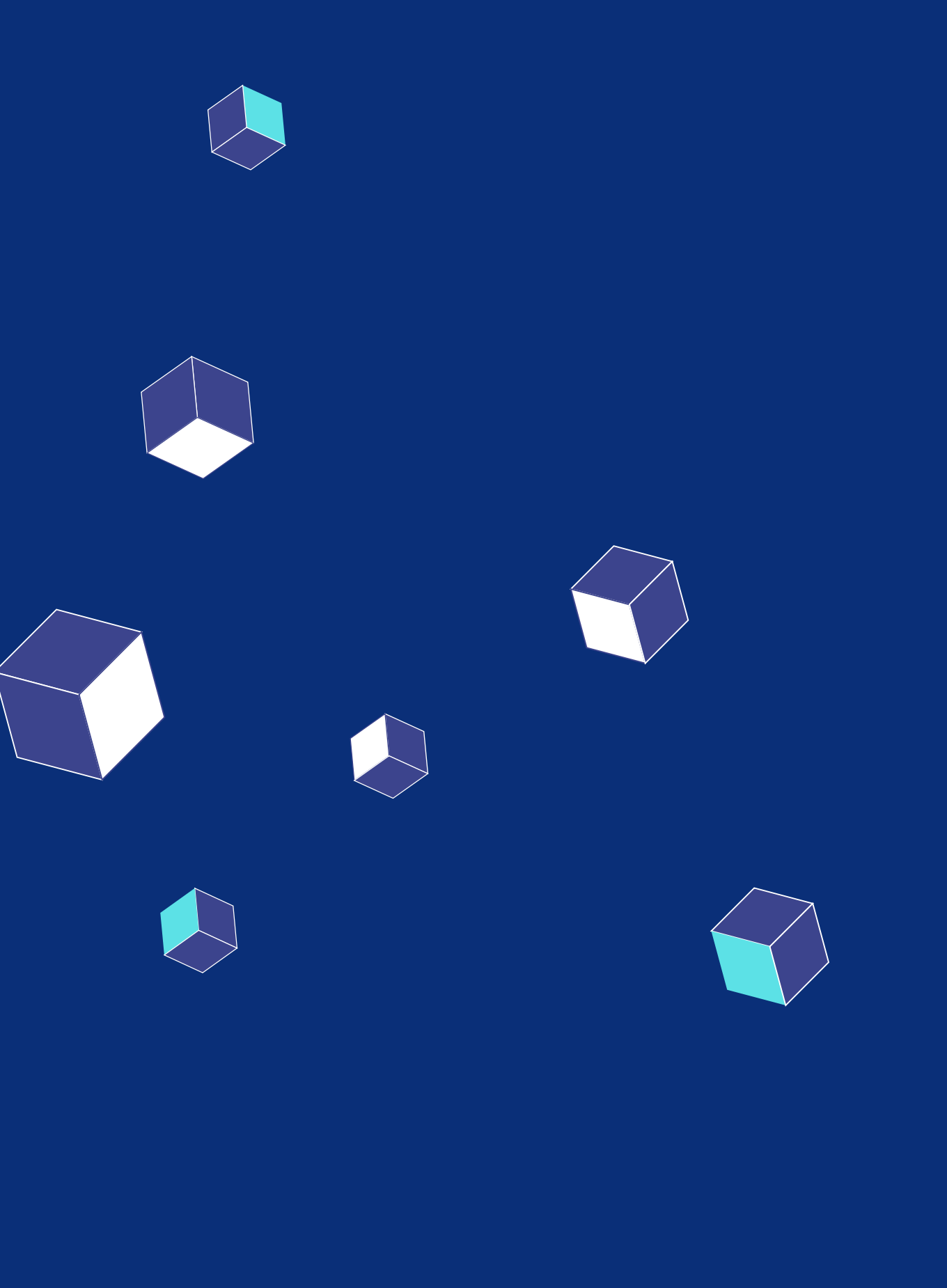
# LEI GERAL DE PROTEÇÃO DE DADOS

*Recomendações do Hospital de Clínicas de Itajubá - HCI para colaboradores e terceiros*



# SOBRE O CSIHCI

O Comitê de Segurança da Informação do Hospital de Clínicas de Itajubá foi criado a partir da vigência da Lei Geral de Proteção de Dados - LGPD, Lei 13.709/18, sendo composto por uma equipe multidisciplinar, responsável pelo tratamento de todos os tipos de dados pessoais no âmbito do HCI.

## *NOTA*

*Este material foi produzido pelo Departamento de Comunicação do HCI em parceria com o Comitê de Segurança da Informação do HCI, que é composto por representantes de vários setores administrativos e tem como finalidade única prestar informações sobre o tema LGPD, bem como orientar colaboradores e terceiros sobre a sua implementação e adequação, com enfoque na proteção dos dados pessoais.*

# APRESENTAÇÃO

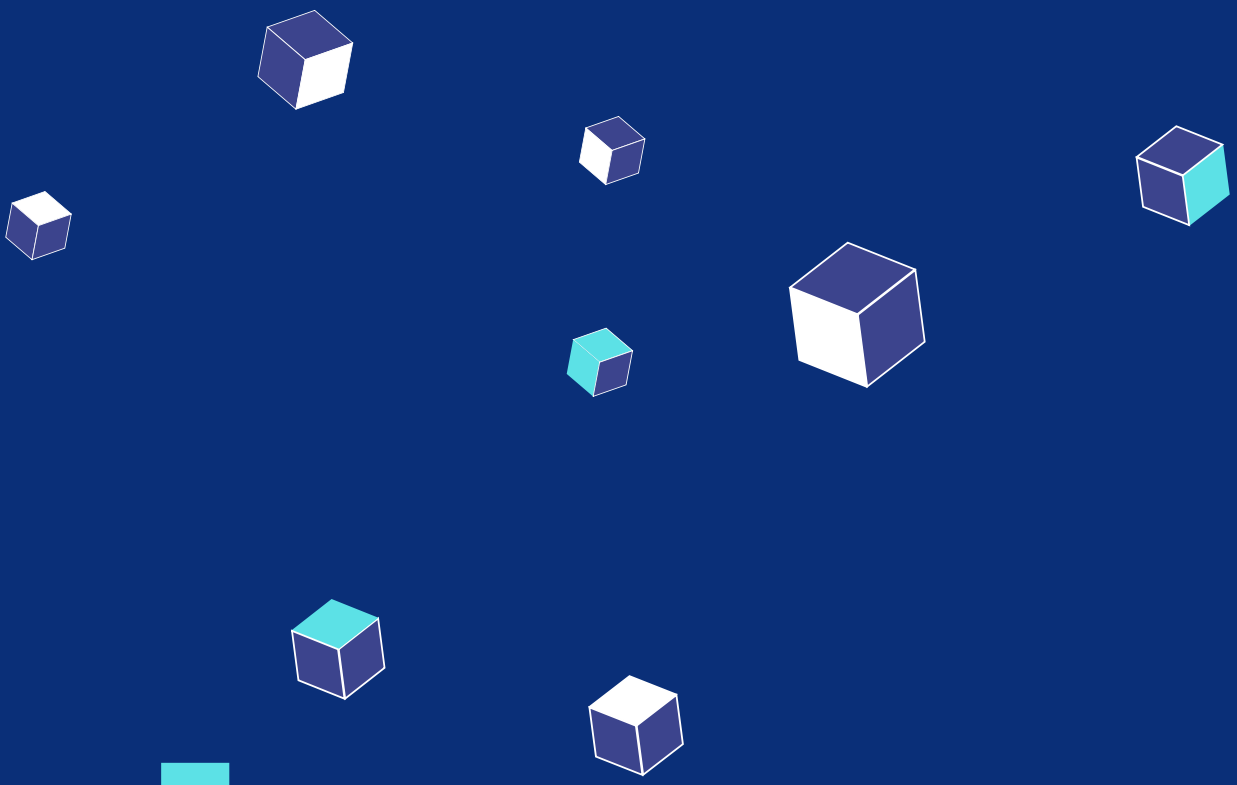
A Lei Geral de Proteção de Dados (LGPD) tem importância singular na construção e consolidação do mercado digital, devendo cada instituição encontrar a melhor maneira de promover sua implantação, assegurando a todas as pessoas, sejam elas colaboradores, clientes e fornecedores, a proteção dos seus dados.

