Manual Melhores Práticas LGPD

Novembro 2020

anahp
associação nacional
de hospitais privados

EXPEDIENTE

Conteúdo

Anahp

Kamila Fogolin, diretora Jurídica e *Compliance*

PG Advogados

Patricia Peck, advogada e sócia *head* de Direito Digital

Sara Cepillo e Vasconcelos, advogada e sócia especialista em Proteção de Dados

Larissa Lotufo, pesquisadora e *Legal Assistant*

Revisão

Ana Paula Machado

Gabriela Nunes

Diagramação

Luis Henrique de Souza Lopes

Novembro/2020

SOBRE A ANAHP

A Associação Nacional de Hospitais Privados – Anahp é a entidade representativa dos principais hospitais privados de excelência do país. Criada em 11 de maio de 2001, durante o 1º Fórum Top Hospital, em Brasília, e fundada em 11 de setembro do mesmo ano, a Anahp surgiu para defender os interesses e necessidades do setor e expandir as melhorias alcançadas pelas instituições privadas para além das fronteiras da saúde suplementar, favorecendo a todos os brasileiros.

Atualmente, a entidade ocupa uma função estratégica no desdobramento de temas fundamentais à sustentabilidade do sistema. Representante de hospitais reconhecidos pela certificação de qualidade e segurança no atendimento hospitalar, a Anahp está preparada para fortalecer o relacionamento setorial e contribuir para a reflexão sobre o papel da saúde privada no país.

CONSELHO DE ADMINISTRAÇÃO

Presidente: Eduardo Amaro | Hospital e Maternidade Santa Joana (SP)
Vice-presidente: Henrique Neves | Hospital Israelita Albert Einstein (SP)

Délcio Rodrigues Pereira | Hospital Anchieta (DF)
Fernando Torelly | Hospital do Coração - HCor (SP)
Henrique Moraes Salvador | Hospital Mater Dei (MG)
Paulo Azevedo Barreto | Hospital São Lucas (SE)
Paulo Chapchap | Hospital Sírio-Libanês (SP)
Paulo Junqueira Moll | Hospital Barra D'Or (RJ)

SUMÁRIO

INTRODUÇÃO

O ano de 2020 entrará para a história por inúmeras razões, não só por ser o ano em que o Regulamento Europeu de Proteção de Dados (*General Data Protection Regulation* – GDPR) completa dois anos de vigência e a Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) entra em vigor no Brasil, mas, especialmente, porque foi o ano em que o mundo parou em razão da pandemia ocasionada pelo novo coronavírus (SARS-CoV-2).

Este novo vírus, originário da região de Wuhan, na China, surgiu nos noticiários de todo o mundo em dezembro de 2019 e se espalhou rapidamente por 177 países nos primeiros meses de 2020, apresentando um lamentável saldo de mais de 30 milhões de infectados e quase 1 milhão de mortos em todo o globo[1].

A COVID-19 resultou em uma situação atípica de pandemia, surpreendendo até mesmo órgãos internacionais, como a Organização Mundial da Saúde (OMS), que se equivocou quanto à classificação da doença ao considerá-la como de risco moderado no início da crise.

Com sua rápida proliferação, a OMS retificou seu posicionamento, alterando o status da disseminação do novo coronavírus para risco alto e anunciando a situação de pandemia em todo o mundo .

E, se até grandes instituições internacionais como a OMS[2], que está habituada a lidar com situações novas e desafiadoras, apresentaram

1 https://www.worldometers.info/coronavirus/?utm_campaign=homeAdvegas1?%22 Informações do jornal The New York Times, última atualização em 14 de abril de 2020.

2 A OMS admitiu o erro de classificação de risco no dia 28 de janeiro e decretou a situação de pandemia no dia 11 de março, ambos de 2020.

dificuldades durante a gestão de informações e equipes diante da crise da COVID-19, como os hospitais e profissionais da saúde em geral devem se portar diante de tal cenário?

Os desafios impostos pela pandemia também trouxeram a necessidade de mudanças, não a curto, médio ou longo prazo, mas já. E isso também modificou de forma radical os processos. Ferramentas como a telelemedicina, que ainda estavam sendo discutidas no Brasil, foram imediatamente implementadas e se tornaram essenciais.

Os investimentos no mundo digital deixaram de ser complementares e passaram a ser o ponto chave em qualquer relação social cotidiana e, no centro de cada uma dessas mudanças, está a capacidade de coleta, análise e armazenamento seguro de dados e informações, para evolução do atendimento, ciência, tecnologia e demais setores da sociedade.

O manual nasce nesse momento, em que a Anahp – Associação Nacional de Hospitais Privados também se reconstrói para continuar sendo uma entidade de relevante representatividade para o setor de saúde, ciente de seu papel de fomentar melhores práticas e auxiliar seus hospitais-membros e demais instituições de saúde a se adequarem a essa nova fase que o mundo enfrenta e que, por certo, desencadeará uma nova era.

Nesse momento, se faz necessário buscar o máximo de informação disponível e adotar um posicionamento proativo e preventivo, adotando melhores práticas e planejamento estratégico. Uma coisa é certa: nunca foi tão importante implementar proteção de dados pessoais considerando todo este contexto, que vem exigindo imensurável fluxo de informações sensíveis, especialmente relacionadas à saúde e aos pacientes em todo o mundo.

Com tudo isso, a Anahp, em parceria com o escritório PG Advogados, desenvolveu o presente Manual Melhores Práticas LGPD, focado na aplicação de questões práticas envolvendo a proteção de dados pessoais e cujo resultado é fruto de uma ampla pesquisa baseada nas regulamentações de proteção de dados pessoais GDPR e LGPD, na melhor prática adotada em diversos países, compartilhada através do site da *Global Privacy Assembly (GPA)* e do *European Data Protection Board* (EDPB), além das recomendações de segurança presentes nas ISOs 27001, 27701 e pelo *The Health Insurance Portability and Accountability Act of 1996* (HIPAA).

1 PROTEÇÃO DE DADOS: ASPECTOS CONTEMPORÂNEOS

A aplicação de ações e a implementação da cultura de proteção de dados não é uma atividade que se realiza do dia para noite. Por isto mesmo, é sempre importante observar e analisar quais as melhores práticas na temática.

E, por essa razão, este manual se propõe a dar direcionamentos práticos às atividades envolvendo proteção de dados.

De maneira geral, observa-se que mesmo os países mais consolidados do ponto de vista cultural em relação à proteção de dados vêm enfrentando dificuldades na implementação das regras impostas pelos regulamentos.

É o caso dos países que compõe a União Europeia (UE). Segundo informações do portal Financial Times empresas menores têm se mostrado mais "particularmente afetadas pelos custos de conformidade com o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR)"[3].

3 ESPINOZA, Javier. EU admits it has been hard to implement GDPR. Finacial Times, 23 jun 2020.

De todo modo, diversos setores e organizações têm sentido dificuldades na aplicação prática do *compliance* em proteção de dados, entendendo que "mais desafios estão à frente para esclarecer como aplicar os princípios a tecnologias específicas"[4]. A principal razão desta dificuldade é atribuída à "falta de uma abordagem consistente"[5] entre as autoridades de proteção de dados de cada país membro da UE.

No caso específico do Brasil, são dois os principais desafios: i) a instabilidade regulatória do país frente ao tema, ii) a falta de direcionamento por parte da Autoridade de Proteção de Dados Nacional. E, neste aspecto, a pandemia causada pela COVID-19 tem colaborado com a maior confusão do cenário brasileiro.

Isso porque, em razão da pandemia e consequente imposição de políticas de quarentena, o poder legislativo nacional discutiu a postergação do início da vigência da Lei Geral de Proteção de Dados (LGPD), que

4 ESPINOZA, Javier. EU admits it has been hard to implement GDPR. Finacial Times, 23 jun 2020.

5 Idem à nota 4

acabou por entrar em vigor no dia 18/09/2020.

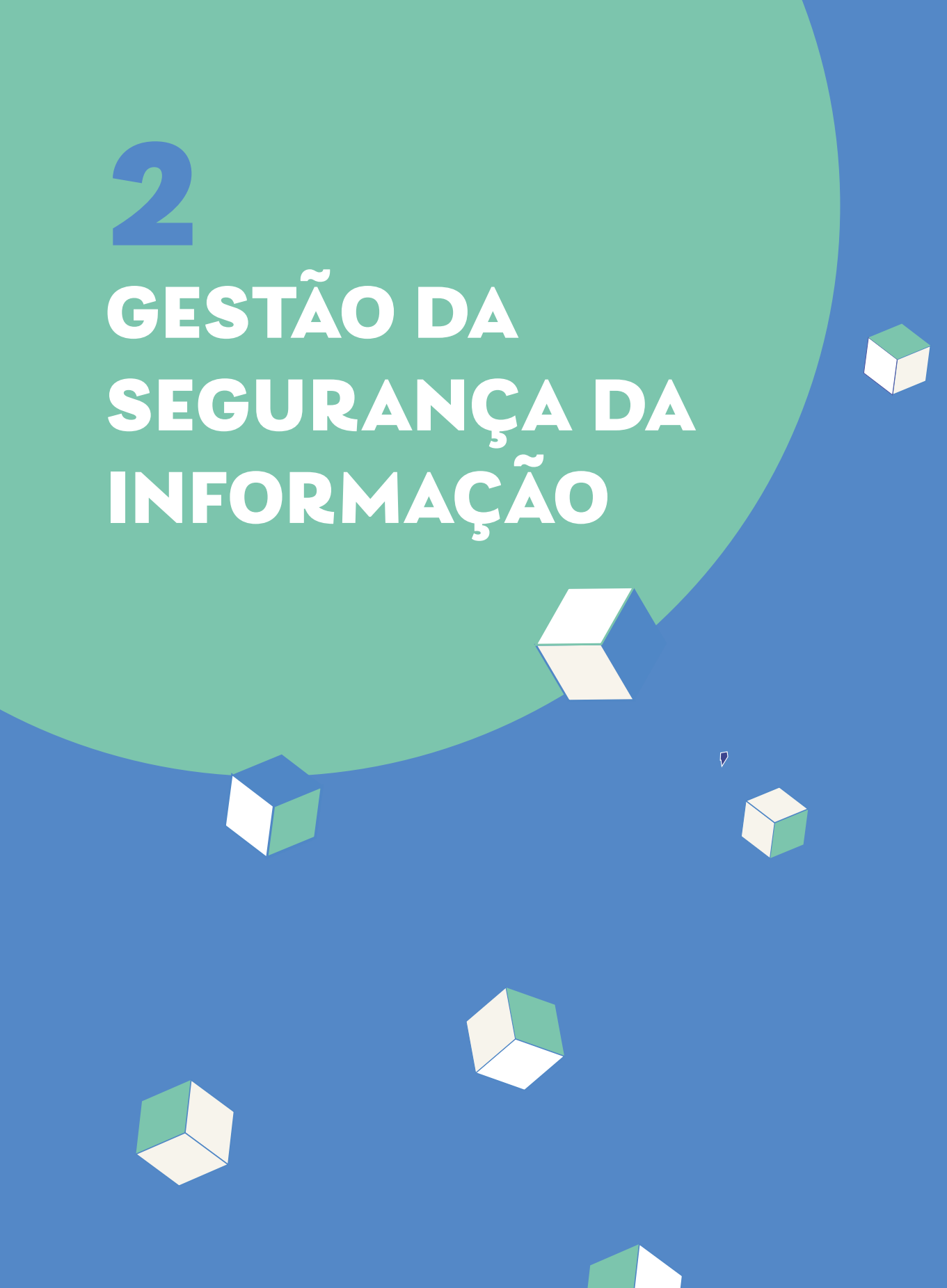
Independentemente dos desdobramentos políticos, é sabido que a necessidade de implementação e desenvolvimento de uma cultura de proteção de dados é essencial para o pleno desenvolvimento de toda e qualquer instituição do século 21.

Com isto, pode-se afirmar que as organizações – públicas e privadas – devem, sim, adotar políticas internas de **conformidade de proteção de dados** em todas as etapas de sua operação – desde a concepção *(by design)* e por padrão *(by default)*.

Mas isso não significa que as organizações precisarão limitar as suas atividades para estar em *compliance* com as regulações nacionais e internacionais: é tudo uma questão de adaptação de rotinas. E é isto que essa segunda publicação da Anahp sobre o tema busca mostrar.

