Protocolo: 956249
Data: 23/01/2024
Título: RESOLUÇÃO CVL Nº 220
Página(s): a

RESOLUÇÃO CVL Nº 220 DE 22 DE JANEIRO DE 2024

Regulamenta a norma de Segurança de Desenvolvimento de Sistemas no âmbito da Administração Pública Municipal.

O SECRETÁRIO MUNICIPAL DA CASA CIVIL, no uso das atribuições que lhe são conferidas pela legislação em vigor e,

CONSIDERANDO o disposto no Inciso II do Art. 7º do Decreto Rio Nº 53.700, de 08 de dezembro de 2023, que instituiu a Política de Segurança da Informação - PSI no âmbito do Poder Executivo Municipal, o qual atribui competência à Secretaria Municipal da Casa Civil - CVL para deliberar, analisar e revisar normas complementares;

CONSIDERANDO o disposto no artigo 13 do Decreto Rio Nº 53.700, de 08 de dezembro de 2023, que estipula prazo de cento e oitenta dias para regulamentação da Política de Segurança da Informação - PSI;

CONSIDERANDO o disposto na Seção X - Dos Sistemas de Informação, art. 13 da Resolução CVL Nº 216 de 15 de dezembro de 2023, que trata das diretrizes ao tema no âmbito do Poder Executivo Municipal;

CONSIDERANDO a crescente transformação digital da Administração Pública, em que processos e serviços encontram-se cada vez mais apoiados por ativos tecnológicos;

CONSIDERANDO que o nível de segurança destes serviços é resultado do nível de segurança dos sistemas de informação que os suportam, que está fortemente relacionado aos seus processos de desenvolvimento e manutenção,

RESOLVE:

Art. 1º Regulamentar a Norma de Segurança de Desenvolvimento de Sistemas no âmbito da Administração Pública Municipal.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º A Norma de Segurança de Desenvolvimento de Sistemas tem como objetivo definir os requisitos de segurança a serem atendidos durante o ciclo de vida de desenvolvimento dos sistemas de informação, sendo complementar à Política de Segurança da Informação - PSI.

Art. 3º Esta norma aplica-se a todas as pessoas, físicas ou jurídicas, envolvidas no ciclo de vida de desenvolvimento de sistemas da Administração Pública Municipal.

Art. 4º Para fins desta Resolução, considera-se:

I - ambiente de desenvolvimento: é o ambiente de Tecnologia da Informação e Comunicação (TIC) responsável por hospedar as ações de desenvolvimento e manutenção dos sistemas e aplicativos da organização;

II - ambiente de produção: é o ambiente de TIC responsável por processar as informações que sustentam os processos e serviços da organização;

III - ambiente de homologação: ambiente de TIC responsável por simular o ambiente de produção de forma a hospedar os testes de aceitação, a fim de garantir que o sistema atenda a todos os requisitos necessários à sua entrada em produção;

IV - autenticação: processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica. Há diversas técnicas de autenticação como senhas, impressão digital, certificado digital e reconhecimento da íris;

V - autorização: concessão de um conjunto de permissões de acesso às informações ou funcionalidades de um sistema de informação a um usuário após sua autenticação;

VI - ativo da informação: informação, processo ou ativo físico, tecnológico ou humano que suporta as operações de coleta, armazenamento, processamento, compartilhamento ou descarte de informações;

VII - desenvolvimento seguro: refere-se a uma atualização do ciclo de vida de desenvolvimento de sistemas (SDLC) a partir da inserção de um conjunto de atividades relacionadas à segurança em todo o ciclo (SSDLC), por exemplo, incorporando itens como: levantamento e análise de ameaças, práticas de codificação segura, testes estáticos e dinâmicos de segurança e gestão contínua de vulnerabilidades.