No mundo contemporâneo, inovações tecnológicas surgem a todo momento e impactam diretamente a sociedade, influenciando na maneira como se relacionam e consomem produtos e serviços. Evidentemente, este novo cenário significa progresso e acesso à informação, mas ao mesmo tempo, nos deparamos com um mundo totalmente sem fronteiras, e é justamente esse o desafio nesse momento: dar segurança jurídica e maior proteção aos direitos dos titulares dos dados, apoiando e orientando sobre a implantação, de forma harmoniosa, da LGPD. Não é uma missão fácil e tampouco simples. O objetivo desta cartilha é contribuir com a implementação da LGPD, trazendo conceitos para compreensão dos impactos na prática do dia a dia das instituições hospitalares.

## ATUAÇÃO DO CSIHCI

o Comitê de Segurança da Informação tem como objetivo fiscalizar e deliberar sobre todos assuntos que estejam ligados direta ou indiretamente à questão dos dados pessoais no âmbito do HCI.

# SUMÁRIO



# I

# VISÃO GERAL DA PROTEÇÃO DE DADOS NO BRASIL

# A.
# CONCEITOS

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

***1) Dado pessoal:*** informação relacionada à pessoa natural identificada ou identificável. Essa informação representa todo e qualquer dado que possa tornar uma pessoa identificável, seja ela diretamente relacionada ao seu ti- tular (como um nome ou número de documento) ou mesmo indire- tamente relacionada, mas com potencial de identificá-lo(a) (como endereço, idade, informações sobre hábitos de compra, etc);

***2) Dado pessoal sensível:*** dado pessoal sobre origem racial ou ét- nica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referen- te à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

***3) Dado anonimizado:*** dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razo- áveis e disponíveis na ocasião de seu tratamento;

***4) Banco de dados:*** conjunto estruturado de dados pessoais,

estabelecido em um ou em vá- rios locais, em suporte eletrônico ou físico;

***5) Titular:*** pessoa natural a quem se referem os dados pesso- ais que são objeto de tratamento;

***6) Controlador:*** pessoa natural ou jurídica, de direito público ou privado, a quem compete as deci- sões referentes ao tratamento de dados pessoais;

***7) Operador:*** pessoa natural ou jurídica, de direito público ou pri- vado, que realiza o tratamento de dados pessoais em nome do controlador;

***8) Encarregado (DPO):*** pes- soa indicada pelo controlador e operador para atuar como canal de comunicação entre o contro- lador, os titulares dos dados e a Autoridade Nacional de Prote- ção de Dados;

***9) Agentes de tratamento:*** o controlador e o operador;

***10) Tratamento:*** toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, proces- samento, arquivamento, armaze- namento, eliminação, avaliação ou controle da informação, modi- ficação, comunicação, transferên- cia, difusão ou extração;

***11) Anonimização:*** utilização de meios técnicos razoáveis e dispo- níveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, dire- ta ou indireta, a um indivíduo;

***12) Consentimento:*** manifes- tação livre, informada e inequí- voca pela qual o titular concor- da com o tratamento de seus dados pessoais para uma fina- lidade determinada;

***13) Bloqueio:*** suspensão temporária de qualquer operação de tra- tamento, mediante guarda do dado pessoal ou do banco de dados;

***14) Eliminação:*** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

***15) Transferência internacional de dados:*** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

***16) Uso compartilhado de dados:*** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por en- tidades e órgãos públicos no cum- primento de suas competências legais, ou entre entes privados, reciprocamente, com autorização específica, para uma ou mais mo- dalidades de tratamento permiti- das por esses entes públicos, ou entre entes privados;

***17) Relatório de impacto à proteção de dados pessoais:***

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

***18) 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, tec- nológico ou estatístico;

***19) Autoridade nacional:*** órgão da administração pública responsável por zelar, implementar e fis- calizar o cumprimento desta lei.

# B.
# PRIVACIDADE DOS DADOS PESSOAIS

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

### *1. O regime jurídico brasileiro de privacidade*

A privacidade é protegida por diversas fontes, dentre as quais destacamos a Constituição Federal (CF) (artigo 5º, incisos X e XII), o Código de Defesa do Consumidor (CDC) (artigo 43) e o Marco Civil da Internet (MCI) (artigo 3, inciso II e III).

Desta maneira, a privacidade do indivíduo e, por consequência, as informações do titular dos dados pessoais, é considerada um direito fundamental.

### *2. A privacidade dos dados pessoais na LGPD*

Como não poderia ser diferente, a LGPD prevê que toda a pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.

Ela aplica-se independentemente do meio e/ou forma de tratamento dos dados coletados ou recebidos, isso significa que todo aquele que faz uso do dado se impõe às regras da LGPD.

Assim, para que haja o cumprimento das obrigações e procedimentos enumerados na lei, o conceito de privacidade dos dados pessoais deverá sempre permear qualquer tratamento de dados realizados pelos controladores e operadores.

Um exemplo que demonstra a necessidade de respeito à privacidade, consiste na possibilidade de o titular dos dados possuir direito ao acesso facilitado às informações sobre o tratamento de seus dados, de forma a especificar a finalidade do tratamento e informar quais dados estão sendo compartilhados e a sua finalidade. Para que o princípio da privacidade dos dados pessoais seja, de fato, implementado e observado, a LGPD informa que os controladores e os operadores poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização e procedimentos no tratamento de dados pessoais.

Dentre os pontos listados, ressalta-se que, o controlador poderá implementar o programa de governança em privacidade que, no mínimo:

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

certificação de privacidade quando da criação de projetos, fluxos, serviços ou produtos que envolvam dados pessoais (*privacy by design*).

