data® expert.

Data Science & Machine Learning

1 - Segurança e LGPD

Consultor: Jonas Galindo

Jonas Galindo

Cyber Security Consultant @Capgemini

Experiência consultiva em projetos de Privacidade e Segurança da Informação

MBA em Gestão e Tecnologia em segurança da informação (Daryus)

Information Security Foundation based on ISO/IEC 27001

Data Protection Officer (DPO)

OneTrust Privacy Professional

O que veremos neste módulo:

01

Introdução a Segurança da Informação

02

LGPD (Lei Geral de Proteção de Dados)

03

Dados pessoais e Anonimização

04

Criptografia

data expert.®

Data Science & Machine Learning

2 - Introdução a Segurança da informação

Consultor: Jonas Galindo

Segurança da Informação

1 **Introdução**
Você deve entender o contexto de informação.

2 **Conceito**
Diferença entre dados e informações
Entender os conceitos do CID (Confidencialidade, Integridade e Disponibilidade);

Conceitos de Informação

Informação é a compreensão dos relacionamentos entre os dados

Informação

É o resultado de aplicar contexto aos dados

Dados

São uma série de fatos discretos

Conceitos de Informação

Dados

ID CLIENTE
714644844869
000566658506
211220021225
309583942623
978545004651
212155500054
026516569520
655454500156
546450015498
069898582001
326510001654

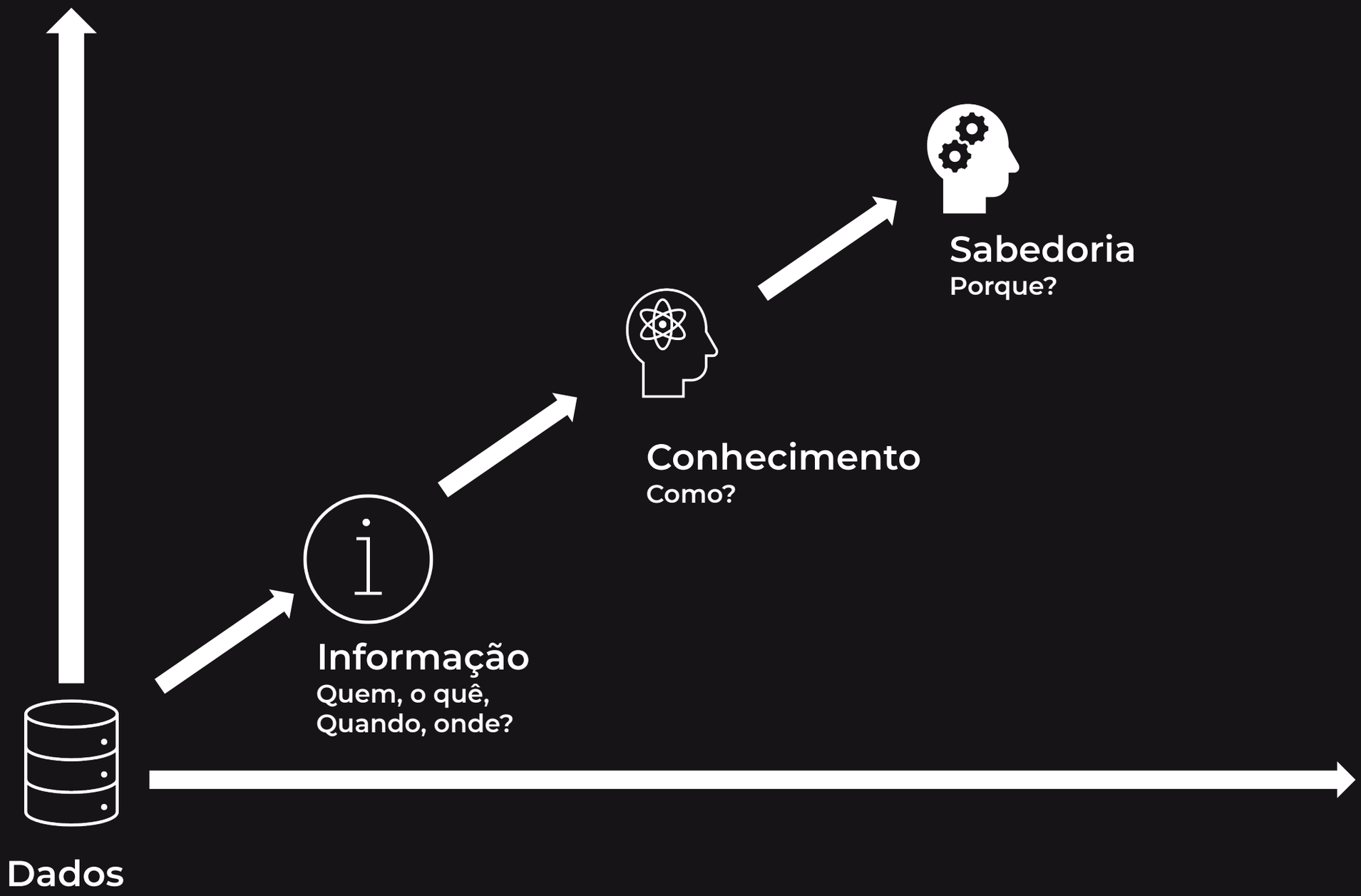
Informação

CPF	RG	E-MAIL
052.295.221-22	0554520002	adaltocristinao@o
052.295.221-22	0554520002	adaltocristinao@o
158.552.212-54	6600032248888	emanu2019@gma
258.985.554-55	3200222545	benetito.m.c@gm
158.552.212-54	6600032248888	emanu2019@gma
259.566.335-56	555552500455	viniciosferrari@gr
158.552.212-54	6600032248888	emanu2019@gma
226.545.545-22	65554550525	mariaparecida22
052.295.221-22	0554520002	adaltocristinao@o
226.545.545-22	65554550525	mariaparecida22
258.985.554-55	3200222545	benetito.m.c@gm
259.566.335-56	555552500455	viniciosferrari@gr
158.552.212-54	6600032248888	emanu2019@gma
259.566.335-56	555552500455	viniciosferrari@gr
259.566.335-56	555552500455	viniciosferrari@gr
958.785.542-25	603078501	josedasilvaberna

Dados se tornam informação quando adquirem significado.

