CARTÓRIO

PORTO NACIONAL

Serviço do 2º tabelionato de notas, de protestos de títulos,
registro de pessoas jurídicas e títulos e documentos

Lei Geral de Proteção de dados

e comportamentos para a proteção de dados no cartório

Lei Geral de Proteção de Dados (Lei nº 13.709) tem como objetivo garantir a transparência no uso dos dados das pessoas físicas em quaisquer meios.

Foi sancionada em 14 de agosto de 2018 e entrou em vigor em 16 de agosto de 2020.

PROVIMENTO 134/22 CNJ

1. Nomear encarregado pela proteção de dados;
2. Mapear atividades de tratamento e realizar seu registro;
3. Elaborar relatório de impacto e risco das atividades o faça necessário;
4. Adotar medidas transparência aos usuários sobre o tratamento de dados pessoais;
5. Definir implementar Política de Segurança da Informação;
6. Definir implementa Política Interna de Privacidade e Proteção de Dados;
7. Criar procedimentos internos eficazes, gratuitos, e de fácil acesso para atendimento aos direitos dos titulares;
8. Zelar para que terceiros contratados estejam em conformidade com a LGPD;
9. Treinar e capacitar os prepostos.

O QUE VOCÊ PRECISA SABER SOBRE ESSA LEI PARA TRABALHAR NO CARTÓRIO?

BASES LEGAIS **PARA TRATAMENTO DE DADOS PESSOAIS**

1. Consentimento;
2. Cumprimento de obrigação legal;
3. Execução de políticas públicas;
4. Estudos por órgãos de pesquisa;
5. Execução de contrato;
6. Exercício regular de direitos;
7. Proteção da vida;
8. Tutela da saúde;
9. Interesses legítimos do controlador;
10. Proteção ao crédito.

- Lei 8935/94
- Lei 6015/74 de Registros públicos
- Protestos Lei 9.492/97
- Atos digitais Prov. nº 100/2020 CNJ
- Provimento n.º 50/2015 do CNJ – temporalidade
- Apostilamento Art. 6º, II, Resolução CNJ nº 228/16
- Atas notariais para usucapião Art. 216-A, I, Lei nº 6.015/73 e Atas Notariais Art. 7º, III, Lei nº 8.935/94 e Prov. CNJ nº 100/2020.
- Administrativo - Para o cumprimento de obrigação contratual, legal, administrativa ou regulatória.
- Cópias autenticadas Art. 7º, V, Lei nº 8.935/94 e Prov. CNJ nº 100/2020.
- Abertura de cadastro em notas Art. 7º, IV, Lei nº 8.935/94 e Prov. CNJ nº 100/2020.
- CENSEC - Central Notarial de Serviços Eletrônicos Compartilhados (Provimento CNJ nº 18/12, art. 7º);
- Secretaria da Receita Federal - Art. 962 da CNNR e Instrução Normativa RFB nº 1.112/10;
- COAF (Conselho de Controle de Atividades Financeiras) –Provimento nº 88/2019-CNJ;
- Secretaria de Coordenação e Governança do Patrimônio da União - envio mensal da Declaração sobre Operações Imobiliárias em Terrenos da União (DOITU), conforme normas estabelecidas pela Portaria SPU/ME nº 24.218, de 26 de novembro de 2020;

O QUE SÃO DADOS PESSOAIS?

Dados pessoais:

- ✓ Nome
- ✓ Endereço
- ✓ Número de identificação
- ✓ Dados de localização
- ✓ Identificadores eletrônicos (e-mail, endereço de IP)
- ✓ Geolocalização
- ✓ Número de telefone e dados de conexão

Dados pessoais sensíveis:

- ✓ Origem racial ou étnica
- ✓ Opiniões políticas
- ✓ Convicções religiosas ou filosóficas
- ✓ Filiação sindical
- ✓ Dados genéticos
- ✓ Dados biométricos tratados simplesmente para identificar um ser humano
- ✓ Dados relacionados à saúde
- ✓ Dados relativos à vida sexual ou orientação sexual

ONDE VOCÊ TRATA DADOS PESSOAIS NO CARTÓRIO?