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

# C.
# SEGURANÇA DA INFORMAÇÃO

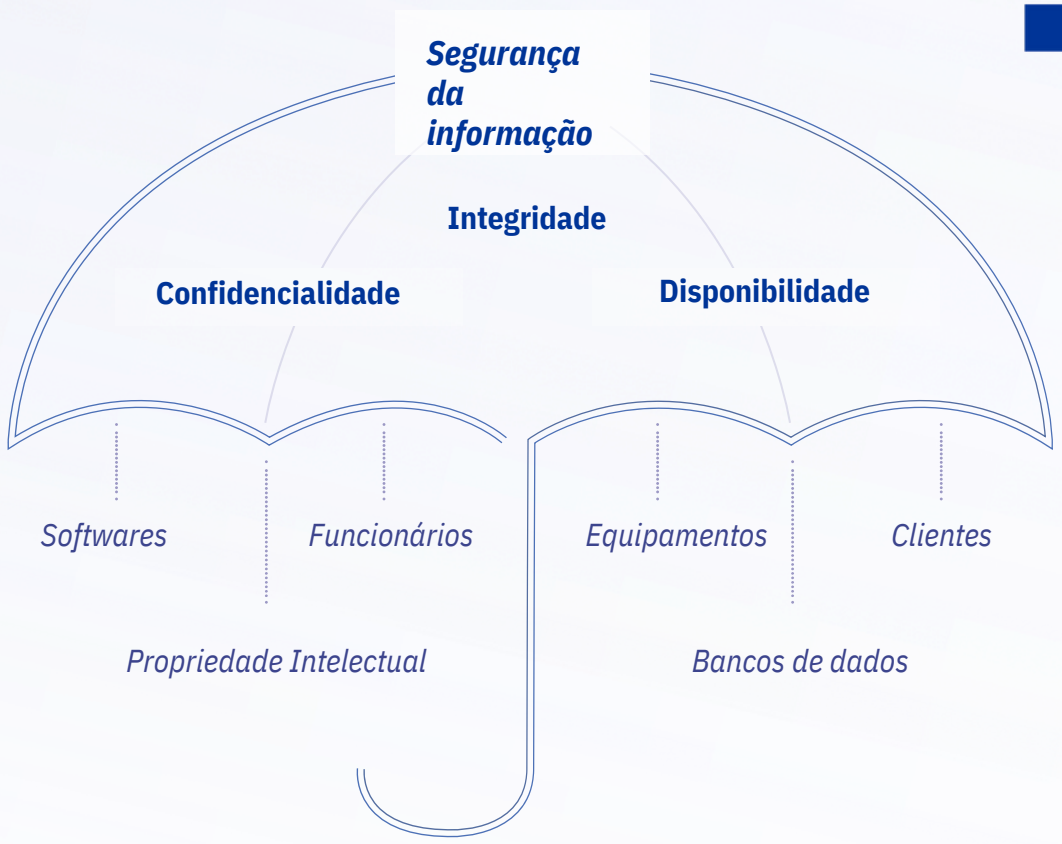
### *1. Conceitos fundamentais*

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

***Confidencialidade:*** restrição de acesso a dados exclusivamente aos usuários legítimos, protegendo-os do acesso por estranhos;

***Integridade:*** manutenção dos dados na mesma condição à qual eles foram disponibilizados por seu titular;

***Disponibilidade:*** garantia de que os dados concedidos pelo titular e os dados gerados a partir destes estarão disponíveis mediante solicitação do titular ou de seu responsável.




A segurança da informação é o elemento chave da governança de dados, devendo ser operada por meio de práticas e atividades, tais como a elaboração de processos internos e externos, treinamentos e estabelecimento de Políticas de Segurança da Informação (PSI).

Por meio desses esforços, a segurança da informação irá proteger todos os ativos de informação da empresa: dados, pessoas, softwares, equipamentos físicos, entre outros.

## *2. Passos para a implementação de segurança da informação*

Neste tópico, descreveremos de forma objetiva e geral os passos para a efetivação das práticas de

segurança da informação. Recomendamos que cada instituição adote as ferramentas e, se necessário, contrate prestadores de serviços especializados, que indicarão quais são os melhores métodos à cada empresa.

### *Classificação das Informações*

O primeiro passo para dar início às práticas de segurança da informação é a classificação das informações detidas pela empresa. Dessa forma, será possível compreender quais medidas serão aplicáveis e os esforços necessários para garantir a confidencialidade, integridade e disponibilidade dos dados e informações sob custódia.

Além dos pilares da segurança da informação descritos acima, insere-se neste ponto um quarto elemento, a ser levado em consideração: o valor atribuído à informação. Seja diretamente de seu proveito econômico, seja indiretamente, em decorrência dos prejuízos a serem arcados em caso de vazamento ou perda, o valor da informação será fator indispensável para aplicação relevante de uma efetiva PSI.

Neste sentido, é indispensável conhecer quais ameaças seriam aplicáveis à informação objeto de proteção. Seguem alguns exemplos:

- Os concorrentes têm interesse nesses dados?
- Há risco reputacional elevado em caso de perda ou vazamento?
- Há risco de pagamento de indenizações em caso de perda ou vazamento?
- Há determinação legal ou regulamentar de sigilo e/ ou segurança de tais dados ou informações?

Esclarecidos esses pontos, cada instituição poderá atribuir uma forma de classificação de tais informações que lhe seja mais apropriada. Abaixo propomos a seguinte classificação como sugestão:

| NÍVEL | DESCRIÇÃO | EXEMPLOS |
|---|---|---|
| **PÚBLICO** | Dados públicos são informações que podem ser divulgadas a qualquer pessoa, independentemente da sua relação com a instituição. A classificação pública não se limita aos dados que sejam de interesse público ou destinados ao público, a classificação é aplicável para dados que não necessitam de proteção contra a divulgação. | Catálogos de cursos, formulários de candidatura e de solicitação, entre outras informações que, em geral, são abertamente compartilhadas. Informações que são divulgadas no site institucional são bons exemplos de dados públicos. |
| **INTERNO** | Esta informação é aquela que a instituição não tem interesse em divulgar e o acesso por parte de indivíduos externos deve ser evitado. Entretanto, caso a informação seja disponibilizada por alguma razão, não causará danos sérios à instituição. | Memorandos, correspondências e atas de reuniões, listas de contatos que contêm informações que não estão disponíveis publicamente e documentação processual que deve permanecer na esfera interna. |
| **CONFIDENCIAL** | Informação interna da instituição cuja divulgação pode causar danos financeiros ou à imagem da organização. Essa divulgação pode gerar vantagens a eventuais concorrentes e perda de clientes. | Demonstrações financeiras, prontuário do paciente, estatísticas e indicadores. |
| **RESTRITO** | Derivação da informação confidencial, cuja restrição de acesso possui maior grau interno. | Dados de acesso limitado a profissionais da saúde, dados finan- ceiros não objeto de divulgação pública, atas de assembleias ou reuniões de sócios não registradas na junta comercial, entre outros. |

### *Implementação de ferramentas e políticas*

Uma vez estabelecida a ordem de classificação das informações e dados objeto de tratamento na instituição, será necessário implementar e executar ações que visem a adoção de uma cultura de segurança da informação. Exemplificamos abaixo algumas sugestões:

- Adoção de medidas de segurança apropriadas ao acesso de dados de acordo com a sua classificação, como a utilização de senhas, confirmação por duplo fator, adoção de tokens, entre outros;
- Análise interna do banco de dados, a fim de verificar os processos de tratamento e os riscos envolvidos;
- Adoção de medidas tecnológicas internas que garantam a segurança das informações, tais como a eliminação de dados desnecessários, anonimização e pseudonimização de dados, criptografia, etc;
- Elaboração de uma Política de Segurança da Informação, com orientações objetivas de métodos e processos para o tratamento de dados e medidas de segurança apropriadas;
- Realização de treinamentos e divulgação de materiais de conscientização para funcionários e clientes.