Modelo DICS

Dados, Informação, Conhecimento e Sabedoria



Modelo DICS

Dados, Informação, Conhecimento e Sabedoria

Dados	Informação	Conhecimento	Sabedoria
Peso e Altura de um paciente	A partir dos dados anteriores é possível determinar o IMC do paciente	Consultando outras bases é possível saber se o paciente está acima ou abaixo do peso	Considerando o IMC e outras informações do paciente o médico pode prescrever uma dieta ou algum outro tratamento

Valor da informação

Agora que já sabemos o que é informação, qual é o valor de dados e informações para as organizações?

UBER

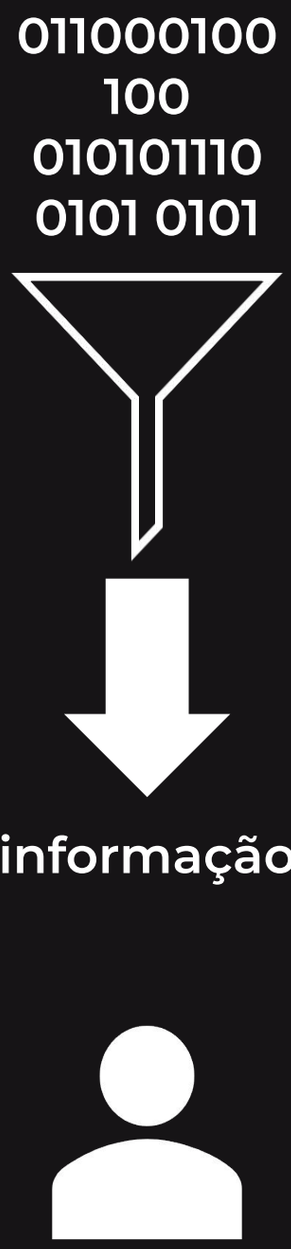
A maior empresa de táxi do mundo não tem carros.
Sabe onde está os passageiros e sabe conectar aos motoristas.

A rede social mais popular do mundo, não cria conteúdo.
Mas conhece as pessoas para criar e distribuir os conteúdos.

airbnb

A maior provedora de hospedagem do mundo não possui imóvel.
Mas sabe quem possui imóveis disponíveis e quem deseja se hospedar.

Valor dos Dados



O DADO inicialmente não possui contexto

Mas quando passa pelo PROCESSAMENTO
é transformado em informação

O VALOR desta informação é atribuído por seu usuário

Informação
É um Produto

Organizações não existiriam sem informação

Algumas organizações têm a informação como seu produto final

Na atualidade, os maiores produtores de riqueza são a informação e o conhecimento

Como Proteger Dados e informações

Garantindo que a informação é acessada somente por pessoas ou entidades autorizadas

Garantindo que a informação permanece íntegra, completa e verdadeira

Garantindo que a informação está sempre disponível quando necessário

Quiz

Qual a diferença entre dados e informação?

- [ ] Os dados são elementos que a princípio não fazem sentido algum ou conclusões, já a informação é o processamento de tais dados que fornecem ao usuário “a lógica”.
- [ ] Os dados são elementos que fazem sentido nas conclusões, já a informação é o processamento de tais dados que fornecem ao usuário “a informação”.
- [x] Os dados são elementos que a principio não fazem sentido algum ou conclusões, já a informação é o processamento de tais dados que fornecem ao usuário “a informação”

data expert.®

Data Science & Machine Learning

3 - Segurança da informação

Consultor: Jonas Galindo

Segurança da Informação

1. **Introdução**
   O que é Segurança da Informação?

2. Quais são os pilares da segurança da informação?
   - Confidencialidade
   - Integridade
   - Disponibilidade

O que é?

1. É a proteção de informações contra ameaças, para garantir a continuidade do negócio, minimizar o risco do negócio e maximizar o retorno sobre os investimentos e oportunidade de negócio.

2. É a preservação de confidencialidade, integridade e disponibilidade da informação.
Fonte: ISO/IEC 27000:2014.

