PORTARIA Nº 7475, DE 11 DE NOVEMBRO DE 2022

Aprova a Norma Complementar para Gerenciamento de Vulnerabilidades.

A GESTORA DE SEGURANÇA DA INFORMAÇÃO, no uso das atribuições que lhe confere o inciso XII, do art. 2º, da Portaria nº 67/SEI-MCOM, de 4 de março de 2021, e tendo em vista o disposto no art. 15, inciso III, do Decreto nº 9.637, de 26 de dezembro de 2018, a Portaria MCOM Nº 2.454, de 22 de abril de 2021, os Arts. 10, 15 e 19, da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança institucional da Presidência da República, resolve:

Art. 1º Aprovar a Norma Complementar para Gerenciamento de Vulnerabilidades.

Art. 2º Esta Norma Complementar entrará em vigor na data de sua publicação.

WANESSA QUEIROZ DE SOUZA OLIVEIRA
Gestora de Segurança da Informação

NORMA COMPLEMENTAR PARA GERENCIAMENTO DE VULNERABILIDADES

OBJETIVO

Estabelecer as diretrizes para o Gerenciamento de Vulnerabilidades no âmbito do Ministério das Comunicações - MCOM.

O objetivo da Norma Complementar de Gerenciamento de Vulnerabilidades é estabelecer as regras relacionadas às atividades de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades. Além disso, contempla ações e boas práticas que devem ser observadas para se evitar que vulnerabilidades estejam presentes nos ativos da organização.

A revisão, a avaliação, a aplicação e a verificação das atualizações de ativos de informação auxiliam a mitigar as vulnerabilidades no ambiente de Tecnologia da Informação e Telecomunicações, bem como os riscos associados a tais vulnerabilidades.

APLICAÇÃO

Esta norma se aplica aos sistemas e ativos informacionais do Ministério das Comunicações, incluindo funcionários, gestores, prestadores de serviços e contratados que tenham acesso e/ou utilizem ativos informacionais.

Os serviços de TI críticos do Ministério das Comunicações devem ser formalmente elencados pela Coordenação Geral de Tecnologia da Informação e Comunicação.

A Coordenação Geral de Tecnologia da Informação e Comunicação é responsável por elaborar, manter e fazer cumprir a Norma Complementar de Gerenciamento de Vulnerabilidades no Ministério das Comunicações.

Exceções: Pode ocorrer de alguns ativos de informação não serem contemplados por possíveis dificuldades técnicas ou obrigações contratuais e normativas. Quaisquer exceções a esta norma deverão ser documentadas e aprovadas por meio de um processo de gerenciamento de exceções.

Público: Esta Norma Complementar de Gerenciamento de Vulnerabilidades do Ministério das Comunicações se aplica a indivíduos responsáveis pela gestão e a indivíduos que utilizam qualquer Ativo de Informação da Rede Computadores em nome do órgão. Além disso, a presente norma se aplica a quaisquer provedores e entidades terceirizadas com acesso a informações, redes e aplicativos do órgão.

REFERÊNCIA LEGAL E NORMATIVA

Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

Instrução Normativa nº 2, de 24 de julho de 2020, altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

Instrução Normativa nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

Portaria MCOM Nº 2.454, de 22 de abril de 2021, que aprova a Política de Segurança da Informação do Ministério das Comunicações;

Portaria MCOM nº 2.120, de 4 de março de 2021, que institui a Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR);

Portaria MCOM Nº 67, de 4 de março de 2021, que designa a Gestora de Segurança da Informação do Ministério das Comunicações;

Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI);

Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022;

Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD);

Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER);

Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC);

Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados;

Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI); e

Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o glossário de segurança da informação.

1 DISPOSIÇÕES GERAIS

1.1 Um processo de Gerenciamento de Vulnerabilidades (PGV) deve ser criado, implementado, mantido e aplicado.

1.2 O processo deve conter a implementação de mecanismos para obter informações oportunas sobre vulnerabilidades técnicas dos sistemas e ativos de informação, a avaliação da exposição da organização a tais vulnerabilidades e a implementação de salvaguardas apropriadas para lidar com o risco associado.

1.3 O processo deve contemplar o gerenciamento de vulnerabilidades dos diversos ativos que sustentam os serviços da organização, como a ativos que compõe a rede da organização, aplicações web, aplicativos móveis, sistemas operacionais, dentre outros.

1.4 O processo deve incluir atividades de suporte, incluindo, mas não se limitando a métricas de relatório e treinamento para implementação eficaz do PGV.

1.5 O processo deve incluir funções e responsabilidades das equipes/funções para realizar todas as atividades de maneira oportuna e eficaz para o Ministério das Comunicações.

1.6 O processo deve estabelecer mecanismos para obter atualizações de software quando emitidas pelo fabricante ou fornecedor oficial regularmente utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

1.7 A consistência e a eficácia do processo devem ser medidas por meio de métricas de gerenciamento de vulnerabilidades.

1.8 As métricas de gerenciamento de vulnerabilidades devem ser definidas pelo Gestor de Segurança da Informação e suas medições devem ocorrer, no mínimo, a cada 3 meses.