## *3. O incidente de segurança da informação*

Segundo o ISO/IEC 27035-1/2016, em livre tradução, um Evento de Segurança da Informação pode ser considerado como uma ocorrência indicando uma possível violação de segurança da informação ou falha de controles. Já o Incidente de Segurança da Informação, por sua vez, são um ou vários Eventos de Segurança

da informação, com potencial de causar dano aos ativos de uma organização ou comprometer suas operações[1].

Diante dos diuturnos avanços tecnológicos, da difusão da utilização de bases de dados por *outsourcing* e do crescimento constante do interesse financeiro por dados, vemos que a ocorrência de Incidentes de Segurança da Infor- mação vem crescendo exponen- cialmente. Somente no Brasil, em 2018, foram detectados 120,7 milhões de links maliciosos[2], ao passo que a pesquisa do mesmo ano "*Global State of Information Security*", realizada em 122 países, revelou que 54% das empresas não possuem um processo de resposta a incidentes[3].

As causas de um Incidente de Segurança da Informação são as mais variadas, podendo ser deliberadas (como ataques ao banco de dados ou utilização de engenharia social), ou acidentais (decorrentes de erros humanos ou causas naturais). Dentre as consequências estão o acesso não autorizado às informações, a implicação de danos à base de dados ou até mesmo a perda desses dados.

Especificamente no que se refere a dados pessoais, é indispensável destacar que a LGPD reputa que o controlador dos dados é responsável direto e objetivo por tais incidentes que causem danos a titulares de dados pessoais, inclusive de natureza coletiva, além das multas e sanções descritas na lei, como o bloqueio temporário dos dados objeto de tratamento e até mesmo o pagamento de multa no valor de até 2% do faturamento da pessoa jurídica ou grupo econômico.

Ainda nos termos do ISO/IEC 27035-1/2016, os objetivos de um plano de abordagem do incidente de informação precisam conter:

- A detecção rápida do incidente, com imediata classificação dos riscos relacionados;
- Resposta apropriada e eficiente ao incidente;

- Aplicação de controles que possam minimizar os efeitos adversos;
- O estabelecimento de elos com os processos de administração de crises já adotados pela empresa;
- Aprendizagem rápida das falhas exploradas no incidente, com correção de vulnerabilidades.

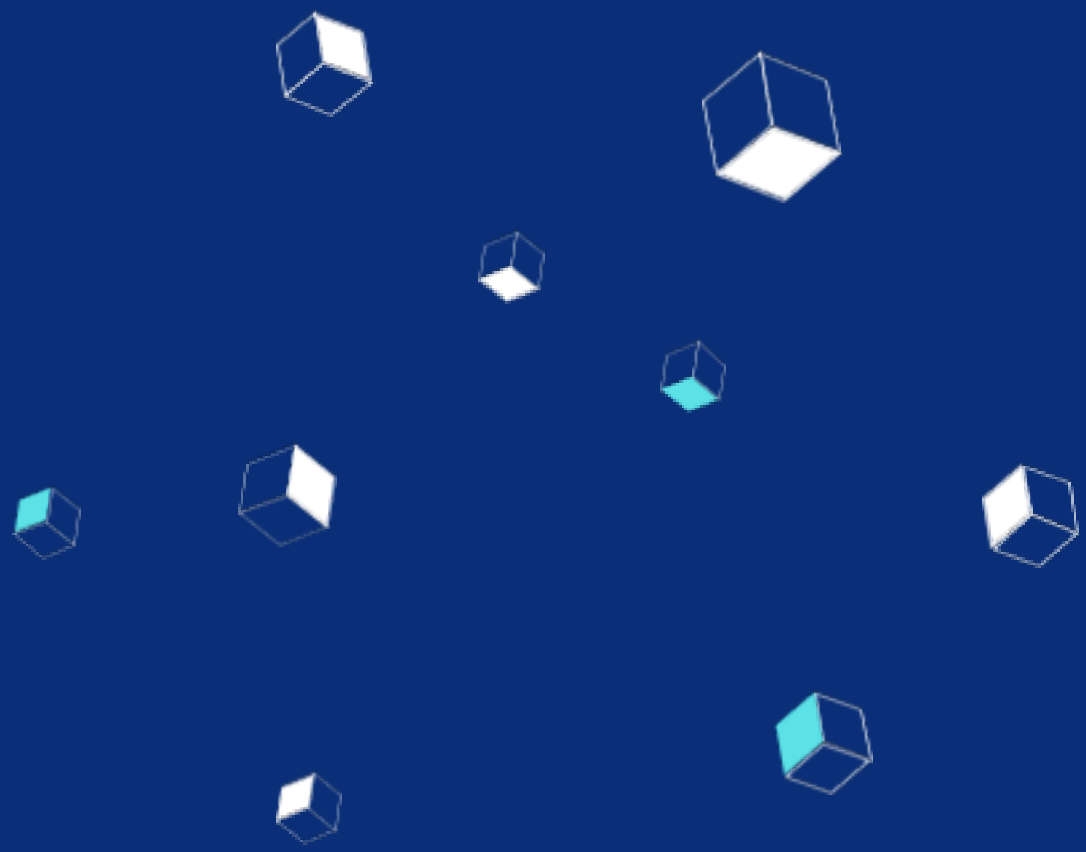
Destacamos que, além dos pontos descritos acima, a partir da vigência da LGPD, em caso de in- cidente que envolva o tratamento de dados pessoais, o controlador deverá ainda decidir, de acordo com a classificação de risco, se será realizada a comunicação à Autoridade Nacional de Proteção de Dados. Isso porque, segundo a lei, deve ser comunicado o incidente "que possa acarretar risco ou dano relevante aos titulares". Por esta razão, é indispensável que as instituições se preparem, tanto criando ferramentas assertivas de segurança da informação, como desenvolvendo respostas eficientes aos incidentes.

Adotadas as devidas ferramentas e políticas, não somente a instituição poderá operar o tratamento de dados com segurança, mas também terá seus riscos minimizados em caso da ocorrência de incidente.

[1] ISO/IEC 27035-1/2016, 4, 4.1: "An information security event is an occurrence indicating a pos- sible breach os information security or failure of controls. An information security incident is one or multiple related and identified information security events that meet established criteria and can harm an organization's assets or compromise its operations."

[2] Relatório da Segurança Digital no Brasil: Disponível em https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf

[3] Fortalecendo a Sociedade Digital contra o caos cibernético. Disponível em https://www.pwc.com.br/pt/publicacoes/assets/2017/fortalecimento_sociedade_digital_17_gsiss.pdf



# II

# PROTEÇÃO DE DADOS EM SAÚDE

# A.
# ARCABOUÇO NORMATIVO DA PROTEÇÃO DE DADOS EM SAÚDE NO BRASIL

Conforme a Constituição Federal de 1988:
"...são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação" (Constituição Federal de 1988, art. 5º, inciso X).

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

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

No Brasil, algumas ações vêm sendo tomadas para padronizar este tipo de informação. No caso da saúde privada, a Agência Nacional de Saúde Suplementar (ANS) padronizou as informações de saúde entre prestadores de serviço, operadoras e governo através do TISS (Troca de Informações da Saúde Suplementar).

Existem vários esforços para que haja padronização e normas claras para a proteção de dados em saúde. A Lei do Marco Civil da Internet - Lei 12.965 de abril/2014 - já é um princípio para proteção de dados da informação, porém muito vinculada apenas ao uso da internet.