Segurança da Informação

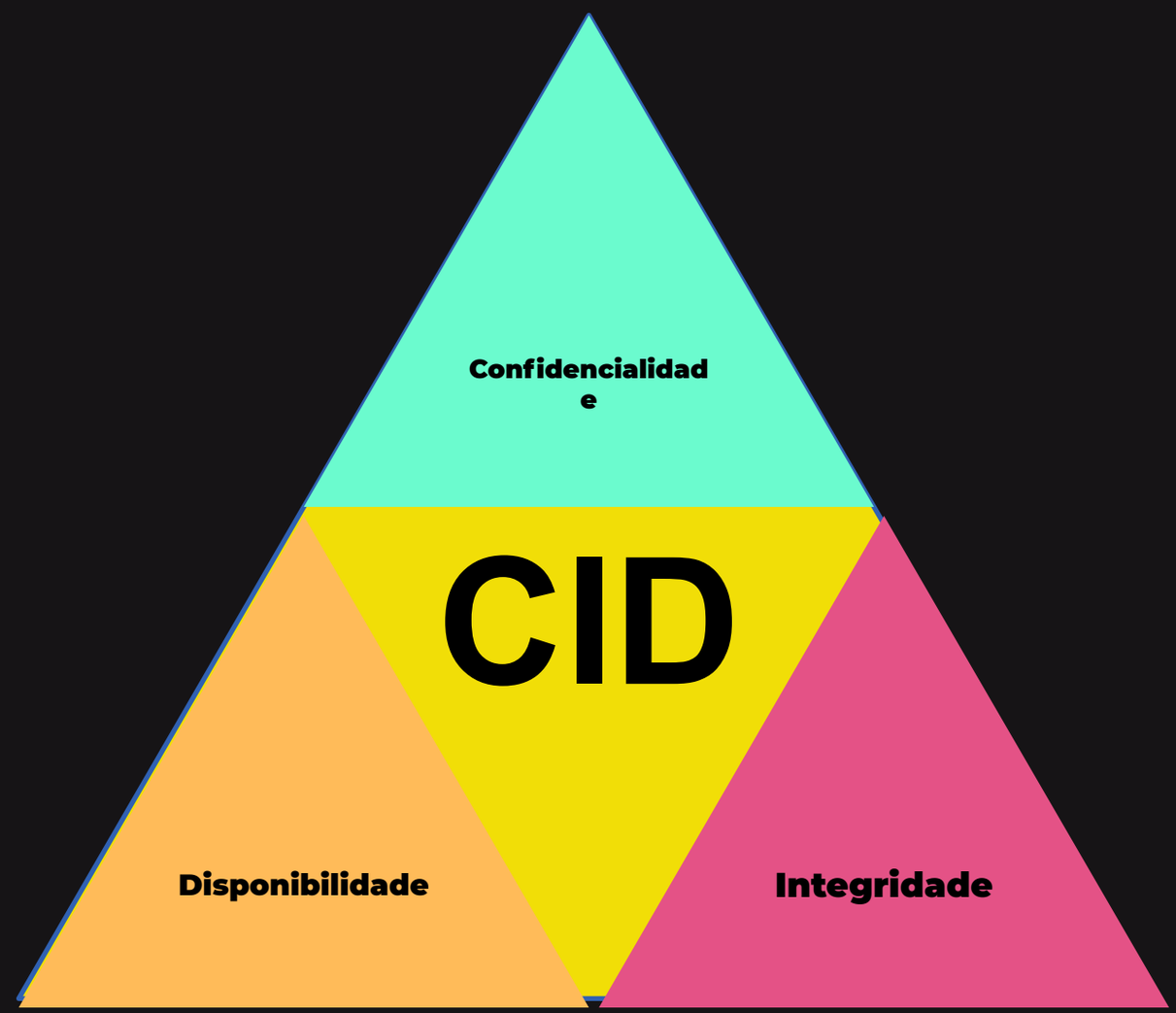
Razões para se investir

- Previne a perda/roubo de dados
- Assegura a privacidade
- Protege a propriedade intelectual da organização
- Minimiza perdas financeiras a partir de incidentes de segurança
- Garante a continuidade do negócio durante um desastre
- Maximiza o retorno de investimentos em novos projetos e oportunidades de negócios

Aspectos da Confiabilidade

A confiabilidade da informação é determinado por 3 aspectos

C - Confidencialidade
I - Integridade
D - Disponibilidade



Confidencialidade

Propriedade que a informação não é disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados.

Fonte: ISO/IEC 27000:2014

São características de confidencialidade:

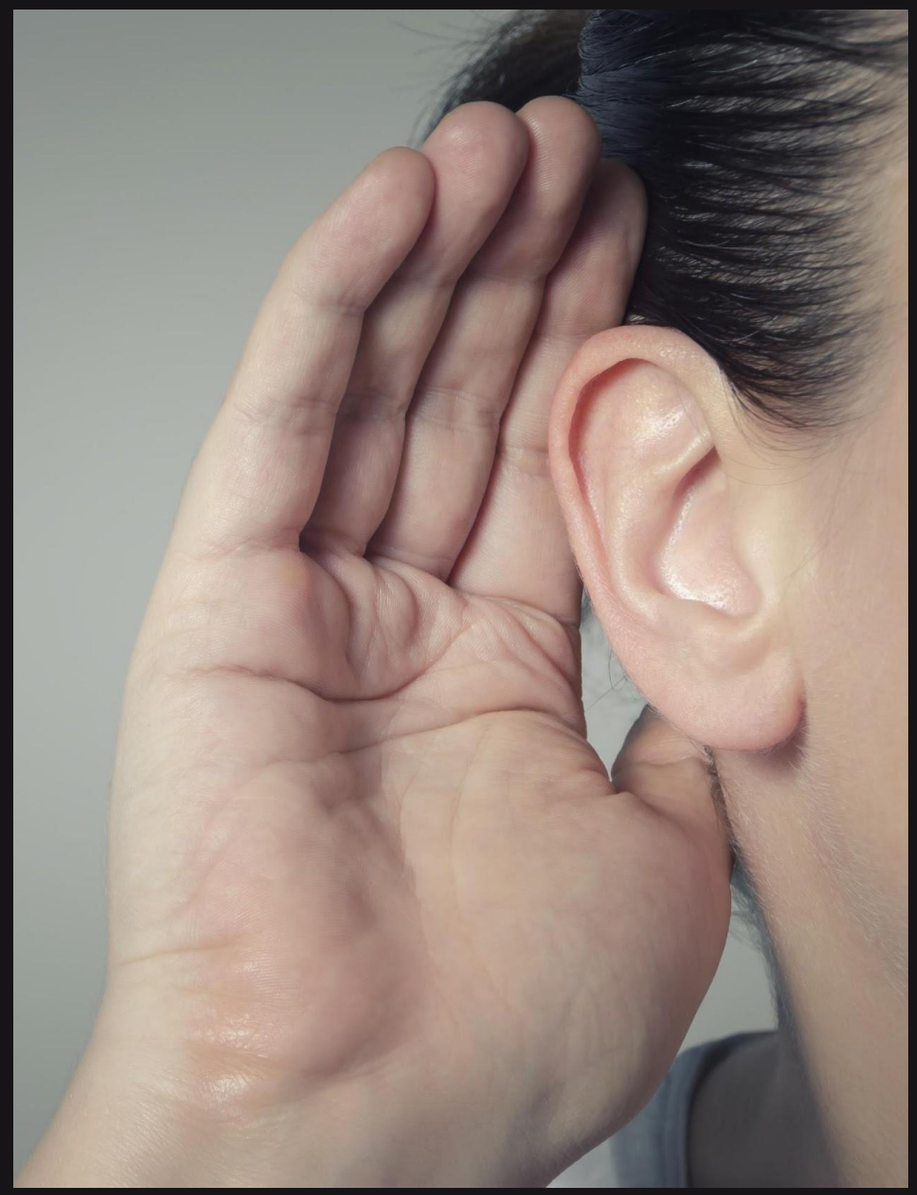
- **PRIVACIDADE:** Consiste em limitar o acesso a informações pessoais.

- **EXCLUSIVIDADE:** Dados disponíveis somente para pessoas autorizadas.

Perda de Confidencialidade

Pode ser quebrado de diversas formas:

1. Alguém pode ter acesso a um documento confidencial em cima da mesa;
2. Alguém pode conseguir uma senha ou invadir um sistema e ler informações que não poderia ter acesso;
3. Alguém com acesso autorizado pode transferir o acesso para alguém não autorizado;



Confidencialidade

Na mídia

Invasores sequestram documentos de celebridades

Da Redação
10/05/2020

O escritório é o Grubman Shire Meiselas & Sacks (GSMLaw), de Nova York, que atende artistas como Madonna, Lady Gaga, Elton John, Robert de Niro e as bandas Usher e U2

O grupo de ransomware Sodinokibi, o mesmo suspeito de receber US$ 2,3 milhões de resgate da corretora de câmbio Travelex, afirma ter roubado documentos do escritório de advocacia Grubman Shire Meiselas & Sacks (GSMLaw), de Nova York. O escritório atende dezenas de estrelas e celebridades internacionais, de uma lista que inclui artistas famosos como Chris Brown, Madonna, Lady Gaga, Nicki Minaj, Elton John, Timbaland, Robert de Niro, Usher, U2 e Timbaland.

