Protocolo: 956247
Data: 23/01/2024
Título: RESOLUÇÃO CVL Nº 218
Página(s): a

RESOLUÇÃO CVL Nº 218 DE 22 DE JANEIRO DE 2024

Regulamenta a norma de Conscientização em Segurança da Informação no âmbito 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 a crescente transformação digital da Administração Pública, em que processos e serviços encontram-se cada vez mais apoiados por ativos tecnológicos;

CONSIDERANDO o disposto na Seção XIII - Da Capacitação, art. 16 da Resolução CVL Nº 216 de 15 de dezembro de 2023, que trata das diretrizes ao tema no âmbito do Poder Executivo Municipal;

CONSIDERANDO que a segurança das informações tratadas por estes ativos tecnológicos é requisito vital à manutenção da confiabilidade destes processos e serviços junto ao cidadão;

CONSIDERANDO que a conscientização dos usuários destes ativos tecnológicos em Segurança da Informação é medida imprescindível à redução dos riscos relacionados ao tratamento dessas informações,

RESOLVE:

Art. 1º Regulamentar a Norma de Conscientização em Segurança da Informação no âmbito da Administração Pública Municipal.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

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

Art. 3º Esta norma aplica-se a todos os órgãos e entidades municipais.

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 - conscientização em segurança da informação: refere-se a um conjunto de ações concebidas para mudar comportamentos e reforçar boas práticas de segurança da informação;

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

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

X - 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);

XI - 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;

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

CAPÍTULO II
DAS REGRAS GERAIS

Seção I
Do Programa de Conscientização em Segurança da Informação

Art. 5º Um programa de conscientização em Segurança da Informação deve ser criado, implementado e mantido em todos os órgãos e entidades municipais, atendendo aos seguintes requisitos:

I - contemplar ações para as seguintes etapas do ciclo de vida da conscientização em Segurança da Informação:

a) planejamento: refere-se à etapa de identificação de necessidades e prioridades, temas a serem abordados, assim como seus respectivos materiais de suporte e recursos de custeio do programa;

b) desenvolvimento: refere-se à etapa de elaboração ou aquisição dos materiais a serem utilizados nas ações de conscientização;

c) implementação: refere-se à etapa de comunicação do planejamento, entrega dos materiais, realização e avaliação das ações de conscientização.

I - as pessoas físicas ou jurídicas que desempenham atividades no programa devem possuir capacitação comprovada para o cumprimento de seus respectivos papéis e responsabilidades;

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

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

Seção II
Do Ciclo de Vida do Programa

Subseção I
Do Planejamento

Art. 6º A etapa de planejamento deve atender aos seguintes requisitos:

I - um processo de avaliação deve ser implantado para identificação das necessidades de conscientização em segurança da informação do órgão ou entidade;

II - o planejamento das ações de conscientização deve contemplar, pelo menos, os seguintes itens:

a) escopo do programa;

b) papéis e responsabilidades das equipes que devem projetar, desenvolver, implementar e manter o material de conscientização;

c) metas a serem cumpridas e sua ordem de prioridade;

d) recursos orçamentários necessários;

e) objetivos de aprendizagem;

f) temas a serem abordados;

g) métodos de implementação;

h) definição da documentação de suporte ao feedback e evidências de aprendizagem.

Subseção II
Do Desenvolvimento

Art. 7º O material a ser utilizado no programa de conscientização em segurança da informação contemplar, pelo menos, os seguintes temas:

I - embasamento conceitual, contendo:

a) princípios de segurança da informação;

b) classificação da informação;

c) conceito de ciclo de vida da informação;

d) conceito de ativos da informação;

e) conceitos de ameaça, vulnerabilidade, impacto e risco;

f) tipos de ameaças e vulnerabilidades;

g) conceito de incidentes de segurança;

h) medidas de proteção da informação;

i) política de segurança da informação;

j) controle de acesso;

k) noções básicas de criptografia e certificação digital.

II - melhores práticas, contendo:

a) segurança da estação de trabalho;

b) segurança em dispositivos móveis;

c) proteção contra códigos maliciosos;

d) segurança de senhas;

e) cópias de segurança (backup);

f) atualização de softwares;

g) soluções de proteção;

h) Identificação e relato de incidentes de segurança;

i) golpes na internet e fraudes eletrônicas;

j) uso seguro da internet;

k) segurança e privacidade de informações em redes sociais.

Subseção III
Da Implementação

Art. 8º A implementação das ações de conscientização em segurança da informação deve atender aos seguintes requisitos:

I - ser amplamente divulgadas no âmbito do órgão ou entidade;

II - ser medidas por meio de métricas e indicadores de eficiência e eficácia.

CAPÍTULO III
DAS DISPOSIÇÕES FINAIS

Art. 9º Aplicam-se ao programa de conscientização em segurança da informação, no que couber, as disposições da Política de Segurança da Informação - PSI e suas normas complementares.

Art. 10 Esta Resolução entra em vigor na data de sua publicação.

Rio de Janeiro, 22 de janeiro de 2024.

EDUARDO CAVALIERE