DATASIGH.
TECNOLOGIA EM SAÚDE

Conhecendo a LEI GERAL DE PROTEÇÃO DE DADOS.

SUMÁRIO

1. APRESENTAÇÃO

DATASIGH é uma empresa provedora em soluções tecnológicas voltada para área da Saúde. São 21 anos de destaque oferecendo soluções de softwares robustas e inteligentes.

Possuímos um sistema moderno de gestão hospitalar que reúne um conjunto de módulos integrados proporcionando uma visão transparente nos processos organizacionais e clínicos, bem como soluções complementares de análise de dados e de comunicação com pacientes.

Temos como característica desenvolver relacionamentos de longo prazo, por isso atuamos como um parceiro de negócio, com uma equipe multidisciplinar altamente capacitada, utilizando tecnologias de ponta e processos inteligentes para garantir maior Segurança, Produtividade e Satisfação.

DATASIGH E LGPD

Desde à sua concepção, a DATASIGH adota políticas de segurança e, após a aprovação da LGPD vem intensificando ainda mais estudos, capacitações e desenvolvimento em suas soluções a fim de atender todas as exigências legais quanto ao tratamento de dados.
Na empresa a política de proteção de dados é aplicada em todas as operações de tratamento de dados, desde a coleta até o descarte seguro. Também há exigência que todos os seus colaboradores envolvidos no tratamento de dados assinem o Termo de Confidencialidade, bem como promove treinamentos em matéria de Segurança da Informação, aplica as medidas apropriadas para garantir a integridade dos dados e também assegura a disponibilidade por meio de backup e plano de resposta a incidentes, por exemplo.

- Contratação de Assessoria Jurídica
- Criação de Programa de Compliance em Proteção de Dados
- Capacitação de profissionais através de cursos, eventos, feiras
- Solução com armazenamento de logs e auditorias ativas, possibilitando a rastreabilidade e identificação das ações tomadas pelos usuários.
- Solução com administração de perfis de acesso conforme suas atribuições e um gerenciamento de concessões/revogações de direitos.
- Solução com cadastro de senhas fortes conforme padrões estabelecidos

A LEI Nº 13.709 (LEI GERAL DE PROTEÇÃO DE DADOS LGPD) foi aprovada em 14 de agosto de 2018.

O Brasil avançou na criação de uma regulação geral das operações de tratamento de dados, pautada em princípios éticos como a transparência, a não discriminação e a prestação de contas, e na consagração do direito dos titulares de dados à autodeterminação informativa.

Sua aprovação significou um marco do início de uma nova cultura tanto no setor privado como público: uma cultura de transparência centrada na pessoa física, na minimização do impacto e no aumento da segurança aplicada ao tratamento dos dados pessoais.

Em agosto de 2020, entrará em vigor a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), já conhecida como LGPD, que foi redigida com o intuito de mitigar os riscos relacionados ao tratamento indevido e/ou abusivo de dados e, ao mesmo tempo, viabilizar que novos negócios e tecnologias sejam desenvolvidos em um ambiente de segurança jurídica. A aplicação da LGPD impactará não somente os negócios das empresas brasileiras, mas também de todas as empresas nacionais ou estrangeiras que ofertam produtos e/ou serviços para o mercado brasileiro ou que monitorem o comportamento de titulares de dados localizados no Brasil, independentemente de sua nacionalidade ou local de residência.

Este Manual Básico tem como objetivo destacar os principais pontos da LGPD, de forma que o leitor consiga entender como a lei refletirá em suas decisões negociais, parcerias comerciais, revisão e adequação de processos internos e desenvolvimento de novos produtos ou serviços. Apesar de o documento contar com exemplos práticos, o tema abordado não está esgotado – e isso porque o intuito deste material é de informar e convidar a todos os profissionais que lidam, direta ou indiretamente, com o tratamento de dados pessoais a conhecerem a LGPD.

Vale lembrar que cada segmento de atividade econômica, principalmente o segmento de SAÚDE, tem suas particularidades, inclusive em relação a normas específicas, que requerem, portanto, análises direcionadas.

Convidamos o leitor a ter uma visão ampla e prática da LGPD e a participar deste debate essencial para a proteção de dados pessoais e para o desenvolvimento de um ambiente de negócios pautado em boas práticas de governança.

PROTEÇÃO DE DADOS EM SAÚDE

Arcabouço Normativo da Proteção de Dados em Saúde no Brasil

Conforme a Constituição Federal de 1988: "...são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação" (Constituição Federal de 1988, art. 5º, inciso X). Considerando-se que o direito à privacidade já é um item assegurado em nossa Constituição, a questão da proteção de dados em saúde vem sendo discutida com bastante ênfase pelo setor. Há uma crescente utilização dos recursos da Tecnologia da Informação e Comunicação dentro da saúde, onde dados transitam em grande volume e nem sempre de forma ordenada - sendo usados em recursos como prontuário eletrônico do paciente (PEP), telemedicina, troca de informações entre instituições, troca de informações entre a área assistencial, etc. Com isso, surge a real necessidade de padronização e regulamentação do assunto para a correta utilização de tais dados, que devem ter como principal objetivo a assistência adequada ao indivíduo, uma vez que o uso inadequado da informação pode trazer problemas e causar dano direto ou indireto ao indivíduo (por exemplo: discriminação, preconceito ou utilização de recursos para benefícios próprios).

O e-Health (Electronic Health), como é determinado pela Organização Mundial da Saúde (OMS), é a utilização da Tecnologia da Informação e Comunicação em saúde, utilizada para a assistência ao paciente, pesquisa, educação e capacitação das pessoas da área, monitoração do paciente e avaliação. No entanto, normatizar essa quantidade de informações geradas sobre os pacientes é um enorme desafio, com alto nível de complexidade.

No Brasil, algumas ações vêm sendo tomadas para padronizar este tipo de informação. No caso da saúde privada, a Agência Nacional de Saúde Suplementar (ANS) padronizou as informações de saúde entre prestadores de serviço, operadoras e governo através do TISS (Troca de Informações da Saúde Suplementar). Existem vários esforços para que haja padronização e normas claras para a proteção de dados em saúde. A Lei do Marco Civil da Internet - Lei 12.965 de abril/2014 - já é um princípio para proteção de dados da informação, porém muito vinculada apenas ao uso da internet.

Em 2016, a Política Nacional de Informação em Saúde (PNIS) estabeleceu alguns princípios com o objetivo de garantir a confidencialidade, o sigilo e a privacidade da informação de saúde pessoal como direito do indivíduo. Tais legislações foram complementadas com a Lei 13.709/2018 - Lei Geral de Proteção de Dados, que é voltada para a proteção de dados do indivíduo e, consequentemente, complementando a proteção de dados e informações na área da saúde.

A LGPD traz em seu texto a questão de tratamento de dados e a forma pelas quais os dados poderão ser utilizados, como nos trechos abaixo: "... para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;" (LGPD 13709/2018, Art 7º, inciso VIII) "...É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:" (LGPD 13709/2018, Capítulo II, Seção II, Art. 11, parágrafo 4). Os esforços para se atender à nova legislação são enormes, uma vez que há muitas dúvidas e o tempo é escasso.

2. CONHECENDO A LGPD

A edição de uma Lei Geral de Proteção de Dados Pessoais no Brasil não é assunto recente. Há cerca de 8 (oito) anos, o tema proteção de dados pessoais foi lançado para consulta pública pelo Ministério da Justiça, por meio de uma plataforma online (culturadigital.org) que permitia ampla contribuição por indivíduos, empresas, academia e terceiro setor.