2

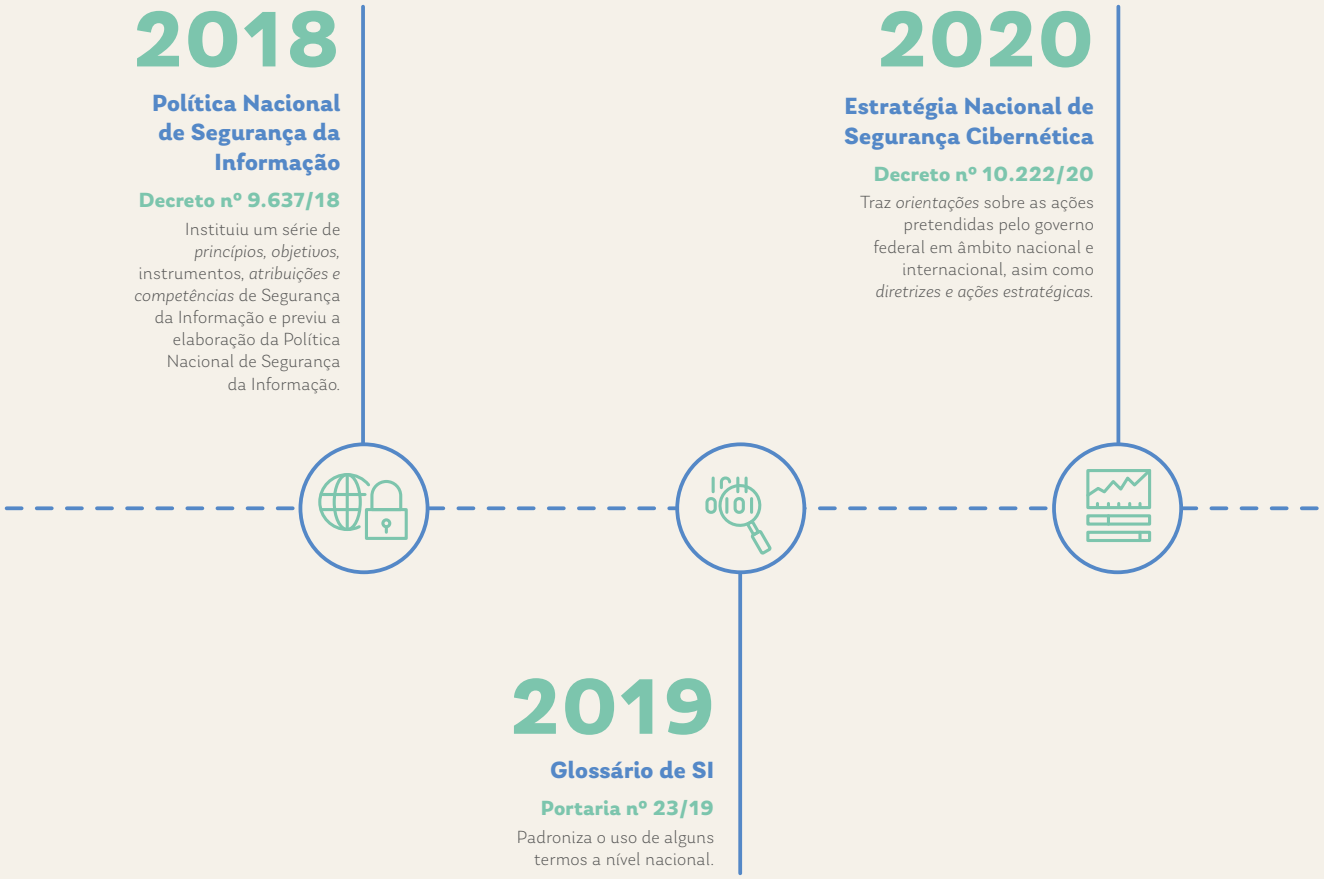
GESTÃO DA SEGURANÇA DA INFORMAÇÃO



Do mesmo modo em que o Brasil vive uma instabilidade regulatória em relação à proteção de dados, isso acontece também com a questão da segurança da informação.

De maneira sucinta, o panorama regulatório brasileiro atual sobre a regulação cibernética segue a linha do tempo a seguir.

***Figura 1** | Linha do tempo da regulação cibernética no Brasil*



Fonte: PG Advogados, 2020.

Assim como na questão da proteção de dados, a regulação brasileira em relação à gestão da informação não traz indicações práticas para a sua aplicação. O que leva as organizações a adotarem padrões de aplicação com base na boa-fé das relações.

2.1 SISTEMA DE SEGURANÇA DA INFORMAÇÃO

O primeiro passo para que uma instituição consiga realizar uma boa gestão da informação é a aplicação de um Sistema de Gestão de Segurança da Informação. Através deste sistema, os processos internos conseguem se manter seguros contra as ameaças cibernéticas de maneira muito mais coesa e preventiva.

É praticamente um senso comum a ideia de que as ameaças virtuais têm aumentado exponencialmente nos últimos anos – tanto no volume quanto na sofisticação dos ataques. E as pesquisas comprovam esta sensação.

De acordo com o levantamento "*Allianz Risk Barometer*", de janeiro de 2020, os incidentes cibernéticos são classificados como o mais temido risco de negócio mundialmente, representando 39% das respostas dos participantes[6].

6 O estudo da Allianz analisou a resposta de mais de 2.700 especialistas em gerenciamento de riscos em mais de 100 países do mundo. Para maiores informações, acesse: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html.

No ambiente da saúde esta preocupação é, particularmente, maior, tanto porque os dados em tratamento nestas instituições são dados sensíveis e de protocolo confidencial, quanto porque com a maior introdução do uso do *big data* na rotina de saúde[7] e o desenvolvimento da Internet das Coisas (IoT) na área médica a atenção deve ser maior[8].

De forma sucinta, considera-se Sistemas de Gestão de Segurança da Informação (SGSI) sistemas corporativos que incluem os processos organizacionais ou parte deles, cuja meta é a proteção das informações da instituição dentro dos critérios de confidencialidade, integridade e disponibilidade (CID) da organização [9,10].

Em resumo, pode-se dizer que o SGSI são os planos, estratégias, políticas, medidas e controles desenvolvidos em prol da segurança da informação, de modo que este sistema tem como objetivo a implementação, monitoração, análise, manutenção e otimização da segurança da instituição.

---

7 Com o avanço da tecnologia, tem se tornado cada vez mais possível utilizar os dados de aplicativos de saúde para avaliar a qualidade de vida geral de um paciente. Na Universidade de San Diego, nos Estados Unidos, há um grande núcleo de pesquisa voltada ao uso de *big data* para a melhoria da rotina e procedimentos de saúde, mostrando que o uso do *big data* em favor da saúde é uma realidade a cada dia mais desenvolvida.

8 Segundo a Pesquisa Global de Segurança da Informação de 2017, realizada pela PwC, a expansão da Internet das Coisas introduz "novos riscos que ainda não são bem compreendidos e podem ter implicações abrangentes". A pesquisa ainda destaca que 46% das organizações planejam investir novos modelos de segurança baseados nas necessidades mais recentes do mercado.

9 FONTES, Edison. Políticas e normas para segurança da informação. Rio de Janeiro: Brasport, 2012. p.17-22.

10 Para relembrar o que é a CID, consulte o Manual LGPD – Recomendações Anahp para os hospitais, disponível em: https://conteudo.anahp.com.br/cartilha-lgpd-anahp.

Como se pode notar, o SGSI tem a meta de tornar o risco em gestão da informação o menor possível, haja visto que tornar este risco igual a zero não é possível[11].

Ao mesmo tempo, é preciso entender que um SGSI envolve máquinas e pessoas. Portanto, de nada adianta adotar um *software* super moderno e completo para cuidar da segurança da informação de seu hospital, se as pessoas que manuseiam tal sistema não estão introduzidas em uma cultura em prol da segurança da informação.

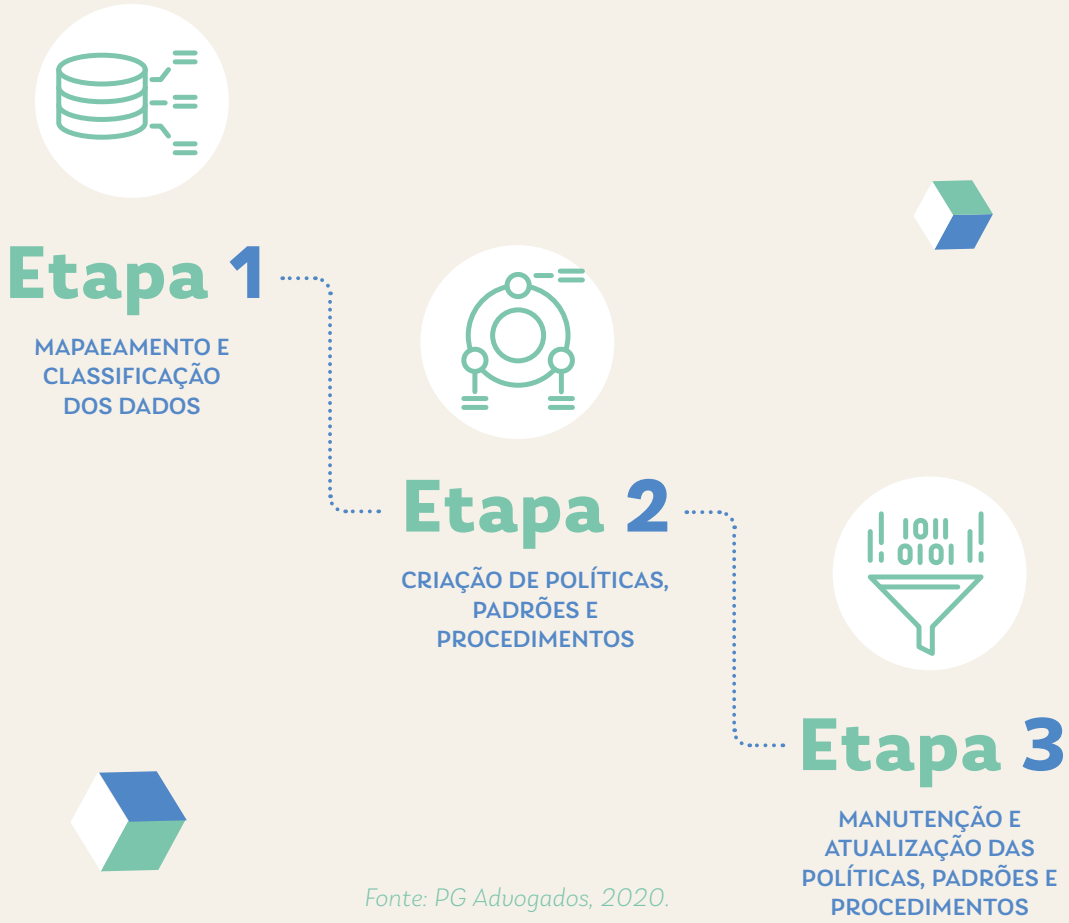
Da mesma forma, é necessário dizer que certas situações ainda devem ser avaliadas sob a perspectiva da subjetividade humana, para que a melhor decisão seja tomada diante de situações reais.

---

11 Tácito Leite aponta que "não existe sistema ou *software*, por mais avançado que seja, que resolva por si questões relacionadas a riscos e defina sozinho qual a melhor decisão a ser tomada". LEITE, Tácito Augusto Silva. **Gestão de Riscos na Segurança Patrimonial**. Rio de Janeiro: Qualitymark, 2016. p. 52

Em linhas gerais, para o pleno funcionamento de um SGSI, é necessário serem cumpridas algumas etapas, como aponta a figura a seguir:

Figura 2 *| Etapas de desenvolvimento de um SGSI*



Fonte: PG Advogados, 2020.

ETAPA 1

A primeira etapa a ser cumprida é o mapeamento e classificação das informações. E esta classificação deve ser realizada sob o parâmetro dos impactos, ou seja, cada informação é analisada e classificada de acordo com as consequências que sua perda traria à instituição.

A classificação das informações, usualmente, segue os indicadores:

I) Pública: pode ser compartilhada interna e externamente;

II) Interna: deve ficar restrita ao ambiente interno da instituição;

III) Confidencial: informação a qual somente alguns funcionários específicos têm acesso e deve ser restrita a estas pessoas e ambiente.

Com a regulamentação de proteção de dados, estes passaram a ser classificados como dado pessoal e dado pessoal sensível, sendo que quando enquadrados neste perfil devem receber medidas de proteção.

ETAPA 2

O segundo passo é a criação de políticas, padrões e procedimentos voltados ao escopo de ações e práticas em prol da segurança da informação e da proteção de dados. Para que a instituição supra suas necessidades internas e esteja em conformidade com as obrigações legais e contratuais que tem para com o Estado, seus clientes, colaboradores e demais *stakeholders*, deverá considerar a segurança de

informação como um aspecto essencial ao conjunto operacional da gestão empresarial. Esta mentalidade deve permear toda a instituição, de forma que pessoas em todos os níveis hierárquicos estejam conscientizadas da importância das ações de adequação e manutenção de um programa de proteção de dados.

Sob a ótica da proteção de dados, pode-se apontar seis domínios de implementação essenciais para toda e qualquer instituição, dos quais:

1. ***Governança de proteção de dados;***
2. ***Gestão de dados pessoais;***
3. ***Segurança da informação;***
4. ***Gestão de risco dos dados pessoais;***
5. ***Gestão de dados pessoais em terceiros;***
6. ***Gestão de incidentes.***

ETAPA 3

O terceiro e último passo é a manutenção dos padrões e modelos estabelecidos, de maneira que todas as atualizações e melhorias necessárias sejam realizadas ao longo do tempo.

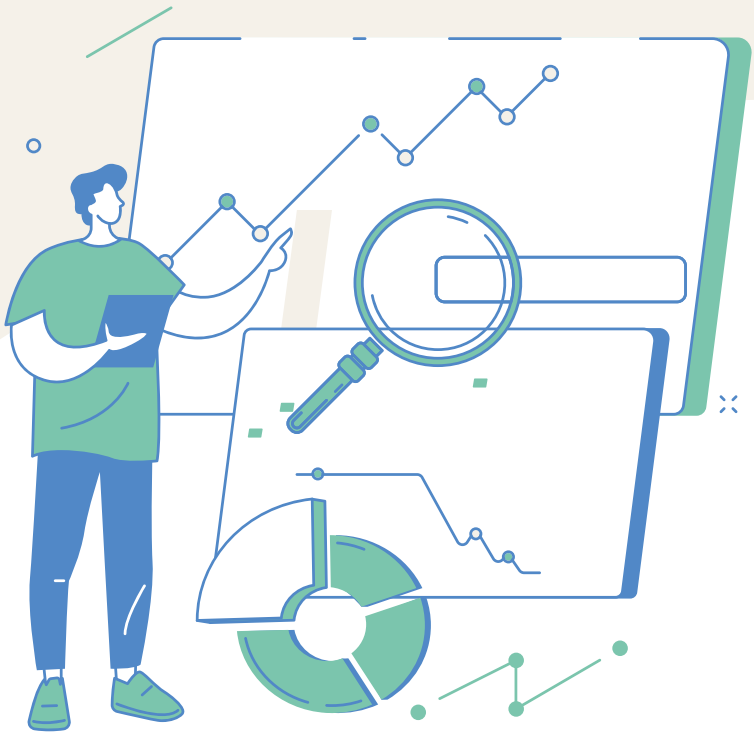
Nessa etapa, é muito comum que se realizem testes de vulnerabilidade, para que seja possível identificar as vulnerabilidades em uma rede ou sistemas, com o objetivo de garantir a segurança da informação.

No processo de análise de vulnerabilidades é possível identificar ameaças e mensurar os riscos que elas representam. Usualmente, utiliza-se

ferramentas de automatização que geram relatórios de avaliação de vulnerabilidade. Contudo, apesar deste material apontar as ameaças, é importante ter um time especializado em segurança da informação para estudar os resultados, pois assim é possível priorizar com um olhar crítico os possíveis riscos.

Um bom relatório de avaliação de vulnerabilidade deve conter os nomes das ameaças, a descrição e a gravidade – baixa, média ou alta. Com estes dados em mãos, é possível avaliar as fraquezas e realizar as correções e aprimoramentos necessários.

