

Segurança e Privacidade na Concepção de Projetos



Anderson Oliveira da Silva

Ph. D. Ciências em Informática

Engenheiro de Computação

Gestor de Segurança da Informação

anderson@inf.puc-rio.br



[linkedin.com/in/anderson-oliveira-da-silva-58221680](https://www.linkedin.com/in/anderson-oliveira-da-silva-58221680)

Departamento de Informática
PUC-Rio



Informática

Prof. Anderson Oliveira da Silva - anderson@inf.puc-rio.br



LGPD – Motivação

Uso indiscriminado de dados pessoais sem o devido consentimento do titular dos dados.

- Tratamento dos dados pessoais **sem anuência ou conhecimento** do indivíduo titular dos dados visando determinar...
 - preferências de um indivíduo;
 - estado físico (saúde) de um indivíduo;
 - rede de relacionamento de um indivíduo.
- Comercialização dos dados pessoais **sem anuência ou conhecimento** do indivíduo titular dos dados para...
 - pesquisas de mercado;
 - marketing de produtos;
 - marketing eleitoral;
 - influenciadores.

LGPD – Motivação

Uso indiscriminado de dados pessoais sem o devido consentimento do titular dos dados.

Ano	Empresa	Venda de dados	Situação
2020	BaseUp	informações pessoais de milhares de brasileiros	MPDFT abriu investigação para apurar venda de bases de dados pessoais sem consentimento

Ano	Empresa	Compartilhamento de dados	Situação
2020	Cyrela	Dados pessoais de cliente compartilhados com vários parceiros comerciais sem consentimento	Condenada pelo TJ-SP, com base na LGPD, a pagar R\$ 10.000,00 de indenização de dano moral para o cliente

LGPD – Motivação

Vazamento de dados pessoais por falta de proteção adequada.

- Vazamento de dados pessoais de indivíduos que estão **sob custódia de agentes** que assumem a responsabilidade do armazenamento e controle de acesso aos dados.
 - Proteção **inadequada do armazenamento** dos dados de um indivíduo.
 - Ausência de controles de integridade, autenticidade, confidencialidade (sigilo) e disponibilidade;
 - Proteção **inadequada do controle de acesso** aos dados de um indivíduo.
 - Ausência de controle de autenticação apropriado;
 - Ausência de controle de delegação apropriado;
 - Ausência de controle de acesso privilegiado apropriado.

LGPD – Motivação

Vazamento de dados pessoais por falta de proteção adequada.

Ano	Empresa	Dados vazados	Situação
2017	Uber	nome, endereço de e-mail e telefone celular associada à conta do usuário	notificação por e-mail de mais de 196 mil usuários brasileiros
2018	Banco Inter	comprometimento dos dados cadastrais de correntistas (dados bancários, como número da conta, senha, endereço, CPF e telefone), dados de clientes de outros bancos que fizeram transações com usuários do Inter, exposição dos certificados digitais, já revogados, e da chave privada do banco	MPDFT pede a condenação do banco ao pagamento de R\$ 10 milhões acordo destinará R\$ 1,5 milhão para caridade e combate a crimes cibernéticos.

LGPD – Motivação

Vazamento de dados pessoais por falta de proteção adequada.

Ano	Empresa	Dados vazados	Situação
2018	Sky Brasil	nome completo, data de nascimento, e-mail, senha de login do serviço, endereço IP, métodos de pagamento, número de telefone e endereço residencial	inquérito civil público para investigar suposto incidente de segurança
2019	Netshoes	nome, CPF, e-mail, data de nascimento e histórico de compras	acordo para pagar indenização de R\$ 500 mil, que serão recolhidos mediante depósitos no Fundo de Defesa de Direitos Difusos (FDD)

LGPD – Motivação

Vazamento de dados pessoais por falta de proteção adequada.

