PORTARIA IPLANRIO Nº 242 **DE 29 DE MAIO DE 2015.**

Regulamenta o acesso à informação no âmbito da Prefeitura da Cidade do Rio de Janeiro.

O DIRETOR PRESIDENTE DA EMPRESA MUNICIPAL DE INFORMÁTICA S.A.- IPLANRIO, no uso das atribuições que lhe são conferidas pela legislação em vigor e,

CONSIDERANDO os termos do art. 9º do Decreto Municipal "N" nº 29385 de 30 de maio de 2008,

CONSIDERANDO a Portaria "N" Nº 241 de 29 de maio de 2015, que regulamenta a Política de Segurança da Informação da Prefeitura da Cidade do Rio de Janeiro – PCRJ;

CONSIDERANDO os níveis elevados de relevância e criticidade dos sistemas de informações que sustentam a missão de cada um dos órgãos e entidades municipais;

CONSIDERANDO que o acesso indevido à informação pode expor a PCRJ a riscos elevados no cumprimento de sua missão, com possibilidades de repercussões administrativas, sociais, legais, políticas e econômicas;

RESOLVE:

Art. 1º Regulamentar a NORMA PARA ACESSO À INFORMAÇÃO no âmbito da Prefeitura da Cidade do Rio de Janeiro, conforme anexo da presente portaria.
Art. 2º Esta Portaria entra em vigor na data de sua publicação, revogadas as disposições em contrário, em especial a Portaria "N" nº 125 de 28 de maio de 2010.

D. O RIO 01.06.2015
Republ. em 03.06.2015

ANEXO

CAPÍTULO I

DISPOSIÇÕES INICIAIS

Art. 1º A Norma para acesso à informação define as regras a serem seguidas com relação ao controle de acesso às informações e aos sistemas de informação da Prefeitura da Cidade do Rio de Janeiro - PCRJ, sendo complementar à Política de Segurança da Informação.

Art. 2º Esta norma aplica-se a todos os usuários, independentemente de sua função, cargo, ou vínculo empregatício, aos prestadores de serviços, estagiários, ou quaisquer pessoas e/ou instituições que estejam autorizadas a acessar informações e sistemas de informação da PCRJ.

CAPÍTULO II

TERMOS E DEFINIÇÕES

Art. 3º Para fins desta Portaria considera-se:

I - Acesso – capacidade de usar um recurso tecnológico (por exemplo: ler, criar, modificar ou excluir um arquivo; executar um programa; se conectar a um dispositivo ou a uma rede);

II - Agente responsável por gerenciamento de acessos – servidor municipal que tenha sido designado pela alta gestão do órgão ou entidade à qual presta serviço como responsável pelo gerenciamento dos acessos dos servidores sob seu comando aos diversos Sistemas de Informação da PCRJ;

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

IV - Autenticação – processo de identificação e 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, etc);

V - Autorização – concessão de um conjunto de permissões de acesso às informações ou funcionalidades de um sistema de informação a um usuário após a autenticação deste;

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

VII - Chave de Acesso (conta) – código de identificação/acesso atribuído a cada usuário;

VIII - Chave de Acesso com Privilégios Especiais – chave de acesso que permite execução de ações diferenciadas (por ex.: funções administrativas, funções de segurança, administradores dos sistemas);

IX - Confidencialidade – propriedade que garante que a informação só está disponível a indivíduos ou processos autorizados;

X - Controle de Acesso (Lógico) – medidas e procedimentos que possuem o objetivo de proteger as informações contra acessos não autorizados;

XI - Criptografia – conjunto de técnicas pelas quais a informação pode ser transformada de sua forma original para outra codificada, de maneira que possa ser reconhecida apenas por seu criador (emissor) e seu destinatário (receptor);

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

XIII - Gerenciamento de contas do usuário – conjunto de atividades que envolvem o processo de solicitação, criação, ciência pelo usuário e encerramento de contas; registro e acompanhamento de contas de usuários e suas autorizações de acesso, incluindo o gerenciamento destas atividades;

XIV - Identificação – processo pelo qual um usuário fornece sua identidade para o sistema de informação;

XV - Identificação do usuário (user ID ou ID de usuário) – identificação única formada por símbolos ou seqüência de caracteres associada a um usuário;

XVI - 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, audio, etc.;

XVII - Informações sensíveis – informações que divulgadas, modificadas ou destruídas sem autorização provocarão danos relevantes à organização;