É importante considerar que os processos de segurança estão em constante atualização e modificação. Por isso, esta última etapa é muito fundamental, já que não basta apenas criar e aplicar um bom sistema de segurança da informação, é necessário sempre atualizar o modelo desenvolvido frente às novas necessidades de proteção que surgem.



2.2
ANÁLISE DE RISCO: CONTRATAÇÃO ENTRE CONTROLADOR E O OPERADOR

Quanto aos controles adequados relativos à Governança da Proteção de Dados e ao próprio SGSI, faz-se necessária a compreensão e identificação dos agentes que atuam e compõem a relação de tratamento de dados pessoais.

Seguindo as práticas adotadas internacionalmente, a Lei 13.709/2018 (LGPD)[12] define como agentes de tratamento aqueles indivíduos que efetuarão, efetivamente, a manipulação e compartilhamento dos dados pessoais dos titulares, distinguindo-os em razão da sua capacidade de decisão, sendo eles:

I) Controlador: pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais;

II) Operador: pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

12 Art. 5º, VI e VII/LGPD

Estes agentes são muito importantes quando o tema são as sanções previstas em casos de violação. Isso porque a legislação estabeleceu atribuições a cada um dos agentes de tratamento de acordo com o seu respectivo papel decisório. A diferenciação entre ambos se encontra, portanto, em relação ao seu poder de decisão e papéis no tratamento de dados pessoais. De todo modo, a responsabilidade em relação ao tratamento de dados é solidária[13,14].

A LGPD ainda traz a previsão de que, caso identifique-se que o operador agiu em desconformidade com a lei ou com as orientações recebidas pelo controlador, deve responder pelos danos causados, de maneira que a responsabilidade solidária pode ser superada. O referido também é válido para as situações em que os agentes comprovem culpa exclusiva do titular de dados ou terceiros[15].

Neste sentido, uma boa prática para mitigação de riscos consiste na **identificação da posição ocupada pela instituição no tocante ao tratamento de dados pessoais,** que deverá ser analisado caso a caso.

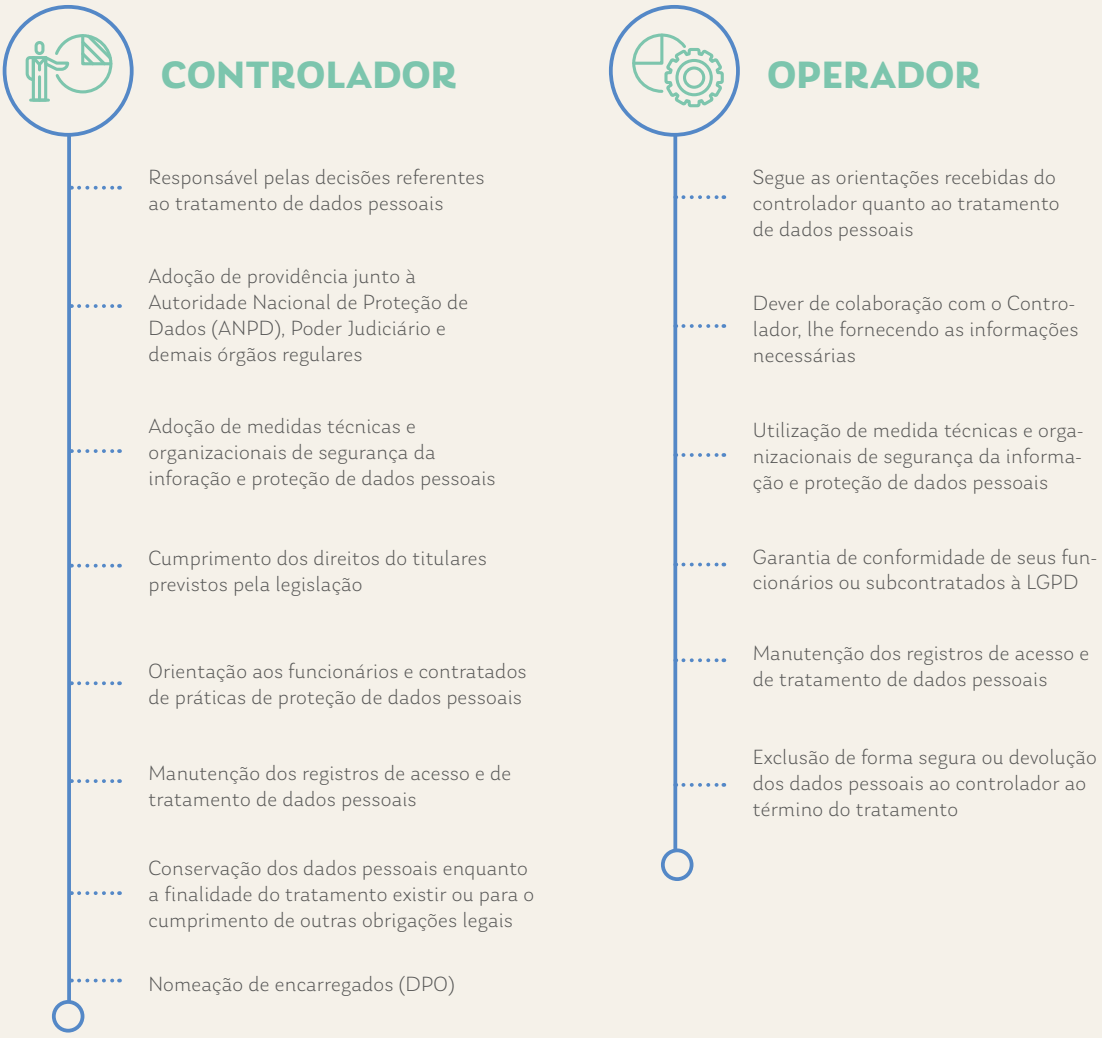
13 Em linhas gerais, responsabilidade solidária quer dizer que as partes compartilham das responsabilidades em relação ao tratamento de dados.

14 Art. 42/LGPD.

15 Art. 43/LGPD.

A partir de então, ações pontuais serão necessárias, conforme quadro a seguir:

Figura 3 *| Atribuições de controlador e operador*



Fonte: PG Advogados, 2020.

Especificamente com relação ao ambiente hospitalar, é importante observar que existem fluxos constantes de compartilhamento de dados pessoais, muitos deles de saúde e classificados como sensíveis[16], seja entre profissionais de saúde, pacientes, operadoras de planos de saúde, laboratórios, clínicas, serviços de transporte de urgência e emergência etc.

Isso aumenta ainda mais a necessidade da adoção de tais medidas, uma vez que um incidente de segurança ou vazamento de dados pessoais pode acarretar sérios prejuízos.

A partir de tal análise, recomenda-se atenção às seguintes etapas com relação ao tratamento:

I) IDENTIFICAÇÃO DA POSIÇÃO OCUPADA: verificar se é a de controlador ou operador, uma vez que ela pode variar conforme o grau de autonomia para tratamento dos dados pessoais e sua relação com o titular;

II) APLICAÇÃO DAS MEDIDAS: elencadas na Figura 4;

III) ADITIVOS CONTRATUAIS E/OU CLAUSULADOS: formalização por meio de aditivo contratual e/ou clausulados contratuais das posições ocupadas e obrigações assumidas, deixando mais claro as responsabilidades e os deveres, controles de segurança,

16 Conforme já explanado no Manual LGPD – Recomendações Anahp para os hospitais (disponível em: https://conteudo.anahp.com.br/cartilha-lgpd-anahp), dados pessoais sensíveis, conforme o artigo 5º. Inciso II da LGPD é o dado pessoal sobre 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 vinculado a uma pessoa natural.

finalidades específicas, limites de utilização dos dados pessoais, bem como o acordo de níveis de serviço (*Service Level Agreement* – SLA) para informação sobre possíveis situações de violação e dever de reporte;

Ressalta-se que a adição de cláusulas contratuais entre as partes é de fundamental importância, já que poderá destacar as obrigações específicas que devem ser observadas em relação ao tratamento de dados pessoais, como formas de utilização, compartilhamento, confidencialidade, tempo de armazenamento e exclusão.

A identificação e definição de tais conceitos é crucial para o desenvolvimento, não só da mitigação dos riscos que envolvem o processo de tratamento de dados pessoais, como também para a implementação das ações a serem praticadas.

Além disso, traz uma visão clara e ampla de quais são as obrigações legais a serem observadas, bem como daquelas previsões que deverão ser estipuladas a partir de instrumentos contratuais, diante das necessidades do caso.

A LGPD define, ainda, no tocante à responsabilidade, em seu artigo 42, que: o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Isso significa que respondem pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança, der causa ao dano.

Figura 4 *| Aplicação das medidas*

Responsabilidade do controlador	**Responsabilidade do operador**
Responde solidariamente (diretamente envolvido no tratamento, salvo exceções)	Responde solidariamente quando descumpridas as obrigações da legislação de proteção de dados ou quando não forem seguidas instruções lícitas do controlador

Fonte: PG Advogados, 2020.

A própria legislação traz, ainda, a exceção de responsabilidade, mostrando que é fundamental ter evidência que demonstre a quem cabia o dever e, por isso, é tão relevante a averiguação do incidente e reunião das provas adequadamente, conforme o artigo 43, que diz que "não haverá responsabilização quando comprovado que":

I - não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados, ou;

III - o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Portanto, se puder ser comprovada a culpa exclusiva, seja de um titular ou de terceiros, evidenciando que a instituição controladora dos dados não foi responsável pelo vazamento e, sim, um parceiro ou fornecedor, ela não será responsabilizada, recaindo apenas sobre o terceiro.

Na hipótese de eventual judicialização, o magistrado poderá inverter o ônus da prova a favor do titular. E aquele que reparar o dano poderá agir em direito de regresso contra os demais responsáveis. Com isso, verifica-se a importância de manter tudo documentado, desde os contratos até a resposta a um incidente de segurança da informação, para fins de atendimento de conformidade à LGPD e melhor gestão institucional dos riscos.

Não obstante a possibilidade de judicialização, a Autoridade Nacional de Proteção de Dados (ANPD) também poderá ser acionada para manifestação de seu entendimento em casos de responsabilidade dos agentes de tratamento.

2.3
SEGURANÇA DE DADOS EM *CLOUD*

Diante do grande volume de dados e informações eletrônicas gerados e utilizados no cotidiano das instituições de saúde, torna-se necessária a identificação das melhores estratégias para a sua gestão, especialmente no uso de recursos de *cloud computing* (serviço de computação ou armazenagem na nuvem), mantendo-se sempre os critérios de segurança da informação, tais como confidencialidade, integridade e disponibilidade.

Além de estar de acordo com os procedimentos e documentos existentes e de integrarem a segurança da informação da instituição, é fundamental que a opção por tal modalidade de gestão seja pensada junto à análise de determinados requisitos com relação à segurança dos dados.

Inicialmente, deve-se verificar se o fornecedor escolhido disponibiliza de recursos como:

I) Garantias de privacidade e segurança;

II) Criação de backups e salvaguardas dos conteúdos das comunicações realizadas e a possibilidade de consulta de dados;

III) Procedimentos e metodologias para contenção e resposta a incidentes de segurança da informação e dados pessoais;

IV) Garantia do ciclo de vida da informação;

V) Documentações e processos formalizados de gestão e mudanças;

VI) Garantia de auditabilidade e rastreabilidade;

VII) Acordos de níveis de serviço (SLAs).

Com relação à segurança dos dados pessoais, cabe à instituição avaliar junto ao fornecedor a sua capacidade de atestar informações referentes às medidas adotadas neste aspecto, devendo ser capaz de demonstrar:

I) Diretrizes de tratamento de dados pessoais;

II) Modo de atendimento a solicitação de titulares de dados pessoais;

III) Medidas protetivas para garantia da confidencialidade dos dados pessoais;

IV) Medidas protetivas durante as comunicações com a instituição (como exemplo, aplicação de proteção para credenciais de acesso, criptografia, outros padrões de segurança aplicados em transmissão e/ou armazenagem de dados);

V) Registros de atividades de tratamento de dados pessoais (a guarda das evidências é fundamental, bem como a definição do tempo de guarda – tabela de temporalidade);

VI) Monitoração de atividades suspeitas e disparo de alertas (avisos), lembrando que é importante haver o aviso legal de ambiente monitorado;

VII) Solicitação de autorização na subcontratação de terceiros para atividades de tratamento de dados pessoais;

VIII) Medidas de devolução/descarte dos dados.

Caso a solução de gestão de dados em nuvem seja implementada, tais considerações são muito importantes para ser realizada com enfoque na proteção de dados. Uma recomendação de melhor prática importante é a solicitação de uma declaração do fornecedor, em que apresente conformidade com a nova regulamentação de proteção de dados pessoais vigente no Brasil. Isso pode ser feito de forma apartada (documento em separado) ou inserido em uma cláusula contratual.

Além de mitigar os riscos de eventuais incidentes e/ou violações, tais aspectos auxiliaram a instituição em sua adequação às normas legais atinentes.

Importante destacar que, dada a característica de grande parte dos dados pessoais tratados em ambiente hospitalar, a segurança destas informações deve ser o ponto de principal atenção para a garantia de sua adequada utilização, não sendo possível renunciar a tais requisitos.

2.3.1 MECANISMOS DE PREVENÇÃO DE PERDA DE DADOS - *DATA LOSS PREVENTION*

No contexto da disseminação do uso de guarda de dados em nuvem, é de pontual relevância adotar Mecanismos de Prevenção de Perda de Dados. Em suma, tais mecanismos são centrados na proteção dos dados e buscam evitar problemas de acesso ou armazenamento. Neste sentido, apontam-se algumas boas práticas:

1. ***Mantenha os procedimentos e sistemas sempre atualizados*** – deste modo, é possível evitar ameaças e proteger os dados de maneira contínua;

2. ***Adote políticas de acesso personalizadas às necessidades da corporação*** – nem sempre é necessário que todos os funcionários tenham acesso ao ambiente geral da corporação, por isso, adotar políticas de permissão de acesso de acordo com níveis e necessidades reais é uma ótima estratégia;

3. ***Garanta a adesão dos procedimentos de segurança da informação em todos os dispositivos*** – com a possibilidade da mobilidade de acesso aos dados, nem sempre o colaborador vai

acessar as informações por meio das ferramentas da instituição, por exemplo, podendo utilizar *smartphones, tablets* e computadores pessoais. Todavia, cabe à instituição garantir que em todos estes ambientes os padrões de segurança sejam adotados quando é feito o acesso aos dados, como conexões de rede privada (VPN) ou até mesmo localização do IP;

4. ***Forneça mecanismos de identificação dos dados –*** categorizar os dados de acordo com seu uso (em uso ou ocioso), movimento (trafegando pela rede) e armazenamento (local ou *cloud*) é essencial para garantir maior controle das informações.