Ao longo desses anos, diversos fatores políticos e econômicos impulsionaram a criação de três projetos de Leis principais: 4.060/2012, 330/2013 e 5.276/2016, os quais foram essenciais para a construção do Projeto de Lei nº 53/2018, que viria a ser aprovado pelo Congresso Nacional e sancionado pela Presidência da República em 14 de agosto de 2018. Dentre esses fatores, podemos citar a CPI da Espionagem, a aprovação do Marco Civil da Internet e a entrada em vigor, em maio de 2018, do Regulamento Geral de Proteção de Dados da União Europeia (GDPR). Nasce assim a LGPD, com o propósito de harmonizar os interesses legítimos de titulares de dados e de empresas. A lei não tem como fim frear o desenvolvimento tecnológico, mas tão somente compatibilizar direitos e expectativas, de forma a fomentar a inovação e viabilizar o tratamento legítimo dos dados pessoais. Além disso, a lei é essencial para a harmonização de normas sobre proteção de dados já vigentes no Brasil (como por exemplo o Código de Defesa do Consumidor, a Lei de Acesso à Informação, a Lei do Cadastro Positivo e a Resolução BACEN 4.658/2018); e colocar o Brasil no patamar dos países que conferem segurança jurídica adequada à proteção de dados pessoais, o que tem reflexos importantes na transferência internacional de dados.

Por fim, é fundamental destacar a importância de uma autoridade supervisora e específica, a Autoridade Nacional de Proteção de Dados (ANPD) que terá como função:

- fiscalizar o cumprimento da legislação, tanto pelas empresas privadas quanto pelo poder público;
- assegurar o respeito aos direitos dos titulares de dados pessoais;
- editar normas e diretrizes que complementem e esclareçam disposições da lei, como, por exemplo, sobre a indicação de prazos para notificação em caso de incidentes, padrões mínimos de segurança, manuais de boas práticas e requisitos para a interoperabilidade dos sistemas; e
- aplicar sanções administrativas.

3. PRINCIPAIS CONCEITOS

A Lei Geral de Proteção de Dados (LGPD) apresenta conceitos específicos para as expressões mencionadas em seus artigos. Para facilitar a leitura deste manual e sua interpretação conjunta com o texto legal, serão utilizados os seguintes conceitos e principais pontos, cujo sentido é o mesmo adotado pela lei:

Dado Pessoal

informação relacionada à pessoa natural identificada ou identificável. Essa informação representa todo e qualquer dado que possa tornar uma pessoa identificável, seja ela diretamente relacionada ao seu titular (como um nome ou número de documento) ou mesmo indiretamente relacionada, mas com potencial de identificá-lo(a) (como endereço, idade, informações sobre hábitos de compra, dados de geolocalização de dispositivo móvel, cookies, endereços IP e demais identificadores eletrônicos). Isso porque essas informações indiretas podem ser utilizadas para o monitoramento do comportamento, definição de perfis e, como resultado, identificação das pessoas a quem se referem);

Dado Anonimizado

Informações que se referem a pessoas físicas, mas que não podem ser ligados a nenhuma pessoa física específica nem direta, nem indiretamente, considerando-se os meios técnicos disponíveis. Exemplo: "mulher", "faixa de 20 a 25 anos", "vendedora", "Estado de São Paulo". Apenas com essas informações, não é possível determinar uma pessoa específica, um único CPF. Em geral, dados anonimizados são utilizados em estudos estatísticos.

Dado Pessoal Sensível

Dentro da categoria de dados pessoais, os dados pessoais sensíveis são exclusivamente as informações relacionadas à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico quando vinculadas a uma pessoa física.

Também são sensíveis os dados referentes à saúde ou à vida sexual e os dados genéticos ou biométricos. Esses dados mereceram uma proteção mais rigorosa. Como resultado, o tratamento de dados sensíveis demanda, via de regra, o consentimento específico e destacado dos titulares de dados – separado das demais cláusulas contratuais, portanto. Há situações, todavia, em que os dados sensíveis podem ser tratados sem a necessidade do consentimento do titular. É o caso, por exemplo, do cumprimento de obrigação legal ou regulatória pelo controlador (a pessoa física ou jurídica responsável pelas decisões sobre o tratamento de dados pessoais), da tutela da saúde por profissionais da área de saúde ou por entidades sanitárias, da proteção da vida ou da incolumidade física do titular e da realização de estudos por órgãos de pesquisa (desde que assegurem a anonimização dos dados pessoais, se isso for possível).

Autoridade Nacional

Orgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei.

Titular de Dados

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Agentes de Tratamento

Controlador e o operador;

Tratamento

Toda e qualquer operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Consentimento

aanifestação livr , informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Controlador

Pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais;

Anonimização

utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Banco de dados

Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Encarregado (DPO):

Também chamado de Data Protection Officer (DPO), o Encarregado pela Proteção de Dados é uma pessoa indicada pelo Controlador/Operador para agir como canal de comunicação entre o Controlador e os titulares de dados, e entre o Controlador e a Autoridade Nacional de Proteção de Dados (ANPD). O DPO pode tanto ser interno à organização como externo, em regime de contratação de prestação de serviços (também conhecido como "DPO as a service").

Eliminação

Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

Uso Compartilhado de Dados

Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por entidades e órgãos públicos no cumprimento de suas competências legais, ou entre entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

Transferência Internacional de Dados

Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

Bloqueio

suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

Relatório de impacto à proteção de dados pessoais:

Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

Órgão de Pesquisa

Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

PRIVACIDADE DOS DADOS PESSOAIS

Como é sabido, a informação tornou-se um dos bens de maior valia. Assim, no nosso dia a dia usamos, absorvemos, produzimos e transmitimos informação o tempo todo. Desta maneira, um dos grandes desafios atuais é assegurar a proteção devida para estes dados e, consequentemente, a privacidade.

a) O regime jurídico brasileiro de privacidade

A privacidade é protegida por diversas fontes, dentre as quais destacamos a Constituição Federal (CF) (artigo 5º, incisos X e XII), o Código de Defesa do Consumidor (CDC) (artigo 43) e o Marco Civil da Internet (MCI) (artigo 3, inciso II e III). Desta maneira, a privacidade do indivíduo e, por consequência, as informações do titular dos dados pessoais, é considerada um direito fundamental.

b) A privacidade dos dados pessoais na LGPD

Como não poderia ser diferente, a LGPD prevê que toda a pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. Ela aplica-se independentemente do meio e/ou forma de tratamento dos dados coletados ou recebidos, isso significa que todo aquele que faz uso do dado se impõe às regras da LGPD

Assim, para que haja o cumprimento das obrigações e procedimentos enumerados na lei, o conceito de privacidade dos dados pessoais deverá sempre permear qualquer tratamento de dados realizados pelos controladores e operadores. Um exemplo que demonstra a necessidade de respeito à privacidade, consiste na possibilidade de o titular dos dados possuir direito ao acesso facilitado às informações sobre o tratamento de seus dados, de forma a especificar a finalidade do tratamento e informar quais dados estão sendo compartilhados e a sua finalidade. Para que o princípio da privacidade dos dados pessoais seja, de fato, implementado e observado, a LGPD informa que os controladores e os operadores poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização e procedimentos no tratamento de dados pessoais. Dentre os pontos listados, ressalta-se que, o controlador poderá implementar o programa de governança em privacidade que, no mínimo:

- Seja adaptado à estrutura, à escala e ao volume de suas operações, bem como a sensibilidade dos dados tratados;
- Forneça a gestão de consentimento e finalidades na utilização de dados pessoais;
- Forneça a gestão dos fluxos de dados pessoais, desde a coleta até seu descarte;
- Estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- Seja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos.

Em que pese a LGPD não dispor acerca da obrigatoriedade do controlador possuir um Manual de Boas Práticas e de Governança, recomenda-se que as instituições de saúde implementem tais medidas, pois a Autoridade Nacional de Proteção de Dados (ANPD) poderá solicitar a efetividade de seu programa de governança em privacidade, com o intuito de comprovar o cumprimento da lei.

