A **Política de Gestão e Controle de Acessos** tem como objetivo estabelecer as diretrizes para garantir que o acesso às aos ativos de informação ou sistemas de informação do Instituto de Previdência do Município de Caucaia-CE (**IPM**), garantindo os níveis adequados de proteção.

Esta **Política** complementa as normas estabelecidas pela **Política Geral de Segurança da Informação (PGSI).**

1. ACESSO A SISTEMAS DE INFORMAÇÃO

O **IPM** fornece a seus **Usuários Autorizados** (colaboradores e/ou prestadores de serviços) contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais e rede corporativa que permitem o exercício das atividades como colaboradores.

As referidas contas de acesso são fornecidas exclusivamente para que os **Usuários** possam executar suas atividades laborais e/ou de prestação de serviços.

Toda conta de acesso é pessoal do **Usuários** a qual foi delegada, sendo intransferível. Desta forma, o **Usuário** é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso.

Os **Usuários** deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo:

- Não anotar ou registrar senhas de acesso em qualquer local, exceto nas ferramentas oficialmente fornecidas pelo **IPM**;
- Não utilizar sua conta, ou tentar utilizar qualquer outra conta, para violar controles de segurança estabelecidos pelo **IPM**;
- Não compartilhar a conta de acesso e senha com outro colaborador e/ou terceiro;
- Informar imediatamente ao gestor imediato ou ao(a) Secretário(a) caso identifique qualquer falha ou vulnerabilidade que permita o acesso não autorizado às informações, sistemas e/ou recursos computacionais do **IPM**.

Qualquer acesso, ainda que de forma tentada, não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo uma análise da infração pelo Superior Imediato ou pelo Secretário(a) e aplicação das sanções e punições previstas na **PGSI**, conforme a gravidade da violação.

2. SENHAS DE ACESSO

Para acesso dos dados e sistema interno do **IPM** é obrigatório o uso de uma única identificação (login) e de senha de acesso.

Os benefícios de acesso dos colaboradores ou prestadores de serviço ao sistema interno, seja qual for a função, cargo ou atividade exercida, devem ser definidos pelo líder do setor do qual este seja integrante, limitando-se a atividades estritamente necessárias à realização de suas tarefas. Após o encerramento das atividades do colaborador, seus acessos concedidos são bloqueados imediatamente.

Indicamos um padrão mínimo para o formato da conta de acesso do colaborador (servidor ou não) ou prestador de serviços de, no mínimo, 8 caracteres, contendo números, letras maiúsculas e minúsculas e caracteres especiais.

Ao criar uma senha, usuários devem estar atentos às seguintes recomendações:

- Não utilizar nenhuma parte de sua matrícula ou função na composição da senha;
- Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil obtenção como, por exemplo, placa do carro, data de aniversário, ou endereço;
- Não utilizar repetição ou sequência de caracteres, números ou letras;
- Qualquer parte ou variação do nome **Instituto de Previdência do Município de Caucaia**;
- Qualquer variação dos itens descritos acima, ainda que sob a forma de duplicação ou escrita invertida.

3. PAPÉIS E RESPONSABILIDADES

a. Gestor da Informação

Os Gestores da Informação serão determinados pelo(a) Secretário(a), e suas atribuições são:

- Autorizar a concessão e revogação de acesso a ativos/sistemas de informação sob sua responsabilidade;
- Autorizar a concessão e o controle de acesso administrativo a ativos/sistemas de informação sob sua responsabilidade.

b. Gestores e Coordenadores

É responsabilidade dos gestores de informação e coordenadores:

- Reportar, em tempo hábil, o desligamento de colaboradores a equipe responsável por revogar o acesso as contas de usuário;

- Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação fornecendo informações sobre os empregados.

- Solicitar a concessão de acesso novos a todos que necessitem conforme mudanças em suas atividades;

- Solicitar a concessão de acesso a terceiros/prestadores de serviços contratados justificando a necessidade de acesso a ativos/sistemas de informação, desde que estes sempre estejam pautados na exigência da atividade e com o devido regramento de privacidade (seja em contrato, seja em termo de confidencialidade).

c. DESCUMPRIMENTO DA POLÍTICA

As violações, ainda que por omissão ou tentativa não consumada, desta **Política**, bem como demais normas e procedimentos de segurança, serão passíveis de sanções internas como advertência e suspensão.

A aplicação de sanções será realizada de forma objetiva, conforme o caso concreto e considerando a gravidade da infração, efeito alcançado e recorrência para aplicação das sanções. Desse modo, a sanção será proporcional à ocorrência e ao seu impacto para a segurança do **IPM**.

No caso de terceiros contratados ou prestadores de serviço, o(a) Secretário(a) deve analisar a ocorrência e deliberar sobre a efetivação das sanções conforme termos previstos em contrato.

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano ao órgão, o infrator será responsabilizado pelos danos ocasionados, cabendo aplicação das medidas judiciais pertinentes, sem prejuízo aos termos descritos nesta **Política**.

d. DISPOSIÇÕES GERAIS

Esta **Política** está de acordo a cultura de proteção de dados adotada pelo **Instituto de Previdência do Município de Caucaia-CE** e em consonância com o ecossistema normativo implantado em seu Programa de Compliance de Proteção de Dados.