DECRETO RIO Nº 44276 **DE 01 DE MARÇO DE 2018**

Estabelece a Política de Segurança da Informação da Prefeitura da Cidade do Rio de Janeiro – PCRJ.

O PREFEITO DA CIDADE DO RIO DE JANEIRO, no uso das atribuições que lhe são conferidas pela legislação em vigor, e

CONSIDERANDO ser estrategicamente imprescindível proteger as informações que suportam a missão do Poder Executivo Municipal;

CONSIDERANDO ser a informação um dos ativos mais importantes para qualquer instituição, bem como para seus processos de trabalho;

CONSIDERANDO a necessidade de aprimoramento contínuo da gestão da Segurança da Informação no âmbito municipal;

CONSIDERANDO a importância de manter e zelar pela integridade, disponibilidade e confidencialidade das informações corporativas como meio eficaz para a consolidação de sua credibilidade junto ao cidadão.

DECRETA:

Art. 1º Fica instituída a Política de Segurança da Informação da Prefeitura da Cidade do Rio de Janeiro, com 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 do Programa de Segurança da Informação; e

V - disseminar a cultura da Segurança da Informação em todos os níveis organizacionais dos órgãos e entidades municipais.

Art. 2º Para fins deste Decreto, considera-se:

I - Ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

II - 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;

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

IV - Comitê de Governança da Tecnologia da Informação e Comunicação (CGTIC-Rio): instância estratégica responsável por tratar e deliberar sobre Segurança da Informação no âmbito da PCRJ;

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

VI - Confidencialidade: propriedade que garante que a informação só está disponível a indivíduos ou processos autorizados;

VII - Dados: trata-se da informação não processada;

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

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

X - Grupo de Tratamento e Resposta a Incidentes: agentes responsáveis por receber, analisar e responder às notificações e atividades relacionadas a incidentes de Segurança da Informação;

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

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 - Recurso de TIC (Tecnologia da Informação e da Comunicação):

são os recursos tecnológicos que transformam, transportam, guardam e descartam dados ou informações;

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

XVI - Usuário: qualquer pessoa autorizada a ler, inserir ou atualizar informações;

XVII - 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.

Art. 3º As ações de Segurança da Informação devem buscar, alcançar e preservar os seguintes princípios:

I - autenticidade;

II - confidencialidade;

III - disponibilidade;

IV - integridade;

V - legalidade.

Art. 4º Ao Comitê de Governança da Tecnologia da Informação e Comunicação - CGTIC-Rio, presidido pela IPLANRIO, compete:

I - regulamentar as políticas e normas de Segurança da Informação;

II - acompanhar e orientar a implantação das políticas e normas de Segurança da Informação nos órgãos e entidades municipais;

III - receber, analisar e consolidar os resultados relativos à auditorias de nível de conformidade dos órgãos e entidades municipais às políticas e normas de Segurança da Informação;

IV - propor programa orçamentário específico para suporte às ações de tratamento dos riscos relacionados à Segurança da Informação.

Art. 5º À Empresa Municipal de Informática S.A. – IPLANRIO compete:

I - propor regulamentação sobre Segurança da Informação;

II - planejar e coordenar as atividades relativas à Segurança da Informação;

III - promover a divulgação das políticas, normas e melhores práticas de Segurança da Informação para todos os órgãos e entidades municipais;

IV - promover a cultura da Segurança da Informação por meio de ações de sensibilização e conscientização;

V - definir, prover e administrar, direta ou indiretamente, modelos e métodos de gerenciamento que promovam a segurança dos serviços de TIC;

VI - garantir os níveis de alinhamento das atividades de TIC a todas as políticas, normas e procedimentos de segurança estabelecidos;

VII - instituir e coordenar um Grupo de Tratamento e Resposta a Incidentes;

VIII - realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na Segurança da Informação;

IX - elaborar, implantar e gerenciar o programa de continuidade de negócios dos serviços corporativos hospedados no Datacenter da PCRJ.

Art. 6º Ao Grupo de Tratamento e Resposta a Incidentes, de que trata o inciso VII do art. 5º, em seu âmbito de atuação, compete:

I - coordenar as atividades de tratamento e resposta a incidentes de Segurança da Informação;

II - promover o tratamento e a recuperação de serviços de TIC;

III - cooperar com outras equipes de Tratamento e Resposta a Incidentes.

Art. 7º À Auditoria Geral da Controladoria Geral do Município compete avaliar o cumprimento da Política de Segurança da Informação e de suas normas complementares.

Art. 8º Aos demais órgãos e entidades da Administração Pública Municipal, direta e indireta, em seu âmbito de atuação, compete:

I - coordenar as ações de Segurança da Informação;

II - quando cabível, aplicar as ações corretivas e disciplinares nos casos de tratamento de incidentes de Segurança da Informação;

III - propor programa orçamentário específico para as ações de Segurança da Informação;

IV - instituir Comitê de Segurança da Informação.

Art. 9º Ao Comitê de Segurança da Informação, de que trata o inciso IV do art. 8º, em seu âmbito de atuação, compete:

I - gerenciar os riscos de segurança da informação associados aos processos de negócio e serviços do órgão ou entidade;

II - deliberar sobre a implementação das ações de Segurança da Informação;

III - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação;

IV - elaborar e propor normas locais de Segurança da Informação em conformidade com esta política e suas normas complementares;

V - solicitar apurações quando da suspeita de ocorrências de incidentes de Segurança da Informação;

VI - elaborar, implantar e gerenciar o programa de continuidade de negócios dos serviços e sistemas de informação do órgão ou entidade;

VII - nomear o Gestor de Segurança da Informação do órgão ou entidade.

Art. 10. Ao Gestor de Segurança da Informação, de que trata o inciso VII do art. 9º, em seu âmbito de atuação, compete:

I - promover a cultura de Segurança da Informação;

II - acompanhar as investigações e as avaliações dos danos decorrentes de incidentes de Segurança da Informação;

III - propor recursos necessários às ações de Segurança da Informação;

IV - propor normas relativas à Segurança da Informação;

V - apoiar técnica e administrativamente as reuniões e demais atividades do Comitê, incluindo o gerenciamento da execução de suas resoluções.

Art. 11. Este Decreto entrar em vigor na data de sua publicação, revogadas as disposições em contrário, em especial o Decreto nº 29.385, de 30 de maio de 2008.

.

Rio de Janeiro, 01 de março de 2018 - 454º da Fundação da Cidade.

MARCELO CRIVELLA

D. O RIO 01.03.2018