Guia de Segurança da Informação – Connecta Contabilidade

Introdução

A Connecta Contabilidade trabalha todos os dias com informações muito importantes de seus clientes, como dados pessoais e financeiros.

Um problema de segurança — como um vazamento de dados ou um ataque digital — pode causar prejuízos financeiros e, principalmente, abalar a confiança dos clientes.

Este guia apresenta regras básicas para proteger essas informações, manter a reputação da empresa e garantir que os serviços continuem funcionando mesmo diante de imprevistos.

Controle de Acesso e Uso de Contas

Objetivo: Garantir que cada pessoa acesse apenas o que precisa para trabalhar, com segurança e responsabilidade.

Conta pessoal e exclusiva

Cada funcionário deve ter seu próprio login para acessar os sistemas da empresa. Não é permitido compartilhar contas ou senhas.

Por quê: Isso permite saber quem fez o quê e evita confusões em caso de problemas.

Senhas seguras e verificação em dois passos

As senhas devem ter pelo menos 12 caracteres. Além disso, é obrigatório usar uma verificação extra (como um código enviado por SMS ou aplicativo) para acessar sistemas pela internet.

Por quê: Mesmo que alguém descubra a senha, não conseguirá entrar sem essa segunda verificação.

Acesso limitado por função

Cada pessoa terá acesso apenas aos arquivos e sistemas que precisa para realizar seu trabalho.

Por quê: Se uma conta for invadida, o acesso restrito ajuda a evitar que dados importantes sejam expostos.

Desativação de contas ao sair da empresa

No último dia de trabalho, todas as contas do funcionário devem ser bloqueadas até o fim do expediente.

Por quê: Isso evita que ex-funcionários acessem sistemas ou informações da empresa.

Uso de Celulares, Notebooks e Redes

Objetivo: Proteger os dados da empresa fora do escritório e evitar riscos à rede interna.

Uso de aparelhos pessoais

É permitido usar o celular pessoal para acessar e-mail e calendário da empresa, desde que:

- Tenha senha ou desbloqueio por digital
- Esteja com o sistema atualizado
- Tenha um aplicativo que permita apagar os dados da empresa remotamente em caso de perda ou roubo

Por quê: Se o aparelho for perdido, é possível apagar os dados à distância e evitar vazamentos.

Conexão segura à internet

Não é permitido usar redes públicas (como de cafés ou aeroportos) com o notebook da empresa sem uma conexão segura (VPN).

Por quê: Redes abertas podem ser usadas por invasores para interceptar informações.

Separação das redes no escritório

Devem existir duas redes Wi-Fi:

- Uma exclusiva para os equipamentos da empresa
- Outra para celulares pessoais e visitantes

Essas redes não devem se comunicar.

Por quê: Se um aparelho pessoal estiver infectado, isso evita que o problema se espalhe para os sistemas da empresa.

Como Agir em Caso de Problema de Segurança

Objetivo: Ter um plano claro para agir rapidamente e reduzir prejuízos.

Relatar imediatamente, sem punição

Se alguém clicar em um link suspeito ou notar algo estranho, deve avisar o responsável de TI na hora.

Por quê: Quanto mais rápido o problema for identificado, menor o risco de se espalhar.

Isolar o equipamento

Se um computador estiver comprometido, ele deve ser desconectado da internet, mas mantido ligado.

Por quê: Isso ajuda na investigação, pois mantém informações importantes na memória do aparelho.

Comunicação oficial

Em casos graves, como vazamento de dados, apenas o responsável designado pode falar com clientes ou parceiros.

Por quê: Isso evita confusão e garante que as informações sejam passadas com clareza.

Cópias de Segurança e Recuperação

Objetivo: Garantir que os dados possam ser recuperados e que a empresa volte a funcionar rapidamente após qualquer problema.

Regra das 3 cópias

Todos os dados importantes devem seguir esta regra:

- Ter 3 cópias
- Usar 2 tipos de armazenamento diferentes (por exemplo, servidor e HD externo)
- Manter 1 cópia fora do escritório, de preferência na nuvem

Por quê: Isso protege contra falhas de equipamentos, acidentes e ataques digitais.

Backup na nuvem

Além das cópias locais, deve haver um serviço específico para salvar e-mails e arquivos na nuvem.

Por quê: Evita perda de dados por erro humano, como exclusão acidental.

Testes regulares de recuperação

A cada três meses, o responsável de TI deve testar a recuperação de arquivos.

Por quê: Ter backup não basta — é preciso garantir que ele funcione quando for necessário.

Considerações Finais

Essas regras são o primeiro passo para uma cultura de segurança sólida.

Para que tudo funcione bem, é essencial:

- Investir em ferramentas adequadas (verificação em dois passos, VPN, backup)
- Realizar treinamentos regulares com os funcionários sobre segurança digital e boas práticas