SEGURANÇA DA INFORMAÇÃO

a) Conceitos fundamentais

Segurança da informação é a prática que visa garantir a confidencialidade, integridade e disponibilidade de dados aos interessados pelo gestor de um banco de dados, por meio de métodos que assegurem a manutenção de tais características dos dados que são objeto de tratamento e acesso. Em detalhes, tais características são:

- Confidencialidade: restrição de acesso a dados exclusivamente aos usuários legítimos, protegendo-os do acesso por estranhos;
- Integridade: manutenção dos dados na mesma condição à qual eles foram disponibilizados por seu titular;
- Disponibilidade: garantia de que osdados concedidos pelo titular e os dados gerados a partir destes estarão disponíveis mediante solicitação do titular ou de seu responsável.

A segurança da informação é o elemento chave da governança de dados, devendo ser operada por meio de práticas e atividades, tais como a elaboração de processos internos e externos, treinamentos e estabelecimento de Políticas de Segurança da Informação (PSI). Por meio desses esforços, a segurança da informação irá proteger todos os ativos de informação da empresa: dados, pessoas, softwares, equipamentos físicos, entre outros.

5. APLICAÇÃO DA LEI

a) Aplicações

De acordo com o artigo 3º da LGPD, estão sujeitas à aplicação da lei todos os tratamentos de dados pessoais:

- realizados no Brasil;
- que envolvam a oferta de bens ou serviços para titulares que se encontram no Brasil, - seja de modo gratuito ou oneroso -, e independentemente do país em que o tratamento ocorra, e
- que envolvam dados pessoais coletados no Brasil.

b) Exceções

Já o artigo 4º da Lei traz exceções expressas à aplicação da LGPD, que se resumem aos tratamentos de dados pessoais realizados para fins:

.

- particulares e não econômicos;
- exclusivamente jornalísticos, artísticos ou acadêmicos;
- exclusivamente de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, e
- que não tenham nenhum contato com o Brasil em toda a cadeia do processamento.

6. PENALIDADES

A LGPD estabelece diversas sanções administrativas a serem aplicadas pela Autoridade Nacional aos agentes de tratamento (controlador e/ou operador) que infringirem as normas previstas na Lei:

- a advertência, com indicação de prazo para adoção de medidas corretivas;
- a multa simples de até 2% (dois por cento) do faturamento da empresa, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, e limitada no total de R$50.000.000,00 (cinquenta milhões de reais) por infração;
- multa diária, observado o limite previsto no item acima;
- a publicização da infração;
- bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- eliminação dos dados pessoais a que se refere a infração.

Lembre-se: para a aplicação das sanções serão considerados os parâmetros e critérios estabelecidos na Lei, dentre eles: a gravidade e a natureza das infrações e dos direitos pessoais afetados; a boa-fé do infrator; a vantagem econômica auferida pelo infrator e sua condição econômica; a reincidência; a cooperação do infrator; a adoção demonstrada de mecanismos e procedimentos para minimizar os danos; e, a adoção de políticas de boas práticas e governança.

7. PRINCÍPIOS

A LGPD concede ao titular de dados pessoais o direito de obter informações claras, adequadas e ostensivas a respeito do tratamento de seus dados. O artigo 6º da Lei estabelece que OS SEGUINTES PRINCÍPIOS DEVEM SER OBSERVADOS NO TRATAMENTO DE DADOS PESSOAIS:

a) Finalidade

Tratar os dados pessoais para objetivos legítimos, específicos, explícitos e informados ao titular

b) Adequação

Tratar os dados pessoais de forma compatível com as finalidades informadas ao titular dos dados.

c) Livre Acesso

Garantir ao titular de dados a consulta gratuita e facilitada aos seus dados pessoais tratados, bem como à forma e duração do tratamento.

d) Não discriminação

Não utilizar o tratamento para fins discriminatórios ilícitos ou abusivos

e) Necessidade

Tratar somente os dados necessários - tanto em questão de categorias de dados, como em proporção -, o mínimo possível para atingir as finalidades

f) Prevenção

Adotar todas as medidas possíveis para evitar danos ao (ou em decorrência do) tratamento de dados pessoais.

g) Qualidade de dados

Garantir exatidão, clareza, relevância e atualização dos dados

h) Responsabilização e prestação de contas

Demonstrar a adoção de medidas eficazes para comprova a observância e o cumprimento das normas de proteção de dados.

i) Segurança

Utilizar medidas técnicas e administrativas/organizacionais para proteger os dados pessoais de tratamento não autorizado, seja intencional ou acidental

j) Transparência

Dar acesso aos titulares a informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados pessoais, resguardados os segredos comercial e industrial.

As informações sobre o tratamento de dados pessoais devem ser claras, objetivas, facilmente compreensíveis e acessíveis ao titular durante todo o período em que o tratamento ocorre. Cláusulas de autorização genéricas para tratamento de dados pessoais serão consideradas nulas!

Tratamento de Dados engloba a coleta, produção, recepção, classificação, utilização, o acesso, a reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados pessoais.

8. FUNDAMENTOS LEGAIS PARA O TRATAMENTO LEGÍTIMO DE DADOS PESSOAIS

Historicamente, o consentimento foi o fundamento central para o tratamento de dados pessoais, o que se refletiu na redação de textos legais como o do Marco Civil da Internet. Uma das principais novidades da LGPD é a indicação de outras hipóteses legais para o tratamento legítimo de dados pessoais, ou seja, o estabelecimento expresso dos casos em que as operações de tratamento estarão em conformidade com a lei. São elas:

- Tratamento mediante consentimento: deve ser dado por escrito ou por outro meio que demonstre inequivocamente a manifestação da vontade do titular de dados pessoais;
- Tratamento para cumprimento de obrigação legal ou regulatória pelo controlador: é o caso do armazenamento dos registros de acesso a aplicações de internet pelo provedor de aplicações, como determinado pelo Marco Civil da Internet, ou da preservação de prontuários médicos;
- Tratamento para execução de políticas públicas: hipótese de tratamento pela administração pública, para execução de políticas previstas em leis, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
- Tratamento no exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Tratamento para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
- Tratamento para proteção de crédito: fazendo menção à lei específica – atualmente, há a Lei do Cadastro Positivo em vigor, apesar de estar sendo revisada pelo Congresso Nacional.
- Tratamento para execução de contrato: caso em que o tratamento de dados é necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual é parte o próprio titular;
- Tratamento para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- Tratamento para atender aos interesses legítimos do controlador ou de terceiro: desde que não se sobreponham aos direitos e liberdades fundamentais dos titulares dos dados. Pode-se citar como exemplo, compartilhamento com empresas terceiras para fins de prevenção à fraude, marketing direto, proteção da integridade física do titular, dentre outras possibilidades;
- Tratamento para realização de estudos e pesquisas: desde que realizado por órgão de pesquisa e garantida, sempre que possível, a anonimização dos dados pessoais. Para evitar o uso indevido desta hipótese, a LGPD conceituou órgão de pesquisa como "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Além das previsões do art. 7º, a LGPD ainda estabelece, em seu art. 11, inciso II, alínea g, a hipótese para o tratamento de dados pessoais sensíveis sem o consentimento do titular quando for indispensável para prevenção à fraude e a segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, exceto no caso de preponderância dos direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
Em qualquer um dos casos, o tratamento de dados pessoais nas ocasiões em que o acesso é público, deve considerar a finalidade, a boa-fé e o interesse público que justificarem sua disponibilização.