2.4
PADRÕES DE ACORDOS DE NÍVEIS DE SERVIÇO (*SERVICE LEVEL AGREEMENT* – SLA) EM CONTRATOS COM TERCEIROS

Realizar as atividades da instituição junto a terceiros traz alguns riscos ao ambiente interno[17]. Deste modo, é preciso assegurar que os procedimentos e garantias internas sejam validados na empresa parceira.

Neste contexto, confira a seguir algumas dicas valiosas em relação à contratação de terceiros[18]:

17 De acordo com o Relatório Global de Fraude e Risco, publicado pela Kroll em 2017, dentre os executivos entrevistados, 27% afirmaram que os principais responsáveis pelos incidentes de fraudes foram os funcionários autônomos ou temporários e 26% apontou vendedores/ fornecedores, ou seja, parceiros das empresas centrais.

18 PETERS, Michael. 5 best practices for Outsourcing Cyber Security & Compliance Services. Cybersecurity Ventures, set, 2017.

1. *Estude a empresa parceira:* valide as informações da empresa contratada, solicite referências, se possível verifique se não há inconsistências cadastrais ou de informações, bem como histórico de medidas judiciais relacionadas à prestação do serviço. Certifique-se de que ela aparenta ser responsável, aplica todos os procedimentos para a garantia da segurança da informação e que está, ao menos, no nível mínimo de segurança que a sua instituição espera;

2. *Conheça o processo interno da empresa parceira*: não hesite em pedir informações acerca das auditorias e processos de *compliance* realizados pela empresa a ser contratada, de maneira que seja possível conhecer o processo de validação e garantia de segurança da empresa na prática. Dependendo o tipo de contratação e sua criticidade pode ser relevante solicitar a apresentação de alguma certificação específica ou mesmo um seguro (veja no quadro abaixo);

3. *Documente tudo:* não deixe de registrar tudo o que foi acordado entre a sua instituição e a terceira, pois assim que a documentação é feita a sua garantia – e a do parceiro – é clara, transparente e pode ser checada a qualquer momento, de maneira que, se surgir alguma dúvida, todos saberão onde procurar a resposta e isto é acessível a todos.

Dica: certificações e seguros relacionados à segurança e proteção de dados

Nos últimos anos, aumentou a importância da apresentação da aplicação de medidas de controle auditáveis relacionadas à segurança da informação e proteção de dados pessoais. Sendo assim, há algumas melhores práticas de mercado e ISOs que podem ser consideradas, além de alguns seguros específicos:

1. ISOs 27001, 27002, 27701

2.NIST

3. Seguro Ciber de Risco Cibernético

2.5 DIREITOS DOS TITULARES DE DADOS

Os titulares de dados pessoais têm direitos e garantias especificados pela LGPD. Cabe à instituição assegurar que sejam passíveis de serem acessados e exercidos desde o início do processo de tratamento de dados e ao longo de toda a vida do processamento, inclusive no término. São eles, conforme os artigos 6º, 18 e 20 da LGPD:

1. Confirmação da existência de tratamento;

2. Acesso aos dados;

3. Correção dos dados incompletos, inexatos ou desatualizados;

4. Anonimização, bloqueio ou eliminação (apagamento) dos dados desnecessários, excessivos ou tratados em desconformidade;

5. Portabilidade a outro fornecedor mediante requisição expressa;

6. Eliminação dos dados tratados com o consentimento (pedido de apagamento);

7. Informação das entidades com os quais houve compartilhamento dos dados pessoais;

8. Informação sobre consequências de não fornecer o consentimento;

9. Revogação de consentimento;

10. Não discriminação no uso dos dados;

11. Revisão de decisões automatizadas.

Isso também significa que a instituição deve estar apta a atender ao dever de *report* dentro de um tempo hábil – a legislação brasileira não pontua, mas o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR) define o tempo de reporte de até 72 horas (art. 48/LGPD e art. 33/GDPR) – e para atender à requisição do titular o regulamento brasileiro aponta o prazo de 15 dias (art. 18 e 19/LGPD). Caso o fluxo não respeite estes aspectos, a instituição está passível a sanções, haja visto o princípio da responsabilização e prestação de contas.*

* Conteúdo atualizado em 20/11/2020.

2.6
ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

Primeiramente, a LGPD traz claramente o conceito de anonimização, que consiste em seu artigo 12: Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Sendo assim, é considerado anonimizado o dado pessoal se não houver reversibilidade do processo aplicado.

A própria lei traz também o conceito de pseudonimização em seu artigo 13, § 4º, definindo como: o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Existem várias metodologias de anonimização, entre elas por agregação/ƙ-anonimato ou por diversidade, em que os dados pessoais específicos ficam generalizados, como ocorre com a idade, que vira uma faixa etária, ou com o endereço, que fica apenas com alguns números de referência, conforme os exemplos a seguir[19]:

19 Fonte: https://personal.utdallas.edu/~mxk055100/courses/privacy08f_files/ldiversity.pdf

TABELA COM DADOS SENSÍVEIS			
QUASE-IDENTIFICADOR			ATRIBUTO SENSÍVEL
ID	IDADE	CEP	DOENÇA
1	5	15	Gripe
2	15	25	Febre
3	28	28	Diarreia
4	25	15	Febre
5	22	28	Gripe
6	32	35	Febre
7	38	32	Gripe
8	35	25	Diarreia

TABELA COM DADOS ANONIMIZADOS			
QUASE-IDENTIFICADOR			ATRIBUTO SENSÍVEL
ID	IDADE	CEP	DOENÇA
1	0-20	10-30	Gripe
2	0-20	10-30	Febre
3	20-30	10-30	Diarreia
4	20-30	10-30	Febre
5	20-30	10-30	Gripe
6	30-40	20-40	Febre
7	30-40	20-40	Gripe
8	30-40	20-40	Diarreia

Para que os procedimentos de anonimização e pseudonimização possam ser realizados de maneira efetiva e eficaz, é necessário observar alguns aspectos processuais e procedimentais, entre eles:

1. Elencar os processos de trabalho;

2. Identificar os dados a serem anonimizados ou pseudonimizados;

3. Analisar o ciclo de vida dos dados sob o aspecto da mitigação de riscos, de modo a propor o arquivamento ou eliminação de informações desnecessárias;

4. Avaliar o risco de identificação dos titulares dos dados anonimizados e/ou pseudonimizados;

5. Definir um plano de comunicação de incidentes em caso de violação de dados;

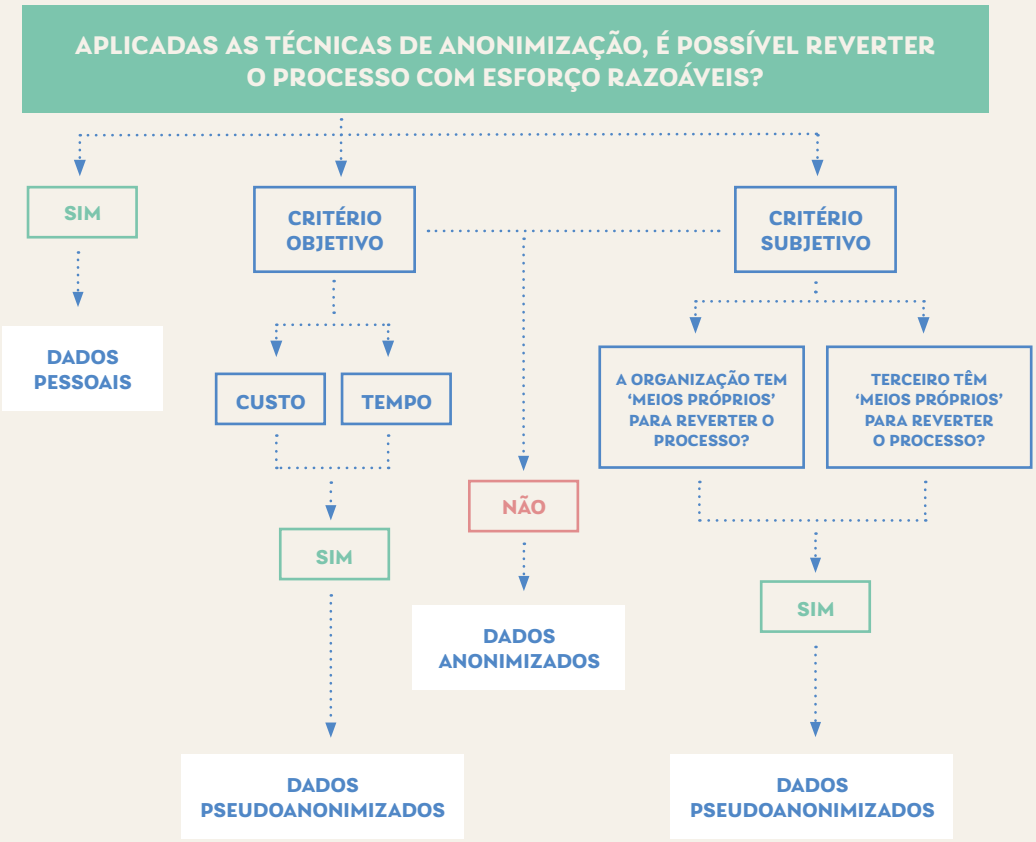
6. Documentar e relatar violações e incidentes;

7. Adotar uma política de análise de riscos periódica;

8. Conscientizar todos os colaboradores e equipes acerca dos processos e procedimentos necessários para a garantia da segurança dos dados;

E para não haver dúvidas sobre a efetividade do processo de anonimização ou pseudonimização dos dados, é necessário seguir o seguinte fluxo de checagem:

Figura 5 | *Fluxo de checagem em processo de anonimização*



Fonte: Releitura de BIONI, 2020[20] .

20 BIONI (2020) apud BIONI (2020).

Caberá à Autoridade Nacional de Proteção de Dados (ANPD) se posicionar e dispor sobre padrões e técnicas aplicados em processos de anonimização, além de verificar a segurança da informação utilizada para tanto. Até que isso aconteça, todavia, as instituições poderão se orientar pela metodologia sugerida neste manual, visto que estão em conformidade com as melhores práticas disponíveis na atualidade.

A *Health Insurance Portability and Accountability Act* (HIPAA) – lei norte-americana responsável por estabelecer as condições para o uso e o compartilhamento de dados referentes à saúde –, recomenda que, para que dados de pacientes possam ser considerados devidamente anonimizados, certos tipos de informação devem ser eliminados como nome, número de telefone, rua, cidade, CEP ou informações equivalentes, CPF, registro do paciente, número do plano de saúde, número da conta, dados biométricos, entre outros elementos que permitem a identificação do titular.

Ainda no que se refere à realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas. Além disso, devem ser mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico, e devem incluir, sempre que possível, a anonimização ou pseudonimização dos dados, considerando os padrões éticos[21] adequados e compatíveis com estudos e pesquisas em seres humanos, e levando em conta também as normativas da Comissão Nacional de Ética em Pesquisa (CONEP).

Neste sentido, a LGPD prevê expressamente que a divulgação dos

21 Artigo 13, LGPD.

resultados ou de qualquer excerto de estudo ou da pesquisa em saúde pública, realizados por órgãos de pesquisa, não poderão revelar dados pessoais. Conclui-se, portanto, pela necessidade de aplicação de técnicas de anonimização, sempre que possível, ou ao menos pseudonimização.

2.7
RELATÓRIO DE IMPACTO DE PROTEÇÃO DE DADOS

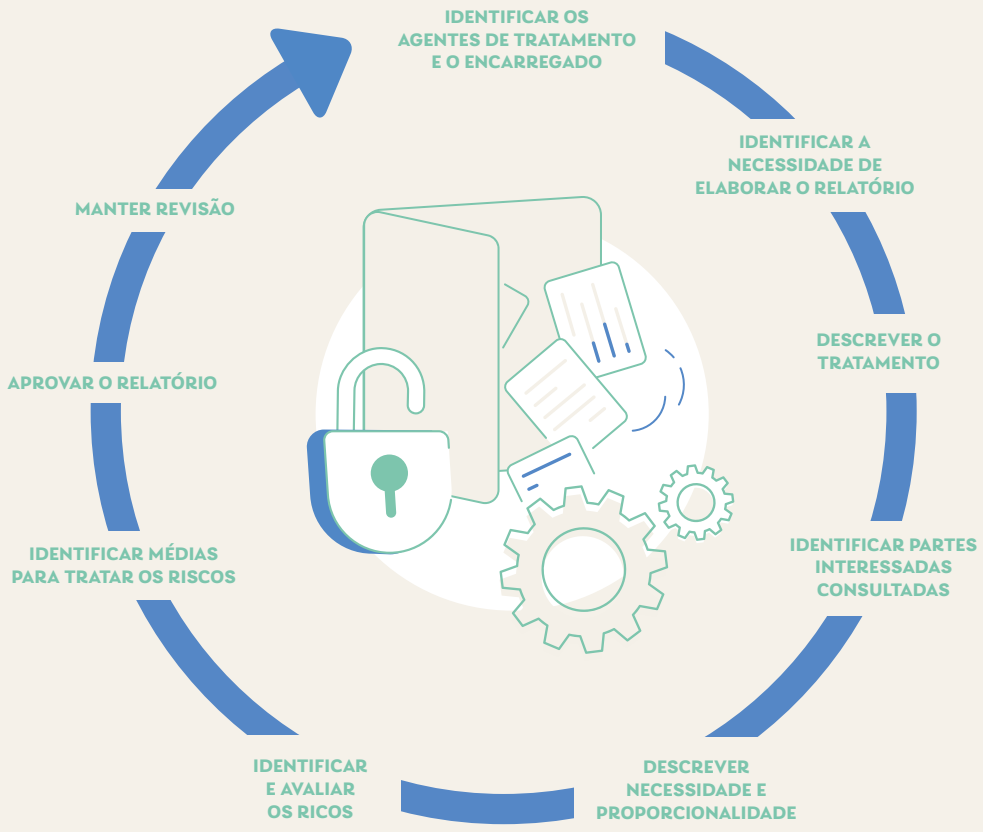
Dentre os procedimentos obrigatórios das organizações em relação ao tratamento de dados pessoais, há a necessidade de emissão de Relatórios de Impacto de Proteção de Dados (RIPD), conforme previsto pelos artigos 5º, inciso XVII e 10, § 3º, da LGPD.

