UNIVERSIDADE DA PRIVACIDADE

MANUAL DO CURSO

Governança e LGPD
aplicada ao Setor da Saúde

Capacitação executiva para instituições de saúde em conformidade com a Lei Geral de Proteção de Dados

CARGA HORÁRIA: 8 HORAS | MODALIDADE: AO VIVO ONLINE

Edição 2026

Ficha Técnica do Curso

CARGA HORÁRIA	MÓDULOS	DATAS	MODALIDADE
8h	4		AO VIVO

Informações Gerais

Campo	Descrição
Nome do curso	Governança e LGPD aplicada ao Setor da Saúde
Instituição	Universidade da Privacidade (UP) — DPOnet
Carga horária total	8 horas, distribuídas em 2 dias
Modalidade	Ao vivo online, via plataforma de videoconferência
Material de apoio	Apostila digital, templates práticos e certificado de conclusão
Idioma	Português (Brasil)
Pré-requisito	Nenhum formal. Recomenda-se noções gerais de LGPD.
Certificação	Certificado digital de 8h, emitido após conclusão e aproveitamento mínimo

O Contexto: LGPD no Setor da Saúde

Por que a saúde é o setor mais crítico em proteção de dados

Desde a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), o setor da saúde passou a ser tratado com o maior rigor regulatório existente no ordenamento brasileiro. Isso ocorre porque os dados relacionados à saúde — diagnósticos, exames, prontuários, informações genéticas, condições psicológicas e dados de planos de saúde — são classificados pela lei como dados pessoais sensíveis, sujeitos a um regime jurídico especialíssimo.

Ao mesmo tempo, o ecossistema de saúde brasileiro envolve uma teia complexa de atores: hospitais, clínicas, laboratórios, médicos autônomos, operadoras de planos de saúde, cooperativas, sistemas de prontuário eletrônico, empresas de telemedicina, farmácias, seguradoras, órgãos reguladores (ANS, Anvisa, ANPD) e o próprio Sistema Único de Saúde. Cada um desses atores processa dados sensíveis de pacientes e responde, direta ou indiretamente, pelos tratamentos que realiza.

Panorama de Riscos no Setor da Saúde

- Ataques de ransomware a hospitais brasileiros vêm crescendo de forma significativa, com paralisação de unidades assistenciais e exposição de dados de milhares de pacientes.
- A Autoridade Nacional de Proteção de Dados (ANPD) já publicou sanções relevantes para o setor, inclusive com multas e exigência de medidas corretivas específicas.
- Vazamentos de dados clínicos podem gerar, além das sanções administrativas da LGPD, responsabilização civil e ética perante conselhos profissionais (CFM, COREN, CFF, entre outros).
- A interoperabilidade — cada vez mais exigida por programas como o SUS Digital e a RNDS — cria novos pontos de atrito entre utilidade clínica e proteção da privacidade.

A proposta do curso

A proposta da UP neste curso é romper a abordagem puramente teórica da LGPD e entregar uma metodologia prática, baseada em casos reais do setor. Em 8 horas de conteúdo ao vivo, com instrutores experientes em compliance hospitalar, o participante sairá capaz de diagnosticar vulnerabilidades em fluxos clínicos, definir bases legais adequadas, estruturar governança interna, responder a incidentes e atender aos direitos dos pacientes — tudo isso com templates prontos para aplicação imediata.

Objetivos de Aprendizagem

Ao final do curso, os participantes serão capazes de:

- **Identificar e classificar:** Diferenciar fluxos de dados comuns de dados sensíveis e aplicar as bases legais corretas — como Tutela da Saúde e Proteção da Vida — para cada tratamento realizado na instituição.
- **Mapear riscos:** Executar um diagnóstico preliminar de vulnerabilidades em prontuários eletrônicos e fluxos de atendimento, tanto físicos quanto digitais.
- **Estruturar governança:** Definir papéis e responsabilidades (DPO, Comitê de Privacidade e Operadores) e compreender como gerir contratos com fornecedores de tecnologia e operadoras de planos de saúde.
- **Responder a incidentes:** Elaborar um esboço de plano de contingência para vazamentos, ataques de ransomware e outros incidentes em ambientes clínicos, incluindo a comunicação à ANPD e aos titulares.
- **Aplicar direitos:** Operacionalizar o atendimento aos direitos dos pacientes — acesso, correção, portabilidade e eliminação — de forma ágil, segura e juridicamente defensável.

