COMITÊ DE GOVERNANÇA DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – CGTIC-Rio

DELIBERAÇÃO Nº 001 DE 28 DE MARÇO DE 2018.

Regulamenta a Política de Segurança da Informação - PSI da Prefeitura da Cidade do Rio de Janeiro – PCRJ.

O PRESIDENTE DO COMITÊ DE GOVERNANÇA DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – CGTIC-Rio, no uso das atribuições que lhe são conferidas pela legislação em vigor e, em especial, pelas descritas no Decreto nº 43.096 de 05 de maio de 2017;

CONSIDERANDO os termos do inciso I do artigo 5º do Decreto Municipal nº 44276 de 1º de março de 2018, que estabelece a Política de Segurança da Informação da PCRJ;

CONSIDERANDO ser imprescindível a realização de ações estratégicas que visem à redução dos riscos à segurança das informações da PCRJ, ou seja, do possível comprometimento da confidencialidade, integridade e disponibilidade das informações dos diferentes órgãos e entidades municipais, estas representadas pelas autarquias, fundações, empresas públicas e sociedades de economia mista.

DELIBERA:

Art.1º. A regulamentação da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI no âmbito da Prefeitura da Cidade do Rio de Janeiro – PCRJ, conforme anexo da presente deliberação.

Art.2º. Esta Deliberação entra em vigor na data de sua publicação, revogadas as disposições em contrário.

ORIGINAL ASSINADO

FÁBIO PIMENTEL DE CARVALHO
Presidente do Comitê de Governança da Tecnologia da Informação e Comunicação

Publicado DO Rio nº 11 • 02 de Abril de 2018

ANEXO

CAPÍTULO I

DOS OBJETIVOS

Art. 1º - A Política de Segurança da Informação – PSI da PCRJ tem os seguintes objetivos:

I. definir diretrizes, responsabilidades, competências e princípios de Segurança da Informação – SI no âmbito da PCRJ;

II. conduzir os órgãos e entidades municipais a níveis de risco gerenciáveis, no que diz respeito à segurança de suas informações;

III. garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações que suportam as atividades e os objetivos estratégicos dos órgãos e entidades municipais;

IV. fomentar o comprometimento de todos os agentes municipais na implantação e melhoria contínua de uma cultura de Segurança da Informação em todos os órgãos e entidades municipais.

CAPÍTULO II

DA ABRANGÊNCIA

Art. 2º - Esta política e suas normas complementares aplicam–se a todos os órgãos e entidades da Administração Pública Municipal, bem como aos funcionários públicos municipais independentemente de sua função, cargo, ou vínculo empregatício, aos prestadores de serviços, estagiários, ou quaisquer pessoas e/ou instituições que estejam autorizadas a acessar os ativos da informação da PCRJ.

Art. 3º - Todos os processos de contratação de produtos e serviços, convênios, acordos e outros instrumentos congêneres celebrados pelos órgãos e entidades da PCRJ devem ser analisados quanto aos aspectos relacionados à Segurança da Informação de forma que, sempre que pertinente, estejam sujeitos a requisitos de conformidade a esta política e às suas normas complementares.

CAPÍTULO III

DOS TERMOS E DEFINIÇÕES

Art. 4º - Para fins desta política, considera-se:

I. **Acesso**: capacidade de usar um ativo da informação físico ou tecnológico (por exemplo: ler, criar, modificar ou excluir um arquivo; executar um programa; se

conectar a um dispositivo ou entrar em áreas de acesso restrito que hospedem 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 (ex. incêndio, falha de equipamentos, furto ou destruição de informações sensíveis, dentre outras);

III. Área de gestão de Tecnologia da Informação e da Comunicação (TIC): é a área responsável pela administração da infraestrutura de TIC do órgão ou entidade;

IV. Ativo da informação: elementos que transformam, transportam, guardam e descartam dados ou informações, incluindo a própria informação e que se dividem em 6 (seis) grupos: equipamentos, aplicações, usuários, ambientes, informações e processos;

V. Autenticação: processo de reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica. Há diversas técnicas de autenticação (por ex.: utilização de senhas, impressão digital, certificado digital, reconhecimento da íris, dentre outros);