Em 2016, a Política Nacional de Informação em Saúde (PNIS) estabeleceu alguns princípios com o objetivo de garantir a confidencialidade, o sigilo e a privacidade da informação de saúde pessoal como direito do indivíduo.

Tais legislações foram complementadas com a Lei 13.709/2018 - Lei Geral de Proteção de Dados, que é voltada para a proteção de dados do indivíduo e, consequentemente, complementando a proteção de dados e informações na área da saúde.

A LGPD traz em seu texto a questão de tratamento de dados e a forma pelas quais os dados poderão ser utilizados, como nos trechos abaixo: *"... para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;" (LGPD 13709/2018, Art 7º, inciso VIII)*

*"...É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter van-*

*tagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:" (LGPD 13709/2018, Capítulo II, Seção II, Art. 11, parágrafo 4).*

Os esforços para se atender à nova legislação são enormes, uma vez que há muitas dúvidas e o tempo é escasso.

# B.
# HIPÓTESES DE TRATAMENTO

As hipóteses de tratamento dos dados de acordo com a LGPD são:

- Consentimento do titular, para uso das informações;
- Cumprimento das obrigações legais ou regulatórias pelo controlador;
- Uso da administração pública, para o tratamento e uso compartilhado de dados necessários para cumprimento de políticas públicas;

- Órgão de pesquisa clínica, assegurando a anonimização;
- Execução de contrato;
- Exercício regular de direitos em processo (judicial, administrativo ou arbitral);
- Proteção da vida e segurança física do titular ou de terceiros;
- Tutela da saúde exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Atendimento ao legítimo interesse do controlador ou de terceiros (exceto quando os direitos e liberdades fundamentais do titular exijam a proteção dos dados pessoais); ou
- Proteção do crédito.

Em qualquer um dos casos, o tratamento de dados pessoais nas ocasiões em que o acesso é público, deve considerar a finalidade, a boa-fé e o interesse público que justificarem sua disponibilização.

Material de consulta


- https://www.scielosp.org/pdf/csp/2018.v34n7/e00039417
- https://nupef.org.br/sites/default/files/downloads/artigo%20politics_esaude%20e%20priva- cidade.pdf
- LGPD na Saúde - O que as empresas precisam saber - Machado Nunes

C.

# COMUNICAÇÃO E COMPARTILHAMENTO DE DADOS EM SAÚDE PARA PRESTAÇÃO DE ASSISTÊNCIA

O tratamento de dados pessoais sensíveis somente poderá ocorrer:

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

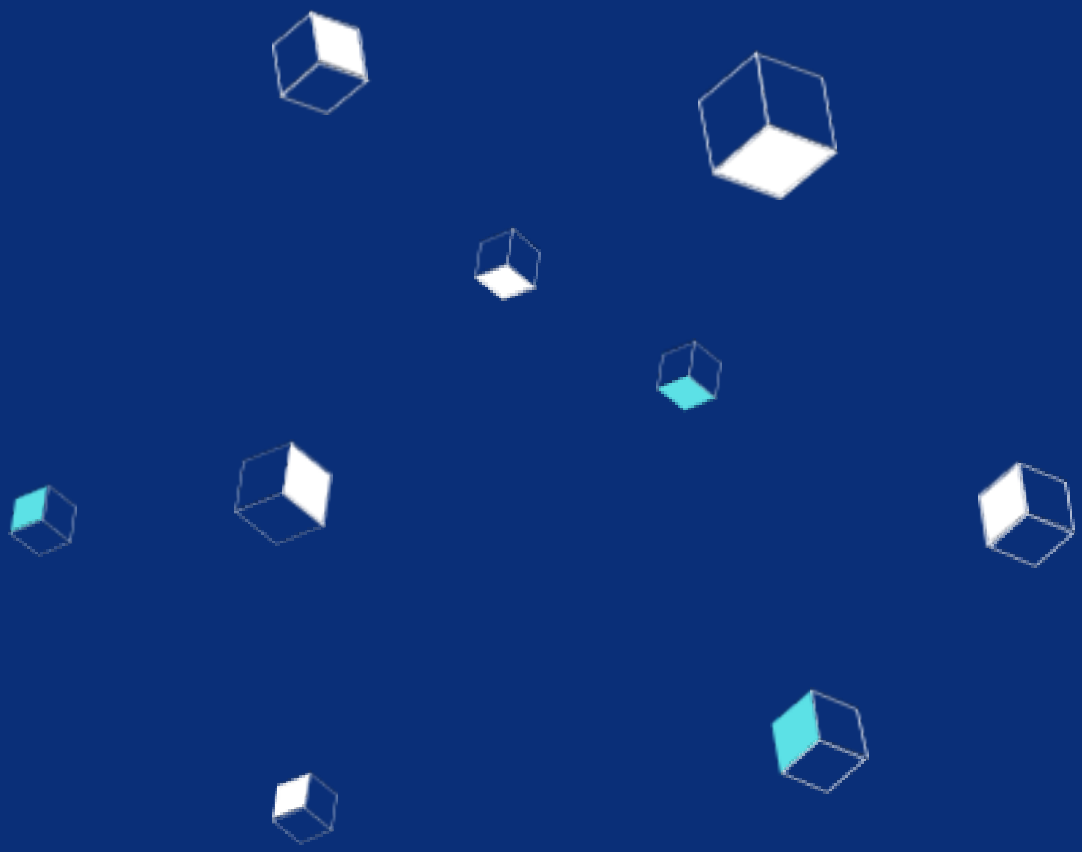
- Sem o consentimento do titular quando for indispensável e estiver dentro das hipóteses taxativamente previstas no art. 11: "tutela da saúde exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária".

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

# D.
# NOTIFICAÇÃO COMPULSÓRIA

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

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



# III

# AGENTES DE TRATAMENTO

# A.
# DEFINIÇÃO

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

O controlador, na definição legal (art. 5º, VI) é *"pessoa natural ou jurídi- ca, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". Já o operador (art. 5º, VII) é "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".*