- Recepção
- Cadastro
- Reprodução
- Arquivamento por temporalidade (como? onde? Quem?)
- Trânsito por diversos meios físicos e eletrônicos
- Envio para outros órgãos
- Compartilhar cadastro
- Eliminação

QUEM É QUEM NA LEI E TODOS SÃO TITULARES DE DADOS PESSOAIS?

O QUE É TRATAMENTO DE DADOS E O QUE TEM A VER COM O CARTÓRIO?

SEGURANÇA DA INFORMAÇÃO:

MAPEAMENTO - INVENTÁRIO DE DADOS PESSOAIS

- ✓ Finalidade do tratamento de dados
- ✓ Categoria e dados pessoais e descrição dos dados nas respectivas atividades
- ✓ Identificação da forma/coleta de dados
- ✓ Base legal da coleta
- ✓ Descrição da categoria dos titulares
- ✓ Se compartilha com terceiros
- ✓ Categoria de destinatários
- ✓ Prazo de conservação
- ✓ Medidas de segurança organizacionais
- ✓ Atualizar sempre que necessário, não podendo ultrapassar um ano o inventário dos dados
- ✓ Arquivar o inventário de dados pessoais e disponibilizá-lo em caso de solicitação da CGJ ou ANPD

O QUE É TRATAMENTO IRREGULAR DOS DADOS

1. Desrespeitar um dos Princípios de tratamento de dados da LGPD
2. Art. 44 – Não fornecer a segurança que o titular pode esperar.
3. Art. 46 – Não adotar as medidas técnicas mínimas para assegurar a segurança dos dados contra vazamentos.
4. Desrespeitar os direitos dos titulares sem base legal.
5. Quebrar o sigilo de titulares de dados pessoais (clientes e funcionários)

PRINCIPAIS ELEMENTOS DO COMPLIANCE

- Código de ética
- Educação digital corporativa
- Política de Privacidade e Proteção de dados
- Canal de denúncias
- Análise de riscos
- Relatório de não conformidade
- Auditoria
- Cultura de Proteção de dados pessoais
- Treinamentos

O QUE É UM ATO DE INFRAÇÃO?

No contexto da Lei Geral de Proteção de Dados (**LGPD**), um **incidente** de segurança da informação pode ser compreendido como acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados pessoais.

COMPLIANCE E SEGURANÇA DA INFORMAÇÃO

Existem várias ações para assegurar ou mitigar riscos de vazamento de informações

1. Regulamento Interno de Segurança da Informação: atribuição de responsabilidades, direitos, expectativas de acesso, penalidades e criação de uma cultura de proteção aos sistemas. Conheço as regras e sei que o controle existe.
2. Termos de responsabilidade com a LGPD- conheço as regras, meus direitos e responsabilidades. Sei que o controle existe.
3. Consciência – o obvio pode não ser tão obvio.

PRINCÍPIOS

1. A informação produzida ou recebida como resultado do seu trabalho pertencem ao seu trabalho. novas medidas de segurança, técnicas e administrativas, aptas a proteger os DADOS PESSOAIS entram na rotina de trabalho para EVITAR PERDAS, DESTRUIÇÃO, ALTERAÇÃO OU VAZAMENTO – PROTEÇÃO DOS DADOS.
2. A segurança da informação depende de pessoas comprometidas, processos gerenciais de controle e sistemas de segurança da informação.
3. Divulgar informações confidenciais ou estratégicas é crime previsto nas leis de propriedade intelectual, industrial (Lei nº 9279) e de direitos autorais (Lei nº 9610).

PARA QUE SERVE A SEGURANÇA DA INFORMAÇÃO?

