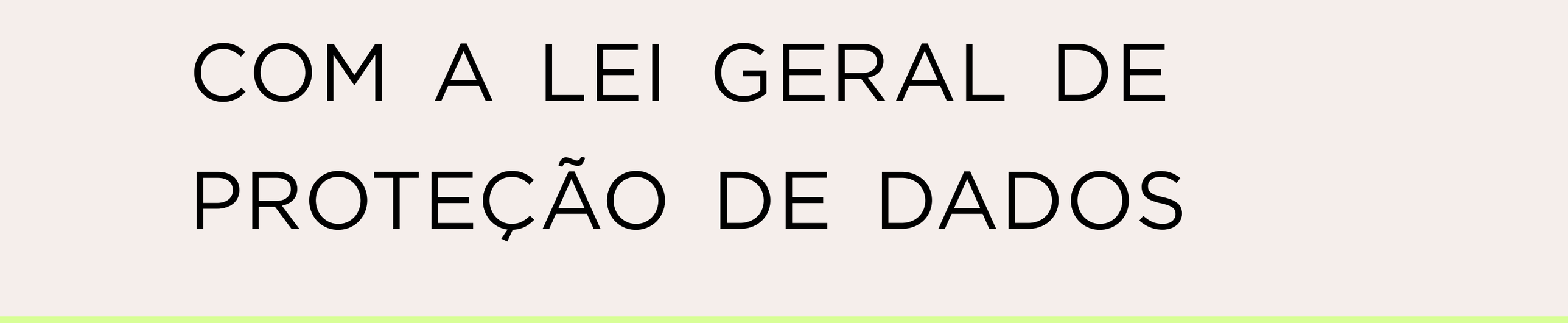
eBooks | F&CSP

CHECKLIST LGPD PARA PEQUENAS EMPRESAS

PASSO A PASSO PARA SE MANTER EM DIA COM A LEI GERAL DE PROTEÇÃO DE DADOS

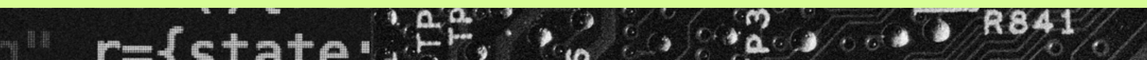


INTRODUÇÃO

O tratamento de dados pessoais se refere a qualquer operação realizada com informações pessoais que envolva coleta, produção, transmissão, distribuição, processamento, armazenamento, eliminação, avaliação, modificação, difusão etc.

Para uma empresa, isso abrange uma série de elementos sobre empregados e clientes, tais como: origem, etnia, raça, religião, opinião política, filiação a sindicato ou organização religiosa ou política, saúde e vida sexual, além dos dados genéricos e biométricos. Lembre-se de que vários deles são caracterizados como sensíveis – por terem uma proteção especial na Lei Geral de Proteção de Dados (LGPD) – e seguem regras mais rigorosas quanto ao seu tratamento.

Confira, a seguir, as medidas de uso interno para empresas, com um *checklist* para facilitar a visualização das sugestões em relação a treinamento de empregados, segurança no armazenamento, controle de acesso a sistemas e muito mais!



A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PODE SER SIMPLES

Crie uma política interna de proteção para garantir que os dados de clientes e funcionários armazenados pela empresa permaneçam confidenciais e íntegros (sem alterações não intencionais) e que estejam disponíveis a seus titulares, de modo que possam solicitar alterações ou sua exclusão. Esta política, no geral, trata das práticas de gestão da segurança reunidas nos tópicos a seguir.

Mesmo que o negócio tenha pouquíssimos departamentos, saiba como cada um utiliza dados pessoais e com qual finalidade.

Identifique potenciais riscos a dados pessoais, quais deles são danosos e quais são as vulnerabilidades nos sistemas ou equipamentos.

Faça este gerenciamento de riscos periodicamente, já que se trata de uma das garantias de que existe comprometimento com as boas práticas.

Mantenha softwares atualizados e utilize antivírus completos – estas são ações que podem tornar o processo mais simplificado.

> *A atualização constante certificará que a empresa se mantém em dia com as correções de segurança liberadas pelos desenvolvedores. É importante que os funcionários não desativem nenhum aplicativo de defesa.*

Lembre-se de conferir se há senhas sendo divididas/compartilhadas. Caso positivo, crie senhas individuais nas estações de trabalho e proíba o compartilhamento delas.