Competências Desenvolvidas

Dimensão	Competência-chave
Jurídica	Interpretar a LGPD à luz das especificidades do setor saúde (CFM, Anvisa, ANS)
Técnica	Aplicar controles de acesso (RBAC), anonimização e pseudonimização em bases clínicas
Operacional	Desenhar fluxos assistenciais compatíveis com os princípios da LGPD
Gerencial	Estruturar o Comitê de Privacidade e o papel do DPO em instituições de saúde
Estratégica	Transformar conformidade em diferencial competitivo de confiança

Público-Alvo

O curso foi desenhado para profissionais que atuam na intersecção entre a saúde e a gestão de dados. O perfil multidisciplinar é intencional: a conformidade no setor só se concretiza com diálogo entre clínica, tecnologia, jurídico e gestão.

1. Gestores e Administradores Hospitalares

Diretores de clínicas, hospitais e laboratórios que precisam entender o impacto financeiro, operacional e jurídico da conformidade. São os responsáveis por aprovar investimentos em privacidade, priorizar projetos de governança e responder à alta administração por eventuais sanções.

2. Corpo Técnico de TI e Segurança da Informação

Profissionais responsáveis pela infraestrutura tecnológica e pela proteção de dados médicos. Administradores de sistemas de prontuário eletrônico (como Tasy, MV, Philips), equipes de redes, CISOs e analistas de segurança encontram aqui o vocabulário jurídico necessário para dialogar com a área de compliance.

3. Profissionais de Direito e Compliance

Advogados, consultores e encarregados (DPOs) que buscam especialização no nicho regulatório da saúde. O curso aprofunda a interface da LGPD com a legislação setorial (Código de Ética Médica, Resoluções do CFM sobre prontuário, regulamentos da ANS, Lei do SUS).

4. Gestores de Prontuários e Faturamento

Lideranças administrativas que lidam diretamente com o fluxo de dados sensíveis entre prestadores e operadoras. São frequentemente o ponto de contato do paciente com pedidos de acesso a dados, e precisam dominar os prazos e requisitos legais.

5. Profissionais de RH de Saúde

Responsáveis pela cultura organizacional e pelo treinamento de equipes assistenciais que manuseiam dados de pacientes diariamente. A conscientização do corpo clínico e administrativo é, na prática, o controle mais eficaz — e o RH é o protagonista dessa construção.

Perfil Ideal do Participante

Atua em instituição de saúde (hospital, clínica, laboratório, operadora, healthtech) ou presta serviços a esse setor.

> Possui noções gerais da LGPD, ainda que básicas, e busca aprofundar a aplicação setorial.
> Tem acesso, na sua rotina, a dados de pacientes — ou a decisões que envolvem tais dados.
> Busca ferramentas práticas, templates e metodologias aplicáveis de imediato.

Estrutura Curricular

O curso é organizado em 4 módulos, totalizando 8 horas de conteúdo ao vivo. A arquitetura pedagógica combina exposição dialogada, estudos de caso reais do setor, atividades práticas e um workshop de elaboração de Relatório de Impacto (RIPD).

Módulo	Título	Carga	Foco
1	O Ecossistema de Dados na Saúde	1h30	Base conceitual e legal
2	Governança de Dados e Compliance	2h30	Estrutura organizacional
3	Riscos, Segurança e Incidentes	2h00	Proteção técnica e resposta
4	Prática e Cultura Organizacional	2h00	Aplicação e sustentação
	TOTAL	8h00	

Detalhamento dos Módulos

Módulo 1 — O Ecossistema de Dados na Saúde

Carga horária: 1h30 | **Objetivo:** estabelecer a base conceitual e legal do tratamento de dados em saúde.

Conteúdo Programático

- **Dados pessoais:** conceito, exemplos práticos e fronteiras. Por que tratamos dados pessoais no ambiente de saúde?
- **Dados sensíveis:** o que caracteriza um dado sensível e por que o tratamento recebe regime rigoroso. Exemplos do cotidiano assistencial.
- **Atores do tratamento:** o papel de hospitais, clínicas e médicos (controladores), operadoras de saúde, laboratórios e softwares de gestão (operadores e coadjuvantes).
- **Bases legais específicas:** indo além do consentimento. Tutela da Saúde, Proteção da Vida e Incolumidade Física. Quando cada base se aplica.
- **Interoperabilidade vs. privacidade:** o desafio de compartilhar dados entre redes de cuidado, RNDS, interoperabilidade HL7/FHIR.

