Protocolo: 956251
Data: 23/01/2024
Título: RESOLUÇÃO CVL Nº 222
Página(s): a

RESOLUÇÃO CVL Nº 222 DE 22 DE JANEIRO DE 2024

Regulamenta a norma para Gestão de Softwares 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 II - Da Gestão de Ativos da Informação, art. 5º 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 a gestão dos softwares que suportam os processos e serviços municipais é medida imprescindível à redução dos riscos de segurança da informação,

RESOLVE:

Art. 1º Regulamentar a norma para Gestão de Softwares no âmbito da Administração Pública Municipal.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º A presente norma estabelece as regras a serem observadas na gestão de softwares no âmbito da Administração Pública Municipal, sendo complementar à Política de Segurança da Informação - PSI.

Art. 3º Esta norma aplica-se a todos os softwares instalados nos equipamentos de TIC que integram a rede corporativa da Administração Pública Municipal.

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

I - ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos seus ativos ou prejuízos decorrentes de situações inesperadas (por exemplo: incêndio, falha de equipamentos, indisponibilidade de sistemas ou serviços, destruição de informações sensíveis, dentre outros);

II - aplicação: sistema de informação ou serviço digital desenvolvido especificamente para suporte aos processos de negócio e serviços de uma organização (por exemplo: FINCON, SINAE, Matrícula Digital, PSM, SaúdeRio, TaxiRio, etc);

III - ativo tecnológico: equipamento de TIC, software ou aplicação que suporta as atividades, processos de negócio e serviços de uma organização;

IV - confidencialidade: propriedade que garante que a informação só está disponível a indivíduos ou processos autorizados;

V - disponibilidade: propriedade que garante que a informação está disponível às pessoas e aos processos autorizados a qualquer momento em que sejam requeridas;

VI - equipamento ou equipamento de TIC: equipamento componente da infraestrutura de Tecnologia da Informação e Comunicação -TIC (por exemplo: computador, notebooks, *tablets*, *smartphones* , servidores, roteadores, *switches* etc);

VII - 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 tecnológicos de uma organização;

VIII - integridade: propriedade que garante que informação está intacta e protegida contra perda, dano ou modificação não autorizada;

IX - rede corporativa: conjunto de equipamentos de TIC interligados responsáveis pelo armazenamento, compartilhamento e processamento das informações que suportam as atividades, processos e serviços de uma organização.

X - risco: probabilidade de ameaças explorarem vulnerabilidades, comprometendo a confidencialidade, integridade ou disponibilidade da informação, causando impactos para uma organização;

XI - *software*: sistema operacional ou aplicativo de terceiros utilizado no suporte às atividades de uma organização (por exemplo: Microsoft Windows, Linux, Microsoft Office, Oracle, Microsoft SQL Server, MariaDB, Thunderbird etc);

XII - vulnerabilidade: fragilidade presente ou associada a ativos tecnológicos que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança.

Art. 5º Ficam todos os softwares instalados nos equipamentos que integram a rede corporativa da Administração Pública Municipal passíveis de monitoração e auditoria.

CAPÍTULO II
DAS REGRAS GERAIS

Seção I
Do Processo de Gestão

Art. 6º Um processo de Gestão de Softwares deve ser criado, implantado e mantido para todos os softwares instalados nos equipamentos que integram a rede corporativa da Administração Pública Municipal, atendendo aos seguintes requisitos:

I - o processo deve contemplar ações para as seguintes etapas do ciclo de vida da gestão de softwares:

a) aquisição: refere-se à etapa de aquisição de novos softwares mediante compra, doação ou quaisquer outros meios legais de aquisição ou locação de bens ou serviços;

b) registro: refere-se à etapa de inclusão do software no inventário de softwares;

c) descoberta: refere-se à identificação e registro de novos softwares por meio da busca ativa na rede corporativa;

d) utilização: refere-se à etapa onde o software é utilizado pelos seus usuários autorizados, seguindo toda a regulamentação aplicável;

e) atualização: refere-se aos procedimentos a serem executados para correção de erros, vulnerabilidades, atualização de funcionalidade ou de versão;

f) remoção: exclusão do software de todos os equipamentos de TIC;

I - os agentes públicos que desempenhem atividades no processo devem ser comprovadamente qualificados para exercer suas competências e responsabilidades;

II - a eficiência e a eficácia do processo devem ser medidas por meio de métricas e indicadores;

III - o processo deve ser revisado, no mínimo, anualmente.

