Logos

Recursos · Material para baixar

Checklist de preparação para due diligence

Uma lista para conferir antes de receber o próximo questionário de segurança de um cliente. Sem cadastro.

1. Quem cuida

- [ ] Uma pessoa dona dos questionários de clientes
- [ ] Quem aprova o conteúdo técnico e quem aprova o que tem efeito de contrato
- [ ] Prazo interno para responder, combinado com a área comercial

2. Documentos

Aprovados, datados, com responsável

- [ ] Política de segurança da informação
- [ ] Controle de acesso
- [ ] Cópias de segurança e recuperação
- [ ] Resposta a incidentes, com prazos de aviso a clientes
- [ ] Continuidade de negócios
- [ ] Desenvolvimento seguro (se desenvolve software)
- [ ] Gestão de fornecedores
- [ ] Privacidade e proteção de dados pessoais

3. Evidências

Atuais

- [ ] Autenticação em dois fatores nos acessos administrativos e remotos
- [ ] Revisão periódica de acessos, com registro
- [ ] Teste de restauração de cópia de segurança, com data
- [ ] Teste de invasão recente, com resumo executivo que possa ser compartilhado
- [ ] Treinamento de segurança dos funcionários, com registro
- [ ] Inventário de sistemas e de onde ficam os dados

4. Privacidade

- [ ] Papel definido por produto ou serviço: controlador ou operador
- [ ] Registro das operações de tratamento
- [ ] Encarregado ou contato de privacidade
- [ ] Lista de subprocessadores, com país
- [ ] Mecanismo usado se os dados saem do Brasil
- [ ] Procedimento de devolução e eliminação de dados no fim do contrato

5. Contrato

- [ ] Minuta de acordo de tratamento de dados
- [ ] Prazo de aviso de incidente que você consegue cumprir

6. Respostas

- [ ] Base de respostas por assunto, com evidência e data de revisão
- [ ] Registro do que foi enviado a cada cliente
- [ ] Certificados e relatórios disponíveis, com as regras de compartilhamento

7. Página de segurança

- [ ] O que é público, o que é sob pedido e o que nunca sai (ver o guia de Trust Center)
- [ ] Contato para aviso de vulnerabilidade