Ano	Empresa	Dados vazados	Situação
2019	Atlas Quantum	nome, e-mail, telefone e saldo em bitcoins	MPDFT pede a condenação das empresas do grupo econômico ao pagamento de R\$ 10 milhões
2019	Banco Pan	carteiras de identidade, carteiras de habilitação, comprovantes de residência, CPFs, cartões de crédito, contratos de financiamento, solicitações de saque e extratos bancários, dentre outros	MPDFT instaurou Inquérito Civil Público (ICP) para apurar responsabilidades Banco informa que os dados foram vazados de um parceiro comercial

LGPD – Objetivo

Combater o uso indiscriminado de dados pessoais sem o devido consentimento.

- A Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
- Determina **sanções** para os agentes responsáveis pelo armazenamento e controle de acesso aos dados pessoais em caso de vazamento ou prejuízo resultante de falha na proteção dos dados.
- Determina **sanções** para o tratamento dos dados pessoais sem a devida autorização de uso com finalidade específica dos titulares a quem se referem os dados pessoais que são objeto de tratamento.

LGPD – Requisitos básicos para proteção de dados

Os cinco pilares da proteção de dados são a base da segurança.

- **Controle de Integridade**
 - Garantir que um dado está íntegro (não está adulterado).
- **Controle de Autenticidade**
 - Garantir que o titular do dado é legítimo (não é falsificado).
- **Controle Confidencialidade**
 - Garantir o sigilo dos dados para o titular dos dados e demais autorizados.
- **Controle de Acesso**
 - Garantir acesso apenas ao titular dos dados e demais autorizados.
- **Controle de Disponibilidade**
 - Garantir que o dado sempre está disponível para uso pelo titular dos dados e demais autorizados.

Informática

LGPD – Segurança da Informação

Conformidade com as normas de segurança da informação para proteção de dados.

- **ABNT NBR ISO/IEC 27001:2022**
Segurança da informação, segurança cibernética e proteção à privacidade – Sistema de Gestão da Segurança da Informação (SGSI) – Requisitos
- **ABNT NBR ISO/IEC 27002:2024**
Segurança da informação, segurança cibernética e proteção à privacidade – Controles de Segurança da Informação.
- **ABNT NBR ISO/IEC 27005:2023**
Segurança da informação, segurança cibernética e proteção à privacidade – Orientações para a gestão de riscos de segurança da informação.
- **ABNT NBR ISO 27701:2019**
Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para a gestão da privacidade da informação – Requisitos

 **diretrizes.**
Informática

LGPD – Compartilhamento de Dados

A lei considera as seguintes definições de termos:

- **titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- **controlador:** **pessoa natural ou jurídica**, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- **operador:** **pessoa natural ou jurídica**, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- **agentes de tratamento:** o controlador e o operador;

LGPD – Compartilhamento de Dados

A lei considera as seguintes definições de termos:

- **tratamento:** toda operação realizada com dados pessoais, como as que se referem a **coleta**, produção, **recepção**, classificação, **utilização**, acesso, **reprodução**, transmissão, **distribuição**, **processamento**, **arquivamento**, **armazenamento**, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
- **consentimento:** manifestação **livre**, **informada** e **inequívoca** pela qual o **titular concorda** com o tratamento de seus dados pessoais para uma **finalidade determinada**;

LGPD – Compartilhamento de Dados

A lei considera as seguintes definições de termos:

- ***uso compartilhado de dados:*** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, **com autorização específica**, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
- ***anonimização:*** utilização de **meios técnicos** razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, **direta** ou **indireta**, a um indivíduo;

LGPD – Compartilhamento de Dados

A lei determina a viabilidade de compartilhamento de dados:

- **Art. 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.
- **Art. 13.** Na 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 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.

LGPD – Técnicas de Básicas de Anonimização

A aplicação das técnicas de anonimização de dados deve ser analisada caso a caso:

- Supressão de atributos
- Supressão do registro
- Encobrimento de caracteres
- Pseudoanonimização
- Generalização
- Perturbação de dados
- Dados sintéticos
- Agregação de dados

LGPD – Técnicas de Básicas de Anonimização

A aplicação das técnicas de anonimização de dados deve ser analisada caso a caso:

• Anonimização (Exemplos)

