Cibersegurança nos gabinetes de contabilidade: checklist para proteger os dados dos clientes

A cibersegurança é essencial para proteger os dados dos clientes e reduzir o risco de incidentes num gabinete de contabilidade.

Sabe até que ponto o seu gabinete está protegido?

Use esta checklist para fazer um autodiagnóstico rápido e identificar os aspetos que deve rever ou melhorar.

Responda a cada questão com **Sim, Parcialmente ou Não.**

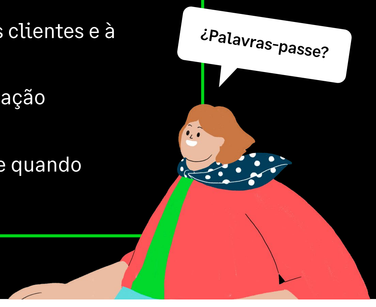


Governação e sensibilização

- Existe uma pessoa responsável pelo acompanhamento da cibersegurança?
- Estão identificados os sistemas, os dados e os fornecedores tecnológicos críticos?
- As medidas de segurança são revistas anualmente e após alterações relevantes?

Acessos e palavras-passe

- Cada colaborador utiliza uma conta individual e acede apenas aos clientes e à informação de que necessita?
- As palavras-passe são robustas e não são reutilizadas, e a autenticação multifator está ativa nos acessos críticos?
- Os acessos são revistos regularmente e eliminados imediatamente quando um colaborador muda de funções ou sai do gabinete?



Equipamentos e sistemas



- Os computadores, dispositivos, sistemas operativos e aplicações são atualizados regularmente?
- Os equipamentos têm proteção antimalware, bloqueio automático e outras medidas de segurança adequadas?
- Os dados críticos têm cópias de segurança regulares, separadas do ambiente principal e cuja recuperação é testada?

Dados dos clientes

- Os documentos dos clientes estão centralizados num local seguro e com as versões controladas?
- Os dados são partilhados através de canais controlados e os pedidos ou instruções anormais são confirmados por outro meio?
- Existe um procedimento para conservar e eliminar documentos quando deixam de ser necessários?

Pessoas e resposta a incidentes

- A equipa recebe formação periódica sobre phishing, fraude e outras ameaças digitais?
- Os colaboradores sabem quem contactar e o que fazer imediatamente perante um possível incidente?
- Existe um plano que defina como proteger contas e equipamentos, identificar os clientes afetados e assegurar a continuidade do gabinete?

E agora?

Quanto mais respostas “Não” ou “Parcialmente” obtiver, maior deve ser a prioridade dada à revisão das práticas de cibersegurança do seu gabinete.

Use os resultados para definir ações concretas, atribuir responsáveis e acompanhar regularmente a evolução.



Sage