VI. Autenticidade: garantia de que os ativos da informação identificados em um processo de comunicação como remetentes ou autores sejam exatamente quem dizem ser;

VII. Autorização: concessão ao usuário, após a sua autenticação, de um conjunto de permissões de acesso a um ativo da informação físico ou tecnológico;

VIII. Características biométricas: características físicas que identificam uma pessoa, como por exemplo: impressões digitais, geometria da íris etc.;

IX. Classificação da informação: é o grau de sensibilidade de uma informação para o negócio diante de uma possível quebra de segurança, ou seja, do comprometimento dos princípios básicos de Segurança da Informação: confidencialidade, integridade e disponibilidade. A partir da classificação da informação é definido o tipo de tratamento a qual ela está sujeita (identificação, acesso, distribuição, uso em correios e fax, reprodução, armazenamento, descarte e transporte);

X. Comitê de Segurança da Informação: instância estratégica responsável por tratar e deliberar sobre Segurança da Informação no âmbito do órgão ou entidade;

XI. Conscientização em Segurança da Informação: processo de iniciação educacional que permita 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 está disponível a indivíduos ou processos autorizados;

XIII. Conta de acesso: identificação única, concedida de forma pessoal e intransferível a um usuário, em conjunto com um método de autenticação (por ex.:

senha). Esse par de informações habilita o seu dono a acessar equipamentos, sistemas e aplicações específicas ou ambientes, de acordo com o perfil de autorização definido;

XIV. Continuidade de negócios: capacidade estratégica e tática de uma organização 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;

XV. Controle de acesso: medidas e procedimentos que possuem o objetivo de proteger as informações contra acessos não autorizados;

XVI. Custodiante: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos da informação que não lhe pertencem, mas que estão sob sua custódia;

XVII. Dados: trata-se da informação não processada;

XVIII. Disponibilidade: propriedade que garante que a informação está disponível às pessoas e aos processos autorizados, a qualquer momento requerido;

XIX. Gestor da Informação: agente responsável pela classificação e gerenciamento dos acessos à informação;

XX. Gestor de Segurança da Informação: agente responsável pelas ações de Segurança da Informação no âmbito do órgão ou entidade;

XXI. Homologação: análise da funcionalidade, testes e aprovações necessárias para a implantação de recursos de TIC;

XXII. Identificação: processo pelo qual um usuário fornece sua identidade para acesso a um ativo da informação físico ou tecnológico;

XXIII. Incidente de Segurança da Informação: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos ativos da informação;

XXIV. 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.;

XXV. Integridade: propriedade que garante que informação está intacta e protegida contra perda, dano ou modificação não autorizada;

XXVI. Manutenção preventiva: conjunto de operações para revisão, inspeção e preservação dos recursos de TIC;

XXVII. Plano de Gerenciamento de Incidentes: plano de ação claramente definido e documentado para ser usado quando ocorrer um incidente. O plano deve cobrir as principais pessoas, serviços e demais recursos necessários para implementar o processo de gerenciamento de incidentes;

XXVIII. Recurso de TIC (Tecnologia da Informação e da Comunicação): são os ativos da informação tecnológicos que transformam, transportam, guardam e descartam dados ou informações;

XXIX. Risco: probabilidade de ameaças explorarem vulnerabilidades, comprometendo a confidencialidade, integridade ou disponibilidade da informação, causando impactos para um sistema ou organização;

XXX. Segurança física: processo que trata da proteção de todos os ativos da informação contra ameaças naturais (ex. incêndios) e humanas (ex. acessos não autorizados);

XXXI. 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;

XXXII. 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 de uma organização;

XXXIII. Treinamento em Segurança da Informação: processo de aprendizagem voltado para o desenvolvimento de competências e habilidades em Segurança da Informação necessárias ao desempenho das atribuições funcionais do indivíduo na organização;

XXXIV. Usuário: qualquer pessoa autorizada a ler, inserir ou atualizar informações;

XXXV. Vulnerabilidade: fragilidade presente ou associada a um ativo ou grupo de ativos da informação, que pode ser explorada por uma ou mais ameaças gerando incidentes de Segurança da Informação.