Se as informações são o novo petróleo, temos que protegê-lo.

U$ 0,50 centavos de dólar um criminoso compra na internet carteiras de identidade, credenciais de acesso. Por U$ 30 pode se ter prontuários médicos e passaportes com foto, digitais.

DE ONDE VEM A AMEAÇA?

- Hackers
- Criminosos comuns
- Líderes ignorantes
- Fornecedores ignorantes
- Funcionários insatisfeitos
- Funcionários ignorantes
- Concorrentes
- Governos
- Fenômenos meteorológicos
- Roubos
- Erros operacionais

DANOS DE UM VAZAMENTO OU INCIDENTE - COMPORTAMENTOS

- Violação de informações confidenciais e estratégicas
- Exposição de dados de clientes, funcionários e terceiros
- Comprometimento da reputação da instituição e gestores
- Comprometimento da continuidade do negócio
- Prejuízos financeiros (indenizações e multa, restabelecimento da segurança, identificação dos envolvidos, processos).
- Risco à segurança física e emocional dos envolvidos e terceiros.

QUAL É O PLANO DE RESPOSTA SE ACONTECER UM INCIDENTE ENVOLVENDO DADOS PESSOAIS

Titulares, seus prepostos, contratados ou terceiros que tratam dados pessoais em nome do titular poderão se deparar com incidentes de segurança que acarretam a violação de dados ou a suspeita de violação.

↓

O que deverá ser feito se detectado um incidente de segurança?
*** Prespostos e operadores deverão comunicar o controlador imediatamente.**
*** Registrar e comunicar o controlador*****

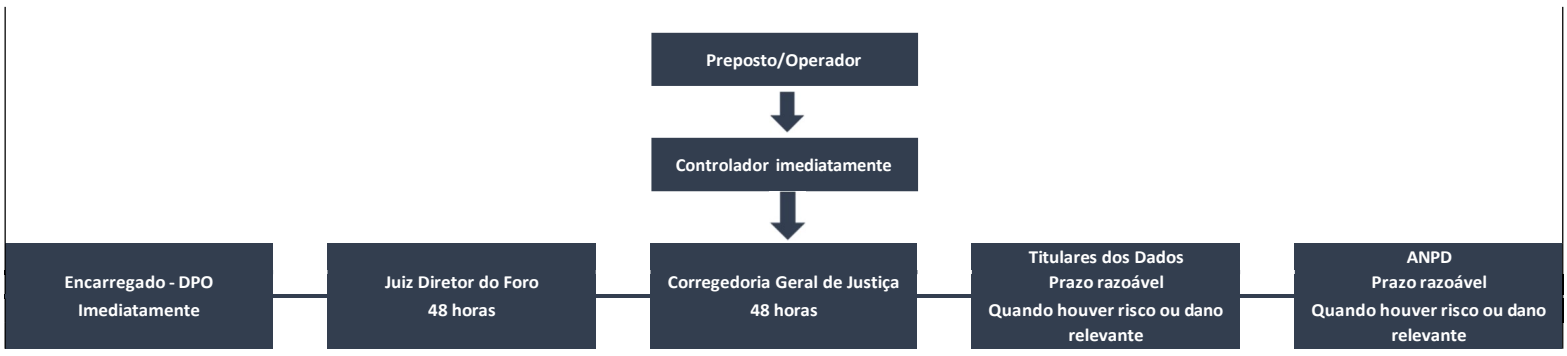
↓

O que o controlador deverá fazer?
*** Determinar se o incidente de fato ocorreu ou se foi apenas uma suspeita.**
*** Determinar a gravidade do incidente e se houve violação de dados pessoais.**
*** Comunicar imediatamente o encarregado.**

↓

Comunicar
*** O Juiz Diretor do Foro e o CGJ no prazo de 48 horas**
*** A ANPD - prazo razoável, quando houver risco ou dano relevante aos titulares de dados**
*** Os titulares de dados - prazo razoável, quando houver risco ou dano relevante aos titulares de dados**

PLANO DE RESPOSTA A INCIDENTES



ANPD

A ANPD (Autoridade Nacional de Proteção de Dados) é o órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no Brasil.