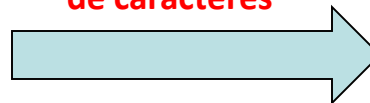
Paciente	CEP	Idade	Médico	Medicamento
Paulo	22775	66	Pedro	Tramol
Sônia	22775	24	Sara	Novalgina
Ana Lucia	22451	43	Robson	Novalgina
Simone	22451	32	Pedro	Flanax
Silvio	22654	26	Gustavo	Tramol
Luiz	22775	38	Sara	Flanax
José	22451	41	Sayão	Novalgina

supressão
de atributos



CEP	Idade	Médico	Medicamento
22775	66	Pedro	Tramol
22775	24	Sara	Novalgina
23451	43	Robson	Novalgina
23451	32	Pedro	Flanax
22654	26	Gustavo	Tramol
22775	38	Sara	Flanax
23451	41	Sayão	Novalgina

encobrimento
de caracteres



CEP	Idade	Médico	Medicamento
22775	66	Pedro	Tramol
22775	24	Sara	Novalgina
23451	43	Robson	Novalgina
23451	32	Pedro	Flanax
22654	26	Gustavo	Tramol
22775	38	Sara	Flanax
23451	41	Sayão	Novalgina

CEP	Idade	Médico	Medicamento
22XXX	66	Pedro	Tramol
22XXX	24	Sara	Novalgina
23XXX	43	Robson	Novalgina
23XXX	32	Pedro	Flanax
22XXX	26	Gustavo	Tramol
22XXX	38	Sara	Flanax
23XXX	41	Sayão	Novalgina

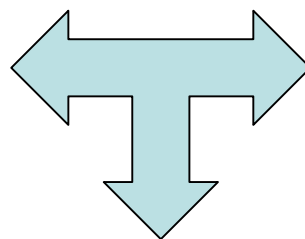
LGPD – Técnicas de Básicas de Anonimização

A aplicação das técnicas de anonimização de dados deve ser analisada caso a caso:

• Pseudonimização (Exemplo)

Paciente	CEP	Idade	Médico	Medicamento
Paulo	22775	66	Pedro	Tramol
Sônia	22775	24	Sara	Novalgina
Ana Lucia	22451	43	Robson	Novalgina
Simone	22451	32	Pedro	Flanax
Silvio	22654	26	Gustavo	Tramol
Luiz	22775	38	Sara	Flanax
José	22451	41	Sayão	Novalgina

substituição por
pseudônimos



Paciente	CEP	Idade	Médico	Medicamento
A0X1Z3D4	22775	66	Pedro	Tramol
A1P0Q0D1	22775	24	Sara	Novalgina
Y0B4C8T0	22451	43	Robson	Novalgina
U0B1G0D2	22451	32	Pedro	Flanax
P3Q0R1S5	22654	26	Gustavo	Tramol
H2K5E3F8	22775	38	Sara	Flanax
L0G3Q1M4	22451	41	Sayão	Novalgina

Pseudônimo	Paciente
A0X1Z3D4	Paulo
A1P0Q0D1	Sônia
Y0B4C8T0	Ana Lucia
U0B1G0D2	Simone
P3Q0R1S5	Silvio
H2K5E3F8	Luiz
L0G3Q1M4	José

A tabela de associação entre os pseudônimos irreversíveis e os dados originais é **mantida de forma segura no controlador e não é compartilhada.**

Segurança e Privacidade – Concepção de Projetos

Quando pensamos em projetos seguros, a pergunta deixa de ser...

Como proteger os dados depois que o projeto estiver pronto?

E passa a ser...

- **Como conceber o projeto** para que ele já nasça respeitando a privacidade, protegendo as pessoas e reduzindo riscos?

Segurança e Privacidade – Concepção de Projetos

Projetos seguros devem ser projetados com base em dois conceitos fundamentais:

- **Security by Design:**
 - Protege principalmente contra ameaças: acesso indevido, vazamento, alteração, perda, destruição, fraude, abuso etc.

Como evitar que algo ruim aconteça com os dados?

- **Privacy by Design:**
 - Questiona finalidade, necessidade, proporcionalidade, exposição, transparência, autonomia do titular e consequências do tratamento.

Devemos tratar esse dado dessa maneira?

Segurança e Privacidade – Concepção de Projetos

Importante: esses conceitos isoladamente não resolvem o problema!

ATENÇÃO!!!