CAPÍTULO IV

DOS PRINCÍPIOS

Art. 5º - As ações de Segurança da Informação devem buscar alcançar e preservar os seguintes princípios:

I. autenticidade;

II. confidencialidade;

III. disponibilidade;

IV. integridade;

V. legalidade.

CAPÍTULO V

DAS DIRETRIZES

Seção I

Do Tratamento das Informações

Art. 6º - As informações são ativos de propriedade do Município, devendo ser tomadas todas as medidas necessárias para protegê-las de alteração, destruição e divulgação não autorizadas.

§1°. As informações devem ser identificadas e classificadas quanto à confidencialidade, integridade e disponibilidade de forma a serem adequadamente acessadas, manipuladas, armazenadas, transportadas e descartadas.

§2°. Os controles de segurança da informação devem ser proporcionais à sua classificação e ao nível de risco ao qual estiver exposta.

§3°. Funcionários públicos, prestadores de serviço e estagiários devem garantir o sigilo das informações a que tiverem acesso em função de suas competências funcionais, tomando o cuidado necessário quanto a sua divulgação interna e externa, de acordo com sua classificação.

§4°. A utilização autorizada dos ativos da informação deve ser condicionada à assinatura de termo de responsabilidade específico do órgão ou entidade proprietária do ativo.

Seção II

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.

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

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

§3°. A duração do acesso dos prestadores de serviço, fornecedores e estagiários deve ter prazo limitado à execução de suas atividades.

§4°. Todas as contas de acesso aos ativos da informação e às instalações físicas da PCRJ devem ser revogadas ou suspensas quando não mais necessárias.

Seção III

Da Segurança Física

Art. 8º - As instalações físicas e áreas de processamento de informações críticas ou sensíveis devem ser protegidas contra ameaças naturais (ex. incêndio) e humanas (ex. acesso indevido).

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

§2°. 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.

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

Seção IV

Da Gestão de Recursos de TIC

Art. 9º - Os recursos de TIC de propriedade da PCRJ são fornecidos para uso corporativo.

§1°. Todos os recursos de TIC devem ser identificados de forma individual, controlados, preservados, protegidos contra acessos indevidos, submetidos à manutenção preventiva periódica e estar com a documentação atualizada e aprovada pelos setores competentes.

§2°. A disponibilização de recursos de TIC somente deve ser permitida após o atendimento às determinações desta Política e de suas normas complementares, a homologação pela área local de Gestão de TIC e a autorização dos setores responsáveis.

§3°. Todos os ambientes operacionais devem possuir procedimentos formais de gerenciamento de segurança de seus recursos de TIC.

§4°. A utilização de recursos de TIC deve ser precedida de assinatura de Termo de Responsabilidade específico do órgão ou entidade proprietária do recurso.

§5°. A movimentação dos recursos de TIC deve ser precedida de registro e devida autorização.

§6°. Em casos de alienação e descarte, devem ser seguidos procedimentos adequados à classificação das informações residentes no recurso, para que não haja risco de vazamento ou perda de informações.

§7°. Os recursos de TIC devem ser inventariados e ter identificados os seus proprietários e custodiantes.

Seção V

Da Segurança dos Sistemas de Informação

Art. 10 - 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 VI

Da Capacitação

Art. 11 - Os funcionários públicos, prestadores de serviço e estagiários devem possuir conhecimento mínimo para a execução eficaz e segura de suas tarefas, assim como conhecer as políticas e normas de segurança da PCRJ.

§1°. Devem ser estabelecidos programas permanentes de sensibilização e conscientização em Segurança da Informação, que alcancem todos os agentes que tenham acesso aos ativos da informação da PCRJ, visando garantir a compreensão das políticas, normas e melhores práticas em Segurança da Informação.

§2°. Devem ser estabelecidos programas permanentes de treinamento em Segurança da Informação, compatíveis com as atribuições profissionais dos funcionários públicos participantes, de modo a permitir o cumprimento de seus papéis e responsabilidades com relação à proteção das informações da PCRJ.