2 PROCEDIMENTOS

2.1 Mapeamento de Ativos de Informação

2.1.1 Um mapeamento de ativos de informação deve constar no escopo do processo de gerenciamento de vulnerabilidades e patches para determinar qual marca, modelo e versão de equipamento de hardware, sistemas operacionais, banco de dados, sistema, servidor web e aplicativos de software são usados no MCOM.

2.1.2 O mapeamento de ativos de informação deve ser atualizado periodicamente ou sempre que ocorrerem alterações significativas para garantir que os recursos informacionais estejam cobertos pelo processo de gerenciamento de vulnerabilidades do MCOM.

2.2 Detecção de vulnerabilidades

2.2.1 As funções e as responsabilidades das equipes/funções para realizar atividades de detecção de vulnerabilidades devem ser estabelecidas.

2.2.2 As ferramentas devem ser configuradas e ajustadas adequadamente de acordo com o escopo avaliado.

2.2.3 Os tipos de varreduras e os tipos de teste devem ser avaliados e ajustados para que sejam congruentes com o escopo avaliado.

2.2.4 A frequência de testes de segurança deve levar em consideração os requisitos legais, regulamentares e contratuais que o MCOM deve cumprir e os riscos associados aos ativos avaliados.

2.2.5 As varreduras de vulnerabilidades na rede corporativa devem ser realizadas por períodos determinados de até 3 meses ou após alteração significativa na rede, por equipe interna ou por terceiro ou uma combinação de ambos.

2.2.6 Os testes de segurança devem utilizar o feed de vulnerabilidade mais recente, de forma a evitar que determinadas vulnerabilidades não sejam detectadas.

2.2.7 Para cada teste, é necessário verificar a integridade da ferramenta utilizada e se ela varreu corretamente os ativos analisados e se existem exceções de vulnerabilidades.

2.2.8 As ferramentas utilizadas devem ser ajustadas continuamente, de forma a evitar que varreduras feitas por ferramentas distintas gerem resultados distintos.

2.2.9 O teste de invasão ou o teste de penetração (Pentest) deve ser realizado conforme critério de necessidade do MCOM, ou pelo menos a cada ano, utilizando especialistas qualificados externos como parte de um exercício planejado, que inclui o escopo da avaliação, os métodos de uso e os requisitos operacionais, a fim de fornecer as informações mais precisas e relevantes sobre as vulnerabilidades atuais, sem afetar o funcionamento normal do MCOM.

2.2.10 A integridade do resultado de detecção de vulnerabilidades deve ser avaliada antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos.

2.2.11 A detecção manual de vulnerabilidades deve ser considerada como complemento à detecção automática de vulnerabilidades.

2.3 Elaboração e manutenção dos relatórios

2.3.1 A Equipe de Análise e Tratamento de Vulnerabilidade deve elaborar relatórios após cada ciclo de detecção para auxiliar o MCOM a entender e mensurar as vulnerabilidades existentes.

2.3.2 Os resultados da varredura devem passar por análise da Equipe de Análise e Tratamento de Vulnerabilidade com o dispositivo ou gerenciador de rede para que possíveis falsos positivos possam ser identificados e eliminados.

2.3.3 Grupos de ativos de informação devem ser determinados por tipo de ambiente, por tipo de sistema, por ID CVE ou por tipo de vulnerabilidade.

2.3.4 A Equipe de Análise e Tratamento de Vulnerabilidade deve adotar métricas para os relatórios de vulnerabilidade e determinar o valor percentual dos ativos de informação vulneráveis por gravidade e CVSS.

2.3.5 A quantidade e a porcentagem de novas vulnerabilidades devem ser monitoradas por: severidade; grupos funcionais; tipo de ambiente; tipo de sistema; autoridade de numeração CVE; e tipo de vulnerabilidade.

2.3.6 O relatório deve ser classificado, durante e após a sua elaboração, de acordo com a sensibilidade das informações presentes nele.

2.3.7 Todas as versões do relatório devem ser remetidas ao Comitê de Segurança da Informação e Comunicação.

2.4 Banco de dados de vulnerabilidades

2.4.1 Deve ser mantido um banco de dados de vulnerabilidades coletadas de várias fontes que precisam ser aplicadas aos sistemas e ativos informacionais do MCOM.

2.4.2 O banco de dados poderá incluir informações de vulnerabilidade, análise de vulnerabilidade para priorização e plano de correção de vulnerabilidade.

2.5 Priorização e correção de vulnerabilidades

2.5.1 O tratamento de vulnerabilidades deve ser priorizado com base em sua classificação de risco e criticidade, tempo esperado para correção, grau de risco, impacto em caso de exploração e no valor que o ativo ou host impactado tem para o negócio do MCOM.

2.5.2 A prioridade no tratamento das vulnerabilidades deve ser tratada, de acordo com o seu nível de severidade e relevância do ativo, nos prazos estipulados abaixo.

