

## POLÍTICA DE ACESSO E SENHA

**IDENTIFICAÇÃO:** PLTL-002

**Autor:** Comissão de Proteção de Dados Pessoais (CPDP)

**Revisor:** Comissão de Proteção de Dados Pessoais (CPDP)

**Versão:** Primeira

**Período:** Ano 2024

**Classificação do documento:** PÚBLICO

## CONTROLE DE DOCUMENTO

Período	Autor	Setor	Versão	Descrição da Alteração
Ano 2024	Comissão de Proteção de Dados Pessoais	Câmara Municipal de Barra do Garças	1ª	Criação

## Sumário

1. OBJETIVO .....	3
2. ABRANGÊNCIA.....	3
3. DIRETRIZES .....	4
4. ACESSO A ATIVOS E SISTEMAS DE INFORMAÇÃO .....	4
5. SENHA DE ACESSO.....	6
6. AUTORIZAÇÃO DE ACESSO (PRIVILÉGIOS DE ACESSO) .....	8
7. CONTROLE DE ACESSO FÍSICO .....	10
8. IDS E CRACHÁS DO USUÁRIO .....	10
9. DEMISSÕES E FIM DO CONTRATO.....	11
10. PAPÉIS E RESPONSABILIDADES .....	12
10.1 Gestor Da Informação.....	12
10.2. Departamento Pessoal .....	12
10.3. Gestores E Coordenadores .....	13
10.4. Gerencia De Tecnologia Da Informação .....	13
11. SANÇÕES.....	14
12. GESTÃO DOS REGISTROS MANTIDOS COM BASE NESTE DOCUMENTO.....	14
13. VALIDADE E GESTÃO DO DOCUMENTO.....	15
14. DISPOSIÇÕES FINAIS .....	15
15. ASSINATURA.....	15

## 1. OBJETIVO

Estabelecer diretrizes para gestão de identidade e acesso aos ativos e sistemas de informação da **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG**.

Entende-se que é vital proteger os sistemas e as informações mantidas e usadas pela **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG** contra o uso ou acesso não autorizado. O Poder Legislativo Municipal possui plena consciência de como esse acesso pode afetar a segurança, informações pessoais e individuais.

O propósito desta política é garantir que o acesso físico ou lógico a qualquer informação, local e /ou sistema seja controlado e, quando aplicável, restrito, usando controles e procedimentos que protegem os dados e sistemas de informação associados.

O Poder Legislativo Municipal está comprometido com a segurança das informações e ativos sob as atribuições e aplica e testa todas as medidas de acesso para garantir sua funcionalidade, eficácia e finalidade.

Esta Política de Controle de Acesso e Senha visa restringir o acesso a informações e/ou sistemas controlados apenas aos funcionários ou terceiros autorizados ou com permissão por escrito da **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG**. Nos casos em que é necessário acesso temporário e / ou parcial as informações ou sistemas são seguidos protocolos rígidos para permitir apenas o acesso às informações ou pela duração exigida pela atividade.

## 2. ABRANGÊNCIA

Esta política se aplica a todos os funcionários/colaboradores da **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG** (ou seja, funcionários permanentes, a termo e temporários, quaisquer representantes ou subcontratados de terceiros, trabalhadores de agências, voluntários, estagiários e agentes envolvidos com o Poder Legislativo Municipal no país ou no

exterior). A adesão a esta política é obrigatória e o não cumprimento pode levar a uma ação disciplinar.

### 3. DIRETRIZES

Os tipos de medidas de controle utilizados pelo Poder Legislativo Municipal são:

**A) Medidas físicas:** garantem que a disponibilidade de sistemas e informações sejam restritos apenas a pessoas autorizadas, impedindo que locais e informações sejam acessíveis a pessoas não autorizadas. Isso inclui [colocar resolução].

**B) Medidas lógicas:** utilizam ferramentas e protocolos para identificação, autenticação e autorização dos sistemas de informações de computadores (incluindo acesso remoto, laptops e sistemas de telefone). Os controles de acesso lógico da **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG** impõem medidas de acesso aos próprios sistemas, programas, processos e informações e incluem protocolos de senha, métodos de autenticação de usuário, criptografia de credenciais de dados e autenticação e firewalls de rede, sistema e usuário.