Se o escritório de advocacia não pagar o resgate, o grupo ameaça publicar os documentos roubados na internet. Para comprovar o que diz, o grupo publicou a imagem de um diretório do Windows numa captura de tela. Vários nomes de pastas são os de artistas e celebridades.

Anonymous vaza dados de cartões de 'corruptos' e seguidores vão às compras

Grupo de hackers vazou os dados de pessoas que, segundo eles, são 'governantes corruptos'

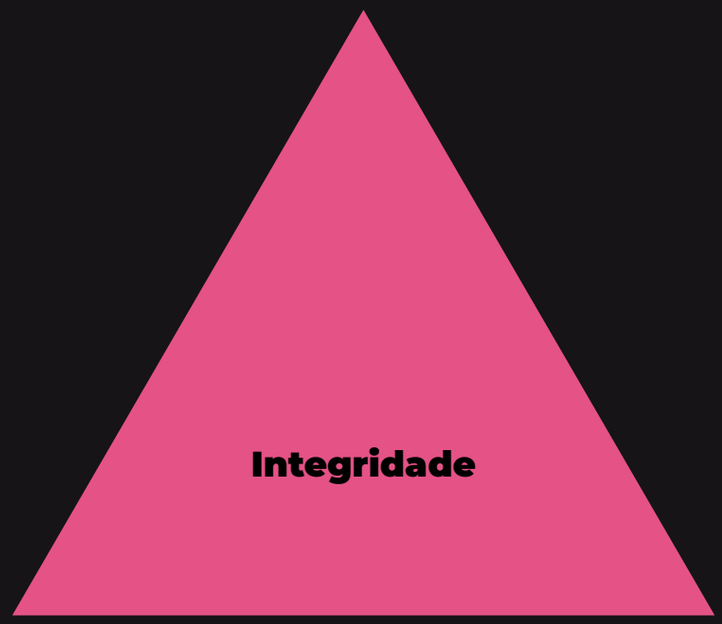
Integridade

o princípio de integridade garante que todas as informações estejam em seu formato original e verdadeiro, a fim de servir para os propósitos para o qual foram designadas. Ou seja, elas devem permanecer íntegras.

Fonte: ISO/IEC 27000:2014

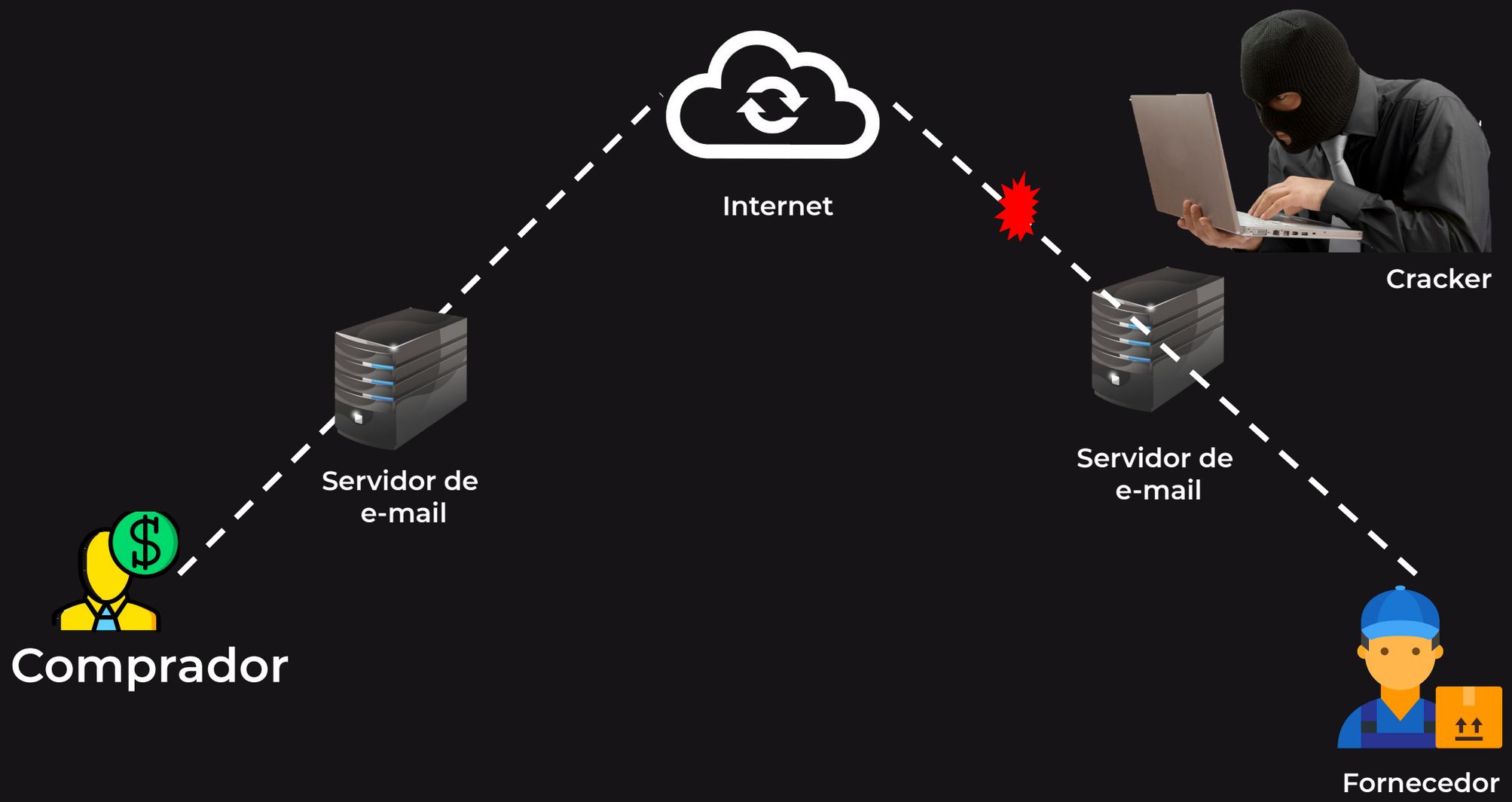
São características de integridade:

- **COMPLETEZA:** Os dados estão completos, inteiros.
- **CORREÇÃO:** Garante que os dados são verdadeiros e exatos.