Tais relatórios são documentos que contêm a descrição dos procedimentos adotados e dados pessoais em tratamento, com enfoque nos aspectos que podem gerar riscos às liberdades civis e nas medidas de mitigação de riscos e salvaguardas adotadas.

O RIPD deve documentar todas as etapas do tratamento de dados, desde a sua concepção (projeto) até sua execução e finalização

De acordo com o Guia de Boas Práticas em LGPD publicado pelo governo federal em abril de 2020, as etapas de elaboração do RIPD seguem o fluxo descrito na figura a seguir:

Figura 6 *| Fluxo de elaboração do RIPD*



Fonte: BRASIL. Guia de Boas Práticas: Lei Geral de Proteção de Dados. Abril, 2020 Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Serpro. Acesso em 03 ago. 2020.

Importante pontuar que pode ser necessário elaborar somente um RIPD para toda a instituição ou um RIPD para cada projeto, a depender da complexidade e riscos envolvidos.

Recomenda-se manter o relatório sempre atualizado, tendo em vista a previsão legal da autoridade de dados solicitar acesso ao documento.

OBRIGAÇÕES CONTRATUAIS E RESPONSABILIDADES

A adequação contratual é de suma importância para a efetivação das diretrizes expostas neste manual. Isto porque, através de instrumento elaborado entre as partes, serão determinadas as devidas obrigações e responsabilidades assumidas por cada parte, sem prejuízo das obrigações estipuladas na legislação aplicável.

Assim, os agentes de tratamento (controlador e operador) possuem obrigações decorrentes de Lei e do contrato, responsabilizando-se por todas elas, nos termos do artigo 42 da LGPD.

Em linhas gerais, os agentes de tratamento serão responsabilizados em caso de danos aos titulares ou a terceiros em decorrência do tratamento por eles realizado e deverão repará-los.

O fornecedor ou parceiro, enquanto operador dos dados pessoais em nome da instituição, sem prejuízo de demais obrigações e responsabilidades previstas neste manual e/ou impostas por instrumentos contratuais ou por lei, observará, obrigatoriamente, os requisitos a seguir. O não cumprimento de qualquer das condições listadas poderá ensejar na possibilidade de a instituição rescindir o contrato com justo motivo.

OPERADOR

Realizar o processo de adequação à LGPD, com o mapeamento dos fluxos de dados e implementação do plano de ação desenvolvido para o fornecedor ou parceiro;

Monitorar os sistemas físicos, lógicos e virtuais onde dados pessoais estão disponíveis;

Estabelecer com fornecedores e colaboradores que tratam dados pessoais o dever de confidencialidade, assinando em contrato ou em acordos de não divulgação (NDA);

Realizar o registro das atividades e operações de tratamento de dados pessoais;

Possuir e implementar políticas e procedimentos de proteção dos dados pessoais ou de normas de qualidade (ISO);

Possuir um responsável pela segurança da informação, *compliance* e/ou risco;

Possuir Política de Segurança da Informação (PSI) implementada e divulgada na empresa;

Adotar medidas técnicas e organizacionais de forma a garantir a confidencialidade, integridade e disponibilidade dos dados pessoais e das informações processadas ou armazenadas na prestação dos serviços (ex.: anonimização, base de dados segregada, plano de continuidade de negócios etc.);

- Possuir plano de contingência instaurado para garantir a disponibilidade de equipe, organização, infraestrutura e TI para cumprimento da LGPD;
- Adotar controles de acesso para que seus colaboradores acessem apenas as informações necessárias para a prestação dos serviços, removendo ou modificando o acesso quando os colaboradores são desligados, transferidos de área ou promovidos;
- Garantir, por meio de cláusulas contratuais, que seus fornecedores terceirizados estejam em conformidade com as políticas de segurança do fornecedor ou parceiro;
- Possuir procedimento de acesso para a instituição às informações a serem processadas e armazenadas na prestação dos serviços;
- Possuir procedimentos de devolução ou apagamento dos dados nos casos em que (i) a instituição solicitar; (ii) o contrato for rescindido.

Para as hipóteses de pluralidade de controladores, a instituição reserva-se no direito de ajustar com seu fornecedor ou parceiro as obrigações e responsabilidades a cargo de cada um, a fim de refletir a relação estabelecida no caso concreto, sem prejuízo das demais obrigações legais aplicáveis e das diretrizes dispostas neste manual.

É assegurado à instituição o direito de regresso em face do fornecedor ou do parceiro em caso de descumprimento das obrigações assumidas, seja por lei ou pelo contrato, com o intuito de preservar a reparação pelo dano que ela não deu causa, nos termos do artigo 42, § 4º, da LGPD e do artigo 934 do Código Civil.

2.8 SUGESTÕES DE REDAÇÃO DE CLÁUSULAS CONTRATUAIS

Em linha com as disposições deste capítulo, sugere-se **a título exemplificativo** a seguinte redação para cláusulas contratuais.

Ressaltando a importância de as instituições buscarem profissionais especialistas em proteção de dados e direito digital para personalizar e customizar seus contratos, termos, políticas e demais documentos internos para que reflitam, clara e objetivamente, a realidade de suas respectivas operações.

1. A **<nome da empresa contratada>** obriga-se a atuar em conformidade com a legislação vigente sobre proteção de dados relativo à pessoa física ("Titular") identificada ou identificável, de acordo com as determinações dos órgãos reguladores/fiscalizadores da matéria, com destaque para a Lei 13.709/2018 ("Lei Geral de Proteção de Dados"). Tal situação é aplicável a **<nome da empresa contratada>** e seus colaboradores.

2. Nas situações em que a **<nome da empresa contratante>** é competente para tomar as decisões sobre o tratamento de dados ("controladora") e que a **<nome da empresa contratada>** vai realizar o tratamento de dados pessoais ("operadora"), a Contratada seguirá as instruções recebidas da Contratante em relação ao tratamento dos Dados Pessoais, além de observar e cumprir as normas legais vigentes aplicáveis, devendo a Contratada garantir sua licitude e idoneidade, sob pena de arcar com as perdas e danos que eventualmente possa causar, sem prejuízo das demais sanções aplicáveis.

3. A **<nome da empresa contratada>** deverá notificar a Contratante sobre as reclamações e solicitações dos Titulares de Dados Pessoais (por exemplo, sobre a correção, exclusão, complementação e bloqueio de dados). A **<nome da empresa contratada>** deverá corrigir, completar, excluir e/ou bloquear os Dados Pessoais, caso seja solicitado pela Contratante.

4. A **<nome da empresa contratada>** compromete-se a adotar medidas, ferramentas e tecnologias necessárias para garantir a segurança dos dados e cumprir com suas obrigações, sempre considerando o estado da técnica disponível.

5. A **<nome da empresa contratada>** deverá cumprir com os requisitos das medidas de segurança técnicas e organiza-

cionais para garantir a confidencialidade, pseudonimização e a criptografia dos Dados Pessoais, inclusive no seu armazenamento e transmissão.

6. A **<nome da empresa contratada>** compromete-se a utilizar tecnologias visando à proteção das informações em todas as comunicações, especialmente nos compartilhamentos de Dados Pessoais pela **<nome da empresa contratada>** à Contratante, a exemplo de padrão seguro de transmissão dados e criptografia.

7. A **<nome da empresa contratada>** deverá realizar o registro de todas as atividades realizadas em seus sistemas/ambientes ("Registros") no mínimo enquanto viger este Contrato, incluindo qualquer atividade relativa à Dados Pessoais tratados sob determinação da Contratante, de modo a permitir a identificação de quem as realizou.

8. A **<nome da empresa contratada>** somente poderá subcontratar qualquer parte dos Serviços que envolvam o tratamento de Dados Pessoais para um ou mais terceiros ("Suboperadores") mediante consentimento prévio e por escrito da Contratante. Neste caso, a Contratada deverá celebrar um contrato escrito com o Suboperador para (i) obrigar o Suboperador às mesmas obrigações impostas por este Contrato em relação à Contratada, no que for aplicável aos Serviços

subcontratados, (ii) descrever os serviços subcontratados e (iii) descrever as medidas técnicas e organizacionais que o Suboperador deverá implementar.

9. A **<nome da empresa contratada>** deverá monitorar, por meios adequados, sua própria conformidade e a de seus funcionários e Suboperadores com as respectivas obrigações de proteção de Dados Pessoais em relação aos Serviços e deverá fornecer à Contratante relatórios sobre esses controles sempre que solicitado por ela.

10. Os relatórios acima citados deverão incluir, pelo menos, (i) o status dos sistemas de processamento de Dados Pessoais, (ii) as medidas de segurança, (iii) o tempo de inatividade registrado das medidas técnicas de segurança, (iv) a (não) conformidade estabelecida com as medidas organizacionais, (v) quaisquer eventuais violações de dados e/ou incidentes de segurança, (vi) as ameaças percebidas à segurança e aos Dados Pessoais e (vii) as melhorias exigidas e/ou recomendadas.

11. A **<nome da empresa contratada>** assegura a si o direito de acompanhar, monitorar, auditar e fiscalizar a conformidade da Contratada com as obrigações de Proteção de Dados Pessoais, sem que isso implique em qualquer diminuição de responsabilidade que a Contratada possui perante a Lei e este Contrato.

12. A **<nome da empresa contratada>** deverá notificar a Contratante em até 24 (vinte e quatro) horas (i) de qualquer não-cumprimento (ainda que suspeito) das disposições legais relativas à proteção de Dados Pessoais; (ii) de qualquer descumprimento das obrigações contratuais relativas ao tratamento dos Dados Pessoais; (iii) de qualquer violação de segurança na Contratada ou nos seus Suboperadores; (iv) de qualquer exposições ou ameaças em relação à conformidade com a proteção de Dados Pessoais; (v) ou em período menor, se necessário, de qualquer ordem de Tribunal, autoridade pública ou regulador competente.

13. A **<nome da empresa contratada>** compromete-se a auxiliar a Contratante: a) com a suas obrigações judiciais ou administrativas, de acordo com a Lei de Proteção de Dados Pessoais aplicável, fornecendo informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança; e b) no cumprimento das obrigações decorrentes dos Direitos dos Titulares dos Dados Pessoais, principalmente por meio de medidas técnicas e organizacionais adequadas.

14. O presente Contrato não transfere a propriedade ou controle dos dados da Contratante ou dos clientes desta, inclusive Dados Pessoais, para a Contratada ("Dados"). Os Dados gerados, obtidos ou coletados a partir da prestação dos Serviços ora contratados são e continuarão de propriedade

da Contratante, inclusive sobre qualquer novo elemento de Dados, produto ou subproduto que seja criado a partir do tratamento de dados estabelecido por este Contrato.

15. Todo e qualquer tratamento de dados fora do Brasil depende de autorização prévia e por escrito pela Contratante à Contratada.

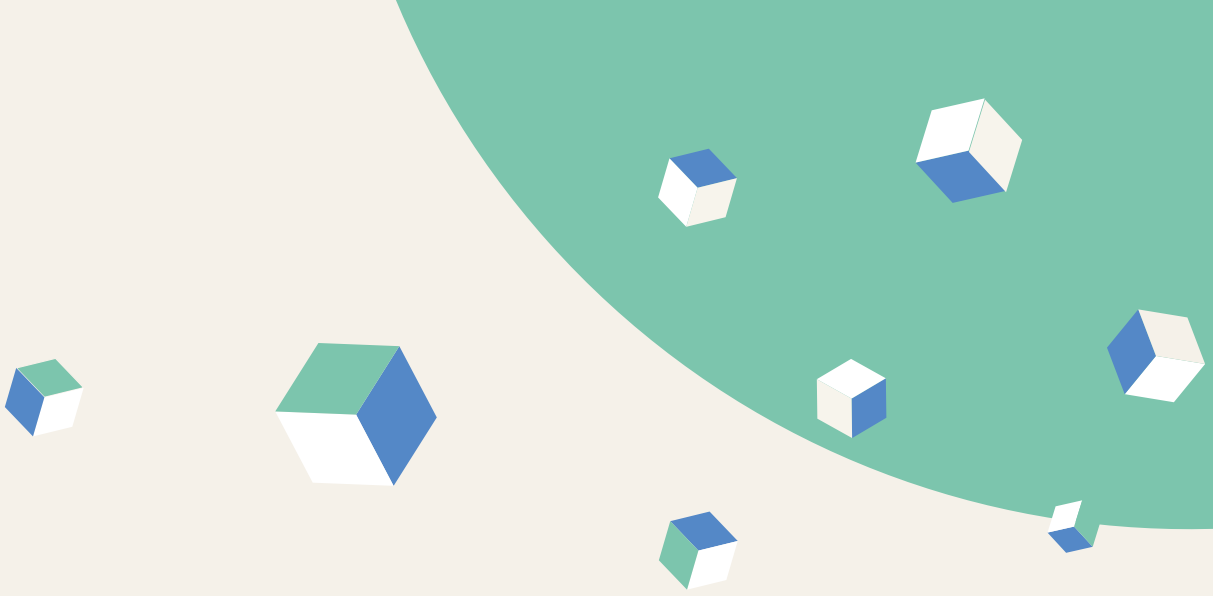
16. Caso exista modificação dos textos legais acima indicados ou de qualquer outro de forma que exija modificações na estrutura da prestação de serviços à Contratante ou na execução das atividades ligadas a este Contrato, a Contratada deverá adequar-se às condições vigentes. Se houver alguma disposição que impeça a continuidade do Contrato conforme as disposições acordadas, a Contratada concorda em notificar formalmente este fato à Contratante, que terá o direito de resolver o presente Contrato sem qualquer penalidade, apurando-se os valores devidos até a data da rescisão.

17. Se qualquer legislação nacional ou internacional aplicável ao tratamento de Dados Pessoais no âmbito do Contrato vier a exigir adequação de processos e/ou instrumentos contratuais por forma ou meio determinado, as Partes desde já acordam em celebrar termo aditivo escrito neste sentido.

