Controladoria-Geral da União

SECRETARIA EXECUTIVA

PORTARIA NORMATIVA SE/CGU Nº 41, DE 29 DE DEZEMBRO DE 2022

Institui a Política de Gerenciamento de Vulnerabilidades no ambiente de computação da Controladoria-Geral da União - CGU.

O SECRETÁRIO-EXECUTIVO DA CONTROLADORIA-GERAL DA UNIÃO, no exercício das atribuições previstas no art. 30, Anexo I, do Decreto nº 11.102, de 23 de junho de 2022, e art. 6º, inciso II, da Portaria CGU nº 1.973, de 31 de agosto de 2021, considerando o disposto no Decreto nº 10.332, de 28 de abril de 2020, Portaria SE/CGU nº 587, de 10 de março de 2021 e Instrução Normativa nº 3, de 28 de maio de 2021 - Gabinete de Segurança Institucional da Presidência da República, bem ainda com base no processo SEI 00190.111415/2022-31, resolve:

Art. 1º Esta Portaria institui a Política de Gerenciamento de Vulnerabilidades e estabelece princípios, diretrizes e responsabilidades relacionadas à gestão de vulnerabilidades no ambiente de computação da Controladoria-Geral da União - CGU.

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 2º Para os efeitos desta Portaria, considera-se:

I - CVSS (Common Vulnerability Scoring System) - sistema comum de pontuação de vulnerabilidade;

II - gerenciamento de vulnerabilidades - processo cíclico e contínuo de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades;

III - NTP (Network Time Protocol) - protocolo de tempo para redes;

IV - patch - uma parte de código adicional desenvolvido para resolver um problema ou falha em um software existente;

V - remediação - o ato de corrigir uma vulnerabilidade ou eliminar uma ameaça;

VI - teste de penetração ou teste de intrusão (pentest) - procedimento fundamental para a análise de vulnerabilidades que consiste no teste dos sistemas em busca de vulnerabilidades conhecidas ou informadas por especialistas e instituições detentoras dos softwares em utilização pelo órgão ou entidade; e

VII - vulnerabilidade - condição que conjuga os fatores suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha e que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores.

Parágrafo único. Na aplicação desta Portaria deverão ser observados, no que couber, os conceitos constantes do Glossário de Segurança da Informação aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

Objetivos

Art. 3º São objetivos da Política de Gerenciamento de Vulnerabilidades:

I - estabelecer as regras relacionadas às atividades de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades; e

II - definir boas práticas a serem observadas para evitar vulnerabilidades nos ativos de informação da organização.

Abrangência

Art. 4º As disposições desta Portaria e regulamentação correlata devem ser aplicadas aos sistemas e ativos informacionais da CGU e observadas pelos respectivos gestores e usuários de sistemas e ativos de informação, bem ainda por provedores e entidades terceirizadas com acesso a informações, redes e aplicativos do órgão.

Art. 5º A Diretoria de Tecnologia da Informação (DTI) é responsável por elaborar, manter e fazer cumprir a Política de Gerenciamento de Vulnerabilidades na CGU.

CAPÍTULO II

DO PROCESSO DE GERENCIAMENTO DE VULNERABILIDADES

Art. 6º O processo de Gerenciamento de Vulnerabilidades de que trata esta portaria deve ser criado, implementado, mantido e aplicado no âmbito da CGU, e necessariamente abrangerá:

I - a implementação de mecanismos para obtenção de 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;

II - o gerenciamento de vulnerabilidades dos diversos ativos que sustentam os serviços da organização em um escopo determinado, como a ativos que compõem a rede da organização, aplicações web, aplicativos móveis, sistemas operacionais, dentre outros;

III - o elenco dos sistemas e ativos informacionais críticos da CGU; e

IV - a definição de funções e responsabilidades das equipes, de modo a viabilizar a realização de todas as atividades de maneira oportuna e eficaz para a CGU.

Parágrafo único. A Diretoria de Tecnologia da Informação (DTI) é responsável por definir a equipe de gerenciamento de vulnerabilidades.

CAPÍTULO III

DO MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

Art. 7º O mapeamento de ativos de informação deve constar no escopo do processo de gerenciamento de vulnerabilidades e patches.

Parágrafo único. O mapeamento de ativos de informação será atualizado periodicamente ou sempre que ocorrerem alterações significativas, como forma de garantir que os recursos informacionais estejam cobertos pelo processo de gerenciamento de vulnerabilidades da CGU.

CAPÍTULO IV

DA DETECÇÃO DE VULNERABILIDADES

Art. 8º As ferramentas de detecção de vulnerabilidades e os tipos de varreduras e testes devem ser configurados, avaliados e ajustados adequadamente de acordo com o escopo avaliado.

Art. 9º A determinação da frequência do procedimento de detecção de vulnerabilidades levará em conta os requisitos legais, regulamentares e contratuais a que a CGU esteja submetida, bem ainda os riscos associados aos ativos avaliados e a capacidade operacional do órgão.

Art. 10. Uma equipe interna, terceiros ou uma combinação de ambos será responsável pelas varreduras de vulnerabilidades na rede corporativa, as quais devem ser realizadas em períodos determinados ou após alteração significativa na rede.

Art. 11. Os testes de penetração (Pentest) serão realizados conforme critérios de necessidade da CGU, com envolvimento de especialistas internos ou externos e sem afetar o funcionamento normal do ambiente computacional do órgão.

Parágrafo único. Os testes de penetração serão planejados de modo a definir o escopo da avaliação, os requisitos operacionais, os procedimentos e métodos a serem adotados.

Art. 12. A integridade do resultado de detecção de vulnerabilidades deve ser avaliada antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos.