Integridade - Exemplo

O requisito de segurança de integridade está associado à confiança e consistência dos dados.



Integridade – Na Mídia

Mãe hackeia site de escola para mudar notas de seus filhos

O que mães não fazem por seus filhos, certo? Algumas são capazes de até mesmo invadirem o sistema online da escola de seus filhos para alterarem suas notas. Foi isso o que fez uma senhora mãe de dois alunos da escola Northwestern Lehigh School. A americana e mãe Catherine Venusto conseguiu acesso à página por possuir a senha da diretora do colégio, já que também trabalhou no local por alguns anos.

Por Thiago Barros; Para O TechTudo

23/07/2012 08h15 · Atualizado há 9 anos

Disponibilidade

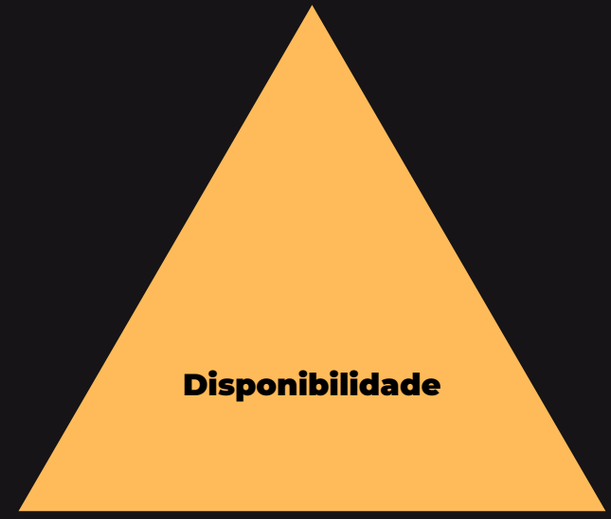
o conceito de disponibilidade diz respeito ao acesso dos dados sempre que este for necessário. Isto é, significa, literalmente, a garantia da disponibilidade das informações.

Fonte: ISO/IEC 27000:2014

São características de disponibilidade:

- **PRONTIDÃO:** Os sistemas de informação precisam estar disponíveis quando necessários;

- **CONTINUIDADE:** Os colaboradores de uma empresa precisam continuar a trabalhar, caso ocorra uma falha;



Disponibilidade - Exemplo

1. Procedimentos de backup;
2. Criação de procedimentos de emergência para garantir que as atividades possam ser retomadas o mais rapidamente;
3. Proteção contra desastres naturais.

Disponibilidade – Na Mídia

Central de atendimento da CVC continua fora do ar após ataque hacker

Ainda não há previsão para o retorno do serviço

Por Denis Kuck, Valor — Rio

05/10/2021 14h44 · Atualizado há um mês

Grupo Fleury sofre ataque *hacker*, e sistema fica fora do ar

Site da empresa exibe mensagem informando indisponibilidade de alguns serviços

Fábio Matos

23 JUN 2021 - 11:40

Quiz

Os princípios básicos da Segurança da Informação:

- ❑ Integridade, disponibilidade, autenticidade
- ❑ **Confidencialidade, integridade, disponibilidade**
- ❑ Disponibilidade, Autenticidade, Confidencialidade

Marque a alternativa do princípio básico da Segurança da Informação que garante o sigilo de uma informação.

- ❑ Disponibilidade
- ❑ Confidencialidade
- ❑ Integridade

data expert.®

Data Science & Machine Learning

5 - LGPD

Consultor: Jonas Galindo

LGPD

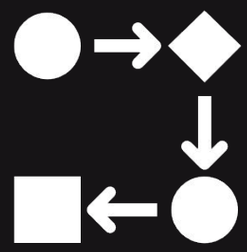
Lei geral de proteção de dados

nº 13.709

Pra que serve?

Lei que assegura a privacidade[1] aos cidadãos através de regras de tratamento[2] de dados pessoais

A privacidade[1] é uma garantia que deve acontecer em relação ao que pode ou não ser feito com os dados dentro desse sistema.



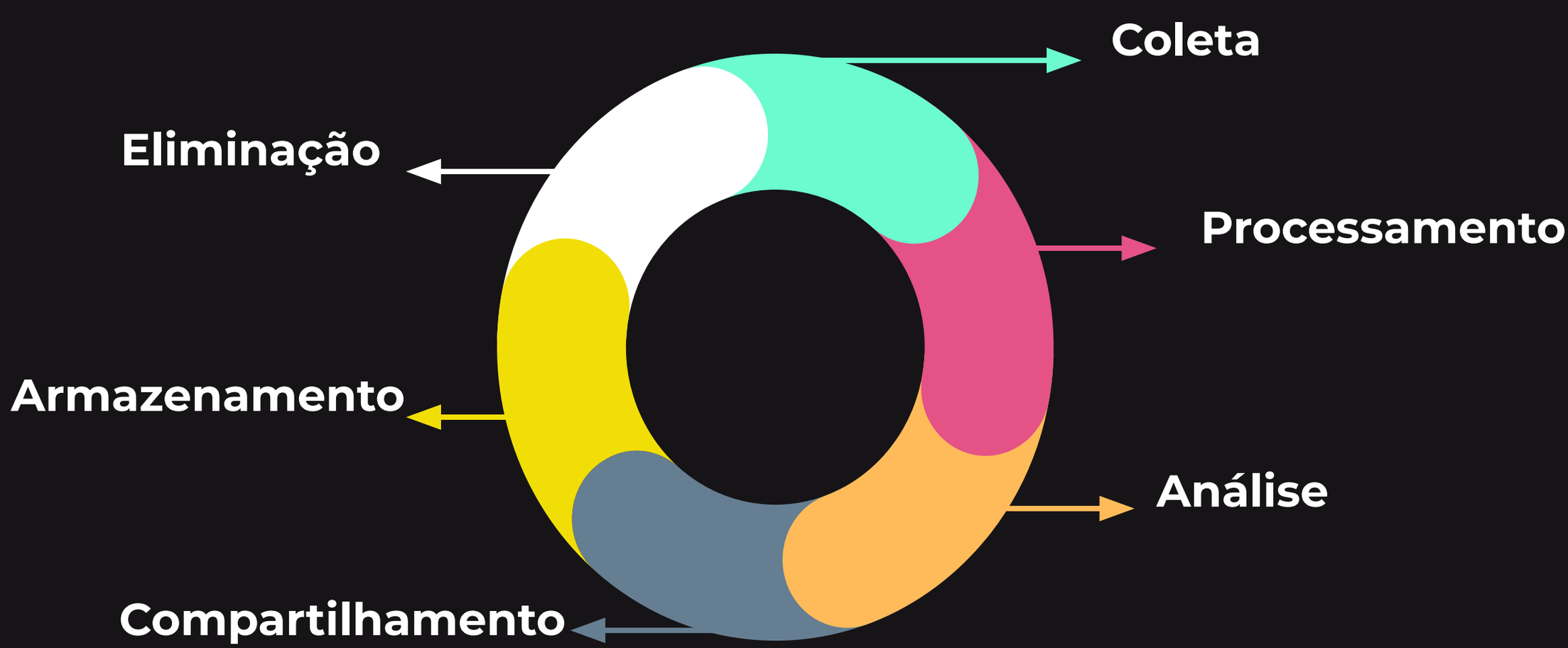
O tratamento[2] de dados consiste em toda e qualquer operação realizada com os dados de uma pessoa.