18. A Contratada se compromete a devolver todos os dados que vier a ter acesso, em até 30 (trinta) dias, nos casos em que (i) a Contratante solicitar; (ii) o Contrato for rescindido; ou (iii) com o término do presente Contrato. Em adição, a Contratada não deve guardar, armazenar ou reter os Dados por tempo superior ao prazo legal ou necessário para a execução do presente Contrato.

3

COMITÊ DE PROTEÇÃO DE DADOS E DPO



A centralização das informações é primordial quando o assunto é proteção de dados. Isso decorre do fato de que a centralização de dados evita o caos e ainda ajuda na execução rápida de planejamento estratégico e inteligente da resposta a incidentes.

Deste modo, apontar um ou mais responsáveis pela gestão de dados pessoais durante a crise de COVID-19 pode garantir a execução das melhores práticas por todo o time.

Estes responsáveis devem ser escolhidos com base em seus conhecimentos úteis ao comitê, de maneira que é indicada a criação de um time multidisciplinar que, em conjunto, seja dotado de conhecimentos jurídicos, técnicos e de comunicação.

Além do comitê de proteção de dados, é necessário a todas instituições a indicação de um encarregado de dados, ou *Data Protection Office* (DPO).

Esta figura é central na gestão de conformidade em proteção de dados, tendo em vista que o encarregado é uma espécie de **porta-voz** da instituição junto aos seus clientes e junto à autoridade de proteção de dados[22]. E também porque é uma figura obrigatória para a realização do tratamento de dados[23].

Em suma, o DPO é responsável por comunicar todas as informações relativas às ações de tratamentos de dados, tanto para os consumidores que assim desejarem, como para o Estado em situações de fiscalização ou de crise – como um vazamento de informações, por exemplo[24].

O DPO pode ser interno ou terceirizado, podendo ainda ser uma pessoa física ou jurídica. Ou seja, é possível que o encarregado seja contratado através de uma empresa prestadora de serviços. Independente disto, a LGPD aponta que o controlador deve indicar este encarregado e divulgar publicamente a identidade e informações de contato do DPO[25].

---

22 Art. 5º, VIII/LGPD.

23 Art. 23, III/LGPD.

24 Lembrando que a LGPD pontua que cabe ao encarregado: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. Art. 41, § 2º/LGPD.

25 Art. 41/LGPD

Recomenda-se que não seja postergada a indicação de um encarregado, seja este um profissional contratado diretamente pela instituição ou prestador de serviços, tendo em vista que o DPO será a ponte de comunicação entre a sua instituição e os titulares/entre a sua instituição e a autoridade nacional. Lembrando que informação sobre quem/qual empresa é o DPO, deve ser pública e acessível a todos.

Como melhor prática, considerando que o DPO tem várias funções, tem sido recomendado dividir suas atribuições para gerar uma maior otimização da estrutura da instituição, conforme seu modelo atual de governança, com melhor aproveitamento do que já existe, como exemplo:

- **Para atender o disposto pelo inciso I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências:** pode ser aproveitado o canal de ouvidoria ou de atendimento do hospital e direcionar a partir daquele ponto para o DPO.

- **Para atender o disposto pelo inciso II - receber comunicações da autoridade nacional e adotar providências:** pode haver o apoio da área do Jurídico ou *Compliance*.

- **Para atender o disposto pelo inciso III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais:** pode contar com apoio do departamento de Pessoas (DP ou RH) bem como a área de Segurança da Informação (SI).

Sendo assim, tem sido criado um Comitê de Proteção de Dados, que pode tomar proveito de algum outro comitê existente, como o Comitê de Riscos, o de Qualidade ou o de Segurança, e neste fórum multidepartamental e multidisciplinar é trazida a pauta da proteção de dados pessoais, nomeado (indicado) um DPO e os demais integrantes colaboram com o atendimento das atribuições.

O modelo de governança de dados pessoais do DPO pode ter um formato totalmente interno ou adotar um formato híbrido (com apoio de um suporte externo de um DPO as a service que conte com especialistas para dar suporte principalmente em situações específicas, como responder a um incidente).

4

TELETRABALHO E TELEMEDICINA: MELHORES PRÁTICAS

O teletrabalho ganhou ampla popularização em 2020, em razão da pandemia da COVID-19, incluindo a telemedicina, que consiste em uma modalidade de atendimento de saúde, em casos de baixa complexidade, realizada remotamente – podendo ser pré-clínico, consulta, suporte assistencial, monitoramento e diagnóstico à distância.

Essa modalidade de atendimento médico conecta conveniência e acessibilidade de informações de saúde, facilitando a comunicação entre médicos e pacientes. Inicialmente, a telemedicina era praticada com o uso da telefonia, de forma que foi sofisticada com a evolução

da tecnologia e, atualmente, pode envolver *softwares* e aplicativos de prontuário e atendimento eletrônico, além de outras tecnologias que viabilizam, inclusive, a elaboração de laudos de exames de imagem realizados à distância, como no caso da telerradiologia.

A possibilidade de atendimento de pacientes de múltiplas localidades é especialmente relevante no Brasil, em razão de sua extensão territorial e concentração de prestadores de serviços médicos em determinadas localidades do país. Esta facilidade se torna ainda mais relevante no cenário de pandemia, visto que contribui para a mitigação dos riscos de contaminação viral.

No Brasil, após a tentativa de regulamentação do tema por parte do Conselho Federal de Medicina (CFM) – ocorrida em 2019 com a publicação da Resolução CFM nº 2.227/2018, posteriormente revogada pela Resolução nº 2.228/2019 –, a telemedicina foi disciplinada em 2020, através da Portaria nº 467 pelo Ministério da Saúde e surgiu como uma medida para reduzir a propagação da COVID-19 durante a pandemia.

Até então, havia previsão normativa para aplicação de telemedicina apenas em situações emergenciais e específicas, como a emissão de laudos à distância e prestação de suporte diagnóstico ou terapêutico remoto, segundo a Resolução CFM nº 1.643/2002, além da telerradiologia, normatizada pela Resolução CFM nº 2.107/2014.

Com a regulamentação temporária trazida em meio à pandemia, a Portaria nº 467/2020 permite que três modalidades de aplicação sejam permitidas: a teleorientação, o telemonitoramento e a teleinterconsulta. De acordo com o CFM é possível realizar tais modalidades, previstas no Ofício CFM nº 1.756/2020 – COJUR:

- **Teleorientação:** situação na qual os médicos, à distância, orientam e encaminham os pacientes em situação de isolamento;
- **Telemonitoramento:** situação na qual o médico monitora à distância os parâmetros de saúde do paciente;
- **Teleinterconsulta:** situação na qual há troca de informações e opiniões entre médicos ou entre médicos e pacientes, para a determinação de diagnóstico ou tratamento terapêutico.

No que se refere à prestação de serviços de telemedicina, verifica-se como indispensável o tratamento de dados sensíveis de saúde, sendo de suma importância que a instituição entenda que somente poderá tratar determinado dado de saúde em conformidade com o artigo 11 da LGPD.

Isto é, nas seguintes hipóteses: (i) quando o titular ou seu responsável legal consentir, de forma específica e destacada para finalidades específicas; ou (ii) sem fornecimento de consentimento do titular para cumprimento de obrigação legal ou regulatória pelo controlador, tratamento compartilhado de dados necessários à execução pela administração pública de políticas públicas, realização de estudos por órgão de pesquisa (garantida, sempre que possível, a anonimização dos dados pessoais sensíveis), exercício regular de direitos (inclusive em contrato e em processo judicial, administrativo e arbitral), para proteção da vida ou da incolumidade física do titular ou de terceiros, tutela da saúde (exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária) ou garantia da prevenção da fraude e à segurança do titular.

Os benefícios da telemedicina, especialmente no atual cenário de pandemia no Brasil, são indiscutíveis, sendo importante destacar o

envolvimento do tráfego bidirecional de dados sensíveis de saúde, entre profissionais de saúde e pacientes nas plataformas digitais, de modo que se torna imprescindível a mitigação dos potenciais riscos de segurança da informação, caso a prática não seja acompanhada de controles e limites bem definidos durante todo o ciclo de vida dos dados pessoais na instituição.

Assim, é essencial que as instituições providenciem avaliações de risco, também conhecidas como *risk assessments*, nas plataformas digitais e procedimentos envolvidos nesta modalidade de prestação de serviços, objetivando assegurar que o tratamento de dados seja realizado em conformidade com a legislação envolvida no tema e melhores práticas de mercado. Neste sentido, deve-se garantir que não há possibilidade de quebra do sigilo médico nas funcionalidades das plataformas digitais.

Diante dos desafios apresentados na operação de negócios digitais no Brasil e recorrentes tentativas de invasão por *hackers* e fraudes, é fundamental que as instituições invistam em procedimentos internos e sistemas que garantam uso e acesso adequados aos dados pessoais sensíveis. Atualmente, existem diversas ferramentas tecnológicas que podem contribuir para mitigar riscos de segurança, tais como criptografia, autenticação de dispositivos eletrônicos utilizados pelos pacientes e identificação *"face-to-face"* dos pacientes nas plataformas digitais.

É muito comum que instituições que utilizam plataformas digitais de telemedicina na prestação de seus serviços tenham a intenção de utilizar dados coletados por meio das plataformas para outras finalidades, buscando o avanço tecnológico e científico do setor da saúde.

Entretanto, em observância aos conceitos trazidos pela LGPD, especialmente o princípio da finalidade e da adequação, constata-se que todo e qualquer tratamento de dados pessoais deve ser compatível com as finalidades para as quais estes foram originalmente coletados, sendo vedada a possibilidade de tratamento posterior de forma incompatível com a informação fornecida ao titular e em desacordo com o contexto do processamento.

No mais, a LGPD restringe o compartilhamento de dados de saúde com objetivo de obter vantagem econômica, caso esse compartilhamento não seja necessário para (i) a prestação de serviços de saúde; (ii) a prestação de assistência farmacêutica; (iii) assistência à saúde, incluindo serviços auxiliares de diagnose e terapia; (iv) a portabilidade, a pedido do titular; e (v) permitir as transações financeiras e administrativas relacionadas ao serviços elencados anteriormente[26].

Desta forma, caso a instituição deseje viabilizar o tratamento posterior dos dados coletados durante a prestação dos serviços de telemedicina para finalidades distintas das informadas ao titular, deverão ser adotadas metodologias que garantam a efetiva anonimização dos dados.

Ressalta-se, ainda, que no decorrer da prestação de serviços de telemedicina, as instituições, ao figurarem como controladores, deverão assegurar aos titulares de dados os direitos que lhes são garantidos pela LGPD, em seu Capítulo III, em especial: (i) confirmação da existência de tratamento; (ii) acesso aos dados; (iii) correção de dados incompletos, inexatos ou desatualizados; (iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei; (v) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (vi) eliminação dos dados pessoais tratados, exceto nas hipóteses previstas no artigo

26 Art. 12, parágrafo 1º da LGPD

16 da Lei[27]; (vii) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e (ix) revogação do consentimento, caso esta seja a base legal que fundamenta o tratamento de dados em questão.

Importante destacar também que o *European Data Protection Board* (EDPB), ou Conselho Europeu de Proteção de Dados – órgão europeu independente cujo objetivo é garantir a aplicação consistente do Regulamento Geral de Proteção de Dados e promover a cooperação entre as autoridades de proteção de dados da UE –, posicionou-se no sentido de que a atual crise de saúde mundial não deve ser utilizada como uma oportunidade de estabelecer hipóteses de coleta e armazenamento de dados pessoais de forma desproporcional, devendo ser consideradas as necessidades reais de cada caso concreto, bem como a relevância médica[28].

Por fim, em linha com o entendimento esboçado pelo EDPB no que se refere a melhores práticas de proteção de dados no cenário da pandemia de COVID-19, caso a instituição deseje desenvolver ou implementar plataformas digitais para viabilizar a telemedicina, recomenda-se a elaboração de um Relatório de Impacto de Proteção de Dados, como descrito no item 2.7 deste manual.

---

27 Art. 16, LGPD: Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
I - cumprimento de obrigação legal ou regulatória pelo controlador;
II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

28 Guidelines 04/2020

5

CIÊNCIA NA PRÁTICA: CONSENTIMENTO E LEGÍTIMO INTERESSE

5.1 CONSENTIMENTO

Devido à natureza sensível dos dados de saúde, é importante assegurar que os dados que estão sendo coletados e processados pela instituição tenham a garantia do consentimento informado de seus titulares.

O consentimento informado deve garantir que o titular de dados está ciente acerca do tratamento de dados pessoais pela instituição. Portanto, uma dica valiosa é associar os conhecimentos jurídicos aos conhecimentos de comunicação da sua instituição, deste modo, garante-se que a informação é passada dentro dos parâmetros e necessidades legais.

E essa boa prática deve ser estimulada, principalmente, no cenário de pandemia, tendo em vista que escândalos envolvendo desencontro de informações ou eventual conduta antiética em relação a seus funcionários ou clientes podem ganhar proporções enormes junto à mídia, prejudicando a imagem da instituição.

5.2
LEGÍTIMO INTERESSE

O legítimo interesse é apontado como um dos requisitos de validação do tratamento de dados, mas este conceito nem sempre é bem compreendido na prática. Isso porque nem tudo é considerado legítimo interesse.

Embora a LGPD não seja taxativa em relação ao que é legítimo interesse, uma boa medida para adotar este parâmetro sem incorrer em abusos é a aplicação da boa-fé.

Por exemplo, imagine que você tem uma loja virtual de sapatos. Para que seu cliente consiga efetuar a compra é necessário que a sua loja tenha em mãos alguns dados básicos, como: informações de pagamento e sobre a entrega, via de contato e dados para emissão da nota fiscal.

Se a sua loja ultrapassa estes pedidos no formulário de compra e pergunta ao cliente sua orientação sexual ou posicionamento político, por exemplo, há um claro excesso do uso do legítimo interesse na execução da venda.

Este exemplo é exagerado, mas mostra como deve ser adotado este parâmetro do legítimo interesse na prática. Neste sentido, antes de lançar mão do legítimo interesse, responda às seguintes questões:

1. Esta informação é essencial para que eu preste o serviço junto ao meu paciente?

2. É possível anonimizar os dados sem prejuízo à prestação do serviço?