**C) Medidas administrativas:** incluem políticas e procedimentos definidos, seguidos por todos os funcionários e terceiros, e fornecem as etapas para áreas como controle de acesso, segurança da informação, protocolos de senha e medidas claras da mesa.

### 4. ACESSO A ATIVOS E SISTEMAS DE INFORMAÇÃO

A **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG** fornece a seus usuários autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa;

As referidas contas de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades laborais;

Toda conta de acesso é pessoal do usuário a qual foi delegada e 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 pela **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG**;
- Não utilizar a própria conta, ou tentar utilizar qualquer outra conta, para violar controles de segurança estabelecidos pela **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG**;
- Não compartilhar a conta de acesso e senha com outro usuário, colaborador e/ou terceiro;
- Informar imediatamente ao Setor de Tecnologia e Informática caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada de ativos de informação, sistemas e/ou recursos computacionais da **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG**.

Usuários que tem acesso autorizado a privilégios administrativos em sistemas de informação devem possuir uma credencial específica para este propósito.

A credencial privilegiada deverá ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso, enquanto a conta de acesso comum deverá ser utilizada em atividades do dia a dia.

Qualquer utilização não autorizada ou tentativa de utilização 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 pela CPDP e aplicação das sanções e punições previstas na Política Geral de Segurança da Informação, conforme a gravidade da violação.

## **5. SENHA DE ACESSO**

As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais da **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG** são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo;

A **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG** adota os seguintes padrões para geração de senhas de acesso a seus ativos/serviços de informação ou recursos computacionais:

- O setor de tecnologia e informática será responsável por fornecer senhas de acesso inicial ao usuário, que deverá proceder com a troca imediata da mesma;
- As senhas possuem validade de 90 (noventa) dias. Passado este prazo, os sistemas solicitarão automaticamente a troca da senha;
- As senhas associadas a contas com privilégio não-administrativo serão compostas usando uma quantidade mínima de 08 (oito) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;

- As senhas associadas a contas que possuem privilégio administrativo serão compostas usando uma quantidade mínima de 15 (quinze) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;
- Após 05 (cinco) tentativas de acesso com senhas inválidas, a conta do usuário será bloqueada, assim permanecendo por, no mínimo, 30 (trinta) minutos;
- Os sistemas de informação manterão um histórico das últimas 12 (doze) senhas utilizadas, não permitindo sua reutilização;
- Quando efetuada uma troca da senha, o usuário não poderá realizar nova alteração dentro de um prazo mínimo de 7 (sete) dias. Caso seja necessário realizar alteração dentro deste período, o usuário deverá solicitar o apoio do setor de tecnologia e informática;

Quando criada uma nova senha, usuários devem estar atentos as seguintes recomendações:

- Não utilizar nenhuma parte de sua credencial 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 **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG**;
- Qualquer variação dos itens descritos acima como duplicação ou escrita invertida.

O Poder Legislativo Municipal está ciente de que vírus, software e golpes de phishing podem tentar obter senhas no nível do usuário.

Embora os firewalls sejam usados para proteger sistemas e software, os funcionários recebem treinamento e orientação sobre phishing e são instruídos a nunca divulgar suas senhas em um ambiente físico ou online. Isso inclui a não divulgação de senhas a terceiros, clientes ou representantes que possam ter uma necessidade legítima de acessar um sistema.

Os campos de senha são sempre exibidos em formato hashtag ou estrela (por exemplo, ### ou \*\*\*) para que o texto não esteja presente quando uma senha é digitada. Isso ajuda a impedir o acesso não autorizado ou a divulgação de senha por meio de métodos de cópia e colar ou impressão eletrônica.

É proibido escrever ou armazenar senhas em qualquer formato escrito ou digital e todos os funcionários são informados disso. A divulgação ou perda não intencional de uma senha que foi gravada em qualquer formato resultará na adoção de medidas disciplinares.

Se um usuário não usar o nome de usuário e / ou senha corretos ao fazer login em um sistema ou dispositivo, são geradas mensagens genéricas de falha que não divulgam a natureza exata do erro de login. Após três tentativas fracassadas, o sistema avisará que o login falhou, mas não divulgará se isso ocorre devido ao nome de usuário, senha ou ambos estarem incorretos. Isso ajuda a impedir ataques de força bruta ou um usuário não autorizado saber que campo está incorreto, o que aumenta suas tentativas de login.