LGPD

Tratamento de dados

Art. 5

Podemos entender o tratamento de dados como um ciclo de vida



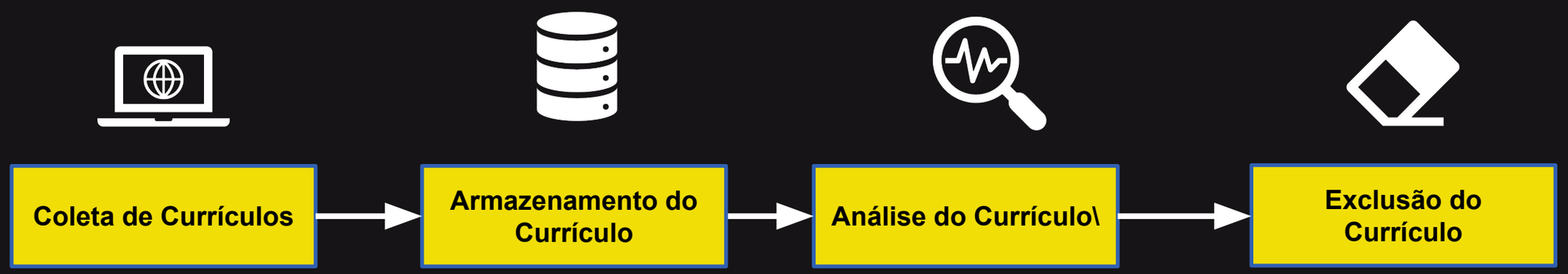
LGPD

Tratamento de dados

Art. 5

Exemplo

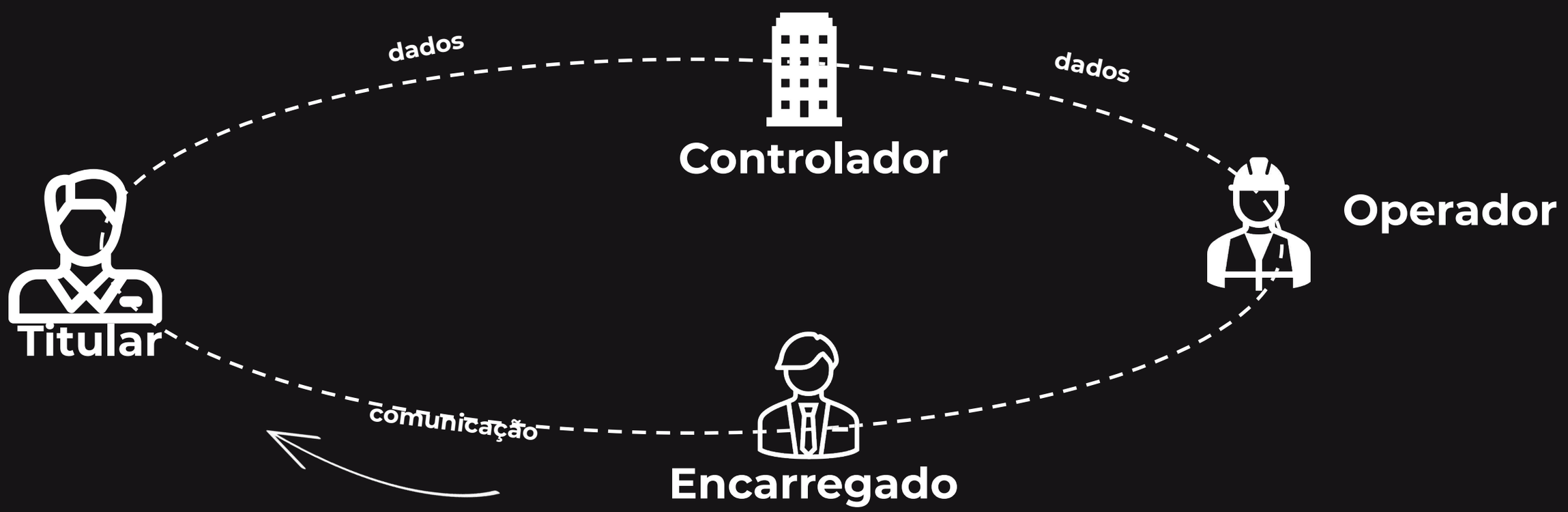
Processo de Candidatura em vagas



LGPD

Agentes de tratamento

A LGPD chama de **agentes de tratamento** todas as pessoas naturais ou jurídicas que sejam responsáveis pelas decisões referentes ao tratamento dos dados pessoais.



Principais pontos

Titulares

(Clientes, funcionários, etc.)