9. COMUNICAÇÃO ECOMPARTILHAMENTO DE DADOS EM SAÚDE PARA PRESTAÇÃO DE ASSISTÊNCIA

O tratamento de dados pessoais sensíveis somente poderá ocorrer:

- Com consentimento que evidencie uma manifestação livre, informada e inequívoca, e destacado para finalidades específicas do titular ou seu responsável legal;

- Sem o consentimento do titular quando for indispensável e estiver dentro das hipóteses taxativamente previstas no art. 11: "tutela da saúde exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária".

Uma alteração trazida pela Lei 13.853 de 2019 é a inclusão do §5º: "É vedado às operadoras de planos privados de assistência à saúde, o tratamento de dados de saúde para prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários."

10. NOTIFICAÇÃO COMPULSÓRIA

O controlador deve comunicar à autoridade competente e ao titular, em prazo razoável a ser definido pela autoridade competente, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48). Essa comunicação deverá conter:

- ·A descrição da natureza dos dados pessoais afetados;
- Os titulares envolvidos;
- As medidas técnicas e de segurança
- utilizadas para a proteção dos dados;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso da comunicação não ter sido imediata;
- As medidas adotadas para corrigir ou mitigar os efeitos do prejuízo causado ao titular pelo incidente.

11. DIREITOS DO TITULAR

Semelhante ao Regulamento Geral de Proteção de Dados da União Europeia, a LGPD assegura ao titular dos dados pessoais o direito de obter do controlador, a qualquer momento e mediante requisição, os seguintes direitos:

- Confirmação e acesso aos dados ao titular dos dados pessoais é garantido o direito de confirmação da existência de tratamento e, por consequência, o de acessar todos os dados pessoais de sua titularidade que estão sendo coletados e tratados pelo controlador. Cabe ao controlador fornecer a informação e a confirmação da existência de tratamento ou o acesso a dados pessoais:

Imediatamente à requisição do titular, em formato simplificado ou

No prazo de até 15 dias contados da data de requerimento do titular, uma declaração clara e completa que indique:

- A origem dos dados;
- A inexistência de registro;
- Os critérios utilizados e a finalidade de tratamento, observados os segredos comercial e industrial.

LEMBRE-SE: Os dados pessoais devem ser armazenados em formato que favoreça o direito de acesso, bem como o da portabilidade dos dados pessoais. O formato no qual serão fornecidos os dados e as informações requisitadas ficará a critério do titular dos dados pessoais. Logo, cabe ao controlador viabilizar mecanismos que garantam o fornecimento por meio eletrônico ou sob a forma impressa.

NOTA: A Autoridade Nacional de Proteção de Dados Pessoais poderá indicar prazos diferenciados para os setores específicos.

- Retificação: os titulares possuem o direito de corrigir dados incompletos, inexatos ou desatualizados que lhes digam respeito.

- Restrição de tratamento: os titulares possuem o direito de restringir o tratamento de dados pessoais, por meio da recusa em fornecer o consentimento.

- Cancelamento ou Exclusão: de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD ou cujo consentimento do Usuário for retirado. LEMBRE-SE: os dados pessoais devem ser eliminados após o término do tratamento, sendo autorizada a conservação destes para: (i) o cumprimento de obrigação legal ou regulatória pelo controlador; (ii) estudo por órgão de pesquisa; (iii) a transferência a terceiro, desde que respeitados os requisitos da lei; e, (iv) uso exclusivo do controlador, desde que anonimizados os dados e vedado seu acesso a terceiro.
- Portabilidade: o titular tem o direito de receber todos os seus dados pessoais que tenham sido fornecidos a um controlador, inclusive em formato eletrônico e interoperável, a fim de que estes sejam transmitidos a outro fornecedor de serviço ou produto, de escolha do titular. NOTA: o Direito de Portabilidade depende de regulamentação por parte da Autoridade Nacional de Proteção de Dados.
- Informação: das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, bem como sobre a possibilidade de o titular não fornecer consentimento e as consequentes negativas. importante: a LGPD traz uma proteção específica ao tratamento de dados pessoais de crianças e adolescentes, de forma que os controladores não devem condicionar a participação destes em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. NOTA: De acordo com o Estatuto da Criança e do Adolescente (ECA), considera-se "criança", a pessoa com até 12 (doze) anos de idade incompletos, e "adolescente" aquela entre 12 (doze) e 18 (dezoito) anos.
- Revogação de Consentimento: o titular dos dados pode revogar o consentimento para tratamento de seus dados pessoais a qualquer momento, mediante manifestação expressa, por procedimento gratuito e facilitado. NOTA: o controlador poderá continuar o tratamento dos dados pessoais obtidos, mediante consentimento, anteriormente ao pedido de revogação, até que a finalidade do tratamento seja alcançada ou nas demais hipóteses previstas em lei.
- Oposição: o titular dos dados tem o direito de se opor a quaisquer tratamentos e informações que não estejam em conformidade com a lei, bem como a decisões automatizadas que afetem seus interesses, como decisões destinadas a definir seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (profiling). NOTA: é de responsabilidade do controlador fornecer informações claras e objetivas sobre os critérios e os procedimentos adotados para a decisão automatizada, observados os segredos comercial e industrial. Em caso de não oferecimento destas informações sob a alegação de segredos comercial e industrial, a Autoridade Nacional de Proteção de Dados poderá realizar uma auditoria para verificar eventuais aspectos discriminatórios do tratamento automatizado.
- Explicação: o titular dos dados tem direito a receber informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados pelo controlador para a tomada de decisão com base em tratamento automatizado de dados pessoais.

12. AGENTES DE TRATAMENTO

a) Definição

Agentes de tratamento são todos os indivíduos que controlam ou tratam informações que contenham dados pessoais. A Lei nº 13.709/2018 elenca expressamente, no art. 5º, IX, que os agentes de tratamento são o controlador e o operador.

- O controlador, na definição legal (art. 5º, VI) é "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

- Já o operador (art. 5º, VII) é "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"..

Os agentes de tratamento de dados neste contexto serão as instituições de saúde, por meio de seus colaboradores, médicos e parceiros (terceiros) que tratam os dados dos pacientes/clientes, em virtude do relacionamento de prestação de serviços de saúde específicos de cada instituição. Uma instituição de saúde pode ser controladora e operadora dos dados ao mesmo tempo, diante de uma atividade (processo) que trate os dados pessoais dos titulares.

Outro cenário é quando uma instituição de saúde terceiriza a operação dos dados, como um laboratório de análises clínicas, diagnóstico por imagem, call center para SAC , por exemplo, caso em que a instituição de saúde seria controladora de dados. Um fluxo comum a considerar será: por força de uma relação estabelecida entre um titular e um controlador de dados que conta com serviços prestados por um operador, o titular dos dados fornece os dados para um operador ou, um operador coleta os dados de um titular sob seu consentimento.

O operador deve atender as determinações de tratamento de dados definidas pelo controlador de dados. O controlador de dados deve estar em conformidade com as definições da LGPD.

Cabe ao controlador de dados nomear um encarregado (DPO) para atuar como canal de comunicação para atender as necessidades dos titulares junto ao controlador e à ANPD.

