Protocolo: 956248
Data: 23/01/2024
Título: RESOLUÇÃO CVL Nº 219
Página(s): a

RESOLUÇÃO CVL Nº 219 DE 22 DE JANEIRO DE 2024

Regulamenta a norma de Segurança 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 art. 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, e na Seção IX - Da rede corporativa, art. 12, ambas Seções 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 segurança 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 de Segurança 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 quanto à segurança dos 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 - acesso: capacidade de usar um equipamento de TIC (por exemplo: ler, criar, modificar ou excluir um arquivo; executar um programa; se conectar a um dispositivo, a uma rede, a um sistema ou a um serviço);

III - 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);

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

V - auditoria: processo de registro contínuo de informações que identifique a autoria, assim como as ações realizadas sobre um objeto (por exemplo: alterações ou exclusões de registros de arquivos, de tabelas de um banco de dados, de campos de uma tabela etc.);

VI - autenticação: processo de reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica. Há diversos métodos de autenticação utilizando mecanismos como senhas, impressão digital, certificado digital, reconhecimento da íris, dentre outros;

VII - autorização: concessão ao usuário, após sua autenticação, de um conjunto de permissões de acesso a ativos tecnológicos;

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

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

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

XI - 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;

XII - informação: resultado do processamento, manipulação e organização de dados de tal forma que represente um acréscimo ao conhecimento da pessoa que a recebe, podendo se apresentar de diversas formas, como texto, imagem, áudio etc.;

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

XIV - 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;

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

XVI - *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);

XVII - usuário: qualquer pessoa autorizada a usar um ativo tecnológico; e

XVIII - 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 equipamentos de TIC que integram a rede corporativa da Administração Pública Municipal passíveis de monitoração e auditoria.

CAPÍTULO II
DOS REQUISITOS DE SEGURANÇA DOS EQUIPAMENTOS DE TIC

Seção I
Da Proteção Física

Art.6º Dos requisitos de proteção física:

I - os equipamentos devem residir em locais seguros e ser protegidos por controles que minimizem os riscos relacionados às ameaças do meio ambiente, bem como aos acessos não autorizados;

II - os equipamentos que precisem ser instalados em ambientes com condições ambientais severas como calor, poeira ou presença de insetos devem ser especificados levando-se em conta estas características ambientais;

III - os equipamentos servidores que suportem sistemas ou serviços vitais à continuidade das atividades dos órgãos e entidades devem ser hospedados em áreas restritas e protegidas, pelo menos, por:

a) controles de acesso físico, com registro de entrada e saída para todas as pessoas que acessem à área;

b) procedimentos formais e especializados de limpeza em áreas restritas, de forma a evitar paralisação ou danos físicos aos equipamentos;

c) controles para minimizar os riscos vinculados às ameaças como fogo, furto, poeira, fumaça entre outros;

d) controles de proteção contra falta de energia e outras interrupções causadas por falhas de infraestrutura;

e) procedimentos de manutenção periódica dos sistemas de ar condicionado e de combate a incêndio, com periodicidade definida atendendo as recomendações de seus respectivos fabricantes e em conformidade às regulamentações específicas;
f) monitoramento dos aspectos ambientais como temperatura e umidade visando prevenir condições que possam afetar negativamente os equipamentos;

g)controles que garantam que a infraestrutura de alimentação elétrica utilizada pelos equipamentos mantenha-se em conformidade com as normas técnicas vigentes;

h) controles que garantam que a infraestrutura física de cabeamento de dados utilizada pelos equipamentos mantenha-se em conformidade com as normas técnicas vigentes.

Seção II
Da Instalação e Manutenção

Art.7º Dos requisitos de instalação e manutenção:

I - os equipamentos devem ser instalados de acordo com as especificações técnicas de seus fabricantes;

II - a instalação e manutenção dos equipamentos devem ser realizadas somente por pessoal especializado e autorizado;

III - deve ser mantido histórico das falhas e das operações de manutenção dos equipamentos, que deve ser armazenado em repositório específico e apartado dos equipamentos;

IV - devem ser implementados procedimentos que garantam que equipamentos que hospedem informações sensíveis tenham suas informações salvas e posteriormente eliminadas antes de serem enviados para manutenção;

V - todo equipamento que tiver que ser deslocado para fins de manutenção deve estar devidamente identificado e protegido contra danos físicos.

Seção III
Da Administração

Art.8º Dos requisitos de administração:

I - os equipamentos devem estar sujeitos a processo formal de administração com relação, pelo menos, aos seguintes aspectos: configuração, falhas, desempenho e segurança;

II - para qualquer equipamento integrante da rede corporativa deve haver pelo menos 2 (dois) administradores capacitados;

III - as soluções corporativas de segurança cibernética instaladas nos equipamentos devem ser mantidas ativas e atualizadas.

Seção IV
Das Contas com Privilégios Administrativos

Art.9º Dos requisitos de uso controlado de contas com privilégios administrativos:

I - as contas com privilégios administrativos devem ser gerenciadas durante todo seu ciclo de vida, de sua criação à sua desativação ou exclusão;

II - as contas de administração dos equipamentos de TIC devem ficar sob a guarda e responsabilidade da área de gestão de TIC;

III - antes do início de operação de qualquer novo equipamento de TIC, todas as contas de administração devem ter suas senhas padrão alteradas;

IV - as contas de administração devem ser utilizadas somente para realização de atividades que requeiram privilégios administrativos;

V - sempre que possível, deve-se utilizar autenticação multifator para suporte ao processo de autenticação das contas com privilégios administrativos;

VI - as atividades que requeiram privilégios administrativos devem ser realizadas somente por agentes competentes;

VII - o acesso aos equipamentos realizados a partir de contas com privilégios administrativos deve ocorrer através de canais de comunicação seguros.

Seção V
Da Reutilização, Descarte e Alienação

Art. 10. Dos requisitos de reutilização, descarte e alienação:

I - os equipamentos devem ser examinados antes da reutilização, descarte ou alienação, para assegurar que todas as informações, softwares e aplicações hospedados no equipamento tenham sido removidos;

II - os equipamentos que contenham informações sensíveis devem ter suas informações destruídas por meio de técnicas que as tornem irrecuperáveis.

Seção VI
Da Movimentação

Art. 11. Dos requisitos de movimentação:

I - todas as movimentações de equipamentos devem acontecer mediante autorização prévia dos setores competentes;

II - todas as movimentações devem ser controladas e ter sua retirada e devolução registradas junto aos setores competentes.

CAPÍTULO III
DAS COMPETÊNCIAS

Art. 12. Compete à IplanRio:

I - definir as soluções de segurança cibernética corporativas a serem instaladas nos equipamentos;

II - prestar suporte aos órgãos e entidades na implementação e utilização das soluções de segurança cibernética corporativas.

Art. 13. Compete aos órgãos e entidades municipais:

I - implementar as soluções de segurança cibernética corporativas em seus equipamentos;

II - garantir que as soluções de segurança cibernética corporativas sejam mantidas ativas e atualizadas em todos os 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 segurança 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 segurança dos equipamentos de TIC, 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. 16. Esta Resolução entra em vigor na data de sua publicação.

Art. 17. Fica revogada a Portaria "N" Nº 127, de 28 de maio de 2010, e demais disposições em contrário.

Rio de Janeiro, 22 de janeiro de 2024.

EDUARDO CAVALIERE