3. O dado que eu busco solicitar tem uso prático, direto e justificável na prestação do serviço?

Respondendo a estas questões, é mais difícil incorrer em erros e abusos em relação ao uso do legítimo interesse.

5.3 PESQUISAS CLÍNICAS E ESTUDOS RETROSPECTIVOS: CONFORMIDADE E SEGURANÇA

As atividades relativas às pesquisas clínicas e estudos retrospectivos tornaram-se essenciais para o desenvolvimento da ciência e, consequentemente, da medicina. De forma que, estão cada vez mais presentes no dia a dia das instituições hospitalares e dos serviços de saúde em geral.

Nesse sentido, ressalta-se o conceito de órgão de pesquisa previsto na LGPD, para que seja possível compreender integralmente as diretrizes específicas da Lei.

Em conformidade com a definição legal, é considerado órgão de pesquisa:

"Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos, com sede e foro no Brasil, 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"[29].

Assim, ao analisar os artigos 7º e 11 da LGPD, apontamos uma clara existência de exceção do consentimento para que os órgãos de pesquisa tratem os dados pessoais e dados pessoais sensíveis para realização de estudos retrospectivos e pesquisas clínicas, devendo dar preferência à anonimização dos dados pessoais. Ressalta-se, ainda, que para definição da base legal melhor aplicável no tratamento de dados em estudos e pesquisas científicas, é preciso analisar o caso concreto.

Ainda que não haja obrigatoriedade de obtenção do consentimento, faz-se necessária a adoção de medidas de segurança e a observância dos princípios[30] gerais de proteção de dados pessoais e direitos[31] dos titulares.

---

29 Art. 5º, XVII/LGPD.

30 LGPD, Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

Assim sendo, considera-se essencial que os titulares de dados sejam informados a respeito da pesquisa clínica ou do estudo retrospectivo que será realizado, devendo receber **informações claras, precisas e de fácil entendimento,** sobre o tratamento de seus dados pessoais.

Deverá ser informado também ao titular todas as instituições envolvidas no projeto de pesquisa que tratarão seus dados pessoais, devendo ser observados os segredos comerciais e industriais.

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas 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 difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

31 LGPD, Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
I - confirmação da existência de tratamento;
II - acesso aos dados;
III - correção de dados incompletos, inexatos ou desatualizados;
IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo

Desse modo, destacam-se duas diretrizes a serem adotadas pelos órgãos de pesquisa:

- É expressamente vedada pela legislação a divulgação de resultados ou de qualquer excerto do estudo ou da pesquisa contendo dados pessoais.

---

com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019)
§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

- O órgão de pesquisa é integralmente responsável pela segurança da informação, de forma que não será permitida, em circunstância alguma, a transferência dos dados pessoais a terceiros.

Ainda neste aspecto, ressalta-se que para a realização de estudos em saúde pública, os órgãos de pesquisa[32] poderão ter acesso a bases de dados pessoais a serem regulamentadas por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a **anonimização** ou **pseudonimização** dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

Tais aspectos, serão objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

Destaca-se, ainda, que, além da LGPD, as instituições envolvidas em projetos de pesquisa e desenvolvimento científico deverão observar a legislação própria deste tema, incluindo, mas não se limitando a Resolução nº 466, de 12 de dezembro de 2012, expedida pelo Conselho Nacional de Saúde (CNS), que aprova diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos.

---

32 LGPD, Art. 5º, XVIII - 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;

6

TRANSFERÊNCIA INTERNACIONAL DE DADOS

A transferência internacional de dados pessoais é inevitável no contexto contemporâneo de digitalização das relações. E a LGPD não invalida tal procedimento, só especifica alguns cuidados diferenciados.

Neste sentido, é importante seguir algumas regras para efetuar a transferência internacional de dados:

1. Adotar a imposição de uma padronização do modelo de cláusulas contratuais a serem observadas pelas instituições, quer seja em suas relações corporativas globais, quer seja em seus códigos internos e certificados;

2. Além de cláusulas padronizadas, é necessário tornar os contratos vinculantes, de modo a prever a indicação do país e região nos quais os serviços serão prestados e o tratamento de dados será necessário, para que o armazenamento, processamento e gestão dos dados seja realizado em conformidade com as normas da LGPD;

3. Assegurar que os preceitos legais e os princípios, direitos, garantias e deveres trazidos pela LGPD sejam observados e praticados ao longo de todo o fluxo processual da instituição, através de regras claras e disseminadas por meio da governança dos contratos entre as partes;

4. Garantir que informações relativas às certificações e aos relatórios de auditoria estejam acessíveis;

5. Em caso de subcontratação de serviços por parte da instituição que recebe a transferência de dados, a instituição vinculada na cadeia deve ser notificada;

6. Quaisquer mudanças relacionadas às garantias fornecidas deverão ser comunicadas à autoridade nacional competente.

Fique ligado!

Para os casos de transferência internacional e elaboração do clausulado contratual, sempre será necessário analisar os casos individualmente, além da legislação específica do país para o qual se pretende transferir os dados pessoais.

Lembre-se também que os artigos específicos de transferência internacional de dados da LGPD (arts. 33 a 36) atualmente estão pendentes de regulamentação pela ANPD.

6.1 REGRAS CORPORATIVAS VINCULANTES – *BINDING CORPORATE RULES* (BCR)

Neste mesmo sentindo, é relevante destacar a adoção de Regras Corporativas Vinculantes (*Binding Corporate Rules* – BCRs), que são um padrão internacional apontado pela União Europeia no GDPR, art. 47.

De maneira pontual, as BCRs[33] são instrumentos de proteção de dados pessoais com nível de segurança e adesão por parte de controladores ou processadores que pertencem a grupos empresariais ou instituições alocadas em mais de um país.

Ou seja, são procedimentos padrões criados para abarcar as necessidades e obrigatoriedades vivenciadas por empresas de atuação multinacional.

A importância das BCRs está em sua praticidade, tendo em vista que, ao segui-las, as empresas de atuação multinacional conseguem se adequar mais facilmente à exigência dos mais diversos países.

33 As BCRs surgiram por uma iniciativa das Autoridades de Proteção de Dados da Europa em 2003.

Apontam-se os seguintes elementos necessários para a adequação de uma instituição às BCRs[34]:

1. Estrutura e detalhes dos contratos do grupo empresarial e cada um de seus componentes;

2. Quais transferências de dados serão realizadas, assim como o tipo de tratamento a ser realizado, finalidades, tipos de titulares afetados, país de atuação e países terceiros;

3. Caráter vinculativo;

4. Observância da aplicação dos princípios gerais de proteção de dados – minimização, limitação do propósito, tempo de armazenamento, qualidade dos dados, base legal para o processamento, tratamento de categorias especiais ou não, padrões de segurança e requisitos para as transferências em curso e a serem realizadas;

5. Direitos dos titulares de dados e os meios para que os sujeitos possam exercer tais direitos – revisão de decisão automatizada, revisão de dados, apagamento de dados, direito a reparação e revogação de consentimento;

6. Aceitação de responsabilidade solidária por parte da instituição, caso haja quaisquer violações das BCRs por algum membro;

7. Transparência sobre como as informações são fornecidas aos titulares;

34 USTARAN, Eduardo. European Data Protection Law and Practice. International Association of Privacy Professionals. 2018. p. 504

8. As atividades dos responsáveis pela proteção de dados ou monitoramento e cumprimento da BCR;

9. Procedimentos de reclamação;

10. Procedimentos de registro e relato de alterações e mudanças de regras junto às autoridades supervisoras;

11. Adoção de mecanismos de cooperação e reporte com as autoridades supervisoras;

12. Fornecimento de treinamento adequado em proteção de dados para todo pessoal com acesso – permanente ou regular – aos dados pessoais em tratamento.

6.2 ADOÇÃO DE CLÁUSULAS CONTRATUAIS PADRÃO

Outro aspecto de grande relevância durante os procedimentos de transferência internacional de dados pessoais é a adoção de clausulado padrão nos contratos.

No caso brasileiro, ainda não se observa um apontamento da Autoridade Nacional de Proteção de Dados (ANPD) neste sentido, mas a União Europeia estabelece um conjunto de termos e condições pré-aprovados por suas autoridades.

Em termos gerais, aponta-se que nestas cláusulas padrões é necessário garantir que sejam abarcados todos os tópicos previamente indicados de maneira que se garantam a vinculação legal e instrumentos de execução palpáveis.

Neste sentido, conforme os artigos 33 e 55 da LGPD, indica-se a previsão de:

I. Códigos de conduta para as instituições hospitalares e seus membros em relação ao tratamento de dados pessoais que podem ser protocolados junto à ANPD;

II. Garantia da adoção de mecanismos de certificação que garantam o *compliance* com as regras de proteção de dados dos países envolvidos;

III. Adoção de procedimento de aprovação por parte das autoridades de proteção de dados, acerca da transferência de dados em curso.

7

PROGRAMA DE PROTEÇÃO DE DADOS

O programa de proteção de dados apresentado tem como ênfase temas práticos e referências internacionais, considerando uma pesquisa feita junto à *Global Privacy Assembly*[35] que reúne conteúdo publicado por 49 países acerca de suas melhoras práticas.

Para chegar à criação deste manual, foram selecionados, entre eles, 12 países para realizar o levantamento e o conteúdo final:

Figura 1 | *Países escolhidos para a pesquisa*

EUROPA	AMÉRICA	ÁSIA E OCEANIA
✔ Albânia ✔ Alemanha ✔ Andorra ✔ Áustria ✔ França ✔ Reino Unido	✔ Argentina ✔ Chile ✔ Canadá ✔ EUA	✔ Hong Kong ✔ Austrália

Fonte: PG Advogados, 2020.

35 https://globalprivacyassembly.org/covid19/

Além da pesquisa realizada ante o cenário regulatório mundial em relação à proteção de dados, associou-se ao estudo o arcabouço legislativo nacional sobre a temática (Lei 13.709/18, Lei 13.853/19, Lei 14.010/2020 e leis correlatas) e o contexto de pandemia causada pela COVID-19.

As recomendações seguintes resumem as melhores práticas para proteção e privacidade dos dados pessoais frente a cenários de crise, considerando especialmente o setor da saúde, podendo ainda acrescentar medidas relacionadas também à telemedicina e isolamento social:

Tabela 1 *| Ações recomendas para o programa de proteção de dados*

AÇÕES RECOMENDADAS		COMENTÁRIOS
1	GARANTA A SEGURANÇA DA INFORMAÇÃO	Uma das principais recomendações para o combate à COVID-19 é o isolamento social e, para isso, muitas organizações têm adotado o modelo de trabalho remoto e a telemedicina se desenvolveu durante 2020. Isso implica, na maior parte dos casos, que os funcionários utilizem seus computadores pessoais, o que não deve impedir a garantia da segurança da informação por parte do empregador. Principalmente, porque serão trocados entre instituição e colaborador informações quase que diárias. Cabe, portanto, à instituição fornecer a seus funcionários mecanismos de proteção digital no ambiente remoto, como

		o uso de VPNs, dispositivos de compartilhamentos de documentos entre a equipe que garantam confidencialidade dos dados, plataformas de comunicação padronizadas e que assegurem a segurança e previnam a exposição dos funcionários.
2	ATUALIZE AS INFORMAÇÕES SOBRE OS SEUS FUNCIONÁRIOS	É muito importante que as instituições garantam que a comunicação com seus colaboradores não seja interrompida durante um período de crise. Por isso, atualizar as informações cadastrais de seus funcionários (como número de telefone pessoal e contato de emergência) é uma medida bastante interessante, todavia, não é necessário obrigar o seu funcionário a fornecer os dados sem explicação alguma. Manter a transparência e fluidez da comunicação é essencial para facilitar o diálogo e evitar problemas. Isso inclui a conscientização dos colaboradores acerca da finalidade da coleta dos dados, seu tempo de guarda e se/com quem os dados serão compartilhados adicionados do aceite formal do trabalhador com a coleta e armazenamento da informação de acordo com os parâmetros estabelecidos.
3	TRATE OS DADOS DE SAÚDE DE MANEIRA CONFIDENCIAL	Os dados de saúde são considerados dados sensíveis e, por isso, recebem um tratamento diferenciado e particular, com maiores restrições de acesso e mais ga-

rantias de confidencialidades do que os demais dados. Isso decorre da vulnerabilidade das informações em tratamento e, principalmente, no cenário de pandemia em que preconceitos podem ser estimulados pelo medo e pânico coletivo, garantir que os dados de saúde vão receber um tratamento especial é primordial. Isso não significa que a sua instituição não possa guardar informações sobre a saúde de seus funcionários, pelo contrário, é um dever organizacional garantir a saúde e o bem-estar de seus colaboradores e, para isso, o monitoramento do estado físico dos funcionários pode ser necessário. Entretanto, a confidencialidade e anonimização das informações deve ser sempre respeitada. Isso significa que a divulgação da identidade de pessoas infectadas ou com suspeita de infecção não deve ser realizada. Sendo o seu compartilhamento permitido apenas para os órgãos de saúde competentes, com o objetivo de garantir o bem-estar coletivo e o acesso à saúde pública por parte do colaborador.

4 CRIE UM COMITÊ DE GESTÃO DE CRISE DE COVID-19

A centralização das informações é primordial durante um período de crise, pois isso evita o caos e ajuda no planejamento estratégico e inteligente da resposta à incidentes. Com a proteção de dados não é diferente, por isso, apontar um ou mais responsáveis pela gestão de dados pessoais durante a pan-

		demia de COVID-19 pode garantir a execução das melhores práticas por todo o time.
5	**GARANTA O ACESSO À INFORMAÇÃO E CONSENTIMENTO DOS TITULARES DE DADOS, DA COLETA AO FINAL DO PROCESSAMENTO DOS DADOS PESSOAIS**	Devido à natureza sensível dos dados de saúde, é importante garantir que os dados coletados e tratados pela instituição tenham a garantia do consentimento informado dos titulares de dados. Esta boa prática deve ser estimulada principalmente neste cenário de pandemia, tendo em vista que escândalos envolvendo desencontro de informações ou eventual conduta antiética em relação a seus funcionários ou clientes podem ganhar proporções enormes junto à mídia, prejudicando a imagem da instituição.

Fonte: PG Advogados, 2020.