Figura 01 | Agentes: fluxo de relacionamento

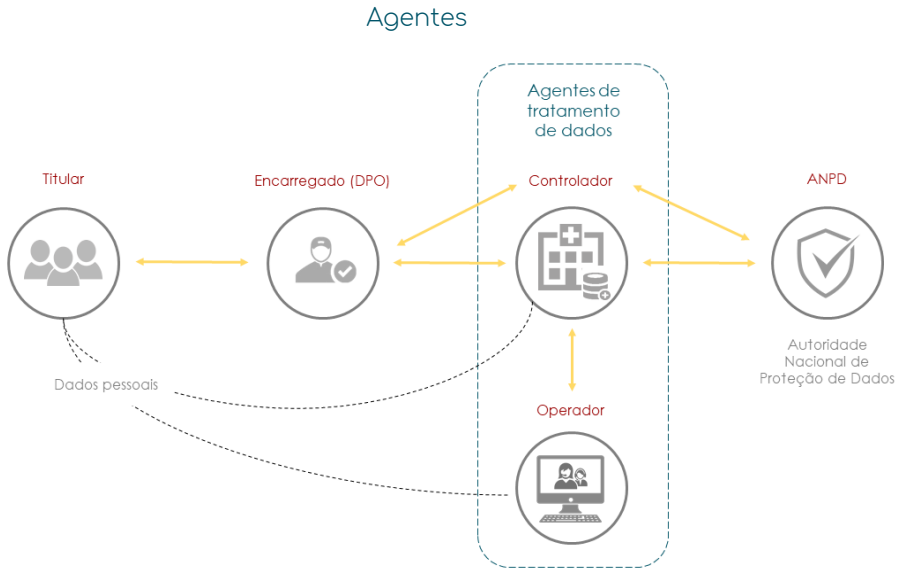
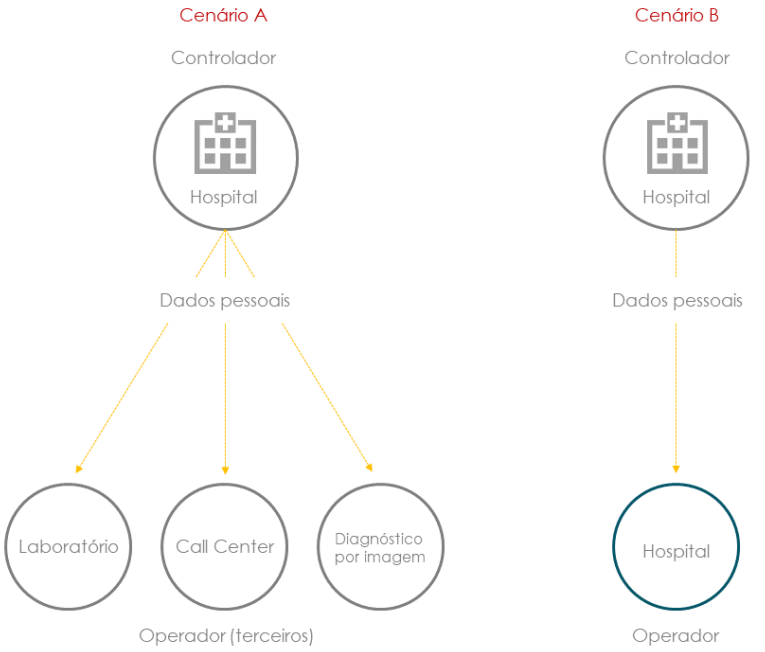


Figura 01 | Agentes de tratamento de dados: exemplos de controlador e operador



Dentro da estrutura organizacional de uma instituição existe mais de uma pessoa ou setor que pode ser qualificado como controlador e operador, de modo que é necessário o adequado mapeamento destes, a fim de fazer com que a implementação das regras editadas pela LGPD se dê de maneira ampla e completa.

b) Obrigações e responsabilidades

A principal obrigação que a LGPD dispõe aos agentes de tratamento (art. 37) é a de que mantenham um registro das operações de tratamento que realizarem, especialmente quando este tratamento de dados se der fundado em legítimo interesse, previsto no art. 10. O controlador tem a específica atribuição de indicar o encarregado pelo tratamento de dados pessoais (art. 41). Por sua vez, cabe ao operador realizar o tratamento de dados "segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria" (art. 39). Importante garantir que as instruções do controlador ao operador sejam claras e, preferencialmente, formais, para que não haja ambiguidade e/ou falha no processo de tratamento de dados. Para tanto, possuem papéis importantes as áreas:

Jurídica

- Responsável por manter os termos contratuais de consentimento atualizados e em aderência com a legislação;
- Apoiar a instituição e o DPO durante processos legais;
- Apoiar na demonstração dos controles existentes para mitigação dos pontos da legislação em caso de abordagem.

Recursos Humanos

- Deve desenvolver medidas disciplinares para colaboradores que descumpram as políticas da instituição;
- Deve conter uma política formal e divulgada para os colaboradores sobre as medidas disciplinares

Assistencial e Corpo Clínico

- Não emprestar credenciais;
- Não salvar informações localmente ou em meios que não sejam controlados pela instituição;
- Não compartilhar informações confidenciais por aplicativos de mensagens instantâneas, redes sociais, e-mail particular ou qualquer outro que não exista controle da instituição;
- Aderir às políticas de privacidade e tomar todas as cautelas necessárias no manuseio de dados sensíveis;
- Não conversar em locais públicos mencionando dados sensíveis de pacientes

Auditoria interna

- Definir metodologia de auditoria interna para garantir que os processos estão sendo seguidos;
- Reportar os resultados das auditorias periodicamente para o DPO e alta direção;
- Desenvolver relatórios de risco e reportá-los para o DPO e alta direção

Gestão de fornecedores/contratos

- Aplicar os termos desenvolvidos pelo jurídico para novos contratos e criar aditivos para os contratos já existentes;
- Auditoria periódica nas operadoras e prestadores de serviço onde exista a transferência de informações que contenham dados pessoais.

Serviço de apoio médico

- Manter a salvaguarda de informações que contenham dados pessoais e sensíveis;
- Coletar consentimento de médicos, assistência e pacientes sempre que necessário.

Tecnologia da Informação e Segurança da Informação:

- Desenvolvimento de meios seguros de armazenamento, processamento e transmissão para proteção de dados pessoais;
- Desenvolvimento e divulgação das Políticas de Segurança da Informação, incluindo Política de
- Classificação da Informação;
- Levantamento e documentação das interfaces de troca de informações com dados sensíveis (arquiteto de dados);
- Segregação de perfis de acesso a dados pessoais e gestão de acessos; Proteção contra vazamento de informação, bloqueio de pendrive e DLP Endpoint para as estações de trabalho;
- Cybersecurity (Monitoração, alerta, segregação de ambientes);
- Definição de tecnologias para gestão dos termos de consentimento de pacientes e colaboradores para uso dos dados (método de armazenamento, pesquisa, tratamento dos casos de não consentimento, revogação/mudança do consentimento, exclusão de dados);
- Definição de tecnologias para processo de transferência segura de dados sensíveis (operadoras nacionais e internacionais); Anonimização e pseudonomização em banco de dados; Continuidade de negócios (possibilidade de multa em caso de perda de informação do paciente);
- Conscientização de colaboradores e prestadores de serviço;
- Processo de desenvolvimento seguro que envolva testes durante todo o ciclo.

13. SEGURANÇA E BOAS PRÁTICAS

A proteção de dados deve ser observada em todas as etapas de desenvolvimento dos produtos e/ou serviços e sempre na forma mais protetiva ao titular dos dados – ou seja, desde sua concepção (by design) e por padrão (by default) devem ser implementadas medidas de segurança, técnicas e administrativas que evitem o acesso não autorizado e de situações de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Segundo o artigo 46 da LGPD, o Controlador e o Operador devem "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito". Isso significa que esses agentes devem (i) implementar sistemas, ferramentas e serviços aptos a proteger e monitorar o tratamento de dados pessoais, e (ii) apresentar políticas, normas e procedimentos internos que orientem a atuação dos colaboradores em prol da proteção de dados pessoais

A lei não indica como obrigatória a elaboração do Relatório, exceto se determinado pela Autoridade Nacional de Proteção de Dados. Contudo, sua elaboração é um exercício fundamental para que a instituição enha ampla visão de seu modelo de negócio e, assim, consiga averiguar eventual falha em seu fluxo de dadose/ ou tomar decisões mais assertivas no desenvolvimento de novos produtos ou serviços. Além disso, em caso de eventual auditoria ou processo administrativo perante a Autoridade Nacional, essa documentação poderá servir como base para demonstrar a boa-fé, a diligência e o comprometimento da instituição em termos de governança, conformidade com a legislação e preocupação com a segurança e sigilo dos dados pessoais dos titulares e, por conseguinte, atenuar eventual sanção administrativa.