Um projeto pode ser **seguro** e ainda assim invasivo à **privacidade**!

- Exemplo:
 - Uma instalação artística **pode** armazenar imagens **dos visitantes em um** servidor perfeitamente protegido, **mas coletar imagens identificáveis sem que de fato isso seja necessário para a** experiência artística **ou consentido pelos titulares.**

Security by Design aplicado a Artes e Design

Security by Design em 6 princípios de projeto:

1. Segurança desde a concepção:

- Segurança é requisito do projeto, não correção posterior.
- Exemplo:
 - Uma instalação interativa que **captura imagens** já deve ser **concebida** definindo **onde ocorrerá** o processamento e o armazenamento.

Security by Design aplicado a Artes e Design

Security by Design em 6 princípios de projeto:

2. Minimização da superfície de ataque:

- Quanto menos componentes, dados e interfaces expostos, menor o risco.
- Exemplo:
 - Se uma obra precisa apenas **detectar presença**, utilizar **sensor de presença** em vez de **câmera**.

Security by Design aplicado a Artes e Design

Security by Design em 6 princípios de projeto:

3. Menor privilégio:

- Cada pessoa ou componente acessa somente o necessário.
- Exemplo:
 - Monitores da exposição podem operar a instalação **sem acessar o banco de imagens.**

Security by Design aplicado a Artes e Design

Security by Design em 6 princípios de projeto:

4. Defesa em profundidade:

- Não depender de uma única proteção.
- Exemplo:
 - Adotar **camadas de segurança independentes**: controle de acesso + autenticação + criptografia + logs + backup.

Security by Design aplicado a Artes e Design

Security by Design em 6 princípios de projeto:

5. Secure Defaults:

- A configuração inicial (padrão) deve ser a mais segura.
- Exemplo:
 - Galeria virtual nasce com **perfis privados**; compartilhamento público **exige ação explícita**.

Security by Design aplicado a Artes e Design

Security by Design em 6 princípios de projeto:

6. Segurança em todo o ciclo de vida:

- Pensar em criação, operação, manutenção e encerramento.
- Exemplo:
 - Ao terminar uma exposição, **eliminar dados coletados que não precisam mais ser mantidos.**

Privacy by Design aplicado a Artes e Design

Privacy by Design em 7 princípios de projeto:

1. Proativo, não reativo — preventivo, não corretivo:

- Não esperar acontecer uma violação de privacidade.
- Exemplo:
 - Um aluno projeta uma instalação que **fotografa visitantes e transforma seus rostos** artisticamente com IA.
- Questões:
 - Tenho o consentimento do titular? Onde ficará a imagem? Será enviada para terceiros? O modelo de IA armazenará a fotografia? Precisamos realmente guardar a imagem?

Privacy by Design aplicado a Artes e Design

Privacy by Design em 7 princípios de projeto:

2. Privacidade como Padrão:

- Se o titular não fizer nada, deve prevalecer a alternativa que melhor protege sua privacidade.
- Exemplo:
 - Imagine um **aplicativo criado** por alunos para **divulgar portfólios**.
- Questões:
 - nome artístico + portfólio ficam públicos.
 - e-mail, telefone e localização permanecem privados.
 - Titular decide posteriormente o que tornar público.

Privacy by Design aplicado a Artes e Design

Privacy by Design em 7 princípios de projeto:

3. Privacidade incorporada ao projeto:

- Privacidade deve influenciar a arquitetura do projeto.
- Exemplo:
 - Se os **visitantes enviam fotos** para compor um grande mosaico na parede em tempo real, a instalação deve ser **projetada para ter privacidade**.
- Questões:
 - O projeto **deve prever** recepção da foto → remoção de metadados → atribuição de identificador aleatório → publicação no mosaico → eliminação da foto ao final da exposição.

Privacy by Design aplicado a Artes e Design

Privacy by Design em 7 princípios de projeto:

4. Funcionalidade Completa – Soma Positiva:

- Privacidade OU Funcionalidade? Procure sempre ter ambos!
- Exemplo:
 - Se for necessário contabilizar quantas pessoas circulam no espaço, não identifique as pessoas que circularam, apenas contabilize o número de pessoas.
- Questões:
 - A experiência artística permanece e o risco à privacidade diminui drasticamente.

