Protocolo: 947765
Data: 18/12/2023
Título: RESOLUÇÃO CVL Nº 216
Página(s): a

RESOLUÇÃO CVL Nº 216 DE 15 DE DEZEMBRO DE 2023

Regulamenta as diretrizes da Política de Segurança da Informação - PSI no âmbito do Poder Executivo 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 ser imprescindível a definição de diretrizes estratégicas que visem dar suporte às ações de gerenciamento dos riscos à segurança das informações tratadas pela Administração Pública Municipal,

RESOLVE:

Art. 1º Regulamentar as Diretrizes da Política de Segurança da Informação - PSI no âmbito da Administração Pública Municipal.

CAPÍTULO I
DOS TERMOS E DEFINIÇÕES

Art. 2º Para fins desta Resolução, considera-se:

I - acesso: capacidade de usar um ativo da informação (por exemplo: ler, criar, modificar ou excluir um arquivo; executar um programa; se conectar a um dispositivo, a uma rede, a um sistema, a um serviço ou entrar em áreas de acesso restrito que hospedam informações sensíveis);

II - 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);

III - ativo da informação: informação, processo ou ativo físico, tecnológico ou humano que suporta as operações de coleta, armazenamento, processamento, compartilhamento ou descarte de informações;

IV - 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);

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

VI - autenticação: processo de reconhecimento formal da identidade dos elementos que entram em

comunicação ou fazem parte de uma transação eletrônica;

VII - autenticidade: garantia de que os ativos da informação identificados em um processo de comunicação como remetentes ou destinatários sejam realmente quem dizem ser, ou seja, diz respeito à veracidade das identidades dos ativos envolvidos em um processo de comunicação;

VIII - autorização: concessão ao usuário, após sua autenticação, de um conjunto de permissões de acesso a um ativo da informação;

IX - classificação da informação: refere-se ao grau de sensibilidade de uma informação diante de uma possível quebra de segurança, ou seja, do comprometimento dos princípios básicos de Segurança da Informação: confidencialidade, integridade e disponibilidade;

X - computação em nuvem: modelo computacional que permite acesso por demanda, independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação como redes de computadores, servidores, recursos de armazenamento, sistemas e serviços, provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

XI - conscientização em segurança da informação: processo de iniciação educacional que visa possibilitar, a cada indivíduo, incorporar à rotina pessoal e profissional as melhores práticas de Segurança da Informação;

XII - confidencialidade: propriedade que garante que a informação só esteja disponível a indivíduos ou processos autorizados;

XIII - continuidade de negócios: capacidade estratégica e tática dos órgãos ou entidades do Município de se planejar e responder a incidentes que gerem interrupções em suas atividades ou serviços, visando minimizar impactos e manter suas operações em um nível aceitável de disponibilidade previamente definido;

XIV - controle de acesso: conjunto de controles que visam proteger as informações residentes em ativos da informação contra acessos não autorizados;

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

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

XVII - gestor da informação: agente responsável pelo gerenciamento do ciclo de vida da informação, no âmbito do órgão ou entidade do Município;

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

XIX - mensagem de cunho institucional: mensagem que contém informações que suportem a atuação dos agentes públicos durante a execução de suas competências e de suas responsabilidades;

XX - plano de gerenciamento de incidentes: plano de ação claramente definido e documentado para ser usado quando ocorrer um incidente;

XXI - rede corporativa: conjunto de recursos de TIC interligados onde circulam as informações corporativas da PCRJ;

XXII - risco: probabilidade de ameaças explorarem vulnerabilidades, comprometendo a confidencialidade, integridade ou disponibilidade da informação, causando impactos para as atividades da Administração Pública Municipal;

XXIII - segurança física: processo que trata da proteção de todos os ativos da informação contra

ameaças naturais (por exemplo: incêndios) e humanas (por exemplo: acessos não autorizados);

XXIV - sensibilização em segurança da informação: ações que visam identificar, recomendar, criar e implantar programas de conscientização, a fim de proporcionar melhorias e mudanças na atitude e na educação organizacional quanto à importância da Segurança da Informação;

XXV - sistema de informação: sistema composto por um conjunto de ativos da informação que tem por objetivo armazenar, transportar e processar informações visando suportar funções, serviços ou processos da Administração Pública Municipal;

XXVI - 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);

XXVII - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

XXVIII - treinamento em segurança da informação: conjunto de ações voltadas para o desenvolvimento de competências e habilidades específicas em Segurança da Informação necessárias ao desempenho das atribuições funcionais dos agentes públicos na Administração Pública Municipal;

XXIX - usuário: qualquer pessoa autorizada a ler, inserir ou atualizar informações em um sistema de informação;

XXX - vulnerabilidade: fragilidade presente ou associada a ativos da informação que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança comprometendo um ou mais princípios de segurança da informação (confidencialidade, integridade e disponibilidade).