GOVERNANÇA CORPORATIVA

As instituições públicas e privadas devem documentar todas as atividades envolvidas no tratamento de dados pessoais e demonstrar todos os esforços para que estejam em conformidade com a LGPD e demais normas aplicáveis integrando os princípios da prevenção, segurança, transparência e prestação de contas (accountability) que fundamentam a LGPD.

Relatório de Impacto

Segundo a LGPD (art. 5º, XVII), o relatório de impacto à proteção de dados é a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco."
O referido relatório poderá ser solicitado ao controlador pela ANPD (art. 38), e deverá conter, no mínimo, "a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados." Caso ocorra algum incidente de segurança que possa implicar em risco ou em dano aos titulares de dados pessoais, caberá ao controlador comunicar à ANPD e ao titular de dados pessoais tal ocorrência (art. 48). Esta comunicação deverá ocorrer em prazo razoável (que será objeto de regulamentação pela ANPD - §1º)

Encarregado pelo tratamento de dados pessoal

Conhecido como Data Protection Officer (DPO), surgiu com a consolidação da GDPR na União Europeia, como um cargo de nível estratégico, que é responsável por disseminar a cultura de proteção de dados na instituição, criar normas e procedimentos que atendam às legislações de proteção de dados vigentes, sendo um canal de comunicação entre instituição, titular das informações e entidades governamentais que controlam e regulam a proteção de dados individuais. Trata-se de uma função multidisciplinar, pois o profissional deve ter conhecimento de como a instituição atua com os dados coletados e sua forma de tratamento. Além disso, precisa ter sinergia ou conhecimento em tecnologia e segurança da informação, aspectos legais, compliance, gestão de riscos, comunicação fluida e clara e ter bom relacionamento, já que será um influenciador dentro da instituição.

Uma de suas principais funções será receber as notificações dos titulares das informações e/ou da entidade fiscalizadora, sendo responsável por sua apuração, tratativa adequada e resposta ao titular e à ANPD. Recomenda-se que tenha autonomia para auditar e fiscalizar as possíveis irregularidades para que possam ser corrigidas e notificadas conforme rege a lei. Figura idêntica existe na diretriz europeia. O Data Protection Officer (DPO) será a pessoa natural ou jurídica), que atuará "como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)" (art. 5º, VIII), será o responsável por disseminar a cultura de proteção de dados na instituição, além de criar normas e procedimentos adequados à lei.

Será o responsável por receber as notificações da ANPD e dos titulares das informações e as colocará em prática. O DPO deverá ter sua identidade e informações de contato divulgadas publicamente de forma clara e objetiva, preferencialmente no site do controlador (art. 41, §1º).)

A LGPD lista as atividades do DPO no art. 41, §2º, sendo de mais destaque as seguintes:

- Garantir a efetividade dos controles relacionados à proteção de dados pessoais sob custódia da organização;
- Coordenar a conformidade do processo com os outros agentes de tratamento;
- Relacionar-se com entidades de autoridade; Em caso de incidente, analisar se aquilo deve ser reportado ou não;
- O DPO será acionado legalmente em caso de incidentes mais graves.

Notificação de Acidentes

Notificação de Incidentes: seguindo os princípios de transparência e informação, é de responsabilidade do controlador comunicar à Autoridade Nacional e ao titular a ocorrência de incidente de segurança da informação que possa acarretar risco ou dano relevante aos titulares. A lei não prevê prazo específico, apenas menciona que a comunicação deverá ocorrer em prazo razoável a ser definido pela Autoridade Nacional. Vale lembrar que a GDPR instituiu o prazo de 72 horas para a notificação de incidentes.

Nota: a notificação deverá conter todas as informações definidas na lei, como a natureza dos dados pessoais afetados, as informações dos titulares envolvidos, as medidas técnicas e de segurança utilizadas para proteção dos dados e as respectivas medidas que foram ou serão adotadas para minimizar os danos. Por isso, a existência de uma Política de Segurança da Informação e de Resposta a Incidentes é imprescindível, em termos de governança, diligência e celeridade.

Contratos

As cláusulas contratuais são de extrema importância na definição e limitação de responsabilidades, seja para o controlador quanto para o operador (pessoa física ou jurídica que realiza o tratamento de dados em nome do controlador). A lei estabelece obrigações gerais e específicas para ambos os agentes de tratamento, de forma que ambos podem ser, inclusive, responsabilizados solidariamente. Por exemplo:

- É de responsabilidade do controlador: comprovar que o consentimento foi obtido, bem como informar ao operador eventual pedido de revogação de consentimento e/ou eliminação de dados pelo respectivo titular, a fim de que este suspenda o tratamento ou providencie a anonimização e/ou o apagamento dos dados;

- É de responsabilidade do operador: seguir todas as medidas técnicas e administrativas de tratamento instruídas pelo controlador, sob pena de responder solidariamente pelos danos causados aos titulares.

14. COMO COMEÇAR

Entender

o propósito e os princípios básicos da LGPD é o primeiro passo. Isto porque, os fins para os quais os dados são coletados e tratados pela instituição devem estar em conformidade com tais princípios, impactando, assim, na tomada de decisões quando do desenvolvimento e/ou implementação de novas tecnologias

Definir

pessoa para liderar um Projeto de Proteção de Dados, bem como uma equipe ou departamento que auxilie no Compliance de Proteção de Dados da sua organização.

Equipe: para auxiliar o Encarregado de Proteção de Dados na criação de um Projeto de Proteção de Dados, é aconselhável estabelecer uma equipe multidisciplinar – ou seja, com integrantes de áreas centrais da instituição e terceirizados, como Tecnologia da Informação (T.I.), Jurídico, Marketing, Financeiro e Recursos Humanos. Isto porque, um Programa Regulatório e de Compliance em Proteção de Dados Pessoais só será efetivo se contempladas todas as perspectivas (visão ampla, prática, cotidiana e que abranja todas as áreas)

Mapear

- As categorias de dados coletadas, inclusive de funcionários;
- O fluxo de dados pessoais (como e por quem são coletados, quais as finalidades do tratamento, onde são armazenados, com quem são compartilhados, quais os mecanismos técnicos e administrativos de segurança dessas informações, etc.);
- Eventual transferência internacional de dados (quais dados, com qual país e/ou organização internacional, com quais finalidades, onde são armazenados, quais os mecanismos técnicos e administrativos de segurança dessas informações, etc.);
- As leis e/ou normas regulatórias aplicáveis ao negócio;
- A localização dos servidores e quem tem acesso (por exemplo, funcionários, departamentos, terceirizados, dentre outros);
- As empresas terceirizadas que prestam serviços para a instituição;
- Contratos e Termos vigentes (verificar se há cláusulas específicas sobre proteção de dados pessoais, confidencialidade e responsabilidades civis, criminais e/ou administrativas concernentes);
- A existência de Políticas, Normas e Processos Internos relacionados à Segurança da Informação, Retenção e Exclusão de Dados, Resposta à Incidentes, Gestão de Riscos;
- A existência de protocolos e processos para opt-in e opt-out em ações de marketing direto da instituição;
- Canais de atendimento e meios de acesso para exercício de direitos pelos usuários; e,
- Demais informações relevantes e especificas do negócio para o desenvolvimento de um Programa de Compliance em Proteção de Dados Pessoais

Criar

um Programa de Compliance em Proteção de Dados Pessoais, o qual deve estar devidamente documentado, indicando todas as políticas e normas que compõem o programa, além de todas as ações a serem realizadas durante o seu prazo de vigência

A LGPD possibilita que as regras de boas práticas e de governança sejam formuladas individualmente pelos agentes de tratamento (controladores e operadores) ou por meio de associações, devendo estabelecer:

Implementar

Durante a efetivação do Programa de Compliance em Proteção de Dados, é muito importante se atentar à/ao:

- Gestão e Segurança das Informações: visto que pode haver mudanças e/ou implementação de novo software para gestão das informações, a fim de evitar perdas e/ou vazamento de dados e informações confidenciais;
- Conhecimento: certificar-se de que todos os colaboradores estejam cientes da implementação e da importância do Programa;
- Cultura: uma instituição que não estava acostumada com um ambiente de transparência e informação pode demorar um pouco mais de tempo para se acostumar com as mudanças. Portanto, recomenda-se ações de incentivo e educativas que auxiliem na mudança de cultura de toda a instituição.

