnerabilidade de execução remota de código quando o Internet Explorer acessa incorretamente objetos na memória. Essa vulnerabilidade pode corromper a memória de forma que um invasor possa executar código arbitrário no contexto do usuário atual*	*A Microsoft lançou atualizações de segurança para as versões afetadas do Internet Explorer.*	*18*
MS15-124: Atualização de segurança cumulativa para o Internet Explorer (3116180)	*A versão do Internet Explorer instalada no ativo não possui a atualização de segurança cumulativa 3116180. Um invasor remoto não autenticado pode explorar esses problemas convencendo um usuário a visitar um site especialmente criado, resultando na execução de código arbitrário no contexto do usuário atual.*	*A Microsoft lançou um conjunto de patches para Windows Vista, 2008, 7, 2008 R2, 8, RT, 2012, 8.1, RT 8.1, 2012 R2 e 10.*	*9*
KB4343888: Atualização de segurança do Windows 8.1 e Windows Server 2012 R2 de agosto de 2018 (Foreshadow)	*O Windows não tem a atualização de segurança 4343888 ou a atualização cumulativa 4343898. Existe uma vulnerabilidade de execução remota de código na maneira como os navegadores da Microsoft acessam objetos na memória. A vulnerabilidade pode corromper a memória de uma forma que pode permitir que um invasor execute código arbitrário no contexto do usuário atual. Um invasor que explorou com êxito a vulnerabilidade pode obter os mesmos direitos de usuário que o usuário atual*	*Aplicar atualização apenas de segurança KB4343888 ou atualização cumulativa KB4343898, bem como consultar o artigo da base de conhecimento para obter informações adicionais.*	*9*

Vulnerabilidade de severidade média*: 84 eram vulnerabilidades de gravidade média. Essas vulnerabilidades geralmente fornecem informações aos invasores que podem ajudá-los a montar ataques subsequentes em sua rede.*

Eles também devem ser corrigidos em tempo hábil, mas não são tão urgentes quanto as outras vulnerabilidades.

Uma lista das vulnerabilidades de gravidade média mais frequentes é fornecida abaixo:

Plugin	Descrição	Remediação	Ativos
Microsoft Windows Remote Desktop Protocol Server vulnerável a Man-in-the-Middle	*A versão do Remote Desktop Protocol Server (Terminal Service) é vulnerável a um ataque man-in-the-middle (MiTM). O cliente RDP não faz nenhum esforço para validar a identidade do servidor ao configurar a criptografia. Um invasor com a capacidade de interceptar o tráfego do servidor RDP pode estabelecer criptografia com o cliente e o servidor sem ser detectado.*	*Forçar o uso de SSL como camada de transporte para este serviço se suportado | ou/e - Selecione a configuração "Allow connections only from computers running Remote Desktop with Network Level Authentication", se estiver disponível.*	*19*
MS KB3009008: Vulnerabilidade no SSL 3.0 pode permitir divulgação de informações (POODLE)	*O ativo não tem uma das soluções alternativas mencionadas no Microsoft Security Advisory 3009008. Se a solução alternativa da chave de registro do cliente não tiver sido aplicada, qualquer software cliente instalado no ativo (incluindo o IE) será afetado por uma vulnerabilidade de divulgação de informações ao usar SSL 3.0.*	*Aplique a solução alternativa da chave do registro do cliente e a solução alternativa da chave do registro do servidor sugerida pelo comunicado da Microsoft.*	*18*
Enumeração de caminho de serviço não cotado do Microsoft Windows	*O Windows tem pelo menos um serviço instalado que usa um caminho de serviço sem aspas, que contém pelo menos um espaço em branco. Um invasor local pode obter privilégios elevados inserindo um arquivo executável no caminho do serviço afetado*	*Certifique-se de que quaisquer serviços que contenham um espaço no caminho incluam o caminho entre aspas.*	*17*
ADV180002: Atualização de segurança do Microsoft SQL Server de janeiro de 2018 (Meltdown) (Spectre)	*Falta uma atualização de segurança no Microsoft SQL Server. Ele é afetado por uma vulnerabilidade existente nos microprocessadores que utilizam execução especulativa e previsão de ramificação indireta, o que pode permitir que um invasor com acesso de usuário local divulgue informações por meio de uma análise de canal lateral.*	*A Microsoft lançou um conjunto de patches para SQL Server 2008, 2008 R2, 2012, 2014, 2016 e 2017.*	*4*
Atualizações de segurança para o Microsoft .NET Framework (janeiro de 2019)	*A instalação do Microsoft .NET Framework no ativo não possui uma atualização de segurança. Um invasor que explorou com êxito a vulnerabilidade pode recuperar conteúdo, que normalmente é restrito, de um aplicativo da Web.*	*A Microsoft lançou atualizações de segurança para o Microsoft .NET Framework.*	*4*

Vulnerabilidade de severidade baixa: 10 vulnerabilidades de baixa severidade não precisam ser corrigidas imediatamente e podem ser resolvidas durante a próxima janela de manutenção de atualizações.