Impeça o acesso não autorizado a dados pessoais de clientes ou empregados, assim como o compartilhamento indevido – ambos são riscos graves que precisam ser evitados.

Quando se trata de dados sensíveis, garanta que o acesso seja restrito e mantenha uma cópia de segurança, pois a sua exclusão indevida também pode gerar problemas.

De forma prática, uma das observações fundamentais a se fazer, por exemplo, é como são armazenados os currículos que chegam, por que estão sendo guardados, quem na empresa tem acesso e se estas pessoas realmente precisam ou devem acessá-los – lembre-se de que elas também estão obrigadas a garantir a segurança.

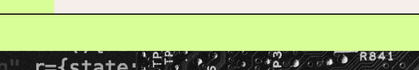
TREINAMENTOS INTERNOS SÃO VALIOSOS

Mesmo que não haja um departamento de Recursos Humanos (RH) próprio, organize treinamentos de conscientização aos empregados sobre suas obrigações relacionadas ao tratamento de dados pessoais.

> *Uma das coisas a se observar, por exemplo, é quando o funcionário pedir algum documento do consumidor para realizar um cadastro. Neste caso, ele precisa entender e explicar ao cliente exatamente o seu propósito e, ainda, como este perfil poderá ser apagado eventualmente.*

De modo geral, o treinamento precisa englobar as orientações a seguir:

- Não se deve deixar documentos físicos com dados pessoais sobre as mesas, mas guardados com segurança.
- Deve-se bloquear o computador quando se sai da mesa de trabalho.
- Como utilizar o antivírus e a importância de mantê-lo sempre atualizado.
- Como evitar contaminação e ataques na rede.
- Como utilizar os controles de segurança dos sistemas de Tecnologia da Informação (TI) relacionados aos trabalhos diários.
- Não se deve compartilhar senhas e logins (tampouco deixar senhas salvas).
- Quais sites podem ser abertos (ou não) nos computadores corporativos.
- Quais os limites de uso pessoal da rede (por exemplo: se o empregado deve clicar em links e pop-ups de ofertas que chegam por e-mail. Lembre-se de que existe o risco de esses links conterem vírus e ataques para roubo de dados).
- Incentive os empregados a relatar quaisquer incidentes ou vulnerabilidades.



ATENÇÃO REDOBRADA AOS CONTRATOS

- [ ] A ANPD recomenda que os funcionários assinem termos de confidencialidade como um compromisso de não divulgar informações confidenciais que envolvam dados pessoais.

- [ ] Quando se trata do relacionamento com fornecedores, veja se nos contratos de serviços, de fornecimento ou de aquisições estejam especificadas as funções e as responsabilidades de cada um quanto à proteção de dados.

  Isso engloba, nos termos contratuais, regras para fornecedores e parceiros, de compartilhamento, de relações sobre quem controla os dados e quem é operador, além de orientações sobre o tratamento correto das informações.

- [ ] Confira se nos contratos consta a proibição para tratamentos de dados que utilizem métodos incompatíveis com as orientações do controlador (a empresa que detém os dados e que toma as decisões sobre eles).

- [ ] Se houver contrato com terceiro para descarte de papéis, dispositivos ou mídias físicas com dados pessoais, certifique-se de que haja cláusula de registro da destruição realizada.

O CONTROLE DE ACESSO AO SISTEMA DA EMPRESA DEVE SER COMPLETO

Caso a pequena empresa conte com uma rede interna de computadores, o ideal é que o gestor implemente um sistema de controle de acesso e o aplique a todos os usuários com login – jamais permitindo o compartilhamento de contas. Veja com o fornecedor do serviço se é possível realizar os procedimentos a seguir:

- [ ] O sistema precisa ter autenticação de quem acessa o sistema, isto é, logins e senhas individuais que não sejam repetidas.

  *Recomenda-se impedir a criação de senhas que contenham o nome do usuário ou que não tenham um determinado nível de complexidade. Utilize letras maiúsculas e minúsculas, caracteres especiais (#, *, @), números e uma quantidade mínima de caracteres (geralmente, pede-se ao menos dez).*

- [ ] Crie níveis de permissão a todos os usuários, veja quais realmente precisam acessar dados pessoais.

  Alguns colaboradores podem ser liberados para criação, aprovação, revisão e exclusão de contas de usuários. O mais adequado é que cada um só tenha acesso ao que realmente precisa em suas atividades, e nada além disso. O acesso total deve ser bem restrito.