VIII - incidente de segurança: conjunto de eventos adversos, confirmados ou sob suspeita, que tenham capacidade de comprometer a confidencialidade, integridade ou disponibilidade das informações residentes nos ativos de uma organização;

IX - remediação: ato de corrigir uma vulnerabilidade ou de implementar controles que reduzam a probabilidade de sua exploração;
X - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

XI - usuário: qualquer pessoa autorizada a utilizar o sistema de informação.

CAPÍTULO II
DAS MEDIDAS DE SEGURANÇA

Seção I
Do Desenvolvimento de Sistemas

Art. 5º Os sistemas devem ser desenvolvidos com base em metodologias que estejam em conformidade com as melhores práticas de desenvolvimento seguro de sistemas.

Art. 6º Os requisitos de segurança e privacidade devem ser identificados na fase de definição de requisitos, acordados, documentados e tratados de forma integrada no ciclo de vida de desenvolvimento do sistema.

Art. 7º Os produtos que suportam o ciclo de vida de desenvolvimento de sistemas como documentos de especificação de requisitos, códigos-fonte, modelos de dados, planos de testes, planos de verificação ou homologação devem estar hospedados em repositórios sujeitos a mecanismos de controle de acesso que garantam que somente agentes autorizados tenham acesso a estes produtos.

Art. 8º Os códigos-fonte dos sistemas devem ser guardados em repositórios centralizados, utilizando soluções de gerenciamento de versões, que devem constar de mecanismos de controle de acesso que suportem identificação, autenticação, autorização e auditoria em todas as interações realizadas por seus usuários.

Art. 9º Durante seu ciclo de vida, os sistemas devem ser submetidos a processos periódicos de identificação, análise e remediação de vulnerabilidades.

Parágrafo único. a periodicidade do processo deve ser definida em função do nível de sensibilidade do sistema considerando um possível incidente de segurança.

Art. 10 Os serviços de desenvolvimento e manutenção terceirizados devem ser acompanhados por agentes públicos formalmente designados, de modo a certificar a qualidade dos serviços prestados e sua conformidade à regulamentação vigente relacionada ao desenvolvimento de sistemas.

Art. 11 Os integrantes das equipes de desenvolvimento e manutenção de sistemas devem ser devidamente capacitados no uso das metodologias e ferramentas homologadas para suporte às práticas de desenvolvimento seguro de sistemas.

Seção II
Do Controle de Acesso aos Sistemas

Art. 12 Os ambientes de desenvolvimento, homologação e produção devem ser segregados e a transferência de quaisquer ativos da informação entre estes ambientes deve seguir processo padronizado pelas áreas competentes.

Art. 13 Os sistemas devem possuir mecanismos de controle de acesso que sujeitem qualquer acesso a procedimentos padronizados de identificação, autenticação, autorização e auditoria.

Art. 14 Os sistemas devem prover a segregação de funções entre seus diversos perfis de acesso em conformidade ao princípio dos privilégios mínimos, ou seja, cada perfil de acesso deve possuir somente as permissões de acesso imprescindíveis à execução de sua função ou papel correspondente.

Art. 15 É vedado o tratamento de informações do ambiente de produção pelas equipes de desenvolvimento.

Parágrafo único. Em caráter excepcional, o tratamento de informações do ambiente de produção pelas equipes de desenvolvimento poderá ser realizado, desde que possua motivação documentada por escrito e aprovada pelo gestor da informação.

Seção III
Dos Componentes de Software do Sistema

Art. 16 Os processos de codificação dos componentes de software dos sistemas devem ser suportados por padrões de melhores práticas de codificação segura.

Art. 17 As bibliotecas e componentes de software de terceiros utilizados na construção dos sistemas devem ser gerenciados por processo de Análise de Composição de Software (SCA) que garanta a segurança de sua utilização.

Art. 18 Os componentes de software de terceiros devem integrar inventário específico que deverá ser mantido atualizado.

Art. 19 Os componentes de software de terceiros só devem ser adquiridos de fontes comprovadamente confiáveis.

Seção IV
Dos Testes de Segurança dos Sistemas

Art. 20 Os testes de segurança dos sistemas devem ser realizados com base em metodologias em conformidade com as melhores práticas, contemplando todos os controles de segurança e privacidade previstos para o sistema.