A lista das vulnerabilidades de gravidade crítica mais frequentes é fornecida abaixo:

Plugin	Descrição	Remediação	Ativos
MS16-153: Atualização de segurança para o driver do sistema de arquivos de log comum (3207328)	*O Windows não possui uma atualização de segurança. Portanto, ele é afetado por uma vulnerabilidade de divulgação de informações no Windows Common Log File System (CLFS) devido ao manuseio inadequado de objetos na memória. Um invasor local pode explorar essa vulnerabilidade por meio de um aplicativo especialmente criado para contornar medidas de segurança e divulgar informações confidenciais.*	*A Microsoft lançou um conjunto de patches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 e 2016.*	*2*
MS15-006: Vulnerabilidade no relatório de erros do Windows pode permitir o desvio do recurso de segurança (3004365)	*O Windows é afetado por uma vulnerabilidade no componente do serviço Relatório de Erros do Windows que permite ignorar o recurso de segurança 'Protected Process Light'. Um invasor remoto pode explorar essa vulnerabilidade para obter acesso à memória de um processo em execução.*	*A Microsoft lançou um conjunto de patches para Windows 8, 2012, 8.1 e 2012 R2.*	*1*
MS15-014: Vulnerabilidade na Diretiva de Grupo pode permitir o desvio do recurso de segurança (3004361)	*A versão do Windows em execução no ativo é afetada por uma vulnerabilidade de downgrade de segurança que afeta estações de trabalho e servidores configurados para usar a Diretiva de Grupo. Um invasor intermediário pode fazer com que o arquivo de diretiva fique corrompido e ilegível, resultando na reversão das configurações de Diretiva de Grupo para seu estado padrão, potencialmente menos seguro.*	*A Microsoft lançou um conjunto de patches para Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1 e 2012 R2.*	*1*
Vulnerabilidade de elevação de privilégios do Microsoft Exchange Server (novembro de 2018)	*A instalação do Microsoft Exchange no ativo contém uma falha não especificada que permite que um invasor man-in-the-middle autenticado se faça passar por outro usuário e aumente os privilégios.*	*Exclua o seguinte valor do Registro: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\DisableLoopbackCheck conforme mostrado no comunicado da Microsoft.*	*1*
MS16-124: Atualização de segurança para o Registro do Windows (3193227)	*O Windows não tem uma atualização de segurança. Ele é afetado por várias vulnerabilidades de divulgação de informações na API do kernel que permitem que um invasor local, por meio de um aplicativo especialmente criado, divulgue informações confidenciais do registro.*	*A Microsoft lançou um conjunto de patches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 e 10.*	*1*

Além disso, a execução das seguintes ações em 9 ativos de informação resolverá 20% das vulnerabilidades na rede.

Ação	*Vulnerabilidades.*	*Ativos*
Adobe Flash Player <= 32.0.0.114 (APSB19-06): Atualizar para a versão 32.0.0.142 ou posterior.	*767*	*1*
MS KB3065823: Atualização para vulnerabilidades no Adobe Flash Player no Internet Explorer: Instalar o Microsoft KB3065823.	*172*	*1*

Instalar KB4489873	*135*	*5*
Instalar KB4489881	*72*	*1*
Instalar KB4489891	*47*	*1*
Google Chrome < 73.0.3683.75 Várias vulnerabilidades: atualizar para a versão 73.0.3683.75 ou posterior.	*18*	*1*
Instalar KB4489880	*16*	*1*
Mecanismo de proteção contra malware da Microsoft < 1.1.14700.5 RCE: habilitar atualizações automáticas para atualizar o mecanismo de verificação para os aplicativos antimalware relevantes. Consultar o artigo 2510781 da base de conhecimento para obter informações sobre como verificar se o MMPE foi atualizado	*11*	*1*

ANEXO II

Ferramentas de varredura de vulnerabilidades

A SGD não endossa nenhum dos Fornecedores ou Ferramentas de Varredura de Vulnerabilidades listados na tabela abaixo. Entretanto, é recomendável a adoção de ferramentas capazes de adotar abordagens para priorização que não se limitem à severidade das vulnerabilidades, mas que incluam outros fatores que lhe são inerentes (ex.: vulnerabilidades mais encontradas em ativos, sua idade e aquelas cuja prioridade de remediação é definida em compliance), além de elementos relativos ao contexto dos ativos a serem protegidos (ex.: seu papel dentro da organização, seu valor comercial e monetário, localização na rede etc.). Essas abordagens podem ser automatizadas, sem prejuízo de que as informações que baseiam a priorização possam ser posteriormente alteradas manualmente.

