

Planalto Capital

DICAS DE SEGURANÇA DA INFORMAÇÃO

Nós da Planalto Capital cuidamos das suas informações com muito cuidado. Possuímos estrutura de informática nos padrões mais modernos e profissionais disponíveis, todas suas informações são criptografadas e o acesso a elas dentro da empresa e na comunicação com outras empresas com as quais nos relacionamos segue procedimentos claros e rigorosos. Nossos colaboradores também monitorados e capacitados constantemente, para evitar ao máximo o risco de algum vazamento. No infeliz caso de qualquer vazamento, seremos o mais transparente e franco possível com você, e faremos nosso melhor para que as falhas não se repitam.

Apesar do nosso esforço, nem tudo está sob nosso controle. Por isso, gostaríamos de passar algumas dicas para você, para evitar que suas informações caiam em mãos erradas:

- Em nenhuma hipótese compartilhe suas senhas com terceiros!
- Troque suas senhas periodicamente, principalmente as senhas de e-mail e de acesso aos seus dados na Planalto.
- Tente sempre usar autenticação de dois fatores, como os *tokens* e códigos de verificação por SMS.
- Use senhas fortes e diferentes para cada serviço. Para diminuir a inconveniência de lembrar várias senhas, recomendamos o uso de aplicativos de gerenciamento de senha, como LastPass, Keeper, RoboForm, ou outro de sua preferência.
- Se em algum momento você precisar trocar o banco que cadastrou com a gente, vamos pedir para você preencher um formulário em papel impresso, assinar e reconhecer a assinatura em cartório. Sim, é inconveniente. Mas alguns inconvenientes nos trazem mais segurança, e acreditamos que este é um procedimento que vale à pena.
- Cuidado com e-mails suspeitos recebidos com o nosso nome. Pode ser alguém mal-intencionado tentando se passar pela gente. Se ficar na dúvida, não hesite em entrar em contato por outro meio de comunicação, como pessoalmente ou por telefone.

No mais, pratique higiene digital: pense duas vezes para clicar em *links* e baixar arquivos que você não conhece, mantenha seus equipamentos sempre atualizados e tente aprender sobre segurança cibernética. Os cuidados mais simples são os mais eficazes!