Nos casos em que o login falha, operamos com uma abordagem de três greves e o sistema ficará indisponível por 15 minutos antes que o login possa ser tentado novamente. Isso protege contra-ataques externos de “bot” e força bruta.

## **6. AUTORIZAÇÃO DE ACESSO (PRIVILÉGIOS DE ACESSO)**



A autorização e o nível permitido de acesso a ativos/serviços de informação da **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG** é feita com base em perfis que definem o nível de privilégio dos usuários.

O acesso à ativos/serviços de informação é fornecido a critério da **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG**, que define permissões baseadas nas necessidades laborais dos usuários;

Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores de cada colaborador.

Solicitações deverão ser encaminhadas ao setor de tecnologia e informática.

Os usuários devem ainda observar as seguintes diretrizes:

A seu critério exclusivo, a **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG** poderá ativar uma cota para armazenamento de arquivos em sua infraestrutura computacional local ou serviços de armazenamento remoto (nuvem). Caso o usuário necessite de mais espaço, deverá realizar uma solicitação ao setor de tecnologia e informática;

É expressamente proibido o armazenamento de informações de caráter pessoal, que infrinjam direitos autorais ou que não sejam de interesse da **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG** tanto na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem);

Usuários não devem ter expectativa de privacidade quanto aos arquivos armazenados na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem) da **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG**.

**Acrescentar parágrafo sobre acesso não autorizado à estação de trabalho do servidor.**

O Poder Legislativo Municipal mantém um Registro de Acesso e detalha quais funcionários ou terceiros têm acesso a quais sistemas e informações. O registro também anota quando o acesso foi concedido, quando será restrito (se for temporário), o tipo de dados ou sistema que está sendo acessado e o motivo do acesso.

## **7. CONTROLE DE ACESSO FÍSICO**

O acesso ao Poder Legislativo Municipal é protegido por nossos controles de acesso ao prédio. Isso aumenta a construção, a informação e a segurança dos funcionários e garante que nenhum acesso não autorizado seja possível.

**A CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG**, possui [inserir número e localização dos pontos de entrada / saída] fornecendo acesso ao prédio / escritório, que é protegido por [inserir medidas de segurança (ou seja, trava, CCTV, alarmes, biometria etc.).] resolução

Todas as janelas estão alarmadas e são mantidas trancadas quando o prédio é desocupado.

As janelas abertas durante o dia são protegidas com dobradiças de acesso restrito para impedir o acesso.

Os visitantes são acompanhados o tempo todo durante a visita e recebem um crachá de identificação. Eles também precisam fazer login e logout em nosso registro de acesso e assinar um contrato de confidencialidade. Nos casos em que um visitante é obrigado a carregar qualquer mala (incluindo laptops), reservamo-nos o direito de revistá-lo ao entrar e sair do prédio.

## **8. IDS E CRACHÁS DO USUÁRIO**

**A CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG** adotou crachás de identificação para todos os funcionários, visitantes e terceiros que estão dentro das

dependências do prédio. Esses crachás são específicos daqueles a que estão atribuídos e os IDs ou crachás que não estão em uso são armazenados em uma área segura e trancada.

Os funcionários devem usar o crachá de identificação o tempo todo enquanto estão nas dependências do prédio e não têm permissão para compartilhar ou copiar o crachá. Todos os crachás de identificação recebem um código de verificação de funcionário exclusivo, específico do funcionário e registrado em um Registro de Controle de Acesso. Se um funcionário perder seu ID, seu código será imediatamente desativado e um novo código será atribuído. Os códigos nunca são reutilizados após a desativação.

Os visitantes do Poder Legislativo Municipal recebem “Crachás de identificação do visitante”, que indicam seu nome, empresa, cargo e pessoa responsável.

Os visitantes são acompanhados nas instalações o tempo todo e são obrigados a entrar e sair do prédio, assinar acordos de confidencialidade e são designados a um funcionário do Poder Legislativo Municipal que é responsável por eles durante sua visita.

## **9. DEMISSÕES E FIM DO CONTRATO**

A operação de um processo de desativação imediata de quaisquer credenciais e direitos de acesso no término e a reativação somente é possível mediante solicitação por escrito e autorização [pessoa designada / gerente de TI].