Parágrafo único. Sempre que possível, os testes devem fazer uso de ferramentas automatizadas.

Art. 21 Os componentes de software dos sistemas devem passar por testes estáticos e dinâmicos de segurança periódicos.

Parágrafo único. A periodicidade dos testes de segurança em sistemas em produção deve ser definida em função da sensibilidade do sistema considerando um possível incidente de segurança.

Seção V
Da Homologação e Produção de Sistemas

Art. 22 A homologação de sistemas deve ser realizada em ambiente segregado dos ambientes de desenvolvimento e produção, simulando condições semelhantes às de produção, bem como ser executada por seus gestores ou prepostos destes.

Art. 23 Os sistemas em produção devem possuir somente as funções formalmente aprovadas por seus gestores.

Art. 24 A passagem de sistemas para a produção fica condicionada ao efetivo atendimento dos seguintes requisitos:

I - funcionamento adequado dos controles de segurança e privacidade previstos;

II - funcionamento do sistema em conformidade com os requisitos de desempenho e capacidade previstos, sem comprometimento dos demais sistemas residentes no ambiente de produção;

III - homologação e aprovação do gestor do sistema e sempre que cabível:

a) aprovação dos procedimentos de operação do sistema pelas áreas competentes;

b) aprovação dos planos de contingência pelas áreas competentes;

c) treinamento dos usuários do sistema;

d) treinamento dos administradores e operadores do sistema.

Seção VI
Da Manutenção de Sistemas

Art. 25 A manutenção de sistemas deve seguir processo formal constando, pelo menos, das seguintes etapas: formalização da demanda, análise, aprovação, documentação, especificação, testes, homologação e passagem para produção.

Art. 26 A passagem dos componentes atualizados para a produção fica sujeita à aprovação do gestor do sistema.

Art. 27 Os sistemas, componentes ou serviços que não são mais utilizados, atingiram o fim de sua vida útil ou não são mais suportados por seus desenvolvedores devem ser substituídos ou descartados.

CAPÍTULO III
DAS COMPETÊNCIAS

Art. 28 Compete aos órgãos e entidades municipais definir e dar publicidade aos gestores titulares e substitutos de seus sistemas.

Art. 29 Compete aos gestores de sistemas:

I - definir e manter atualizadas todas as regras de negócio implementadas pelo sistema;

II - analisar as solicitações de manutenção do sistema à luz de seus objetivos e requisitos, a fim de emitir parecer conclusivo sobre sua pertinência, definir sua prioridade e prover o adequado encaminhamento;

III - homologar o sistema, assim como quaisquer manutenções realizadas;

IV - administrar os acessos dos usuários ao sistema, definir perfis de acesso, prover ou solicitar estes acessos, revisá-los periodicamente e promover, a tempo, a sua suspensão ou encerramento;

V - definir o nível de sensibilidade do sistema diante de um possível incidente de segurança;

VI - analisar e autorizar, por escrito, quaisquer acessos não ordinários às informações do ambiente de produção do sistema;

VII - passar os conhecimentos relativos ao sistema e à função de gestor aos seus sucessores.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 30 Aplicam-se ao ciclo de vida de desenvolvimento de sistemas, no que couber, as disposições da Política de Segurança da Informação e de suas normas complementares.

Art. 31 Os agentes públicos que desempenham papéis no suporte ao ciclo de vida de desenvolvimento de sistemas, desde que comprovada imperícia, imprudência ou negligência em sua atuação que tenha contribuído para incidente de segurança confirmado, ficam sujeitos às sanções administrativas cabíveis, conforme a legislação em vigor.

Art. 32 Esta Resolução entra em vigor na data de sua publicação

Art. 33 Fica revogada a Portaria "N" Nº 126, de 28 de maio de 2010, e demais disposições em contrário.

Rio de Janeiro, 22 de janeiro de 2024.

EDUARDO CAVALIERE