Para exercer este importante papel, a autoridade possui autonomia técnica e decisória assegurada por lei.

PENALIDADES

SANÇÕES ADMINISTRATIVAS

Aplicação de sanções administrativas, civis ou penais definidas em legislação específica.

- Advertência ou até mesmo a proibição total ou parcial de atividades relacionadas ao Tratamento de Dados Pessoais.
- Publicação da infração após devidamente apurada e confirmada a sua ocorrência.
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização.
- Eliminação dos dados pessoais a que se refere a infração.

MULTAS

- **2% do faturamento da empresa,** grupo ou conglomerado no Brasil no seu último exercício.
- Limitado a **R$ 50 milhões,** por infração.

QUAL É O PAPEL DE CADA UM NO PROCESSO?

CONTROLADOR E DPO

- CUMPRIR O PROVIMENTO 134/22 CNJ

FUNCIONÁRIOS

- CUMPRIR AS POLÍTICAS INTERNAS E OS PRINCÍPIOS DA LGPD
- CONTRIBUIR PARA A CULTURA DE PROTEÇÃO DE DADOS

PROTEÇÃO DE DADOS É ESSÊNCIA DA ÁREA DE SEGURANÇA

PILARES DA SEGURANÇA DA INFORMAÇÃO?

1. CONFIDENCIALIDADE – Primeira premissa da segurança das informações em empresas e agora entre pessoas físicas.
2. INTEGRIDADE – Com a era digital, tudo pode ser manipulado. É preciso assegurar que os dados sejam íntegros.
3. DISPONIBILIDADE – Dados devem ser disponíveis para que a empresa possa utilizar e atualizar. Medidas como backup, organização.

PILARES DA SEGURANÇA DA INFORMAÇÃO?

1. A informação produzida ou recebida como resultado do seu trabalho pertence ao seu trabalho. novas medidas de segurança, técnicas e administrativas, aptas a proteger os DADOS PESSOAIS entram na rotina de trabalho para EVITAR PERDAS, DESTRUIÇÃO, ALTERAÇÃO OU VAZAMENTO – PROTEÇÃO DOS DADOS.
2. A segurança da informação depende de pessoas comprometidas, processos gerenciais de controle e sistemas de segurança da informação.
3. Divulgar informações confidenciais ou estratégicas é crime previsto nas leis de propriedade intelectual, industrial (Lei nº 9279) e de direitos autorais (Lei nº 9610).

COMPORTAMENTOS PARA A PROTEÇÃO DE DADOS PARA COLABORADORES

1) Respeitar as diretrizes da Política de Segurança da Informação.
2) Responder pelo uso exclusivo e intransferível de suas senhas de acesso e certificados digitais.
3) Fazer log-off ao se afastar da máquina é tão importante quanto guardar os documentos físicos ao se afastar do seu posto de trabalho.
4) Ativar suas senhas de proteção para Correio Eletrônico e Sistema Operacional, sob orientação do Gestor de Liberações da área de TI;
5) Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software.
6) Relatar prontamente ao Gestor (DPO) e à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus etc;
7) Assegurar que as informações e dados de propriedade do seu trabalho não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável hierárquico.
8) Relatar para o seu responsável hierárquico e à Gestão – DPO-, o surgimento da necessidade de um novo software para suas atividades.
9) Responder prejuízo ou dano que vier a provocar a organização ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas ou dos princípios da Lei Geral de Proteção de Dados.
10) É obrigatório armazenar os arquivos inerentes ao trabalho no servidor de arquivos para garantir o backup de dados.
11) É proibida a abertura de computadores para qualquer tipo de reparo, seja em departamentos ou laboratórios. Caso seja necessário o reparo, este deverá ser feito pelo departamento técnico da área de infraestrutura de TI que tenha contrato de prestação de serviços e compromisso com a LGPD.
12) Não envie informações de trabalho para o seu e-mail pessoal.
13) Ao colaborador não é permitido tirar fotografias das dependências e de nenhum documento ou tela de computador.
14) Não salve informações de trabalho no seu pendrive.
15) O resultado do seu trabalho é propriedade do Tabelionato.

