Protocolo: 956252
Data: 23/01/2024
Título: RESOLUÇÃO CVL Nº 223
Página(s): a

RESOLUÇÃO CVL Nº 223 DE 22 DE JANEIRO DE 2024

Regulamenta a norma para Gestão de Equipamentos de TIC 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 equipamentos de TIC 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 Equipamentos de TIC 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 equipamentos de TIC no âmbito da Administração Pública Municipal, sendo complementar à Política de Segurança da Informação - PSI.

Art. 3º Esta norma aplica-se a todos os 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 equipamentos 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 equipamentos de TIC que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança.

Art. 5º Ficam todos os equipamentos de TIC 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 Equipamentos de TIC deve ser criado, implantado e mantido 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 equipamentos de TIC:

a) aquisição: refere-se à etapa de aquisição de novos equipamentos 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 equipamento no inventário de equipamentos de TIC;

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

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

e) descarte: refere-se aos procedimentos a serem executados ao término da vida útil do equipamento ou diante de incidentes como perda ou furto.

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

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

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

Seção II
Do Ciclo de Vida de Gestão de Equipamentos de TIC

Subseção I
Da Aquisição

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

I - os equipamentos a serem adquiridos ou locados devem ser especificados com base nos perfis de configuração definidos pelas áreas competentes;

II - as especificações devem garantir a execução eficaz de todos os softwares e aplicações que serão instalados nos equipamentos.

Subseção II
Do Registro

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

I - todos os equipamentos que integram a rede corporativa devem ser registrados no inventário;

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

a) identificador do equipamento;

b) fabricante do equipamento;

c) descrição do equipamento;

d) número do modelo e número de série, quando aplicáveis;

e) pessoa jurídica, órgão ou entidade proprietário(a);

f) localização física do equipamento, quando aplicável.

Subseção III
Da Descoberta

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

I - os procedimentos de busca e detecção de equipamentos conectados à 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 equipamentos detectados e ainda ausentes do inventário devem ser identificados visando a tratamento específico pelas áreas competentes.

Subseção IV
Da Utilização

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

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

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

III - o usuário deve notificar à área de gestão patrimonial e, sempre que cabível, à área de gestão de TIC, quaisquer incidentes ocorridos com os equipamentos sob sua custódia.

Subseção V
Do Descarte

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

I - os equipamentos a serem desativados ou retirados da rede corporativa devem passar pelos seguintes procedimentos:

a) realização de backup, sempre que cabível, considerando a relevância e sensibilidade de suas informações;

b) exclusão de informações, valendo-se de soluções tecnológicas de exclusão segura, com nível de confiabilidade compatível com a sensibilidade dessas informações;

c) atualização do status do equipamento em todos os sistemas ou serviços em que este seja referenciado.

II - a baixa do equipamento deve ser registrada no inventário;

III - no caso de roubo ou furto do equipamento, devem ser realizados os seguintes procedimentos:

a) comunicação às áreas de gestão patrimonial e de TIC;

b) cancelamento de sua capacidade de acesso à rede corporativa;

c) baixa do equipamento no inventário.

CAPÍTULO III
DAS COMPETÊNCIAS

Art. 12. Compete à IplanRio:

I - definir solução tecnológica corporativa de gestão de inventário de equipamentos;

II - prestar suporte aos órgãos e entidades na implementação e utilização da solução corporativa de gestão de inventário de equipamentos;

III - definir critérios e padrões de obsolescência de equipamentos.

Art. 13. Compete aos órgãos e entidades municipais:

I - implantar processo de gestão de obsolescência de seus equipamentos garantindo que estes mantenham-se em conformidade com perfis de configuração que garantam sua eficácia, considerando requisitos funcionais, de desempenho e de segurança;

II - implementar solução corporativa de gestão de inventário 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. 14. Aplicam-se à gestão de equipamentos de TIC, no que couber, as disposições da Política de Segurança da Informação e de suas normas complementares.

Art. 15. Os agentes públicos que desempenham papéis no suporte ao processo de gestão de equipamentos de TIC, 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. 16. 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