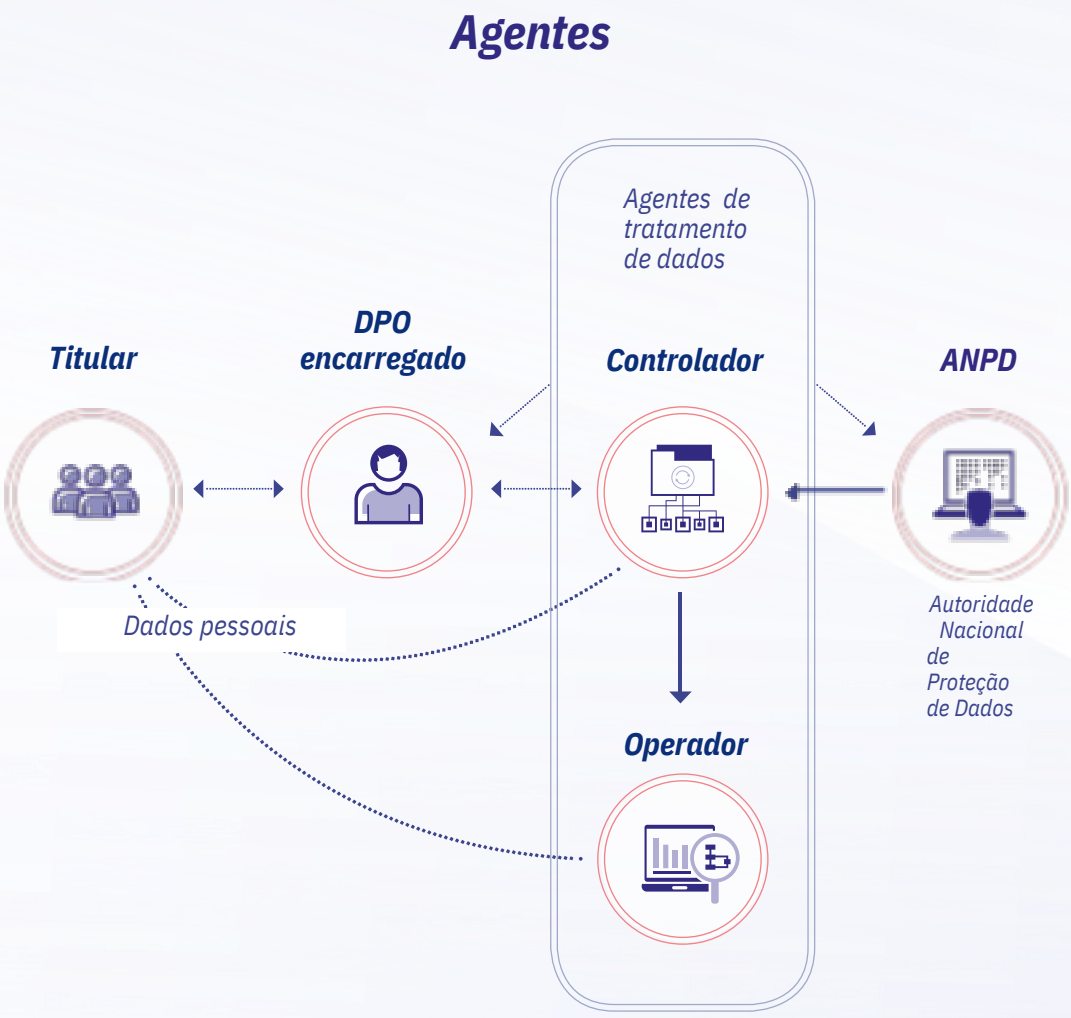
Os agentes de tratamento de dados neste contexto serão os hospitais, por meio de seus colaboradores, médicos e parceiros (terceiros) que tratam os dados dos pacientes/clientes, em virtude do relacionamento de prestação de serviços de saúde específicos de cada instituição.

Um hospital pode ser controlador e operador dos dados ao mesmo tempo, diante de uma atividade (processo) que trate os dados pessoais dos titulares. Outro cenário é quando um hospital terceiriza a operação dos dados, como um laboratório de análises clínicas, diagnóstico por imagem, call center para SAC , por exemplo, caso em que o hospital seria controlador de dados.

Um fluxo comum a considerar será: por força de uma relação estabelecida entre um titular e um controlador de dados que conta com ser- viços prestados por um operador, o titular dos dados fornece os dados para um operador ou, um operador coleta os dados de um titular sob seu consentimento. O operador deve atender as determinações de tratamento de dados definidas pelo controlador de dados. O controlador

de dados deve estar em conformidade com as definições da LGPD. Cabe ao controlador de dados nomear um encarregado (DPO) para atuar como canal de comunicação para atender as necessidades dos titulares junto ao controlador e à ANPD.

*Figura 1 | Agentes: fluxo de relacionamento*




*Fonte: Amaro Neto.*

***Figura 2** | Agentes de tratamento de dados: exemplos de controlador e operador*


*Fonte: Amaro Neto.*

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

# B.
# OBRIGAÇÕES E RESPONSABILIDADES

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

***Jurídica:***

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

### *Assistencial e corpo clínico:*

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

### *Recursos Humanos:*

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

### *Auditoria Interna e Risco:*

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

***Tecnologia da Informação e Segurança da Informação:***

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

- Conscientização de colaboradores e prestadores de serviço;
- Processo de desenvolvimento seguro que envolva testes durante todo o ciclo.

***Gestão de fornecedores/contratos:***

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

***Serviços de apoio médico:***

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

Em seu artigo 18, a LGPD, ainda que em linhas gerais a merecer melhor regulamentação pela ANPD, detalha obrigações do controlador perante o titular de dados pessoais objeto de tratamento:

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários,

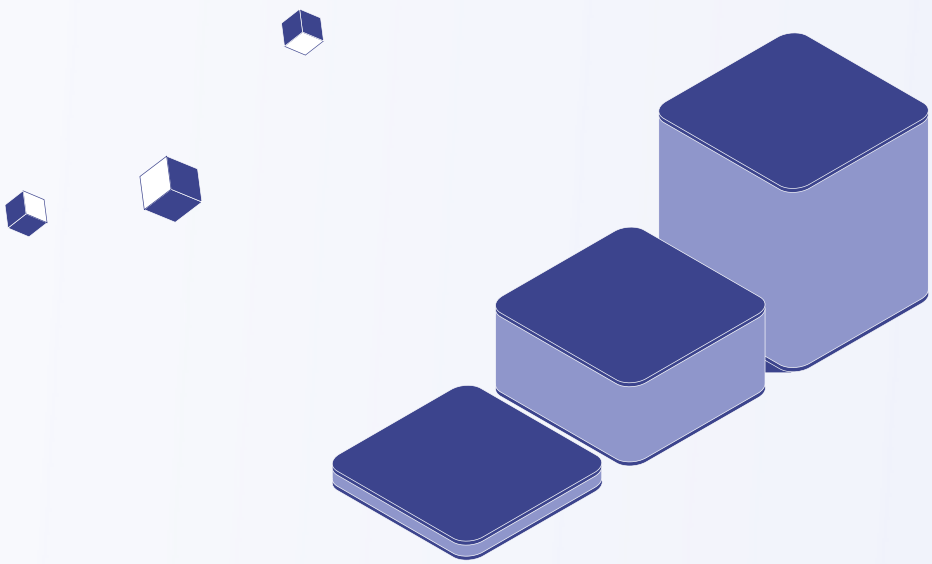
excessivos ou tratados em desconformidade com o disposto na lei;

- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

- Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da lei;
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

- Revogação do consentimento, nos termos do parágrafo 5º do art. 8º da lei.



# C.
# DATA PROTECTION OFFICER (DPO)

O DPO *(Data Protection Officer)* surgiu com a consolidação da GDPR na União Europeia, como um cargo de nível estratégico, que é responsável por disseminar a cultura de proteção de dados na instituição, criar normas e procedimentos que atendam às legislações de proteção de dados vigentes, sendo um canal de comunicação entre instituição, titular das informações e entidades governamentais que controlam e regulam a proteção de dados individuais. Na prática, o DPO agrega funções de uma *Security Officer* ou de um CISO *(Chief Information Se- curity Officer).*

Trata-se de uma função multidisciplinar, pois o profissional deve ter conhecimento de como a instituição atua com os dados coletados e sua forma de tratamento. Além disso, precisa ter sinergia ou conhecimento em tecnologia e segurança da informação, aspectos legais, compliance, gestão de riscos, comunicação fluida e clara e ter bom relacionamento, já que será um influenciador dentro da instituição.