16) Não coloque os documentos em risco.

17) Mantenha o seu WhatsApp limpo de dados pessoais de clientes com regularidade.

18) Revise o código de conduta do Tabelionato para conhecer as boas práticas de comunicação.

19) Dados pessoais armazenados nos servidores e computadores do Cartório (ex.: Fotos, vídeos, documentos etc.) não são de responsabilidade do Cartório.

COMPORTAMENTOS PARA A PROTEÇÃO DE DADOS DOS LÍDERES

1. Quando um colaborador é transferido entre departamentos, o LÍDER que o transferiu deve certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança ainda serão necessários na sua nova função e informar a equipe de infraestrutura de TI qualquer modificação necessária.

2. Quando um funcionário for demitido, o líder responsável deve informar, à equipe Gestão, ao DPO e à equipe de infraestrutura de TI, a desativação dos acessos do colaborador a qualquer recurso de rede e sistemas/aplicativos.

3. Haverá troca de senhas de contas de uso comum ao departamento, evitando o acesso às informações. Além disso, o DPO deverá informar o que deverá ser feito com o e-mail deste usuário: deletar, backup e, caso necessário, para quem deverá ser redirecionado, assim como o WhatsApp.

4. Apoiar e zelar pelo cumprimento desta POLÍTICA DA SEGURANÇA DA INFORMAÇÃO, servindo como modelo de conduta para os colaboradores sob a sua gestão e auditoria.

5. Atribuir na fase de contratação e de formalização dos contratos individuais de trabalho CLT, prestação de serviços ou de parceria, a responsabilidade do cumprimento da POLÍTICA DA SEGURANÇA DA INFORMAÇÃO.

6. Autorizar o acesso e definir o perfil do colaborador junto ao gestor de liberações da área de infraestrutura de TI.

7. Autorizar as mudanças no perfil do colaborador junto ao gestor de liberações da área de infraestrutura de TI.

8. Conscientizar os colaboradores sobre os princípios e procedimentos de Segurança da Informação. Tão importante quanto o treinamento do trabalho em si, a LGPD e a cultura de proteção de dados devem ser atualizados na equipe.

PÚBLICA:

São informações que podem ser adicionadas, inclusive, no site e mídias sociais da empresa.

CONFIDENCIAL:

Informações de acesso exclusivo para cargos de confiança, tais como o departamento financeiro, direção e gestores. Ex.: Planejamento Estratégico, dados financeiros, orçamentos, painel de pilotagem, dados pessoais destinados ao DP.

INTERNA:

Informações de uso exclusivo para quem trabalha na serventia e manuseia esses dados em suas atividades laborais. Essas informações também são divididas em níveis de acesso, conforme a descrição de cargo.

COMPORTAMENTOS PARA A PROTEÇÃO DE DADOS DA ÁREA DE TECNOLOGIA

1. Configurar os equipamentos e sistemas para cumprir os requisitos desta POLÍTICA DA SEGURANÇA DA INFORMAÇÃO.
2. Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.
3. Restringir a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
4. Garantir segurança do acesso público e manter evidências que permitam a rastreabilidade para auditoria ou investigação.
5. Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.
6. Administrar, proteger e testar as cópias de segurança dos programas e dados gerados pela instituição.
7. Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

