POLÍTICA DE CONTROLE DE ACESSO

INTRODUÇÃO

O controle de acesso aos dados tratados pela Câmara Municipal de Jundiaí, atenderá os princípios fundamentais da Segurança da Informação, remete a autenticação como mecanismo para certificar as credenciais de acesso (conta de usuário e senha).

Dentro deste princípio, essas credenciais permitem que um usuário seja logicamente identificado, autenticado e autorizado a acessar um os sistemas, ambientes e serviços.

Assim, esta política vem estabelecer padrões de segurança alinhados com as melhores práticas de mercado no controle de acesso a dados sensíveis. Em conjunto com a presente política serão também observadas as normas do Ato nº 570, de 06 de Fevereiro de 2008, e suas respectivas alterações.

OBJETIVO

A política de controle de acesso tem como objetivo orientar como deve ser o acesso de pessoas aos dados do órgão. A restrição, no entanto, não eliminará completamente os riscos à essa segurança. Porém, deverá mitigar o risco de ocorrência de incidentes que possam comprometer as atividades do órgão.

Definir um padrão mínimo de controle de acesso que resguarde o órgão de acessos não autorizados ou de pessoas que já não possuem vínculo se mantenham realizando atividades ou tenham conhecimento de informações sensíveis, de caráter interno, inerentes ao exercício das atividades funcionais, privilegiadas e/ou sigilosas, ou seja, não públicas; estabelecer responsabilidades e

rotinas de controle tanto para concessão, quanto para cancelamento de acesso, assim como minimizar os riscos nas criações e manutenções das credenciais de acesso.

As diretrizes de acesso e administração está em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), evita que pessoas não autorizadas acessem, alterem, copiem ou excluam informações pessoais, tais como monitoramento de acesso, prevenção de vazamentos etc.

ABRANGÊNCIA

Esta política se aplica a todos os usuários e colaboradores do órgão, quais sejam: vereadores, servidores efetivos ou comissionados, estagiários, menores aprendizes, terceirizados, fornecedores de produtos e/ou serviços, ou indivíduos que direta ou indiretamente utilizem ou prestem serviços de suporte aos sistemas, infraestrutura ou informações do órgão. Todos os esses colaboradores serão tratados nesta política como usuários.

DIRETRIZES DE CONTROLE DE ACESSO

1. Gerenciamento de Identidade

1.1 Acesso Lógico de Usuário

Controle de acesso lógico para verificação dos dados de entrada ajuda a evitar ataques cibernéticos e também inconsistências de base de dados.

a) Deve ser estabelecido um processo de concessão, alteração e cancelamento de acesso para o agente público em todo e qualquer ambiente;

b) Os gestores imediatos são responsáveis por assegurar que as credenciais de acesso do agente público sejam disponibilizadas e utilizadas em

conformidade com as necessidades funcionais do trabalho, por meio de solicitação de acesso ao Setor de Informática;

c) Ao ser disponibilizada as credenciais de acesso com os respectivos logins e senhas, o agente público passa a ser usuário do ambiente tecnológico do órgão;

d) O Acesso Lógico dos Usuários ao ambiente tecnológico do órgão será feito mediante a utilização de Contas de Acesso;

e) O usuário terá um único ID de acesso em cada ambiente que seja necessário o credenciamento. Este ID, será valido pelo período de vínculo ativo de trabalho com o órgão e não deve ser reaproveitado para outros usuários, mesmo após o término da necessidade de uso inicial;

f) As atividades realizadas por meio de determinado ID de Acesso serão de responsabilidade do respectivo Usuário;

g) É proibido aos Usuários compartilharem seus IDs de Acesso, bem como realizarem qualquer ação utilizando ID de Acesso individual ou de grupo para o qual não tenham sido autorizados;

h) Não é permitida a criação nem utilização de contas genéricas (exemplo: temp, quest, usuario, teste, entre outras);

i) O gestor imediato deve abrir um chamado junto ao Setor de informática solicitando o bloqueio das credenciais de acesso dos respectivos usuários afastados;

j) Nos casos em que o usuário afastado for um agente terceirizado ou fornecedor de produtos e/ou serviços, o gestor responsável pelo respectivo contrato deve solicitar que o Setor de Informática faça o bloqueio do acesso desse usuário; Em caso de impedimento do gestor do contrato, a solicitação de bloqueio será feita por seu suplente e, no caso de impedimento deste, a solicitação de bloqueio será realizada pelo Setor de Administração de Bens e Serviços;

k) São considerados visitantes todas as pessoas que acessam fisicamente as instalações, mas que não possuem vínculo de trabalho com o órgão. Neste caso, terão acesso lógico a um ambiente tecnológico separado, controlado e monitorado, quer seja por meio móvel (Wi-Fi) ou fixo, conforme descreve a Política de Uso da Internet;

l) Os registros de atividades com a respectiva identificação dos responsáveis pela requisição, aprovação, concessão, comprovação e revogação de Acesso devem ser armazenados para fins de análise de segurança da informação e auditoria interna.