Uma de suas principais funções será receber as notificações dos titula- res das informações e/ou da entidade fiscalizadora, sendo responsável por sua apuração, tratativa adequada e resposta ao titular e à ANPD. Deverá ter autonomia para auditar e fiscalizar as possíveis irregularidades para que possam ser corrigidas e notificadas conforme rege a lei. Figura idêntica existe na diretriz europeia. O *Data Protection Officer* (DPO) será a pessoa (natural ou jurídica), que atuará "*como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade*

*Nacional de Proteção de Dados (ANPD)*" (art. 5º, VIII), será o responsável por disseminar a cultura de proteção de dados na instituição, além de criar normas e procedimentos adequados à lei. Será o responsável por receber as notificações da ANPD e dos titulares das informações e as colocará em prática.

O DPO deverá ter sua identidade e informações de contato divulgadas publicamente de forma clara e objetiva, preferencialmente no site do controlador (art. 41, §1º). A LGPD lista as atividades do DPO no art. 41, §2º, sendo de mais destaque as seguintes:

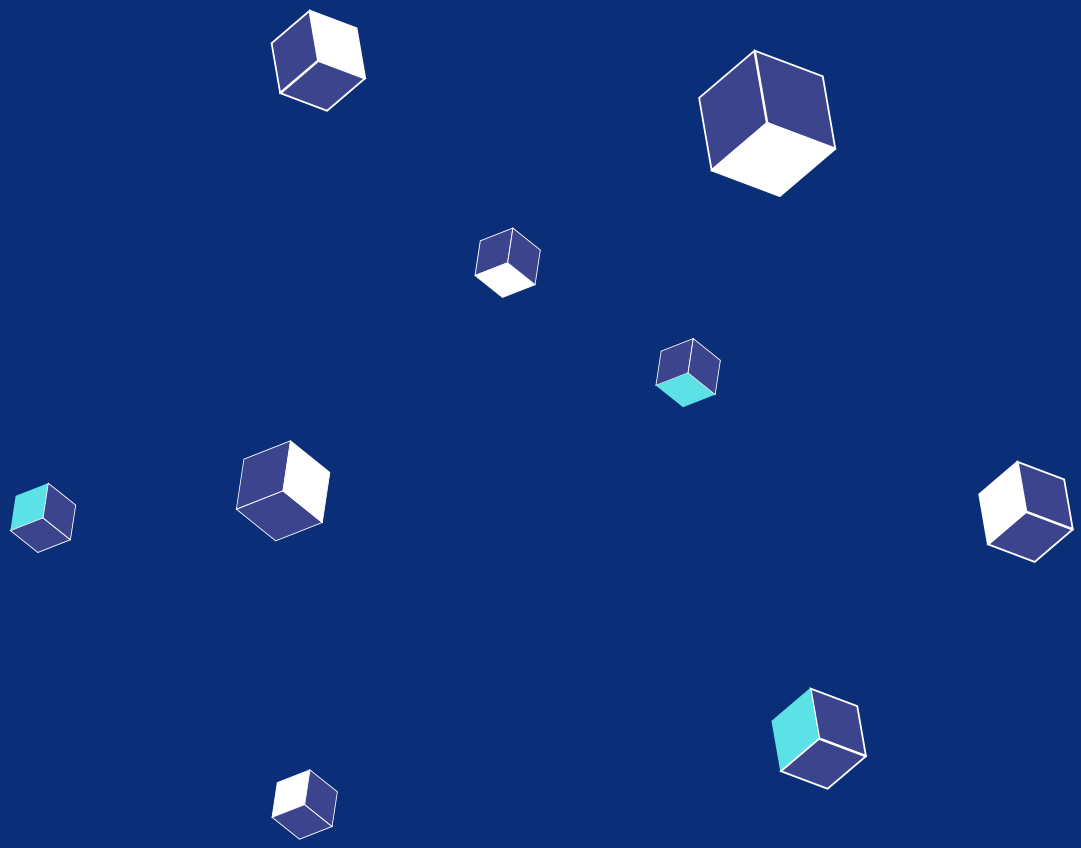
- Garantir a efetividade dos controles relacionados à proteção de dados pessoais sob custódia da organização;
- Coordenar a conformidade do processo com os outros agentes de tratamento;
- Relacionar-se com entidades de autoridade;
- Em caso de incidente, analisar se aquilo deve ser reportado ou não;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

# D.
# RELATÓRIO DE IMPACTO

Segundo a LGPD (art. 5º, XVII), o relatório de impacto à proteção de dados é a *"documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco."*

O referido relatório poderá ser solicitado ao controlador pela ANPD (art. 38), e deverá conter, no mínimo, *"a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados."*

Caso ocorra algum incidente de segurança que possa implicar em risco ou em dano aos titulares de dados pessoais, caberá ao controlador comunicar à ANPD e ao titular de dados pessoais tal ocorrência (art. 48). Esta comunicação deverá ocorrer em prazo razoável (que será objeto de regulamentação pela ANPD - §1º).



# IV

# OPORTUNIDADES E DESAFIOS PARA O SETOR

No Brasil, a ISO/IEC 27000 é um conjunto de padrões que fornece uma estrutura de gerenciamento de segurança da informação, utiliza- da como forma de normalizar grande parte das ações e investimentos realizados pelas instituições em segurança.

As práticas de segurança da informação estão intimamente ligadas à quantidade de recursos que as instituições destinam para este fim todos os anos, e cada um tem seu próprio modelo de segurança implantado.

O fato de termos diferentes produtos e modelos de segurança implanta- dos nas instituições não é um problema, visto que diferentes ameaças são lançadas no mercado a cada dia, explorando diferentes vulnerabilidades e gerando como consequência uma vasta gama de subprodutos para prover o controle. Entretanto, a falta de um padrão dificulta a decisão de qual tecnologia adotar e quanto de recurso destinar.

Este capítulo abordará práticas de segurança considerando o conceito de defesa em camadas e avaliando os modelos mais consolidados. Tais práticas, se aplicadas, além de promoverem segurança para os hospitais, também ajudarão a mitigar os impactos gerados pelas sanções judiciais previstas pela nova lei.

Por fim, é importante considerar que estar de acordo (*compliance*) com a LGPD não é o mesmo que estar seguro. Mas também é verdadeiro que se adaptar às rotinas e políticas nas instituições, conforme previsto na lei, consequentemente aumentará o nível de segurança.

# A.
# NORMAS DE SEGURANÇA

O conceito de segurança da informação está padronizado na ISO/IEC 17799, que também traz o conceito de informação, assim como seguem:

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

A tríade CIA (Confidentiality, Integrity and Availability) -- Confidencialidade, Integridade e Disponibilidade -- representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos importantes são a irretratabilidade e a autenticidade. Com o evoluir do comércio electrónico e da sociedade da informação, a privacidade é também uma grande preocupação.

Os atributos básicos (segundo os padrões internacionais) são os seguintes:

- Confidencialidade - propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

- Integridade - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).

- Disponibilidade - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.


***Fonte: Amaro Neto.***

# B.
# PADRÕES TÉCNICOS

No tempo em que as instituições utilizavam documentos físicos, os padrões de segurança previam que estes fossem armazenados em local que pudesse ter a porta trancada.

No cenário de saúde, os hospitais precisam manter os prontuários físicos por, no mínimo, vinte anos para algumas patologias e, em outras situações, este prazo pode ser ainda maior. Portanto, a digitalização desses documentos facilita seu armazenamento e gestão, ao passo que gera novas demandas para a TI, que deve armazená-los garantindo disponibilidade e segurança.

