Protocolo: 956253
Data: 23/01/2024
Título: RESOLUÇÃO CVL Nº 224
Página(s): a

# RESOLUÇÃO CVL Nº 224 DE 22 DE JANEIRO DE 2024

Regulamenta a norma para Gestão de Vulnerabilidades Técnicas 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 deliberar, analisar e revisar normas complementares à PSI;

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 em seu § 1º da Resolução CVL Nº 216 de 15 de dezembro de 2023, que estipula que todos os ativos da informação devem estar sujeitos a processo formal, estruturado, dinâmico e periódico de gestão de inventário e de vulnerabilidades;

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 das vulnerabilidades técnicas presentes nos ativos tecnológicos que suportam os processos e serviços digitais da PCRJ é medida imprescindível à redução dos riscos a confidencialidade, integridade e disponibilidade das informações tratadas nestes processos e serviços,

**RESOLVE:**

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

## CAPÍTULO I
## DAS DISPOSIÇÕES PRELIMINARES

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

**Art. 3.º** Esta norma aplica-se a todos os ativos tecnológicos que integram a rede corporativa da Administração Pública Municipal.

**Art. 4.º** 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 - ciclo de vida da informação: refere-se às fases de tratamento da informação: coleta, retenção, processamento, compartilhamento e descarte;

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

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

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

VIII - gestão de vulnerabilidade: processo cíclico e contínuo de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades;

IX - 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;

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

XI - remediação: ato de corrigir uma vulnerabilidade ou de implementar controles que reduzam a probabilidade de sua exploração;

XII - 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;

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

*XIV - 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);

XV - tratamento de informações: toda operação realizada com as informações durante seu ciclo de vida, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle, modificação, comunicação, transferência, difusão ou extração;

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

**Art. 5.º** Ficam todos os ativos tecnológicos 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 de Vulnerabilidades*

**Art. 6.º** Um processo de Gestão de Vulnerabilidades deve ser criado, implantado e mantido para todos os ativos tecnológicos 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 vulnerabilidades:

a) mapeamento dos ativos tecnológicos: refere-se à etapa de identificação de todos os ativos tecnológicos que suportam as atividades, processos e serviços de uma organização;

b) detecção de vulnerabilidades: refere-se à etapa de identificação das vulnerabilidades presentes nos ativos tecnológicos;

c) priorização e remediação de vulnerabilidades: refere-se à etapa de priorização das vulnerabilidades que devem ser tratadas e sua efetiva remediação;

d) monitoramento de vulnerabilidades: refere-se à etapa de monitoramento contínuo de novas vulnerabilidades e da eficácia das medidas de remediação.

II - o processo deve dispor de mecanismos que garantam a obtenção de informações oportunas sobre vulnerabilidades, promovam a avaliação da exposição dos ativos tecnológicos a tais vulnerabilidades e orientem a implementação das medidas apropriadas de remediação;

III - o processo deve estabelecer mecanismos que garantam a obtenção das atualizações de segurança dos ativos tecnológicos regularmente, utilizando fontes confiáveis, tais como sites de fabricantes ou bancos de dados de suporte à remediação de vulnerabilidades suportados por organizações de notória especialização;

IV - o processo deve contemplar a gestão de vulnerabilidades de todos os tipos de ativos tecnológicos que suportam as atividades, processos e serviços da Administração Pública Municipal;

V - os agentes públicos que desempenhem atividades no processo devem estar capacitados para exercer suas competências e responsabilidades;

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

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

## *Seção II*
## *Do Ciclo de Vida de Gestão de Vulnerabilidades*

### *Subseção I*
### *Do Mapeamento dos Ativos Tecnológicos*

**Art. 7.º** Um mapeamento de ativos tecnológicos deve constar no escopo do processo de gestão de vulnerabilidades, atendendo aos seguintes requisitos:

I - deve identificar todos os ativos tecnológicos, indicando seu grau de criticidade e o respectivo responsável por sua gestão;

II - deve ser executado periodicamente, com periodicidade definida em função da criticidade e do nível de risco das redes ou sub-redes a serem analisadas.