- Passam a ter mais direitos e controle sobre seus dados em posse de terceiros (Art. 17 a 22);

- Introdução dos 10 princípios de proteção de dados (Art.6);

- Finalidade
- Adequação
- Necessidade
- Livre acesso
- Transparência
- Qualidade
- Segurança
- Prevenção
- Não discriminação
- Prestação de contas

Principais pontos

Empresas

(processadores de dados pessoais)

- Mapeamento de tratamento de dados (art. 37);
- Tratamento de dados com bases legítimas (art. 7);
- Obrigatoriedade de notificação de incidentes (art.48);
- Deve possuir o Encarregado de Proteção de dados (art.41).

Principais pontos

ANPD

(Ag. Nacional de Proteção de dados)

- Regras específicas para dados sensíveis, de menores e caso haja transf. internacional de dados (Art. 11, 14 e 33)
- Realização de assessment de proteção de dados (Art.38);
- Suspensão parcial do banco de dados envolvido
- Multa simples de até 50 milhões ou 2% faturamento anual

Princípios da lei

Podemos entender o tratamento de dados como um ciclo de vida

Princípios da lei

01 Finalidade

"O objetivo desse princípio é que o tratamento dos dados devem ter um resultado específico e os dados obtidos devem servir apenas para esse objetivo".

02 Adequação

“O Objetivo desse princípio é identificar se a compatibilidade do tratamento com as finalidades informadas ao titular estão de acordo com o contexto do tratamento”.

Princípios da lei

03 **Necessidade**

“O princípio visa fazer com que a coleta de dados pessoais seja restrita ao que realmente é necessário para a realização da finalidade pretendida”.

04 **Livre Acesso**

“O Objetivo desse princípio garante aos titulares a consulta facilitada e gratuito da forma que o tratamento está sendo feito”.

Princípios da lei

05 Qualidade dos dados

“O princípio da qualidade dos dados assegura, que os titulares terão acesso a informações confiáveis, para que possam exercer da melhor forma possível a autodeterminação informativa”

06 Transparência

“Este princípio determina que as empresas precisam ser honestas com os titulares dos dados. De acordo com a lei, é a “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento”.

Princípios da lei

07 **Segurança**

“O princípio da segurança envolve a adoção de procedimentos, tecnologias e soluções que garantam maior proteção dos dados pessoais”,

08 **Prevenção**

“Este princípio determina a prevenção justamente sobre o ato de estar preparado para lidar com eventuais problemas envolvendo o tratamento de dados pessoais antes mesmo que eles surjam.”

Princípios da lei

09 **Não discriminação**

O principio da não discriminação, de acordo com a LGPD, refere-se à “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos”.

10 **Responsabilização e prestação de contas**

“O princípio da responsabilização e prestação de contas dispõe sobre o cumprimento da lei com provas e evidências de que medidas e procedimentos foram tomados pela empresa a fim de garantir a proteção dos dados”.

data expert.

Data Science & Machine Learning

6 - Tipos de Dados - Anonimização

Consultor: Jonas Galindo

O que é dados pessoais?

É considerado dado pessoal qualquer informação que permite identificar direta ou indiretamente, uma pessoa que está viva.

LGPD - LEI Nº 13.709

- **Dados pessoais simples**
- **Dados pessoais sensíveis**
- **Dado anonimizado**
- **Dado pseudonimizado**

Dados pessoais

Simples

Art. 5

- Qualquer informação que identifique diretamente ou indiretamente um titular de dados.

Direto: um cliente, ao fazer uma compra online, informa seu nome completo e CPF, ou seja, a loja virtual com essas informações consegue identificar o indivíduo que realizou a compra.

Indiretos: RG, CPF, título de eleito, profissão, hábitos de consumo, entre outros.

Dados pessoais

Sensíveis

Art. 5

- São aqueles dados que podem causar discriminação a uma pessoa, por isso merecem maior proteção

- origem racial ou étnica
- convicção religiosa
- opinião política
- dado referente à saúde ou à vida sexual
- dado genético ou biométrico

Dados pessoais

Anonimizado

Art. 5

A anonimização é uma técnica de processamento de dados que remove ou modifica informações que identificam uma pessoa.

Antes da anonimização

Nome: Adriane

Gênero: Feminino

Nacionalidade: Brasileira

Profissão: Médica

CRM/SP: 202221

Depois da anonimização

Gênero: Feminino

Nacionalidade: Brasileira

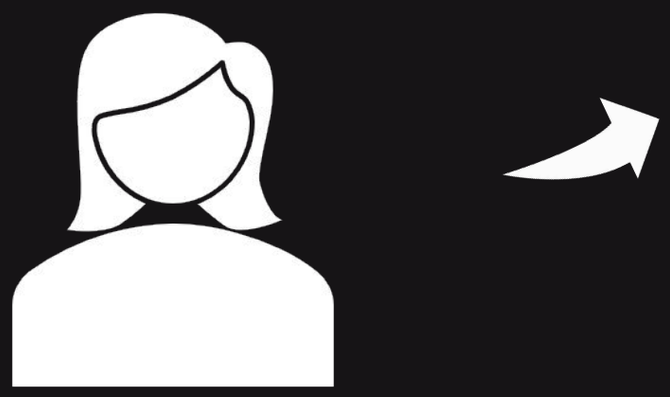
Profissão: Médica

Dados pessoais

Anonimizado

Art. 5

O que acontece com os dados de Adriane?



- São eliminados ou desassociados dados que possam identificar um titular
- Exclusão permanente (sem possibilidade de recuperação/restauração

Dados pessoais Pseudonimizado

Art. 13

A pseudonimização é o "tratamento por meio do qual um dado perde uma possibilidade de associação direta ou indireta, um indivíduo, senão pelo uso de informação adicional mantida pelo controlador em ambiente controlado e seguro.