Ferramenta / Link	Proprietário	Licença	Plataforma	Nota
Abbey Scan	MisterScanner	Comercial	SaaS	
Acunetix	Acunetix	Comercial	Windows, Linux, MacOS	Gratuito (capacidade limitada)
APIsec	APIsec	Comercial	SaaS	Gratuito Pen-test de API limitado
App Scanner	Trustwave	Comercial	Windows	
AppCheck Ltd.	AppCheck Ltd.	Comercial	SaaS	Varredura de avaliação gratuita
AppScan	HCL Software	Comercial	Windows	
AppScan on Cloud	HCL Software	Comercial	SaaS	
AppSpider	Rapid7	Comercial	Windows	
AppTrana Website Security Scan	AppTrana	Gratuito	SaaS	
Arachni	Arachni	Gratuito	Most platforms supported	Gratuito para maioria dos casos de uso
Astra Security Suite	Astra Security	Gratuito	SaaS	Opção paga disponível
Beagle Security	Beagle Security	Comercial	SaaS	Gratuito (capacidade limitada)
beSECURE (formerly AVDS)	Beyond Security	Comercial	SaaS	Gratuito (capacidade limitada)
Blacklock	Blacklock Security	Comercial	Any	Gratuito por 15 dias
BlueClosure BC Detect	BlueClosure	Comercial	Most platforms supported	Gratuito por 15 dias
BREACHLOCK Dynamic Application Security Testing	BREACHLOCK	Comercial	SaaS	
Burp Suite	PortSwiger	Comercial	Most platforms supported	Gratuito (capacidade limitada)

CloudDefense	CloudDefense	Comercial	SaaS or On-Premises	Integra-se a qualquer CI/CD com apenas uma linha de código. Suporta vários tipos de autenticação. Realiza varreduras profundas com facilidade.
Contrast	Contrast Security	Comercial	SaaS or On-Premises	Gratuito (Completo para 1 App)
Crashtest Security	Crashtest Security	Comercial	SaaS or On-Premises	
Cyber Chief	Audacix	Comercial	SaaS or On-Premises	
Deepfence ThreatMapper	Deepfence	Open Source	Linux	Apache v2
Deepfence ThreatStryker	Deepfence	Comercial	Linux, Windows	
Detectify	Detectify	Comercial	SaaS	
Digifort- Inspect	Digifort	Comercial	SaaS	
Edgescan	Edgescan	Comercial	SaaS	
GamaScan	GamaSec	Comercial	Windows	
GoLismero	GoLismero Team	Open Source	Windows, Linux and Macintosh	GPLv2.0
Grabber	Romain Gaucher	Open Source	Python 2.4, BeautifulSoup and PyXML	
Grendel-Scan	David Byrne	Open Source	Windows, Linux and Macintosh	
HostedScan.com	HostedScan.com	Comercial	SaaS	Com versão gratuita
Ikare	Itrust	Comercial	N/A	
ImmuniWeb	High-Tech Bridge	Comercial	SaaS	Gratuito (capacidade limitada)
Indusface Web Application Scanning	Indusface	Comercial	SaaS	Gratuito (para avaliação)
InsightVM	Rapid7	Comercial	SaaS	Gratuito (para avaliação)
Intruder	Intruder Ltd.	Comercial		
IOTHREAT	IOTHREAT	Comercial	SaaS	Versão gratuita (com resultados parciais). Versão Completa (PRO) com 50% de desconto para a comunidade OWASP. CUPOM: ‘OWASP50’
K2 Security Platform	K2 Cyber Security	Comercial	SaaS/On-Premises	Gratuito (para avaliação)
Mayhem for API	ForAllSecure	Comercial	SaaS	Gratuito por 30 dias
N-Stealth	N-Stalker	Comercial	Windows	