Art. 13. A detecção manual de vulnerabilidades será considerada como complemento à sua detecção automática.

CAPÍTULO V

DA ELABORAÇÃO DOS RELATÓRIOS DE VULNERABILIDADES

Art. 14. A equipe de gerenciamento de vulnerabilidades elaborará relatórios após cada ciclo de detecção com vistas a auxiliar no entendimento e mensuração as vulnerabilidades existentes.

Art. 15. A equipe de gerenciamento de vulnerabilidades deve adotar métricas para os relatórios de vulnerabilidades e determinar o valor percentual dos ativos de informação vulneráveis por gravidade ou CVSS.

Art. 16. O relatório deve ser classificado de acordo com a sensibilidade das informações em si presentes durante e após a sua elaboração.

Art. 17. As versões finais dos relatórios gerados serão remetidas ao Comitê Gerencial de Segurança Corporativa.

CAPÍTULO VI

DA PRIORIZAÇÃO E CORREÇÃO DE VULNERABILIDADES

Art. 18. O tratamento de vulnerabilidades será priorizado com base em sua classificação de risco e criticidade.

Art. 19. As correções de vulnerabilidades que forem concluídas com falha serão reiteradamente examinadas até que sua aplicação seja concluída com êxito.

Parágrafo único. Caso não seja possível a aplicação das correções, deve ser avaliada, com base no processo de aceitação de risco, a potencial inclusão da vulnerabilidade na lista de exceções.

Art. 20. As atualizações de software serão executadas mediante o uso preferencial de pacotes franqueados pelo fabricante ou fornecedor oficial.

Art. 21. 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.

CAPÍTULO VII

DAS EXCEÇÕES

Art. 22. Os sistemas e ativos de informação não contemplados por esta política em razão de dificuldades técnicas ou obrigações contratuais e normativas, ou de qualquer outro motivo, deverão ser documentados e aprovados como exceção por meio do gerenciamento de exceções a ser definido pela DTI.

Parágrafo único. As exceções devem ser tratadas no mapeamento de riscos de segurança da informação.

Art. 23. A lista de exceções de sistemas e ativos de informação deve ser revisada periodicamente.

CAPÍTULO VIII

DOS REGISTROS DE LOGS

Art. 24. Ativos físicos ou virtuais, como servidores e recursos de rede, devem regularmente recuperar informações baseadas na mesma unidade de medida de tempo de referência (servidor NTP) para que os relógios de registro sejam consistentes.

Art. 25. As configurações referentes a ativos de informação incluirão configurações de log (registro) para fins de registro das ações que sejam relevantes para a segurança da informação ou que possam vir a afetá-la.

Art. 26. A revisão dos arquivos de logs será conduzida de forma periódica.

Art. 27. Os arquivos de logs devem ser protegidos contra adulteração ou acesso não autorizado.

Art. 28. Registros de logs dos sistemas e ativos informacionais classificados como críticos serão mantidos de acordo com a Política de Backup da CGU.

CAPÍTULO IX

DA COMUNICAÇÃO DA OCORRÊNCIA DE VULNERABILIDADES E CORREÇÕES

Art. 29. As vulnerabilidades e respectivas informações de correção devem ser comunicadas aos responsáveis ou usuários afetados, bem ainda compor o relatório de vulnerabilidades.

CAPÍTULO X

DA IMPLEMENTAÇÃO E VERIFICAÇAO DAS CORREÇÕES DE VULNERABILIDADES

Art. 30. Somente correções de vulnerabilidades que sejam efetivamente testadas e aprovadas devem ser implantadas em produção.

Art. 31. Sempre que instalações de patches de segurança e ajustes de configuração sejam recomendadas para mitigar as vulnerabilidades elas devem ser enviadas por meio do processo de gestão de mudanças, de forma a viabilizar que os controles apropriados sejam implementados para teste, avaliação de riscos e reparação.

CAPÍTULO XI

DISPOSIÇÕES FINAIS

Art. 32. A revisão desta Portaria deve ser realizada a cada dois anos pelo Comitê Gerencial de Segurança Corporativa - CGSC, ou, a critério deste, sempre que se fizer necessário.

Art. 33. Esta Portaria entrará em vigor na data de sua publicação.

JOSE MARCELO CASTRO DE CARVALHO

Ministério Público da União

MINISTÉRIO PÚBLICO FEDERAL

PROCURADORIA REGIONAL DA REPÚBLICA DA 5ª REGIÃO

DECISÃO DE 28 DE DEZEMBRO DE 2022

Referência: PGEA nº 1.05.000.000562/2022-35. Assunto: DECISÃO. Aplicação de Penalidade. Suspensão temporária de participação em licitação e impedimento de contratar com a Procuradoria Regional da República da 5ª Região.

Acolhendo manifestação da Assessoria Jurídica, constante no Parecer Jurídico nº 82/2022, e com base no disposto no artigo 33, inciso XIII, da Portaria SG/MPF n.º 382/2015 (Regimento Interno Administrativo do MPF), APLICO a sanção de suspensão temporária de participação em licitação e impedimento de contratar com a Procuradoria Regional da República da 5ª Região, pelo prazo de 16 meses em desfavor da pessoa jurídica TECNO INDUSTRIAL E COMERCIAL EIRELI, CNPJ 03.764.895/0001-29, com fundamento no art. 87, inciso III, da Lei nº 8.666/93, e do art. 15, inciso VII, da IN nº 2/2020 do MPF, em razão de inexecução total do contrato..

RAFAEL RIBEIRO NOGUEIRA FILHO
Procurador-Chefe da PRR-5ª Região