É necessário que os demissionários entreguem seu crachá de identificação antes de sair do edifício e sejam realizadas verificações rigorosas de segurança e pesquisas pessoais. Os IDs impressos são destruídos e, quando aplicável, os IDs eletrônicos são desativados com efeito imediato.

É responsabilidade dos gerentes de linha garantir que os crachás de identificação sejam devolvidos (ou a responsabilidade [da pessoa designada / gerente de TI] no caso de gerentes, visitantes ou terceiros).

Quando um contrato de projeto ou serviço termina, qualquer acesso ou credenciais fornecidas durante o contrato são desativados e quaisquer crachás ou chaves de identificação são devolvidos e assinados novamente no livro de registro.

Nos casos em que um funcionário está de férias anuais, é possível suspender suas credenciais e direitos de acesso e reativar em seu retorno. Isso reduz o risco de pontos de acesso não tripulados, mas também evita a necessidade de redefinir novas credenciais e níveis de acesso. Se uma conta de usuário estiver inativa por 30 dias ou mais, o sistema desabilitará automaticamente o acesso e solicitará que o usuário entre em contato com o Setor de Tecnologia e Informática para resolver.

## 10. PAPÉIS E RESPONSABILIDADES

### 10.1 Gestor Da Informação

É responsabilidade dos colaboradores apontados como Gestor da Informação:

- 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;
- Realizar a revisão periódica de autorizações de acesso e credenciais de acesso a ativos/sistemas de informação sob sua responsabilidade.

### 10.2. Setor de Recursos Humanos

É responsabilidade do Setor de Recursos Humanos:

- Reportar em tempo hábil o desligamento de empregados da **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG** ao setor de tecnologia e informática para que contas de acesso possam ser revogadas;

- Apoiar a gestão de identidades enviando relatórios periódicos sobre colaboradores desligados ou que mudaram de posição na **CÂMARA MUNICIPAL DE BARRA DO GARÇAS - CMBG**;
- Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação fornecendo informações sobre os empregados.

### **10.3. Gestores E Coordenadores**

É responsabilidade dos gestores e coordenadores:

- Solicitar ao setor de tecnologia e informática a concessão de acesso aos novos colaboradores ou aos que necessitem de novos acessos conforme mudanças em suas atividades laborais;
- Solicitar ao setor de tecnologia e informática concessão de acesso a terceiros/prestadores de serviços contratados justificando a necessidade de acesso a ativos/sistemas de informação;
- Informar ao setor de tecnologia e informática quando do encerramento do contrato com terceiros/prestadores de serviços contratados que tenham acesso a ativos/sistemas de informação.

### **10.4. Setor de Tecnologia e Informática**

É responsabilidade do Setor de Tecnologia e Informática:

- Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para usuários de colaboradores, terceiros/prestadores de serviços;

- Conceder, quando autorizado, o acesso aos usuários de colaboradores, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;
- Revogar, quando solicitado, o acesso dos usuários de colaboradores, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;
- Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação dos usuários de colaboradores, terceiros/prestadores de serviço fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação.

## 11. SANÇÕES

As sanções serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

## 12. GESTÃO DOS REGISTROS MANTIDOS COM BASE NESTE DOCUMENTO

Nome do registro	Local de armazenamento	Responsável pelo armazenamento	Controle para a proteção do registro	Tempo de retenção
PLTL-002 – Política de Acesso e senha	Sítio Eletrônico	Comissão de Proteção de Dados Pessoais.	Somente a Comissão de Proteção de Dados Pessoais pode	Indeterminado

			alterar o documento.	
--	--	--	----------------------	--

### 13. VALIDADE E GESTÃO DO DOCUMENTO

Este documento é válido a partir da data de publicação da Resolução que o aprovar.

O proprietário do documento é a Comissão de Proteção de Dados Pessoais, que deve verificar e, havendo a necessidade, atualizar o documento.

### 14. DISPOSIÇÕES FINAIS

Os casos não previstos ou omissos neste documento deverão ser encaminhados para a Comissão de Proteção de Dados Pessoais.

A norma **PLTL-002 – Política de Acesso e Senha** é aprovada pelo Comissão de Proteção de Dados Pessoais e encaminhada ao Plenário da **CÂMARA DE BARRA DO GARÇAS** para votação através de Projeto de Resolução.

A presente norma foi encaminhada ao Plenário no dia 26/08/2024.

### 15. ASSINATURA