XVIII - Integridade – propriedade que garante que informação está intacta e protegida contra perda, dano ou modificação não autorizada, realizada intencional ou acidentalmente;

XIX - Macros – comandos ou ações tipicamente empregados para automatizar seqüências de instruções, movimentos ou regras freqüentemente usadas;

XX - Privilégio – direito de acesso concedido a algum agente (usuário, aplicação, processo etc.);

XXI - Privilégios Especiais – direitos atribuídos a determinados agentes, que propiciam um grau de acesso diferenciado aos sistemas de informação (por ex.: o acesso a funções administrativas, de gerenciamento ou segurança dos sistemas);

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

XXIII - Sistemas de informação – conjunto de componentes interrelacionados que coletam (ou recuperam), processam, armazenam e distribuem informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização;

XXIV - Token – dispositivo portátil que gera códigos (ou senhas) aleatórias utilizado na autenticação de um usuário a determinado recurso de TIC.

CAPÍTULO III
NORMAS REGULAMENTADORAS GERAIS

Art. 4º Ficam as chaves de acesso sujeitas às seguintes normas regulamentadoras de utilização:

I - Os usuários dos sistemas de informação da PCRJ devem ser identificados por uma chave única de acesso, autenticados e autorizados a usar somente as funcionalidades necessárias ao desempenho de suas competências funcionais;

II - A chave única de acesso do usuário (ID de usuário) deve ser de uso pessoal e intransferível, qualificando-o como responsável por quaisquer ações realizadas por meio desta;

III - A chave de acesso dos servidores aos sistemas de informação é representada por sua matrícula, conforme Decreto Municipal “N” nº 15.834/97;

IV - A chave de acesso sem utilização por um período igual ou superior a 90 (noventa) dias deve ser desativada automaticamente.

Art. 5º O gerenciamento de acessos às informações observará ao que se segue:

I - Somente será liberado após autorização do gestor da informação, devendo possuir, no mínimo, os controles de identificação, autenticação, autorização e auditoria;

II - Para os prestadores de serviço, fornecedores e estagiários será necessário, ainda, que o acesso tenha prazo limitado à execução de suas atividades;

III - O gerenciamento do ciclo de vida de acessos aos sistemas de informação deve ser realizado por meio de procedimentos e responsabilidades formalmente definidos, abrangendo todas as fases deste ciclo: da inclusão de novos usuários, passando pelo controle de seus perfis de autorização, até sua exclusão (ou cancelamento de acesso);

IV - As solicitações relacionadas ao ciclo de vida de acessos aos sistemas de informação e as ações realizadas em resposta a estas solicitações devem ser registradas de forma a possibilitarem a manutenção eficiente e eficaz dos privilégios de acesso a estes sistemas, (por ex.: atualização/cancelamento de privilégios de acesso que deva ser realizada em resposta a eventos como alteração de cargos/empregos, transferência de setor ou desligamento de servidores, prestadores de serviços e estagiários);

V - Os agentes responsáveis pelo gerenciamento de acessos devem comunicar aos gestores dos sistemas de informação as mudanças de cargo/emprego, de setor, ou mesmo do desligamento de servidores municipais, prestadores de serviços ou estagiários sob sua responsabilidade, visando à mudança ou revogação de privilégios destes usuários, em até 3 (três) dias úteis após a confirmação do evento;

VI - Os sistemas de informação devem estar sujeitos a rotinas periódicas de revisão de privilégios de acesso, ou seja, verificação da necessidade de mudanças de privilégios, seja em função de alteração de perfil, da suspensão ou cancelamento de acessos, devido à alteração de cargos/empregos, transferência de setor ou desligamento de servidores, prestadores de serviços e estagiários;

VII - A concessão de privilégios especiais de acesso está sujeita à justificativa formal de seu solicitante, avaliação por agente(s) competente(s) quanto à sua real necessidade e autorização do respectivo gestor do sistema de informação.