Privacy by Design aplicado a Artes e Design

Privacy by Design em 7 princípios de projeto:

5. Proteção durante todo ciclo de vida:

- O designer deve pensar no dado desde a coleta até sua eliminação.
- Exemplo:
 - Coleta → Uso → Armazenamento → Compartilhamento → Arquivamento → Eliminação
- Questões:
 - O que acontece com os dados depois que a exposição termina?

Privacy by Design aplicado a Artes e Design

Privacy by Design em 7 princípios de projeto:

6. Visibilidade e transparência:

- As pessoas devem compreender o que está acontecendo.

- Exemplo:

-  Esta instalação utiliza uma câmera
-  Sua imagem será processada
-  A imagem não será armazenada
-  O processamento ocorre em tempo real
-  Saiba mais

- Questões:

- O próprio design pode ser um mecanismo de transparência da LGPD.

Privacy by Design aplicado a Artes e Design

Privacy by Design em 7 princípios de projeto:

7. Proteção durante todo ciclo de vida:

- O titular deve permanecer no centro do projeto.
- Exemplo:
 - Evitar manipulação, coleta desnecessária e decisões de interface que induzam o titular a abrir mão da privacidade.
- Questões:
 - Evitar a opção única [ACEITAR TUDO]
 - Usar as opções [ACEITAR] [RECUSAR] [CONFIGURAR]

Segurança e Privacidade na Concepção de Projetos

Security by Design

Como evitar que algo ruim aconteça com os dados desde a concepção do projeto?

- 1 Segurança desde a concepção**
Definir a segurança como requisito do projeto.
- 2 Minimização da superfície de ataque**
Reduzir componentes, dados e interfaces expostos.
- 3 Menor privilégio**
Cada pessoa ou componente acessa apenas o necessário.
- 4 Defesa em profundidade**
Combinar diferentes camadas de proteção.
- 5 Secure Defaults**
Configurações mais seguras como padrão.
- 6 Segurança durante todo o ciclo de vida**
Considerar criação, operação, manutenção e encerramento do projeto.

Privacy by Design

Devemos tratar esse dado dessa maneira? Como projetar para proteger a privacidade desde o início?

- 1 Proativo, não reativo**
Prevenir riscos à privacidade desde a concepção, e não apenas corrigi-los depois.
- 2 Privacidade como padrão**
A alternativa que melhor protege a privacidade deve ser a configuração inicial.
- 3 Privacidade incorporada ao projeto**
Integrar a privacidade na arquitetura e nas decisões de design, e não apenas como um complemento.
- 4 Funcionalidade completa (Positive-Sum)**
Buscar soluções que ofereçam privacidade e boa experiência, sem sacrificar uma pela outra.
- 5 Proteção durante todo o ciclo de vida**
Considerar a privacidade da coleta à eliminação dos dados.
- 6 Visibilidade e transparência**
As pessoas devem entender de forma clara o que está acontecendo com seus dados.
- 7 Respeito à privacidade do usuário**
Colocar as pessoas no centro do projeto e evitar coletas desnecessárias, manipulação e usos injustos.

Perguntas?



Anderson Oliveira da Silva

Ph. D. Ciências em Informática

Engenheiro de Computação

Gestor de Segurança da Informação

anderson@inf.puc-rio.br



[linkedin.com/in/anderson-oliveira-da-silva-58221680](https://www.linkedin.com/in/anderson-oliveira-da-silva-58221680)

Departamento de Informática
PUC-Rio



Informática

Prof. Anderson Oliveira da Silva - anderson@inf.puc-rio.br



Obrigado!



Anderson Oliveira da Silva

Ph. D. Ciências em Informática

Engenheiro de Computação

Gestor de Segurança da Informação

anderson@inf.puc-rio.br



[linkedin.com/in/anderson-oliveira-da-silva-58221680](https://www.linkedin.com/in/anderson-oliveira-da-silva-58221680)

Departamento de Informática
PUC-Rio



Informática



Prof. Anderson Oliveira da Silva - anderson@inf.puc-rio.br