Resultados Esperados do Módulo

- Reconhecer fluxos de dados críticos na operação.
- Classificar corretamente cada categoria de dado tratado.
- Fundamentar juridicamente cada tratamento com a base legal adequada.

Módulo 2 — Governança de Dados e Compliance

Carga horária: 2h30 | **Objetivo:** dotar o participante de ferramentas para estruturar a governança institucional.

Conteúdo Programático

- **Framework de Governança:** como estruturar o Comitê de Privacidade em ambientes hospitalares. Composição, periodicidade, decisões típicas e documentação.
- **Privacy by Design em softwares médicos:** como garantir que o prontuário eletrônico seja seguro desde a concepção. Requisitos de segurança em RFP/RFI.
- **Gestão de terceiros:** auditoria em fornecedores de nuvem, prestadores de serviços de manutenção de equipamentos médicos, empresas de outsourcing de TI e laboratórios parceiros.

- **Data Protection Officer (DPO / Encarregado):** o papel técnico-jurídico dentro da instituição. Independência, competências, reporte e responsabilidades.

Atividades Práticas

- Estudo de caso: estruturação do Comitê de Privacidade em um hospital de médio porte.
- Análise de cláusulas LGPD em contratos de software hospitalar.

Módulo 3 — Riscos, Segurança e Incidentes

Carga horária: 2h00 | **Objetivo:** capacitar para a proteção técnica de dados e resposta a incidentes.

Conteúdo Programático

- **Principais ameaças:** ransomware em hospitais brasileiros, sequestro de dados críticos, phishing direcionado a corpo clínico e exfiltração silenciosa.
- **Controle de acesso:** a importância do RBAC (Role-Based Access Control) para médicos, enfermeiros, administrativos, recepção e terceiros. Trilhas de auditoria.
- **Plano de resposta a incidentes:** o que fazer quando há vazamento de exames ou prontuários? Fluxo de comunicação à ANPD, aos titulares e aos órgãos reguladores setoriais.
- **Anonimização e pseudonimização:** técnicas para uso de dados em pesquisas científicas, estudos epidemiológicos e análises estatísticas com observância da LGPD.

Atividades Práticas

- Simulação de incidente: vazamento de base de exames laboratoriais. Tomada de decisão em 72h.
- Matriz RBAC: exercício de definição de perfis de acesso em um hospital-modelo.

Módulo 4 — Prática e Cultura Organizacional

Carga horária: 2h00 | **Objetivo:** traduzir a teoria em rotina e sustentar a conformidade ao longo do tempo.

Conteúdo Programático

- **Treinamento de ponta:** como conscientizar desde a recepção até o corpo clínico, passando por limpeza, manutenção e pesquisa. Linguagem adequada para cada público.

- **Direitos do titular (paciente):** como atender solicitações de acesso, correção, portabilidade e eliminação de dados clínicos dentro dos prazos legais e das exigências éticas.
- **Workshop prático — RIPD:** elaboração guiada de um Relatório de Impacto à Proteção de Dados aplicado a um caso real do setor.
- **Encerramento:** auditoria contínua e KPIs de privacidade na saúde. Como evoluir da conformidade pontual para um sistema de gestão vivo.

Metodologia de Ensino

A metodologia do curso combina exposição dialogada com aplicação imediata. O objetivo é que cada participante saia não apenas com conhecimento, mas com ferramentas prontas para uso em sua instituição.

Pilares Metodológicos

- **Microaprendizagem:** blocos expositivos curtos, seguidos de discussão guiada e aplicação. Nenhum bloco passa de 25 minutos ininterruptos.
- **Casos reais:** o curso trabalha com casos reais anonimizados do setor de saúde brasileiro — incidentes, sanções e boas práticas publicadas pela ANPD.
- **Interação síncrona:** encontros síncronos com câmera aberta, perguntas em tempo real e quadro compartilhado para exercícios colaborativos.
- **Atividades práticas:** cada módulo é encerrado com uma atividade prática que pode ser levada de volta à instituição do participante.

Avaliação e Certificação

Critérios para Certificação

Para obter o certificado de conclusão, o participante deverá cumprir todos os requisitos abaixo:

- Presença mínima de 75% da carga horária total (6 horas de 8).
- Participação na atividade prática de cada módulo.
- Resposta ao formulário de avaliação de reação ao final do curso.

Certificado

O certificado é emitido em até 10 dias úteis após o encerramento do curso, em formato digital PDF, contendo:

- Nome completo do participante.
- Nome e carga horária do curso (8 horas).
- Período de realização.
- Assinatura da coordenação da Universidade da Privacidade.