- [ ] Evite o uso das senhas preestabelecidas pelos fornecedores.

- [ ] Tenha, dentro do sistema, um mecanismo de registro ou auditoria de cada alteração realizada e qual usuário a efetuou.

- [ ] Não permita que as configurações de segurança dos seus sistemas sejam reduzidas, ignoradas ou desativadas pelos usuários.

- [ ] A ANPD sugere o uso de autenticação multifatorial, com códigos de segurança enviados por SMS ou e-mail.

- [ ] Caso o acesso seja feito pelos notebooks e smartphones, utilize os mesmos procedimentos de controle de acesso, principalmente os multifatoriais. Importante: para armazenamento e tratamento de dados pessoais, utilize preferencialmente as máquinas da empresa, com antivírus instalado e atualizado frequentemente.

  Computadores de uso privado dos funcionários são mais vulneráveis, pois podem conter aplicativos de origem desconhecida, antivírus sem licença legal, bem como programas "crackeados" (cracks são softwares utilizados para quebrar um sistema de segurança, geralmente visando a liberar acesso indevido a programas pagos).

- [ ] Serviços nas nuvens também exigem cuidados específicos, tais como contratos com as garantias de segurança do armazenamento de dados, regras e controle para acesso pelos usuários e autenticação multifatorial.

OS CUIDADOS COM O ARMAZENAMENTO DE DADOS

Atualmente, é comum pedir e guardar dados pessoais de clientes que poderão ter serventia futura. Este é um comportamento que precisa ser corrigido para garantir mais segurança à empresa.

- [ ] Colete e armazene apenas os dados pessoais que forem realmente necessários para utilização imediata e concreta, ou seja, aqueles que sejam úteis naquele momento. Não peça informações sem saber qual será o uso (princípio da finalidade).

- [ ] Se for armazenar os dados pessoais, garanta que os usuários não possam ser identificados facilmente, ou faça uso da criptografia.

- [ ] Impeça a transferência de informações pessoais das estações de trabalho para outras máquinas, smartphones, pendrives ou HDs externos não autorizados.

- [ ] Faça backups regularmente e armazene-os em dispositivos diferentes das máquinas ou dos equipamentos principais, e guarde-os em locais seguros. Evite que as cópias sejam sincronizadas online, de modo a não sofrer ataques ou perdas.

- [ ] Se for eliminar algum dispositivo com dados pessoais, não se esqueça de formatar a memória, HD ou SSD, antes do descarte. Destrua papéis, CDs e DVDs antes de descartá-los.

TENHA SEGURANÇA NA COMUNICAÇÃO POR E-MAIL E MENSAGEM

- [ ] Certifique-se de que os e-mails do RH, com dados sobre pagamentos, prontuários etc., sejam cifrados. Utilize conexões cifradas (TLS/HTTPS) ou aplicativos de criptografia total.

- [ ] Proteja os e-mails com serviços antispam, antivírus integrados e filtros. Utilize *firewalls* nos computadores ou nos serviços em rede (*Web Application Firewall* – WAF).

- [ ] Não permita conexão em redes não confiáveis.

- [ ] Remova dados pessoais ou sensíveis que estejam desnecessariamente acessíveis na rede pública da empresa.

- [ ] Confirme se os dados pessoais nos smartphones e computadores portáteis da empresa podem ser apagados remotamente. Isso é essencial para evitar incidentes.

Trata-se de uma lista longa de tarefas. Contudo, é bom ter em mente que os padrões de segurança de dados vieram para ficar. O lado positivo é que uma empresa que consiga adaptar essas práticas à própria realidade – e viabilizá-las no dia a dia – terá implementado a própria política de segurança da informação, e isso certamente já é um fator determinante na escolha do consumidor.

Fique por dentro de todas as novidades que impactam a sua empresa e de orientações essenciais para o seu negócio. Acompanhe o ***Portal FecomercioSP*** e conheça o ***Fecomercio Lab***.

Acesse os podcasts da FecomercioSP no Spotify e no SoundCloud.

SoundCloud

Spotify

FECOMERCIOSP

PUBLICAÇÃO DA FEDERAÇÃO DO COMÉRCIO DE BENS, SERVIÇOS E TURISMO DO ESTADO DE SÃO PAULO

Rua Dr. Plínio Barreto, 285

Bela Vista • São Paulo

11 3254-1700 • fax 11 3254-1650

www.fecomercio.com.br

PRODUÇÃO TUTU NOVEMBRO 2021