CAPÍTULO II
DAS DIRETRIZES

Seção I
Do Tratamento das Informações

Art. 3º As informações são ativos vitais para a eficiência e a eficácia dos órgãos e entidades municipais, devendo ser tomadas todas as medidas necessárias para protegê-las de alteração, destruição ou divulgação não autorizada.

§ 1º As informações devem ser classificadas quanto aos seus requisitos de confidencialidade, integridade e disponibilidade de forma a serem adequadamente tratadas durante todo seu ciclo de vida: da coleta ou criação até o descarte.

§ 2º Agentes públicos e prestadores de serviço devem garantir que o tratamento das informações a que tiverem acesso em função de suas competências funcionais seja realizado de acordo com sua classificação e em conformidade com todas as políticas e normas de segurança e privacidade vigentes.

§ 3º Os controles de segurança da informação devem ser proporcionais à sua classificação e ao nível de risco ao qual esteja exposta.

Art. 4º Qualquer tratamento de informação que, por motivo de força maior, exceda as atribuições de seus agentes executores, necessitará de prévia autorização formal do gestor da informação.

Seção II
Da Gestão de Ativos da informação

Art. 5º Os ativos da informação da Administração Pública Municipal são disponibilizados

exclusivamente para uso corporativo.

§ 1º Todos os ativos da informação devem estar sujeitos a processo formal, estruturado, dinâmico e periódico de gestão de inventário e de vulnerabilidades.

§ 2º Os ativos da informação devem ter um gestor formalmente designado.

§ 3º No inventário deve constar a classificação de criticidade e relevância de todos os ativos da informação no que diz respeito ao suporte aos processos e serviços da Administração Pública Municipal.

§ 4º A disponibilização de ativos da informação somente deve ser permitida desde que atendidas as determinações desta Resolução e das demais que complementem a Política de Segurança da Informação.

§ 5º Em casos de alienação ou descarte, devem ser seguidos procedimentos adequados à classificação das informações residentes no ativo da informação, para que não haja risco de vazamento ou perda de informações sensíveis.

Seção III
Da gestão de riscos

Art. 6º Devem ser estabelecidos processos que possibilitem a identificação, quantificação, priorização, tratamento, comunicação e a monitoração periódica dos riscos à informação.

Parágrafo único. Os processos devem ter por objetivo reduzir as vulnerabilidades, evitar as ameaças, minimizar a exposição aos riscos e atenuar os impactos aos ativos da informação dos órgãos e entidades municipais.

Seção IV
Do controle de acesso

Art. 7º O controle de acesso aos ativos da informação deve ser regido por um processo formal que gerencie a criação, manutenção, suspensão e cancelamento de acessos.

§ 1º O acesso aos ativos da informação deve ocorrer através da utilização de mecanismo de identificação de uso pessoal e intransferível, qualificando seu usuário como responsável por quaisquer ações realizadas por meio deste.

§ 2º A autorização de acessos aos ativos da informação deve se restringir aos privilégios mínimos necessários para que os usuários desenvolvam suas competências funcionais.

§ 3º A duração do acesso aos ativos da informação deve ter prazo limitado à execução de sua finalidade.

Seção V
Da Gestão de Incidentes

Art. 8º A gestão de incidentes de segurança da informação deve ser realizada por meio de processo formal, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.

§ 1º Os incidentes de Segurança da Informação devem ser identificados, monitorados, comunicados e devidamente tratados, nos termos de um Plano de Gerenciamento de Incidentes.

§ 2º O Plano de Gerenciamento de Incidentes deve ser documentado, revisado e testado periodicamente, tendo dentre seus objetivos o restabelecimento dos sistemas de informação e serviços digitais do órgão ou entidade à situação de normalidade nos prazos previstos.

§ 3º O plano deve cobrir todos os ativos da informação necessários à efetiva implementação do

processo de gerenciamento de incidentes.

Seção VI
Da gestão de continuidade

Art. 9º Os ativos da informação considerados críticos à atividade-fim dos órgãos e entidades municipais devem estar resguardados por um Programa de Gestão de Continuidade de Negócios que garanta a continuidade dos serviços, previna e solucione situações de anormalidade.

Parágrafo único. Os planos que integram o Programa de Gestão de Continuidade de Negócios devem ser documentados, periodicamente testados e revisados.

Seção VII
Da guarda e recuperação de informações

Art. 10. Os sistemas de informação da Administração Pública Municipal devem estar cobertos por processo formal e estruturado de guarda e recuperação de informações que garanta sua disponibilidade e integridade.

§ 1º A integridade dos ativos da informação de suporte às estratégias de guarda e recuperação deve ser testada periodicamente.