CONCLUSÃO

Como se pode notar, associar a prática a indicações regulatórias é essencial no alcance da conformidade em proteção de dados. Para tanto, é fundamental observar as experiências internacionais e estar sempre atento às necessidades de cada instituição.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBÂNIA. **Guidelines on the protection of personal data in the context of themeasures taken against COVID-19.** Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, 2020. Disponível em: **https://www.idp.al/2020/03/20/guidelines-on-the-protection-of-personal-data-in-the-context-of-the-measures-taken-against-covid-19/?lang=en.** Acesso em 13 abr. 2020.

ALBÂNIA. **Ligj Nr. 9887, datë 10.3.2008 - Për Mbrojtjen e të Dhënave Personale.** 2008 Disponível em: **http://www.pp.gov.al/web/ligj_mbrojtja_e_te_dhenave_personale_40.pdf.** Acesso em 13 abr. 2020.

ALEMANHA. **Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie.** Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2020. Disponível em: **https://www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/GesundheitSozialesArtikel/Datenschutz-in-Corona-Pandemie.html?nn=5217154.** Acesso em 16 abr. 2020.

ALEMANHA. **DSK gibt Hinweise zu Datenschutz und Corona**. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 2020. Disponível em: **https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/07_Empfehlungen_Datenschutz_Corona.html.** Acesso em 16 abr. 2020.

ALEMANHA. **Hinweise zu Datenschutz und Corona**. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, 2020. Disponível em: **https://www.datenschutz-mv.de/datenschutz/publikationen/Corona/.** Acesso em 16 abr. 2020.

ALLIANZ. **Allianz Risk Barometer 2020**. Disponível em: **https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html.** Acesso em 01 ago. 2020.

ANDORRA. **Informació de les mesures preses arran del COVID-19 I recomendacions de l'agència**. Agència Andorrana de Proteció de Dades, 2020. Disponível em: **https://www.apda.ad/ca/informacio-de-les-mesures-preses-arran-del-covid-19-recomanacions-de-lagencia.** Acesso em 13 abr. 2020.

ANDORRA. **Recomanacions sobre tractament de dades en la crisis del COVID-19.** Agència Andorrana de Proteció de Dades, 2020. Disponível em: **https://www.apda.ad/sites/default/files/2020-03/COVID19.pdf.** Acesso em 13 abr. 2020.

ARGENTINA. **Proteccion de los datos personales:** Ley 25. 326/2000. Congresso de la Nacion Argentina, 2000. Disponível em: **https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion.** Acesso em 13 abr. 2020.

ARGENTINA. **Tratamiento de datos personales ante el Coronavirus.** Agencia de Acesso a la Información Pública, 2020. Disponível em: **https://www.argentina.gob.ar/noticias/tratamiento-de-datos-personales-ante-el-coronavirus.** Acesso em 13 abr. 2020.

AUSTRÁLIA. **Coronavirus (COVID-19): understanding your privacy obligations to your staff.** Office of the Australian Information Commissioner, 2020. Disponível em: **https://www.oaic.gov.au/privacy/guidance-and-advice/coronavirus-covid-19-understanding-your-privacy-obligations-to-your-staff/#ftn3.** Acesso em 13 abr. 2020.

AUSTRÁLIA. **How to respect privacy and protect public sector information when working remotely.** Office of the Victorian Information Commissioner, 2020. Disponível em: **https://ovic.vic.gov.au/wp-content/uploads/2020/03/How-to-respect-privacy-and-protect-public-sector-information-when-working-remotely.pdf.** Acesso em 13 abr. 2020.

AUSTRÁLIA. **Privacy Act 1988.** Federal Register of Legislation, 2020. Disponível em: **https://www.legislation.gov.au/Details/C2018C00034/Html/Text.** Acesso em 13 abr. 2020.

AUSTRÁLIA. **Privacy and COVID-19.** Office of the Victorian Information Commissioner, 2020. Disponível em: **https://ovic.vic.gov.au/wp-content/uploads/2020/04/Privacy-and-COVID-19.pdf**. Acesso em 13 abr. 2020.

ÁUSTRIA. **Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG).** Rechtsinformationssystem des Bundes, 2020. Disponível em: **https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597.** Acesso em 15 abr. 2020.

ÁUSTRIA. **Epidemiegesetz 1950.** Rechtsinformationssystem des Bundes, 2020. Disponível em: **https://perma.cc/EF5A-DER5.** Acesso em 15 abr. 2020.

ÁUSTRIA. **Information der Datenschutzbehörde zum Coronavirus (Covid-19).** Österreichische Datenschutzbehörde, 2020. Disponível em: **https://www.dsb.gv.at/download-links/informationen-zum-coronavirus-covid-19-.html#:~:text=Die%20Datenschutzbeh%C3%B6rde%20weist%20einleitend%20darauf,Datenschutzrecht%20einen%20besonderen%20Schutz%20vorsieht.** Acesso em 15 abr. 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2ªed. Rio de Janeiro, 2020. p. 81.

BRASIL. **Entre a prevenção de perdas e a proteção de dados.** Disponível em: **https://www.serpro.gov.br/lgpd/noticias/prevencaoperdas-protecao-de-dados-pessoais-lgpd.** Serpro. Acesso em 11 ago. 2020.

BRASIL. **Guia de Boas Práticas: Lei Geral de Proteção de Dados.** Abril, 2020 Disponível em: **https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Serpro.** Acesso em 03 ago. 2020.

CANADÁ. **Commissioner issues guidance on privacy and the COVID-19 outbreak**. Office of the Privacy Commissioner of Canada, 2020. Disponível em: **https://priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200320/.** Acesso em 14 abr. 2020.

CANADÁ. **Guidelines for obtaining meaningful consent**. Office of the Privacy Commissioner of Canada, 2018. Disponível em: **https://priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.** Acesso em 14 abr. 2020.

CANADÁ. **Guidelines for obtaining meaningful consent.** Office of the Privacy Commissioner of Canada, 2020. Disponível em: **https://priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.** Acesso em 14 abr. 2020.

CANADÁ. **PIPEDA legislation and related regulations.** Office of the Privacy Commissioner of Canada, 2015. Disponível em: **https://priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/.** Acesso em 14 abr. 2020.

CANADÁ. **Privacy and the COVID-19 outbreak.** Office of the Privacy Commissioner of Canada, 2020. Disponível em: **https://priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/gd_covid_202003/.** Acesso em 14 abr. 2020.

CANADÁ. **Privacy in a Pandemic.** Office of the Information and Privacy Commissioner of Alberta, 2020. Disponível em: **https://www.oipc.ab.ca/resources/privacy-in-a-pandemic-advisory.aspx.** Acesso em 14 abr. 2020.

CANADÁ. **The Privacy Act legislation and regulations.** Office of the Privacy Commissioner of Canada, 2018. Disponível em: **https://priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/r_o_a/.** Acesso em 14 abr. 2020.

CHILE. **¿Se puede revelar el nombre de uma persona contagiada o de um eventual contagio?** Consejo para la Transparencia, 2020. Disponível em: **https://www.consejotransparencia.cl/se-puede-revelar-el-nombre-de-una-persona-contagiada-o-de-un-eventual-contagio/.** Acesso em 16 abr. 2020.

CHILE. **Ley 19.628**. Ministerio Secretaría General de la Presidencia, 1999. Disponível em: **https://www.leychile.cl/Navegar?idNorma=141599.** Acesso em 16 abr. 2020.

CHILE. **Ley 20.584.** Ministerio de Salud; SubSecretaría de Salud Pública, 2000. Disponível em: **https://www.leychile.cl/Navegar?idNorma=1039348.** Acesso em 16 abr. 2020.

CHILE. **Oficio nº 211.** Consejo para la Transparencia, 2020. Disponível em: **https://www.consejotransparencia.cl/wp-content/uploads/2020/03/Oficio-CPLT_000211_17-Marzo-1.pdf.** Acesso em 16 abr. 2020.

ESPINOZA, Javier. **EU admits it has been hard to implemente GDPR.** Finacial Times, 23 jun 2020. Disponível em: **https://www.ft.com/content/66668ba9-706a-483d-b24a-18cfbca142bf.** Acesso em 20 jul 2020.

ESTADOS UNIDOS. **COPPA Guidance for Ed Tech Companies and Schools during the Coronavirus.** FTC, 2020. Disponível em: **https://www.ftc.gov/news-events/blogs/business-blog/2020/04/coppa-guidance-ed-tech-companies-schools-during-coronavirus.** Acesso em 16 abr. 2020.

ESTADOS UNIDOS. **Coronavirus Scams: What the FTC is Doing.** FTC, 2020. Disponível em: **https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing.** Acesso em 16 abr. 2020.

ESTADOS UNIDOS. **FTC, FDA Send Warning Letters to Seven Companies about Unsupported Claims that Products Can Treat or Prevent Coronavirus.** FTC, 2020. Disponível em: **https://www.ftc.gov/news-events/press-releases/2020/03/ftc-fda-send-warning-letters-seven-companies-about-unsupported?utm_source=slider.** Acesso em 16 abr. 2020.

ESTADOS UNIDOS. **Remote learning and children's privacy.** FTC, 2020. Disponível em: **https://www.consumer.ftc.gov/blog/2020/04/remote-learning-and-childrens-privacy.** Acesso em 16 abr. 2020.

ESTADOS UNIDOS. **Telemedicine in the face of the COVID19 pandemic.** NCBI, 2020. Disponível em: **https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7164871/.** Acesso em 19 ago. 2020.

FONTES, Edison. **Políticas e normas para segurança da informação.** Rio de Janeiro: Brasport, 2012.

FRANÇA. **Code du travail.** Partie législative, 2020. Disponível em: **https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072050.** Acesso em 16 abr. 2020.

FRANÇA. **Coronavirus (COVID-19): les rappels de la CNIL sur la collecte de données personnelles.** CNIL, 2020. Disponível em: **https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles.** Acesso em 16 abr. 2020.

GOOGLE. **Mapa do *Coronavirus (COVID-19).*** 2020. Disponível em: **https://google.com/covid19-map/?hl=pt-BR.** Acesso em 16 abr. 2020.

HONG KONG.**使用社交媒體上的資料以追蹤潛在的 2019 冠狀病毒病(COVID-19)的帶病毒者.** 香港個人資料私隱專員公署, 2020. Disponível em: **https://www.pcpd.org.hk/english/media/media_statements/press_20200226.html.** Acesso em 16 abr. 2020.

HONG KONG.**公署回應傳媒查詢有關2019 冠狀病毒病引起的私隱議題(只有英文).** 香港個人資料私隱專員公署, 2020. Disponível em: **https://www.pcpd.org.hk/english/media/response/enquiry_20200321.html.** Acesso em 16 abr. 2020.

HONG KONG.**對抗**2019冠狀病毒病大流行疫情 Disponível em: **https://www.coronavirus.gov.hk/sim/.** Acesso em 03 nov. 2020.

HONG KONG.**私隱公署提供在疫情期間保障兒童私隱指引.** 香港個人資料私隱專員公署, 2020. Disponível em: **https://www.pcpd.org.hk/english/media/media_statements/press_20200402.html.** Acesso em 16 abr. 2020.

HONG KONG.**私隱專員回應涉及個人資料私隱的強制檢疫措施.** 香港個人資料私隱專員公署, 2020. Disponível em: **https://www.pcpd.org.hk/english/media/media_statements/press_20200211.html.** Acesso em 16 abr. 2020.

KROLL. **Relatório Global de Fraude e Risco: construindo resiliência em um mundo volátil –** edição anual 2016/17. 2017. Disponível em: **https://ajoficial.com.br/wp-content/uploads/2017/07/relatorioglobaldefraudeerisco2016_17_edicaobr.pdf** Acesso em ago 2018.

LEITE, Tácito Augusto Silva. **Gestão de Riscos na Segurança Patrimonial.** Rio de Janeiro: Qualitymark, 2016.

LIMA, Lindamaria. **Entrada em vigor da Lei Geral de Proteção de Dados Pessoais – Situação atual.** Tripla, 8 jun 2020. Disponível em: **https://triplait.com/entrada-em-vigor-da-lgpd/.** Acesso em 20 jul 2020.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. ***Coronavirus (COVID-19).*** 2020. Disponível em: **https://covid19.who.int/.** Acesso em 16 abr. 2020.

PETERS, Michael. **5 best practices for Outsourcing Cyber Security & Compliance Services.** Cybersecurity Ventures, set, 2017. Disponível em: **< https://cybersecurityventures.com/cybervisors-help-solve-cybersecurity-talent-shortage/>.** Acesso em ago 2018.

REINO UNIDO. **Data protection and coronavirus information hub.** 2020. Disponível em: **https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/.** Acesso em 17 abr. 2020.

REINO UNIDO. **Data protection and coronavirus.** 2020. Disponível em: **https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/data-protection-and-coronavirus/.** Acesso em 17 abr. 2020.

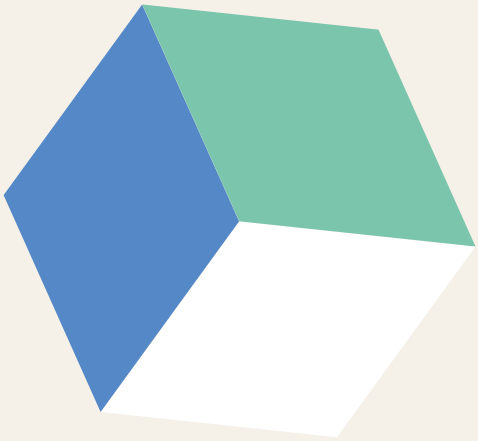
REINO UNIDO. **The ICO's regulatory approach during the coronavius publica health emergency.** 2020. Disponível em: **https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf.** Acesso em 17 abr. 2020.

UNIÃO EUROPEIA. **Statement on the processing of personal data in the context of the COVID-19 outbreak.** Disponível em **https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.** Acesso em 19 ago 2020.

UNIÃO EUROPEIA. **Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.** Disponível em **https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.** Acesso em 19 ago 2020.

USTARAN, Eduardo. **European Data Protection Law and Practice.** International Association of Privacy Professionals. 2018.

給僱主和僱員的指引香港個人資料私隱專員公署，2020. Disponível em: **https://www.pcpd.org.hk/english/media/media_statements/press_20200330.html.** Acesso em 16 abr. 2020.




anahp
associação nacional
de hospitais privados