### *Subseção II*
### *Da Detecção de Vulnerabilidades*

**Art. 8.º** Varreduras periódicas automatizadas para identificação de vulnerabilidades devem ser realizadas na rede corporativa, atendendo aos seguintes requisitos:

I - a periodicidade das varreduras deve ser definida em função da criticidade e do nível de risco das redes ou sub-redes a serem analisadas;

II - o resultado do processo de detecção de vulnerabilidades deve ser avaliado antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos;

III - o processo de detecção de vulnerabilidades deve ser suportado por bases de dados de vulnerabilidades coletadas de fontes confiáveis, tais como sites de fabricantes ou bancos de dados de vulnerabilidades suportados por organizações de notória especialização;

IV - as bases de dados de vulnerabilidades devem conter informações relativas à descrição detalhada das vulnerabilidades, à priorização de tratamento com base em seus níveis de criticidade e às respectivas medidas de remediação;

V - as bases de dados de vulnerabilidades devem ser atualizadas regularmente com suas informações mais recentes, garantindo-se que novas vulnerabilidades sejam adicionadas tão logo tenham sido descobertas.

### *Subseção III*
### *Da Priorização e Remediação de Vulnerabilidades*

**Art. 9.º** Um processo para priorização e remediação de vulnerabilidades deve ser implantado atendendo aos seguintes requisitos:

I - a remediação de vulnerabilidades deve ser priorizada com base em sua classificação de risco e tempo previsto de implementação;

II - as vulnerabilidades que não puderem ser corrigidas devem ser documentadas por meio de processo de exceção, para tratamento pela equipe técnica responsável pela administração do ativo, visando à mitigação de seus riscos vinculados;

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

### *Subseção IV*
### *Do Monitoramento de Vulnerabilidades*

**Art. 10.** Um processo de monitoramento contínuo de informações divulgadas sobre novas vulnerabilidades e suas respectivas medidas de remediação deve ser implantado. Devem ser fontes de consulta preferenciais:

I - vulnerabilidades divulgadas pelos fabricantes dos ativos tecnológicos;

II - vulnerabilidades divulgadas por fabricantes de soluções de Segurança da Informação;

III - vulnerabilidades divulgadas por órgãos governamentais, nacionais ou internacionais, e organizações de notória especialização em Segurança da Informação;

IV - boletins de Grupos de Resposta a Incidentes;

V - fóruns e sites especializados em Segurança da Informação.

### *Seção III*
### *Da Configuração Segura de Ativos Tecnológicos*

**Art. 11.** Um processo de gestão de configuração segura deve ser implantado para todos os ativos tecnológicos.

*Parágrafo único*. O processo deve estabelecer os procedimentos para identificar, aplicar e manter os perfis de configuração segura dos ativos tecnológicos durante toda a sua vida útil.

**Art. 12.** Os perfis de configuração segura definidos devem basear-se em recomendações de segurança dos fabricantes dos ativos e em padrões de mercado definidos por organizações de notória especialização em Segurança da Informação.

**Art. 13.** Sempre que possível, os ativos tecnológicos devem ser submetidos a procedimentos de implementação de configuração segura antes de sua entrada em operação.

**Art. 14.** Os ativos tecnológicos devem ser revisados periodicamente quanto à sua conformidade em relação aos perfis de configuração segura estabelecidos, com periodicidade definida em função de sua criticidade e do nível de risco a que estiverem expostos.

## CAPÍTULO III
## DAS COMPETÊNCIAS

**Art. 15.** Compete à IplanRio:

I - definir solução corporativa de gestão de vulnerabilidades;

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

**Art. 16.** Compete aos órgãos e entidades municipais:

I - implantar processo de gestão de vulnerabilidades de seus ativos tecnológicos em conformidade às determinações descritas nesta norma;

II - implementar a solução corporativa de gestão de vulnerabilidades no escopo de seus ativos tecnológicos.

## CAPÍTULO IV
## DAS DISPOSIÇÕES FINAIS

**Art. 17.** Aplicam-se à gestão de vulnerabilidades, no que couber, as disposições da Política de Segurança da Informação e de suas normas complementares.

**Art. 18.** Os agentes públicos que desempenhem papéis no suporte ao processo de gestão de vulnerabilidades, uma vez 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. 19.** 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**