

POLÍTICA DE CONTROLE DE ACESSO

Princípios e requisitos

A Política de controle de acesso visa permitir que somente aqueles usuários autorizados para a execução de suas tarefas específicas a área de atribuição, e tem como objetivo minimizar o risco de compartilhamento de dados não autorizados com terceiros e setores não complementares, deixando claro que na Câmara dos Vereadores de Gramado/ RS, a existência de uma gestão de acesso baseada no Cargo ou Setor do servidor público/colaborador.

Essa autorização, preferencialmente, deve ser concedida pelo superior direto de cada colaborador e deve ser baseada no princípio da necessidade. Ou seja, apenas serão permitidos os recursos e permissões estritamente justificáveis para cada função. Adotando essa política, é mitigado o risco de deixar passarem despercebidas permissões inadequadas para algum servidor público/colaborador.

Monitoramento

A movimentação funcional de servidores públicos/colaboradores dentro da **Câmara dos Vereadores de Gramado/ RS**, poderá acontecer por mudanças de cargos, de setor, transferências, demissões etc. Todos esses acontecimentos serão refletidos nas permissões dos usuários.

Logo, periodicamente serão verificados se todos os usuários ativos permanecem na organização. Além disso, existirá uma avaliação se suas permissões de acesso estão de acordo com a função que estão ocupando. Esse processo faz parte do fluxo de trabalho em conjunto com o RH, e notificação aos representantes/ gestor de área.

Conscientização e treinamento

Todos os colaboradores que tiverem acesso a recursos de TI da **Câmara dos Vereadores de Gramado/ RS**, precisam estar cientes de boas práticas de uso, dos riscos aos quais estão suscetíveis e da importância da segurança da informação.

Dentre outras coisas, a **Câmara dos Vereadores de Gramado/ RS**, conscientiza e formaliza com treinamentos periódicos sobre a necessidade de manter suas senhas em sigilo, de não deixarem suas máquinas desbloqueadas quando se ausentarem, etc.

Além disso, são implementadas campanhas com atualizações quanto às novas formas de ciberataques, para que não sejam vítimas de phishing, ransomware, malware ou qualquer outro tipo de vírus.

Controles de acesso abordados

Acesso à internet;

A **Câmara dos Vereadores de Gramado/ RS**, recomenda o uso eficiente da internet para os servidores públicos/colaboradores em função das suas necessidades de realização das suas atividades laborais, porém é vedado o conteúdo impróprio, com fins discriminatórios e sexual, bem como ofensivos.

A **Câmara dos Vereadores de Gramado/ RS**, poderá monitorar a rede para definir as regras de navegação, caso seja necessária em função de suspeita de eventos referente aos relatados nesta política.

Acesso a sistemas;

A **Câmara dos Vereadores de Gramado/ RS**, tem como base o acesso a sistemas compatíveis com a área de atribuição do servidor público/colaborador e cargo, realizando a segregação de informações pertinentes ao setor de atuação do respectivo profissional.

Acesso a arquivos;

A **Câmara dos Vereadores de Gramado/ RS**, tem a mesma base prevista para acesso de sistemas, com exceção para determinação de regras e critérios de acesso às informações do proprietário do recurso.

Em poucas palavras, o proprietário da informação define os usuários que podem acessá-la levando em consideração a boa fé e o legítimo interesse previsto na LGPD (**Lei geral de proteção de dados pessoais.**)

Acesso à rede.

O acesso será realizado pelo administrador da rede levando em consideração as permissões necessárias de cada usuário.

Regras de senha segura

A política de controle de acesso privilegia a obrigatoriedade de boas práticas para criação de senhas seguras. Alguns pontos recomendados são a definição de um número mínimo de **7**

dígitos com caracteres e o uso de letras maiúsculas e minúsculas, números e caracteres especiais.

Além disso, as senhas devem ser alteradas periodicamente a cada 180 dias por padrão e o sistema irá bloquear o uso de combinações repetidas dentro de um período de 12 meses, para as últimas 6 já utilizadas.

Boas práticas no uso de senhas

- Use o bom senso na escolha da senha. Não vai adiantar muito se a sua senha for boa, mas tão complicada que você tem que anotar ela por perto, porque nem você consegue se lembrar.
- Não "**empreste**" a sua senha para ninguém. E isso significa também não compartilhar as suas contas, seja com quem for. Lembre-se sempre que é você quem vai responder por ela, em caso de não conformidades.
- Troque a sua senha periodicamente. Novamente, use o bom senso quanto à periodicidade.
- Troque a senha imediatamente quando necessário. Quando for digitar sua senha, não custa nada dar uma olhada e ver se não tem ninguém observando. Na dúvida, troque!
- Nunca use a mesma senha em outras contas. Assim, as suas outras contas não correrão risco, se uma delas for comprometida. Use senhas bem diferentes e não apenas a mesma senha com uma pequena modificação.
- Não reutilize as suas senhas anteriores.
- Use programas de gerenciamento de senhas.
- Mantenha seu sistema atualizado e livre de malware (vírus, spyware e etc). Muitos deles podem capturar as suas senhas e seus dados, tornando inúteis todos os cuidados que você teve até agora, e colocando em risco todas as suas contas.