Corpo Docente

O curso é conduzido por profissionais com atuação prática no setor da saúde e em compliance de dados, selecionados pela coordenação da Universidade da Privacidade a partir de critérios de senioridade técnica, experiência didática e reconhecimento de mercado.

Coordenação Acadêmica

A coordenação acadêmica do curso é realizada pela equipe da Universidade da Privacidade, responsável pelo desenho curricular, pela seleção de instrutores e pela gestão pedagógica de ponta a ponta.

Informações Práticas

Plataforma e Acesso

O curso é realizado em plataforma de videoconferência profissional, com capacidade para interação em tempo real. O link individual de acesso é enviado ao e-mail cadastrado na inscrição.

Requisitos Técnicos

- Computador com câmera e microfone funcionais.
- Conexão de internet estável (mínimo 10 Mbps recomendado).
- Navegador atualizado (Chrome, Edge ou Firefox nas versões mais recentes).
- Ambiente silencioso e propício à concentração.

Política de Presença

A presença é apurada pelo registro de entrada e saída na plataforma. O participante com menos de 75% da carga horária não é elegível à certificação, mas pode participar de uma próxima edição com desconto progressivo, mediante análise da coordenação.

Política de Cancelamento e Remarcação

- Cancelamento com mais de 15 dias de antecedência: reembolso integral.
- Cancelamento entre 7 e 15 dias de antecedência: reembolso de 50% ou crédito integral para próxima turma.
- Cancelamento com menos de 7 dias: crédito integral para próxima turma, sem reembolso financeiro.
- Transferência de titularidade é permitida até 48h antes do início.

Perguntas Frequentes

1. Preciso ter formação jurídica para acompanhar o curso?

Não. Embora a LGPD seja uma lei, o curso é multidisciplinar e a linguagem foi desenhada para gestores, profissionais de TI, compliance e saúde. Conceitos jurídicos são explicados em linguagem acessível e sempre aplicados a casos do cotidiano.

2. O curso é indicado para quem não tem nenhum contato prévio com LGPD?

O curso pressupõe noções gerais da LGPD. Para quem nunca teve contato com a lei, recomendamos complementar com a leitura prévia do material introdutório enviado 7 dias antes do início. Alternativamente, a UP oferece cursos introdutórios que podem ser cursados antes.

3. O certificado é válido para compor horas de atualização profissional em conselhos?

O certificado comprova 8 horas de carga horária e é amplamente aceito em processos internos de comprovação de capacitação.

4. Como funciona o acesso ao material após o curso?

Todo o material é disponibilizado em área exclusiva do aluno por 3 meses após o término do curso. Os templates podem ser baixados e utilizados institucionalmente pelo participante.

5. É possível participar por celular ou tablet?

É possível, porém não recomendado.

6. Posso inscrever minha equipe inteira?

Sim. Oferecemos condições comerciais especiais para inscrições em grupo (a partir de 5 participantes da mesma instituição), incluindo possibilidade de turma fechada in-company. Contate a equipe comercial para condições.

7. Haverá gravação disponível após o curso?

Sim. A gravação de cada encontro é disponibilizada em até 72h úteis na área do aluno, acessível por 3 meses.

8. Posso tirar dúvidas específicas sobre a minha instituição em aula?

Sim, e é encorajado. Uma das riquezas do formato ao vivo é justamente a discussão de casos reais trazidos pelos participantes. Pedimos apenas que as dúvidas envolvendo dados reais sejam formuladas de forma anonimizada.

09. O curso cobre aspectos internacionais, como o HIPAA ou o GDPR?

O foco primário é a LGPD aplicada ao contexto brasileiro. Paralelos com GDPR são traçados pontualmente onde relevantes. Abordagens aprofundadas sobre HIPAA ou GDPR são objeto de cursos específicos do portfólio da UP.

Sobre a Universidade da Privacidade

A Universidade da Privacidade (UP) é a unidade educacional da DPOnet, referência nacional em gestão de privacidade e proteção de dados. A UP tem como missão democratizar o conhecimento aplicado sobre LGPD, governança de dados e IA responsável, capacitando profissionais e instituições a transformarem conformidade em vantagem estratégica.

Acreditamos que privacidade é uma jornada — não um evento. E que cada instituição capacitada é uma peça no ecossistema de confiança digital que o Brasil precisa construir.

Universidade da Privacidade | DPOnet

Educação que transforma compliance em vantagem competitiva.