Nessus	Tenable	Comercial	Windows	
Netsparker	Netsparker	Comercial	Windows	
Nexploit	NeuraLegion	Comercial	SaaS	
Nexpose	Rapid7	Comercial	Windows/Linux	Gratuito (capacidade limitada)
Nikto	CIRT	Open Source	Unix/Linux	
Nmmapper Tool Collections	Nmmapper	Comercial	SaaS	Coleção de ferramentas Kali online
Nuclei	ProjectDiscovery	Open Source	Windows, Unix/Linux, and Macintosh	Scanner de vulnerabilidade rápido e customizável baseado em YAML e DSL.
OpenVAS by Greenbone	greenbone	Open Source	Linux	Scanner de vulnerabilidade Open source completo, desenvolvido e mantido pela Greenbone Networks GmbH.
Probely	Probely	Comercial	SaaS	Gratuito (capacidade limitada)
Proxy.app	Websecurify	Comercial	Macintosh	
purpleteam	OWASP	Open Source	CLI and SaaS	GNU-AGPL v3
QualysGuard	Qualys	Comercial	N/A	
ReconwithMe	Nassec	Comercial	SaaS	Disponível em versão paga
Retina	BeyondTrust	Comercial	Windows	
Ride (REST JSON Payload fuzzer)	Adobe, Inc.	Open Source	Linux / Mac / Windows	Apache 2
ScanRepeat	Ventures CDX	Comercial	SaaS	
ScanTitan Vulnerability Scanner	ScanTitan	Comercial	SaaS	Gratuito (capacidade limitada)
Sec-helpers	VWT Digital	Open Source or Gratuito	N/A	
SecPoint Penetrator	SecPoint	Comercial	N/A	
SecretScanner	Deepfence	Open Source	Linux	Encontre tokens, chaves, senhas etc. em contêineres e filesystems, suportando aproximadamente 140 diferentes tipos de secrets.
Security For Everyone	Security For Everyone	Comercial	SaaS	Gratuito (capacidade limitada)
Securus	Orvant, Inc	Comercial	N/A	
Sentinel	WhiteHat Security	Comercial	N/A	
SmartScanner	SmartScanner	Comercial	Windows	Gratuito (capacidade limitada)

SOATest	Parasoft	Comercial	Windows / Linux / Solaris	
StackHawk	StackHawk	Comercial	SaaS	
ThreatMapper	Deepfence	Open Source	Linux	Detecção e priorização de vulnerabilidades de código aberto para cargas de trabalho baseadas em Kubernetes, Docker, Serverless e host.
Tinfoil Security	Synopsys	Comercial	SaaS or On-Premises	Gratuito (capacidade limitada)
Trustkeeper Scanner	Trustwave SpiderLabs	Comercial	SaaS	
Vega	Subgraph	Open Source	Windows, Linux and Macintosh	
Vex	Ubsecure	Comercial	Windows	
w3af	w3af.org	Open Source	Linux and Mac	GPLv2.0
Wapiti	Informática Gesfor	Open Source	Windows, Unix/Linux and Macintosh	
Web Security Scanner	DefenseCode	Comercial	On-Premises	
WebApp360	TripWire	Comercial	Windows	
WebCookies	WebCookies	Gratuito	SaaS	
WebInspect	Micro Focus	Comercial	Windows	
WebReaver	Websecurify	Comercial	Macintosh	
WebScanService	German Web Security	Comercial	N/A	
Websecurify Suite	Websecurify	Comercial	Windows, Linux, Macintosh	Gratuito (capacidade limitada)
Website Security Check	CyberAnt	Comercial	SaaS	Desconto de 20% com o CUPOM: ‘OWASP20’
WPScan	WPScan Team	Comercial	Linux and Mac	Opção gratuita
Zed Attack Proxy	OWASP	Open Source	Windows, Unix/Linux, and Macintosh	Apache-2.0

ANEXO III

Mudanças da versão 2.0

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nesta versão do Guia de Gerenciamento de Vulnerabilidades.

Primeiramente, ressalta-se que as mudanças inseridas nesta versão em comparação com a anterior visam a adequação do mesmo com o Guia do Framework de Privacidade e Segurança da Informação v1 elaborado e publicado pela SGD em novembro de 2022.

Foram realizadas inclusões de: seção sobre aviso preliminar e agradecimentos; e referência de que controle e medidas do Framework de Privacidade e Segurança da Informação são atendidos pelo Guia de Gerenciamento de Vulnerabilidades.

Além disso, foram feitas inclusões/atualizações nas seções “Referência legal e de boas práticas” e “Anexo I (modelo de relatório)” para melhorar o esclarecimento acerca do seu objetivo. Adicionalmente, os links de referência presentes no modelo foram validados e atualizados.