Fiscalizar

- desde a aplicação e efi cácia do Programa de Compliance em Proteção de Dados até o monitoramento de novos regulamentos e/ou diretrizes a serem publicadas pela Autoridade Nacional de Proteção de Dados.

15. PADRÕES TÉCNICOS

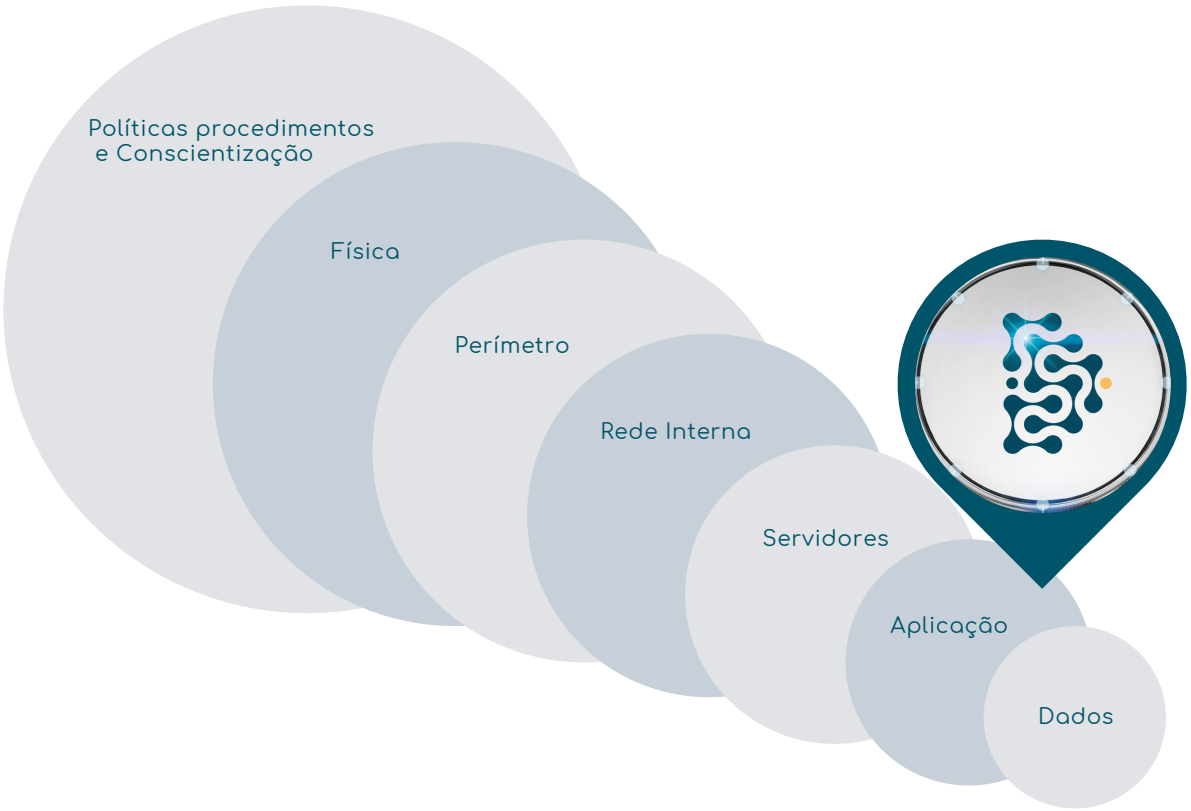
No tempo em que as instituições utilizavam documentos físicos, os padrões de segurança previam que estes fossem armazenados em local que pudesse ter a porta trancada. No cenário de saúde, os hospitais precisam manter os prontuários físicos por, no mínimo, vinte anos para algumas patologias e, em outras situações, este prazo pode ser ainda maior. Portanto, a digitalização desses documentos facilita seu armazenamento e gestão, ao passo que gera novas demandas para a TI, que deve armazená-los garantindo disponibilidade e segurança.

Com a evolução destes documentos para os meios digitais, a ação de manter a segurança foi elevada para níveis complexos, exigindo ambientes sofisticados, com alto custo e necessidade de atualizações constantes.

A construção de políticas, normas e procedimentos, a adoção das melhores práticas de segurança, o monitoramento e a auditoria destas ações, representam que a proteção deve ser elaborada visando mitigar riscos causados por pessoas, ambiente ou sistemas e equipamentos.

No atual cenário virtual, as ameaças chegam aos ambientes de forma silenciosa e invisível, explorando não apenas as vulnerabilidades de hardware e software, mas também as vulnerabilidades das pessoas, exigindo a construção de defesas em todas as camadas envolvidas nos ambientes de TI das empresas. As instituições possuem suas próprias políticas de segurança da informação e todos os seus usuários devem conhecer e praticar as diretrizes ali definidas. Geralmente, as organizações também possuem um processo de detecção e classificação de risco próprio, levando em consideração o valor do seu ativo e a probabilidade do risco. Desta forma concentram seus esforços e investimentos em segurança da informação.

Nesta seção serão abordados os padrões técnicos de segurança da informação necessários para garantir a continuidade de negócios das instituições, considerando os dados como o ativo principal, ou seja, os dados no centro do ambiente de TI.



Para cada camada existe uma variedade de medidas tecnológicas que podem ser implementadas, como forma de prover segurança de suas informações. A seguir, serão utilizados alguns exemplos, dentre muitas possibilidades, para ilustrar cada camada, lembrando sempre que não existe uma receita pronta e que a combinação de soluções/equipamentos resulta em diferentes níveis de segurança, que estarão ligados à quantia de esforço, técnica e investimentos disponíveis para este fim.

Aplicações

Prover segurança exige observar qual linguagem será utilizada, a metodologia de desenvolvimento que deve prover a adequada segurança desde sua escrita, assim como, a utilização de protocolos e servidores web seguros em caso de aplicações desenvolvidas para este meio. Os sistemas devem prever o armazenamento de logs e possuir auditorias ativas, possibilitando a rastreabilidade e identificação das ações tomadas pelos usuários. Deve também prover perfis de acesso conforme suas atribuições e um gerenciamento de concessões/revogações de direitos. Cuidar da segurança do sistema, não significa dizer que está se cuidando da segurança dos dados pessoais/sensíveis, é necessário que sejam observados os aspectos de privacidade. E as equipes de análise, desenvolvimento e testes, deverão ser capacitados, conforme a metodologia privacy by design

Servidores

A metodologia de Hardening é aplicada como padrão de segurança em infraestrutura e servidores, através do processo de mapeamento de ameaças, mitigação de riscos e execução das ações corretivas. O objetivo principal dos padrões recomendados neste modelo é tornar o ambiente menos suscetível a invasões. A efetividade deste modelo deve considerar três fatores: segurança, risco e flexibilidade. Mantê-los balanceados será o desafio desta implementação, visto que, quanto mais seguro for o servidor, menos flexível ele se tornará. Deve ser sempre lembrado que a aplicação de patches de correção/ segurança e a utilização de sistemas operacionais com suporte do fornecedor é regra fundamental para um ambiente seguro.