1.2. Gerenciamento de Privilégio

a) As credenciais de acesso privilegiado, que correspondem ao acesso a atividades de administrador de sistemas ou ativos físicos do ambiente tecnológico, devem ser atribuídas ao agente público com base na sua respectiva função e na necessidade de conhecimento de Informação para as atividades do trabalho, conforme aprovação do Setor de Informática;

b) O compartilhamento do uso de credenciais de acesso privilegiado deve ser individual e restrito. Contudo, quando for necessário o compartilhamento dessas credenciais por questões técnicas, estas devem ser autorizadas pelo Setor de Informática, registradas para fins de auditoria interna, conhecidas apenas pela equipe habilitada, e serão trocadas imediatamente quando houver subtração ou substituição de qualquer membro da equipe;

c) Todos os Usuários detentores de ID de Acesso para execução de atividades privilegiadas devem também possuir ID de Acesso para execução de atividades não privilegiadas, de forma que a utilização de acesso privilegiado só ocorra quando for estritamente necessário.

1.3. Gerenciamento de Senha de Usuário

a) Toda concessão de acesso aos sistemas de informações deve ser controlada por um método que envolva, identificação, autenticação e autorização;

b) Os usuários devem cadastrar e utilizar suas respectivas senhas de acesso aos sistemas de informações em conformidade com a Política de Uso de Senhas.

1.4. Revisão dos Diretos de Acesso

a) Os direitos de Acesso serão revisados periodicamente pelo Setor de Informática, sendo formalizada cada revisão mediante processo administrativo específico para esse fim, e validados pelos respectivos gestores imediatos ou seus substitutos;

b) As requisições geradas devem ser prontamente atendidas e documentadas pelo Setor de Informática;

c) Mensalmente, o Setor de Administração de Recursos Humanos – ARH encaminhará ao Setor de Informática uma relação dos agentes públicos afastados e dos estagiários desligados para que sejam efetuados os respectivos bloqueios de acesso.

1.5. Gerenciamento de Contas de Serviço

a) As Contas de Serviço, terão, individualmente, um responsável pela sua manutenção, bem como pela alteração de sua senha. O responsável não deve utilizar a Conta do Serviço para outros fins que não seja para o qual foi criado conforme sua definição;

b) Sistemas e dispositivos devem ser configurados, quando tecnicamente possível, de modo a prevenir Acesso remoto por meio de Contas de Serviço;

c) Contas de Acesso privilegiado que não se enquadram em Contas de Serviço, terão suas senhas expiradas em observância ao mesmo processo adotado para contas de Acesso não privilegiado.

2. Diretrizes para Acesso Físico

a) Os controles de Acesso físico visam restringir que as pessoas sem a devida autorização acessem o local onde os dados são armazenados e/ou esses dados são processados, o Acesso a equipamentos, documentos e suprimentos do ambiente tecnológico do órgão e à proteção dos recursos computacionais, permitindo-lhes acesso apenas às pessoas autorizadas;

b) Os recursos computacionais críticos do órgão, devem ser mantidos em ambientes reservados, monitorados e com acesso físico controlado permitido apenas para pessoas autorizadas;

c) Periodicamente, o Setor de Informática revisará os acessos aos ambientes tecnológicos reservados, restringindo o acesso apenas a pessoas autorizadas. Tal revisão será formalizada por meio de processo administrativo.

d) Há registro dos visitantes do órgão e os servidores utilizam crachá.

As informações relevantes a respeito dos acessos são gravadas nos registros de logs.

3. Adequação à Política

a) Os novos projetos de desenvolvimento e as novas aquisições e/ou contratações, devem seguir os padrões estabelecidos nesta política.

b) Para estarem adequados a esta política, as implementações para o ambiente tecnológico existente deverão ocorrer no prazo de 1(um) ano a partir de sua publicação.

c) Caso não seja possível a adequação recurso técnico ou processo, ouvido o Comitê de Proteção de Dados Pessoais e o Encarregado pelo Tratamento de Dados Pessoais, o Setor de Informática documentará a ocorrência em processo administrativo competente para fins de fiscalização e auditoria interna.