Art. 6º O gerenciamento e uso de senhas devem seguir as seguintes normas regulamentadoras:

I - As senhas não devem ser incluídas em nenhum processo automático de acesso a sistemas (por ex.: senhas armazenadas em macros ou funções de software);

II - O tamanho mínimo da senha deve ser de 08 (oito) caracteres alfanuméricos e, no primeiro acesso após a habilitação, o usuário terá, obrigatoriamente, que informar uma nova senha e confirmá-la;

III - As senhas têm validade de 45 (quarenta e cinco) dias e sua troca deve ser solicitada automaticamente pelo sistema de informação, podendo o usuário alterá-la a qualquer tempo, sempre que achar necessário;

IV - Não podem ser usadas senhas repetidas dentro de um período de 05 (cinco) trocas;

V - Os sistemas de informação devem ser configurados para que o usuário tenha direito a 05 (cinco) tentativas de autenticação de senha e, ultrapassado este limite, terá seu acesso suspenso até que solicite sua liberação aos gestores (ou administradores) dos sistemas;

VI - As senhas devem ser armazenadas e transmitidas de forma criptografada;

VII - Os sistemas de informação devem prover ao gestor do sistema, ou à pessoa por ele autorizada, a capacidade de reinicializar senhas de usuários que as tenham perdido;

VIII - Os sistemas de informação devem permitir aos seus gestores listarem a relação dos códigos de identificação, incluindo nome e estado do código (ativo ou não), bem como informações sobre o perfil de acesso de todos os usuários destes sistemas;

IX - Ficam os sistemas de informação da PCRJ obrigados a disponibilizar todas as funcionalidades necessárias para que os gestores possam realizar suas competências de forma independente dos técnicos da IplanRio.

Parágrafo único. A concessão inicial de senhas deve ser temporária, ficando o usuário responsável por acusar o seu recebimento e obrigado a alterá-las imediatamente após o recebimento.

Art. 7º Os processos de identificação e autenticação dos sistemas de informação devem seguir as seguintes normas regulamentadoras:

I - Os acessos aos sistemas de informação devem ser realizados por meio de processos padronizados de identificação e autenticação;

II - A validação das informações de identificação e autenticação só deve ser realizada quando todos os dados necessários à sua realização (por exemplo, chave de acesso e senha) tiverem sido integralmente informados;

III - Os sistemas de informação devem realizar desconexão automática com base em tempo de inatividade, sendo este definido em função das características de utilização do sistema;

IV - Os sistemas de informação devem restringir o acesso simultâneo a partir de uma mesma chave de acesso;

V - Os sistemas de informação que hospedem informações sensíveis devem utilizar autenticação forte com dois, ou se for o caso, três fatores de autenticação com os conceitos: o que você sabe, o que você tem e o que você é (por ex.: senha, token e biometria).

Art. 8º Nos casos em que existam transações por meio de integrações entre sistemas, o contexto dessa integração exigirá controle de acesso de usuário apenas no sistema que requisita a transação, na forma prevista nessa Portaria. O sistema requisitado deverá registrar as transações segundo o contexto do negócio para fins de rastreabilidade do evento, dispensando a aplicação dos arts. 4º, 5º e 6º dessa Portaria.

CAPÍTULO IV
DAS RESPONSABILIDADES

Art. 9º São responsabilidades referentes aos acessos às informações da PCRJ:

I - Dos usuários:

a) manter a confidencialidade de suas senhas, estando ciente que a inobservância desta norma implicará na sua responsabilidade direta por qualquer ato praticado por sua utilização indevida;

b) se necessário transmitir ou armazenar senhas, sempre fazê-lo de forma segura;

c) criar senhas fortes, com tamanho mínimo de 8 (oito) posições, contendo caracteres alfanuméricos e especiais, sem utilização de dados pessoais ou palavras presentes em dicionários;

d) criar senha diferente das últimas 5 (cinco) utilizadas anteriormente;

e) trocar as senhas periodicamente, conforme os prazos estabelecidos,

ou sempre que haja indicação de possível comprometimento de sua confidencialidade;

f) não gravar senhas em processos automáticos de acesso a sistemas de informação (por ex.: em macros ou teclas de função).

II. Dos Gestores dos Sistemas de Informação:

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

b) promover a revisão periódica de privilégios de acesso dos usuários dos sistemas de informação sob sua gestão.

III - Dos Agentes Responsáveis pelo Gerenciamento de Acessos:

a) gerenciar os acessos dos servidores aos sistemas de informação da PCRJ;

b) promover a revisão periódica de privilégios de acesso de seus servidores, solicitando aos gestores dos sistemas de informação as atualizações de privilégios que se fizerem necessárias.

IV - Da IplanRio:

a) prestar consultoria aos gestores dos sistemas de informação na realização de suas competências, assim como na criação dos processos e procedimentos de gerenciamento de acessos aos sistemas de informação.