Rede interna

Alnicialmente deve-se pensar na rede de dados interna como o caminho que permite aos usuários chegar até as informações desejadas, sendo assim, prima-se pela continuidade e disponibilidade deste meio, bem como, para dar vazão a todas as necessidades de todos os setores da organização. Como forma de adicionar segurança a este meio, as instituições devem adicionar alguns componentes a ela:

Software de Antivírus

este recurso é utilizado para detectar e deter ameaças, uma vez que já estão salvas e/ou instaladas nos computadores ou servidores.

Senhas Fortes

atualmente já está se falando em abolir a troca periódica de senhas, já tendo publicações realizadas pelo NIST (National Institute of Standards and Tecnology) defendendo esta ação, assim como, a Microsoft também adicionou esta prática como padrão. Ambos afirmam que o uso de senhas complexas e longas são mais seg uras do que a troca periódica de senhas. Considera-se nesta orientação que os usuários tendem a seguir padrões nas trocas de suas senhas, o que torna fácil quebrá-las.

Access Control List (ACL)

ou lista de controle de acesso, referente às permissões atribuídas a um objeto que especificam quais usuários recebem acesso ao mesmo tempo e as operações que ele pode executar.

Segmentação de Rede

é a divisão da rede em sub redes, para evitar que anomalias e ameaças se multipliquem para diversos setores da organização, aumentando a possibilidade de efetividade e danos

Network Access Control (NAC)

já com alternativa open source para algumas distribuições de sistemas operacionais, o NAC é fundamental para colocar os dispositivos em consonância com as regras de segurança estabelecidas pela organização. Com a crescente utilização dos dispositivos BYOD, este protocolo passa a ser um forte aliado.

Física

Esta, sem dúvida, é a prática de segurança mais antiga, pois desde os primórdios guardamos ativos de valor em locais trancados e a chave é oferecida apenas às pessoas que tenham real necessidade de acesso aos objetos ali armazenados. Quando este assunto é associado ao meio digital, a segurança física se dá aos equipamentos que armazenam ou acessam os dados, portanto a utilização de controles de acessos (sejam sensores biométricos, sensores de retina ou apenas uma chave), a concessão ou revogação dos acessos aos indivíduos deve ser rigorosamente gerenciada.

Política, procedimentos e conscientização

Promover a cultura de segurança para as pessoas é o maior desafio das organizações, portanto, é sempre recomendado que as instituições busquem promover treinamento para suas equipes, fomentando a prática de utilização do meio digital com segurança, moderação e sigilo.

O desenvolvimento da Política de Segurança da Informação, Política de Gestão de Mudanças, política de uso de e-mail, política de uso de internet, entre outras, faz parte das ações de construção de diretrizes promovidos pelas organizações, na busca de incutir regras seguras em seus colaboradores. Além disso, devemos adequar a estrutura operacional e técnica das instituições para viabilizar e cumprir com todos os direitos que a lei garante ao titular do dado. Desenvolver mecanismos que permita ao titular exercer o seu direito de forma fácil e gratuita.

16. INCIDENTE DE SEGURANÇA

De acordo com a ISO 27002, um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.
Para a Lei Geral de Proteção de Dados, pode ser considerado um incidente de segurança:

- Qualquer acesso não autorizado a dados que contenham informações pessoais que possam identificar o indivíduo;
- Vazamento de informações de um único registro ou base de dados contendo informações pessoais;
- Perda das informações pessoais.

Incidentes que deverão ser reportados à Autoridade Nacional de Proteção de Dados (ANPD):

- Quando ocorrer um vazamento, acesso não autorizado ou perda de informações pessoais.
- Quando houver um risco muito alto associado a dados pessoais e não tiver controles mitigatórios suficientes aplicados no momento.

Relatório de Impacto

De acordo com a LGPD, Art. 5, Parágrafo XVII, a definição de relatório de impacto à proteção de dados pessoais é: "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

Desta forma podemos considerar que o relatório deve conter minimamente:

- Descrição dos tipos de dados coletados;
- Riscos associados;
- Medidas e controles de segurança da informação adotados;
- Plano de ação de mitigação de riscos

17. MECANISMOS INTERNOS DE SUPERVISÃO

Para que haja um controle adequado dos incidentes de segurança da informação, é necessário que as instituições tenham mecanismos internos de controle e auditoria bem definidos e que sejam atualizados constantemente para que possam identificar e definir os prováveis riscos de forma rápida. Para isto é necessário:

- Conter um processo contínuo de revisão dos relatórios de impacto de proteção de dados, riscos, planos de ação e de fatores que possam alterar o nível do risco;
- Possuir monitoração contínua do ambiente contendo dados pessoais para identificar e alertar um possível incidente;
- Possuir um canal para reporte externo para investigação de um possível incidente;
- Monitorar canais internos e externos de divulgação de incidentes de segurança relacionado a instituição.

18. MEDIDAS DE MITIGAÇÃO DE RISCOS

A lei define como boas práticas e governança a implantação de processos e controles com o objetivo de redução de riscos de vazamento ou perda de informações. A adoção destas medidas será analisada como fator de redução de possíveis multas aplicadas pela ANPD. Recomendamos como principais medidas:

- Conscientização contínua de colaboradores e parceiros:
  - 70% dos incidentes de segurança ocorrem devido à falha humana relacionada à falta de conhecimento ou ações intencionais. Todos os colaboradores devem conhecer as políticas de segurança e privacidade da instituição e serem treinados adequadamente, no mínimo uma vez ao ano.
- Conjunto de políticas com as diretrizes definidas pela instituição para serem utilizadas nos processos de conscientização e para que medidas disciplinares sejam aplicadas em caso de não conformidade, tais como:
  - Política de segurança da informação;
  - Política de privacidade;
  - Política de classificação da informação;
  - Política de controle de acesso
- Levantamento das interfaces de troca de informações contendo dados pessoais e sensíveis:
  - É necessário que a instituição conheça os processos de armazenamento, processamento e transferência de dados pessoais em todos os meios, como, por exemplo, papel e digital;
  - Com base neste levantamento, serão aplicados os controles de proteção e salvaguarda legal, além de fornecer a base inicial para a elaboração de relatórios de impacto de proteção de dados.

- Monitoração contínua e proteção contra vazamento de informação:
    - Mecanismos técnicos para classificar, identificar, alertar e bloquear possíveis vazamentos de dados pessoais;
    - Utilizar os mecanismos como forma de conscientização do usuário final.

- Implantação de um processo de gestão de consentimento:
    - Fornecer uma interface para que o indivíduo possa autorizar, bloquear, revogar o consentimento para o tratamento dos seus dados pessoais;
    - Fornecer relatórios com trilhas de auditoria para comprovação legal do consentimento ou revogação do indivíduo, tanto como a tratativa dos dados e sua portabilidade;
    - Possuir granularidade e especificidade do nível de consentimento de acordo com a exigência da norma.

- Criptografia em base de dados:
    - Possibilitar a anonimização e pseudonomização, evitando que, mesmo os profissionais com acesso privilegiado para administração da base, acessem o seu conteúdo.

- Desenvolvimento seguro (privacy by design):
    - Implementar o desenvolvimento seguro nos novos projetos;
    - Realizar ações de revisão e adequação dos ambientes legados.

- Continuidade de negócios:
    - Garantir a efetividade de cópias de segurança e que testes de recuperação sejam realizados periodicamente;
    - Fornecer infraestrutura e plano de recuperação de desastre para os ambientes que fazem escopo da lei.

DATASIGH.
TECNOLOGIA EM SAÚDE

www.datasigh.com.br