§ 2º As estratégias de guarda e recuperação devem garantir que as informações tenham níveis de disponibilidade, capacidade e celeridade de recuperação compatíveis com sua criticidade e relevância.

Seção VIII
Da Segurança Física

Art. 11. As instalações físicas e áreas de processamento de informações sensíveis devem ser protegidas contra ameaças naturais e humanas.

§ 1º As proteções devem ser proporcionais aos riscos identificados.

§ 2º Os ativos da informação considerados críticos ao desempenho das atividades dos órgãos e entidades municipais devem ser armazenados em áreas com acesso restrito, controlado por dispositivos de controle de acesso preferencialmente biométricos.

§ 3º O acesso de visitantes às áreas que hospedam ativos da informação críticos deve ser autorizado por agente competente e acompanhado de representante deste.

Seção IX
Da rede corporativa

Art. 12. Devem ser implementados processos que possibilitem a identificação, quantificação, priorização, tratamento, comunicação e a monitoração periódica dos riscos à segurança da rede corporativa.

Parágrafo único. Os processos devem ter por objetivo reduzir as vulnerabilidades, evitar as ameaças, minimizar a exposição aos riscos e atenuar os impactos associados aos ativos da informação que suportam a rede corporativa de computadores.

Seção X
Dos Sistemas de Informação

Art. 13. Os sistemas de informação dos órgãos e entidades municipais devem ser desenvolvidos utilizando metodologias em conformidade com as melhores práticas de desenvolvimento seguro de sistemas.

Parágrafo único. Os riscos relacionados à segurança da informação devem ser identificados e tratados em todas as fases do ciclo de vida dos sistemas de informação, de sua concepção à

desativação ou descarte.

Seção XI
Do serviço de e-mail

Art. 14. O serviço de e-mail corporativo deve ser utilizado exclusivamente para fins institucionais.

§ 1º As mensagens constantes das bases de dados do serviço de e-mail corporativo estão sujeitas à auditoria a qualquer tempo.

§ 2º Em todas as trocas de mensagens de cunho institucional, devem ser observados os critérios e medidas de segurança em conformidade com a classificação das informações compartilhadas.

Seção XII
Da computação em nuvem

Art. 15. Todas as iniciativas de criação ou migração de serviços para a nuvem devem ser suportadas por processo formal de gestão de riscos de segurança, mantendo-se em conformidade com esta resolução e as demais que complementem a Política de Segurança da Informação.

§ 1º O processo de gestão de riscos deve possibilitar a identificação, quantificação, priorização, tratamento, comunicação e a monitoração periódica dos riscos à segurança das informações.

§ 2º Os processos devem ter por objetivo reduzir as vulnerabilidades, evitar as ameaças, minimizar a exposição aos riscos e atenuar os impactos à confidencialidade, integridade e disponibilidade das informações.

Seção XIII
Da Capacitação

Art. 16. Os agentes públicos, prestadores de serviço devem possuir conhecimento mínimo para a execução eficaz e segura de suas tarefas, assim como conhecer as políticas e normas de segurança da Administração Pública Municipal.

§ 1º Programas permanentes de sensibilização e conscientização em Segurança da Informação devem ser oferecidos aos agentes públicos que tenham acesso aos ativos da informação.

§ 2º Programas permanentes de treinamento em Segurança da Informação devem ser oferecidos aos agentes públicos, compatíveis com suas atribuições profissionais.

§ 3º Programas permanentes de qualificação continuada no tema de segurança cibernética devem ser oferecidos para as organizações usuárias de TIC da PCRJ.

Seção XIV
Da inteligência artificial

Art. 17. As iniciativas que utilizem Inteligência Artificial (IA) devem ser suportadas por processo formal de gestão de confiança, risco e segurança, mantendo-se em conformidade com esta resolução e as demais que complementem a Política de Segurança da Informação.

Art. 18. Os sistemas de inteligência artificial (IA) devem funcionar de maneira robusta, segura e protegida ao longo de seus ciclos de vida, mantendo-se em conformidade os seguintes princípios:

I - confiabilidade e robustez dos sistemas de inteligência artificial e segurança da informação;

II - a privacidade, a proteção de dados e a autodeterminação informativa; e

III - prevenção, precaução e mitigação de riscos sistêmicos derivados de usos intencionais ou não

intencionais e de efeitos não previstos de sistemas de inteligência artificial.

CAPÍTULO III
DAS DISPOSIÇÕES FINAIS

Art. 19. Esta Resolução entra em vigor na data de sua publicação.

Art. 20. Fica revogada a Deliberação CGTIC-Rio nº 001, de 28 de março de 2018, e demais disposições em contrário.

Rio de Janeiro, 15 de dezembro de 2023.

EDUARDO CAVALIERE