Seção II
Do Ciclo de Vida da Gestão de Softwares

Subseção I
Da Aquisição

Art. 7º Na etapa de aquisição devem ser atendidos os seguintes requisitos:

I - os softwares a serem adquiridos ou locados devem ser especificados com base em requisitos definidos pelas áreas competentes;

II - as especificações de software e seus perfis de configuração devem garantir a eficiência e eficácia de sua utilização considerando todos os requisitos funcionais, de desempenho e de segurança definidos.

Subseção II
Do Registro

Art. 8º Na etapa de registro devem ser atendidos os seguintes requisitos:

I - todos os softwares corporativos devem ser registrados no inventário;

II - no inventário devem constar, pelo menos, as seguintes informações:

a) identificador do software;
b) nome do software;
c) fabricante do software;
d) data de aquisição ou locação;
e) data de instalação;
f) versão do software;
g) órgão ou entidade proprietário(a);
h) data de fim do suporte (EoS), quando conhecida;
i) data de fim de vida (EoL), quando conhecida;
j) informações de licenciamento, por exemplo, prazo de validade.

Subseção III
Da Descoberta

Art. 9º Na etapa de descoberta devem ser atendidos os seguintes requisitos:

I - os procedimentos de busca e detecção dos softwares instalados na rede corporativa devem ser realizados periodicamente, com periodicidade definida em função da criticidade e do nível de risco potencial das redes ou sub-redes a serem analisadas;

II - os softwares não licenciados devem ser desinstalados imediatamente.

Subseção IV
Da Utilização

Art. 10 Na etapa de utilização de softwares devem ser atendidos os seguintes requisitos:

I - os softwares devem ser instalados e configurados somente pelas áreas competentes;

II - os softwares devem ser utilizados somente por usuários devidamente autorizados e exclusivamente para seus fins previstos;

III - a continuidade da utilização de softwares que estejam sem suporte (EoS), descontinuados (EoL) ou desatualizados somente será permitida em caráter temporário, desde que:

a) justificada por resultados baseados em análise de riscos que comprovem que os impactos resultantes de sua remoção ou substituição imediata seriam impeditivos;

b) com ciência e aprovação dos agentes competentes;

c) acompanhada de plano de ações de atualização ou substituição;

d) acompanhada de plano de ações visando à implantação de controles de segurança adicionais nos equipamentos ou ambientes que hospedam o software, visando à redução dos riscos assumidos.

Subseção V
Da Atualização

Art. 11 Na etapa de atualização devem ser atendidos os seguintes requisitos:

I - os softwares devem ser mantidos em versões que ainda estejam cobertas pelos serviços de suporte e atualização de seus fabricantes e preferencialmente em sua última versão;

II - sempre que possível, a atualização automatizada de softwares deve implantada, desde que realizada com nível de risco gerenciável;

III - os softwares devem ser mantidos atualizados com relação às medidas de tratamento de suas vulnerabilidades, assim como com relação aos seus perfis definidos de configuração segura.

Subseção VI
Da Remoção

Art. 12 Na etapa de remoção devem ser atendidos os seguintes requisitos:

I - a remoção deve ser precedida de processo de análise de riscos;

II - a remoção só poderá ser realizada após autorização formal das áreas competentes.

CAPÍTULO III
DAS COMPETÊNCIAS

Art. 13 Compete à IplanRio:

I - definir solução corporativa de gestão de inventário de softwares;

II - prestar suporte aos órgãos e entidades na implantação e utilização da solução corporativa de gestão de inventário de softwares.

Art. 14 Compete aos órgãos e entidades municipais:

I - implantar processo de remoção de softwares descontinuados em seus equipamentos;

II - implementar a solução corporativa de gestão de inventário de softwares em seus equipamentos;

III - em seu âmbito de atuação, adotar todas as medidas de suporte à efetiva implementação das determinações descritas nesta norma.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 15 Aplicam-se à gestão de softwares, no que couber, as disposições da Política de Segurança da Informação e de suas normas complementares.

Art. 16 Os agentes públicos que desempenhem papéis no suporte ao processo de gestão de softwares, uma vez comprovada imperícia, imprudência ou negligência em sua atuação, que tenha contribuído para incidente de segurança confirmado, ficam sujeitos a sanções administrativas cabíveis, conforme a legislação em vigor.

Art. 17 Esta Resolução entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Rio de Janeiro, 22 de janeiro de 2024.

EDUARDO CAVALIERE