1. Os sistemas de Login e senha protegem a identidade do colaborador, evitando e prevenindo que uma pessoa se faça passar por outra. Código Penal Brasileiro art. 307 – falsa identidade.
2. É de responsabilidade de cada colaborador a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.
3. Os recursos de TI alocados aos seus colaboradores são destinados exclusivamente às atividades relacionadas ao trabalho.
4. O colaborador deve cuidar para que papéis, mídias e imagens nos monitores não fiquem expostas ao acesso não autorizado de clientes e colegas de trabalho.
5. O antivírus é atualizado automaticamente na estação de trabalho do colaborador a cada nova versão/vacina disponibilizada pelo fabricante através do aplicativo servidor.
6. Todos os arquivos contidos nos servidores de rede ou nas estações de trabalho dos colaboradores devem ser exclusivamente de interesse do seu empregador.
7. É proibida a criação de pastas pessoais nos servidores de rede ou compartilhar as informações de qualquer forma que não tenha finalidade de trabalho.
8. Caso exista senha de impressão, todo colaborador deverá utilizar a sua senha que é de uso pessoal e intransferível.
9. Se o trabalho enviado para a impressora sair de forma diferente da esperada, e o papel puder ser reaproveitado na sua próxima tentativa, recolocá-lo na bandeja de impressão. Caso contrário, se o papel servir para rascunho, o colaborador deverá levá-lo para sua mesa.
10. Se o papel tiver qualquer dado pessoal ou rastreável, deve ser triturado.
11. Respeitar a áreas que merecem atenção e controle de alçada de acesso como sala do administrativo e arquivos.
12. Para garantir a segurança da informação e a integridade dos documentos físicos, os colaboradores não poderão ingerir alimentos e bebidas em seus postos de trabalho.
13. No posto de trabalho, utilize apenas garrafa vedada sobre a mesa. Chimarrão e comida colocam os dados em risco.
14. Apenas pessoas autorizadas devem acessar as instalações de servidores, financeiro e departamento pessoal, sendo que todos os colaboradores devem usar crachás de identificação.

15. A auditoria dos acessos à Internet leva ao conhecimento dos responsáveis hierárquicos, relatórios com nomes dos colaboradores, páginas consultadas, páginas bloqueadas, tempo de consulta, e o conteúdo navegado.
16. Jogos estão terminantemente proibidos
17. Acesso às redes sociais nos computadores do Cartório não são permitidos.
18. Software pirata é um crime e abre brechas para riscos.
19. Celular no ambiente de trabalho é um risco tanto para o atendimento quanto para um incidente com vazamento de dados.
20. Não execute ou abra arquivos anexados enviados por emitentes desconhecidos ou suspeitos;
21. Não abra arquivos anexados com as extensões .bat, .exe, .src, .lnk e .com se não tiver certeza de que solicitou este e-mail.
22. Desconfiar de todos os e-mails com assuntos estranhos e/ou em outros idiomas.
23. Evitar anexos muito grandes.

DIREITOS DO EMPREGADOR
AO SOCIALIZAR ESTA POLÍTICA

- Para garantir que as regras mencionadas acima estão sendo cumpridas, o empregador se reserva no direito de:
- Coletar o seu termo de compromisso com o treinamento realizado.
- Realizar auditorias periodicamente.
- Solicitar à infraestrutura de TI, relatórios de auditoria contendo o nome, mensagens trafegadas, acessos a Internet e demais informações do colaborador conforme Política de Privacidade e LGPD – Lei Geral de Proteção de Dados.
- Orientar sobre novos treinamentos relacionados à LGPD.

LGPD É UM PROGRAMA DE MELHORIA CONTÍNUA

1. Nós somos aquilo que fazemos repetidamente. Excelência, portanto, não é um ato, mas sim um hábito. Aristóteles.
2. A segurança decorre de atenção plena ao nosso trabalho. Estar com “presença de espírito” no dia a dia- SER CONSCIENTE.
3. A LGPD é um processo que não acaba, faz parte do nosso processo de trabalho e missão como cartórios.