Seção VII

Da Gestão de Continuidade

Art. 12 - 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 VIII

Da Gestão de Riscos

Art. 13 - Deve ser estabelecido processo que possibilite a identificação, quantificação, priorização, tratamento, comunicação e a monitoração periódica dos riscos à informação.

Parágrafo único. O processo deve ter por objetivo reduzir as vulnerabilidades, evitar as ameaças, minimizar a exposição aos riscos e atenuar os impactos associados aos ativos da informação dos órgãos ou entidades.

Seção IX

Da Auditoria e Conformidade

Art. 14 - A PCRJ se reserva o direito de monitorar e avaliar, a qualquer tempo, o uso dos seus ativos da informação visando salvaguardar os interesses do município.

Parágrafo único. Ficam todos os órgãos e entidades municipais sujeitos a auditorias de conformidade à PSI e suas normas complementares, assim como de eficácia e efetividade de seus controles de SI.

Seção X

Da Gestão de Incidentes de Segurança da Informação

Art. 15 - Os incidentes de Segurança da Informação devem ser identificados, monitorados, comunicados e devidamente tratados, em tempo hábil, nos termos de um Plano de Gerenciamento de Incidentes.

Parágrafo único. O Plano de Gerenciamento de Incidentes deve ter por objetivo o restabelecimento das atividades do órgão ou entidade à situação de normalidade nos prazos previstos. Esse plano deve ser documentado, testado e revisado periodicamente.

CAPÍTULO VI

DAS PENALIDADES

Art. 16 - As ações que violem esta política ou suas normas complementares são passíveis de sansões civis, penais e administrativas, conforme a legislação em vigor.

Art. 17 - A análise e tratamento dos casos de violação omissos na legislação vigente devem ser realizados pelo Comitê de Segurança da Informação do órgão ou entidade.

CAPÍTULO VII

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 18 - É de responsabilidade dos órgãos e entidades municipais tomar as medidas necessárias à consecução e manutenção de sua conformidade com todas as políticas e normas de segurança da PCRJ.

§1º. Ao titular do órgão ou entidade e às Chefias Imediatas compete:

I. conscientizar funcionários e quaisquer colaboradores sob sua liderança em relação aos conceitos e às práticas de Segurança da Informação;

II. atuar junto a seus subordinados na construção e implantação de processos de trabalho que promovam a Segurança da Informação;

III. tomar as medidas administrativas necessárias para que sejam adotadas ações corretivas, em tempo hábil, em caso de comprometimento da Segurança da Informação.

§2º. À área de Gestão de Pessoas de cada órgão ou entidade compete:

I. garantir a todos os funcionários públicos e estagiários o conhecimento desta política e de suas normas complementares;

II. notificar aos agentes competentes qualquer movimentação referente a funcionários públicos e estagiários, com vistas a regularizar o acesso aos ativos da informação.

Art. 19 - É de responsabilidade de todos que têm acesso aos ativos da informação da PCRJ manter níveis de segurança adequados, segundo os preceitos desta política e de suas normas complementares.

§1º. A todo funcionário público, prestador de serviço e estagiário compete:

I. realizar suas competências funcionais em aderência a todas as políticas, normas e procedimentos a elas relacionados;

II. observar desvios das políticas, normas e procedimentos estabelecidos e informá-los ao responsável imediato.

§2º. Ao Gestor da Informação compete:

I. administrar os acessos dos usuários às informações: definir perfis de acesso, prover ou solicitar formalmente estes acessos, revisá-los periodicamente e promover, a tempo, o cancelamento dos mesmos;

II. classificar as informações sob sua gestão em níveis de sensibilidade diante de um possível comprometimento dos princípios de confidencialidade, integridade e disponibilidade.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 20 - Estas diretrizes devem ser revisadas e atualizadas pela Iplanrio à medida que se agreguem novos requisitos e valores às atividades da PCRJ, ou dentro do intervalo de 3 (três) anos.

Art. 21 - Complementam a Política de Segurança da Informação as normas a serem editadas em deliberações específicas.