Antes da pseudonimização

Nome: Adriane

Gênero: Feminino

Nacionalidade: Brasileira

Profissão: Médica

CRM/SP: 202221

Depois da pseudonimização

Banco de Dados #1

Gênero: Feminino

Nacionalidade: Brasileira

Profissão: Médica

Identificador: 10212201

Banco de Dados #2

(contém identificadores)

ID: 10212201

data expert.®

Data Science & Machine Learning

8 - Introdução a Criptografia

Consultor: Ricardo Manhães Savii

Criptografia

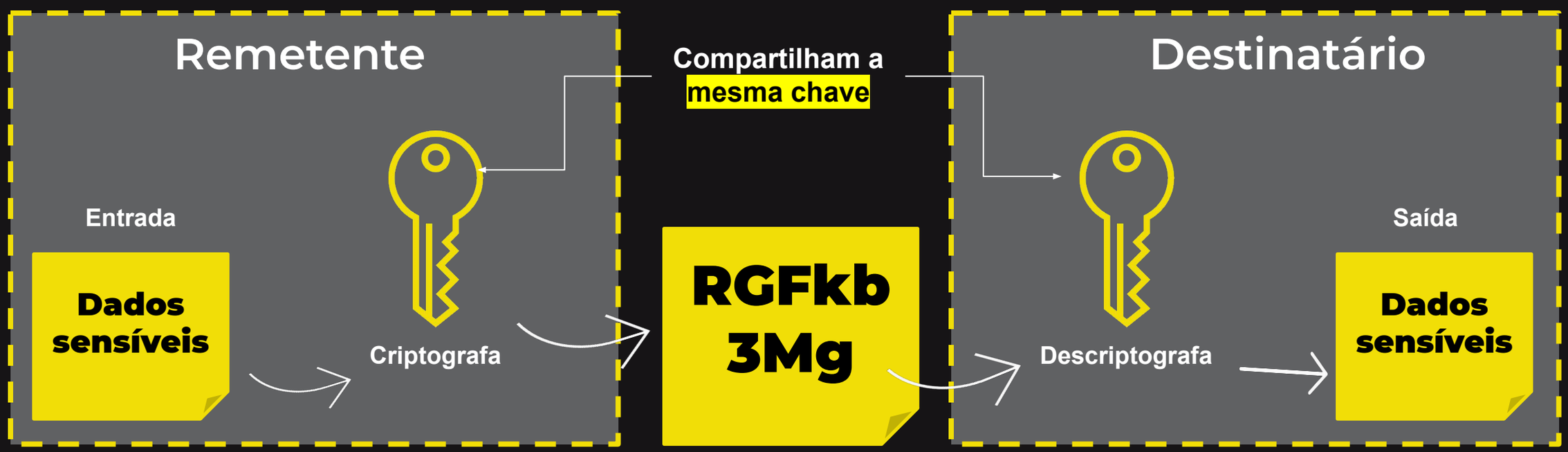
Porque a criptografia é importante para a privacidade?

Criptografar significa escrever uma mensagem através de códigos, onde somente o remetente e o destinatário possuem conhecimento adequado para a leitura das mensagens criptografadas.

De um modo geral, existem três formas de algoritmos criptográficos

Sistema Simétrico

Existe um algoritmo e uma chave secreta que o remetente e o destinatário compartilham



A mesma chave é utilizada tanto pelo receptor quanto pelo emissor

Sistema Assimétrico

Chaves diferentes são usadas para criptografar e descriptografar

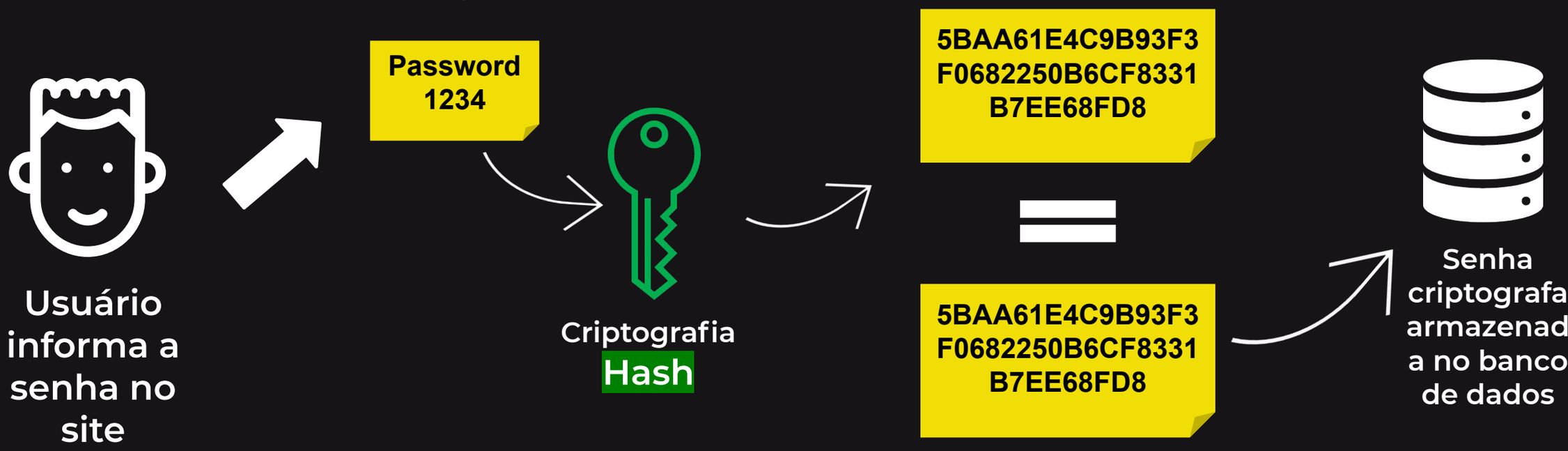
O algoritmo funciona com os chamados pares de chaves:

- A chave secreta é responsável pela descriptografia e apenas a chave pública pode criptografar a mensagem;
- A chave pública pode ser conhecida no mundo todo, enquanto a chave privada é mantida em segredo .

Sistema de Hash

Usando um algoritmo conhecido, o destinatário pode verificar se a mensagem tem o valor de hash coreto.

É um método irreversível;



A mensagem é convertida em **hash:**

- **Uma sequência de bits geradas por um algoritmo de dispersão, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F);**

Criptografia

Porque a criptografia é importante para a privacidade?

Tipos de Tipografia

Simétrica → A mesma chave é usada para criptografar

Assimétrica → Usam diferentes chaves para criptografar e descriptografar

Hash (One-way) → É o cálculo irreversível. Usado para entender se o dado foi alterado.

Criptografia

Tipos de Criptografia

	Simétrica	Assimétrica
Chaves	**Uma única chave para criptografar e descriptografar**	**Usa um par de chaves, UMA para criptografar e outra pra descriptografar**
Desempenho	**Como usa uma única chave, é mais rápido**	**Como usa mais de uma chave, é mais lento**
Quantidade de chaves	**Cresce rápido, conforme o número de usuários aumenta**	**Cresce linearmente, conforme o número de usuários aumenta**
Utilizado para garantir	**Confidencialidade**	**Confidencialidade, Integridade e Autenticação.**

FIM