Prioridade do Tratamento	Prazo de correção	Descrição do risco
Crítico (1)	Até 2 dias	Condição totalmente inaceitável quando medidas imediatas devem ser tomadas para eliminar a materialização do risco e mitigar perigos e impactos.
Alto (2)	Até 30 dias	Pessoas mal-intencionadas podem facilmente obter o controle do host, o que pode comprometer toda a sua rede. As vulnerabilidades incluem acesso de leitura e gravação a arquivos, execução remota de comandos e backdoors.
Médio (3)	Até 60 dias	Pessoas mal-intencionadas podem obter o controle do host ou coletar informações altamente confidenciais, incluindo acesso de "leitura" ao arquivo, backdoors em potencial ou uma lista de todas as contas de usuário no host.

		Pessoas mal-intencionadas podem obter acesso às configurações de segurança no host, o que pode levar ao acesso a arquivos e à divulgação de conteúdo de arquivos, navegação em diretórios, ataques de negação de serviço e uso não autorizado de serviços.
Baixo (4)	Até 120 dias	Pessoas mal-intencionadas podem coletar informações confidenciais do host, como versões de software instaladas, que podem revelar vulnerabilidades conhecidas. Pessoas mal-intencionadas podem coletar informações sobre o host por meio de portas ou serviços abertos, o que pode levar à divulgação de outras vulnerabilidades.

2.5.3 Os testes que forem concluídos com falha devem ser examinados novamente até que sua execução seja concluída com êxito. Caso não seja possível, deve-se avaliar se a vulnerabilidade será incluída na lista de exceções por pessoal autorizado, com base no processo de aceitação de risco.

2.5.4 Devem-se estabelecer mecanismos para obter atualizações de software quando emitidas pelo fabricante ou fornecedor oficial regularmente, utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

2.5.5 Quando as vulnerabilidades não puderem ser corrigidas dentro do prazo estabelecido no item 2.5.2, a Equipe de Análise e Tratamento de Vulnerabilidade deve enviar uma "solicitação de renúncia" a Coordenação de Segurança da Informação do MCOM. A solicitação deve conter as seguintes informações:

a) Detalhes do sistema ou ativo.

b) A justificativa para a solicitação.

c) Detalhes dos controles existentes (se houver).

d) Novo prazo de correção.

e) Plano de ação da remediação (obedecendo o novo prazo de correção).

2.5.6 Os alertas de vulnerabilidades, as correções de patches e as ameaças emergentes que correspondam aos recursos informacionais relacionados no inventário de sistema e ativos de informação devem ser monitorados.

2.6 Das exceções

2.6.1 Para os ativos de informação do MCOM não contemplados por esta norma em função de dificuldades técnicas ou obrigações contratuais e normativas ou quaisquer exceções a esta norma deverão ser documentadas e aprovadas por meio de um processo de gerenciamento de exceções do MCOM.

2.6.2 A lista de exceções de ativos de informação deve ter validade de 12 meses, devendo ser revisada após esse período.

2.7 Dos registros de logs

2.7.1 Ativos, físicos ou virtuais, como servidores e recursos de rede, devem recuperar informações baseadas em tempo de uma única fonte de tempo de referência (servidor NTP) regularmente para que os relógios de registro sejam consistentes.

2.7.2 As configurações referentes a ativos de informação devem incluir configurações de log para registrar ações que possam afetar ou que sejam relevantes para a segurança da informação.

2.7.3 Uma revisão dos arquivos de registro (logs) deve ser conduzida pelo menos a cada 12 meses.

2.7.4 Os arquivos de registro (logs) devem ser protegidos contra adulteração ou acesso não autorizado.

2.7.5 Registros de logs dos sistemas e ativos informacionais classificados como críticos devem ser mantidos por pelo menos 12 meses.

2.8 Comunicação da ocorrência de vulnerabilidades e correções

2.8.1 As vulnerabilidades e respectivas informações de correção devem ser informadas aos usuários afetados, incluindo, mas não se limitando a: administradores de sistema, proprietários de sistema e usuários finais.

2.8.2 As correções bem-sucedidas de vulnerabilidades poderão ser testadas por meio de verificação de vulnerabilidades de rede e host, verificação de logs de patches, testes de invasão/penetração (Pentest) e verificação das definições de configuração.

2.9 Implementação e verificação das correções de vulnerabilidades

2.9.1 Correções de vulnerabilidades, quando possível, devem ser efetivamente testadas e aprovadas antes de serem implantadas em produção. Atividades de correção de vulnerabilidades geralmente incluem, mas não se limitam à instalação de patches de segurança, bem como a ajustes de configuração e/ou remoção de software.

2.9.2 Quando instalações de patches de segurança e ajustes de configuração são recomendadas para mitigar as vulnerabilidades, elas devem ser enviadas por meio do Processo de Gestão de Mudanças para que os controles apropriados sejam implementados para teste, avaliação de riscos e reparação.

2.10 Dos serviços em nuvem ou de terceiros

2.10.1 Para serviços em nuvem, as responsabilidades do provedor de serviços em nuvem pública com o cliente do serviço em nuvem devem ser definidas e acordadas.

2.10.2 Terceiros devem cumprir os requisitos desta norma. Sempre que possível, essa obrigação e outras responsabilidades que envolvam o gerenciamento de vulnerabilidades devem ser incluídas em contratos com terceiros.