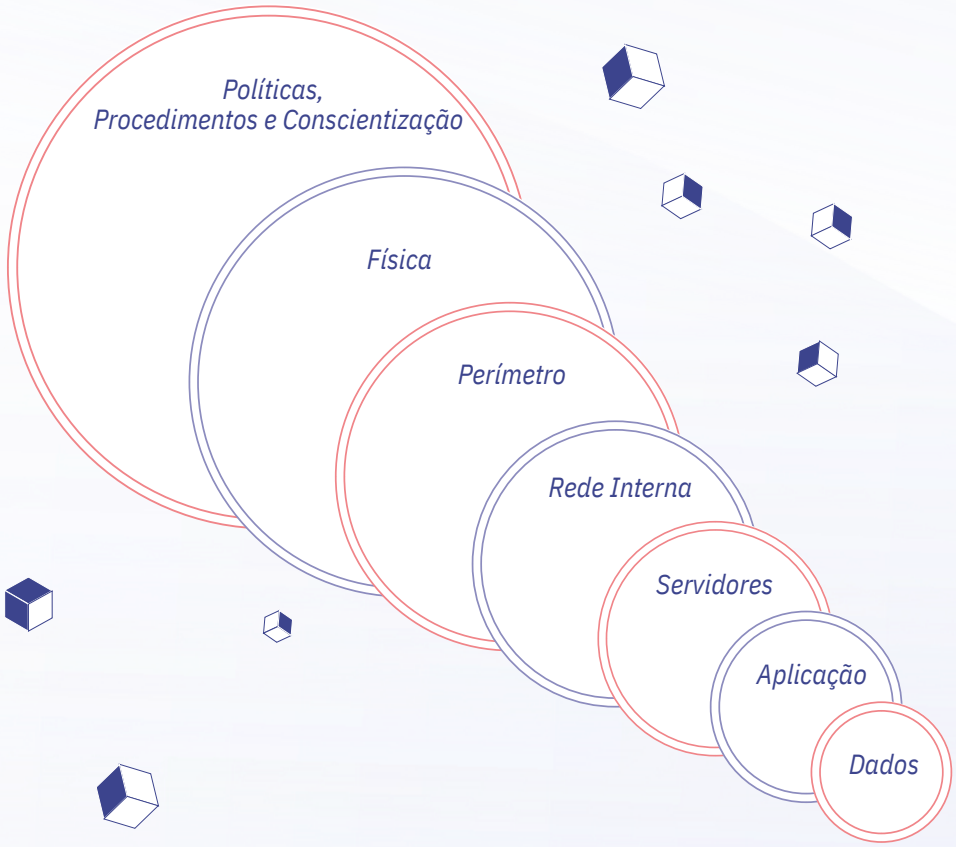
Com a evolução destes documentos para os meios digitais, a ação de manter a segurança foi elevada para níveis complexos, exigindo ambientes sofisticados, com alto custo e necessidade de atualizações constantes.

A construção de políticas, normas e procedimentos, a adoção das melhores práticas de segurança, o monitoramento e a auditoria destas ações, representam que a proteção deve ser elaborada visando mitigar riscos causados por pessoas, ambiente ou sistemas e equipamentos. No atual cenário virtual, as ameaças chegam aos ambientes de forma silenciosa e invisível, explorando não apenas as vulnerabilidades de hardware e software, mas também as vulnerabilidades das pessoas, exigindo a construção de defesas em todas as camadas envolvidas nos ambientes de TI das empresas.

As instituições possuem suas próprias políticas de segurança da informação e todos os seus usuários devem conhecer e praticar as diretrizes ali definidas. Geralmente, as organizações também possuem

um processo de detecção e classificação de risco próprio, levando em consideração o valor do seu ativo e a probabilidade do risco. Desta forma concentram seus esforços e investimentos em segurança da informação.

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



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

### *1. Aplicações*

Prover segurança exige observar qual linguagem será utilizada, a metodologia de desenvolvimento que deve prover a adequada segurança desde sua escrita, assim como, a utilização de protocolos e servidores web seguros em caso de aplicações desenvolvidas para este meio.

Os sistemas devem prever o armazenamento de logs e possuir auditorias ativas, possibilitando a rastreabilidade e identificação das ações tomadas pelos usuários. Deve também prover perfis de acesso conforme suas atribuições e um gerenciamento de concessões/revogações de direitos.

Cuidar da segurança do sistema, não significa dizer que está se cuidando da segurança dos dados pessoais/sensíveis, é necessário que sejam observados os aspectos de privacidade. E as equipes de engenharia, análise, desenvolvimento e testes, deverão ser capacitados, conforme a metodologia *privacy by design*.

### *2. Servidores*

A metodologia de *Hardening* é aplicada como padrão de segurança em infraestrutura e servidores, através do processo de mapeamento de ameaças, mitigação de riscos e execução das ações corretivas. O objetivo principal dos padrões recomendados neste

modelo é tornar o ambiente menos suscetível a invasões.

A efetividade deste modelo deve considerar três fatores: segurança, risco e flexibilidade. Mantê-los balanceados será o desafio desta implementação, visto que, quanto mais seguro for o servidor, menos flexível ele se tornará.

Deve ser sempre lembrado que a aplicação de patches de correção/segurança e a utilização de sistemas operacionais com suporte do fornecedor é regra fundamental para um ambiente seguro.

### *3. Rede interna*

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

- Software de antivírus: este recurso é utilizado para detectar e deter ameaças, uma vez que já estão salvas e/ou instaladas nos computadores ou servidores.
- Segmentação da rede: é a divisão da rede em sub redes, para evitar que anomalias e ameaças se multipliquem para diversos setores da organização, aumentando a possibilidade de efetividade e danos.
- *Access Control List* (ACL): ou lista de controle de acesso, referente às permissões atribuídas a um objeto que especificam quais usuários recebem acesso ao mesmo tempo e as operações que ele pode executar.
- *Network Access Control* (NAC): já com alternativa *open source* para algumas

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

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

### *4. Perímetro*

No perímetro são instalados equipamentos (*firewall*, roteador, etc.), e neles são definidas regras para evitar acessos a sites que contenham conteúdos e/ou arquivos nocivos ao ambiente de TI. Outro aliado é o protocolo DLP (*Data Loss Prevention*), geralmente é uma funcionalidade oferecida pelo equipamento de firewall, mas também pode ser uma solução in- dependente. Ele é responsável por garantir que dados sensíveis não saiam da rede interna para a rede externa (internet).

### *5. Física*

Esta, sem dúvida, é a prática de segurança mais antiga, pois des- de os primórdios guardamos ati- vos de valor em locais trancados e a chave é oferecida apenas às pessoas que tenham real

necessidade de acesso aos objetos ali armazenados.

Quando este assunto é associado ao meio digital, a segurança física se dá aos equipamentos que armazenam ou acessam os dados, portanto a utilização de controles de acessos (sejam sensores biométricos, sensores de retina ou apenas uma chave), a concessão ou revogação dos acessos aos indivíduos deve ser rigorosamente gerenciada.

### *6. Política, procedimentos e conscientização*

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

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

## Contamos com a colaboração de todos para continuarmos lutando pela Segurança da Informação e pela Proteção dos Dados Pessoais no âmbito do HCI!

A presente cartilha foi elaborada com base nas informações da ANAHPD - Associação Nacional de Hospitais Privados