O que é a LGPD?

Lei Geral de Proteção de Dados Pessoais é a Lei Nº 13.709, de 14 de agosto de 2018. Que determina como os dados dos cidadãos podem ser coletados e tratados, e que prevê punições para transgressões

Medida Provisória 869/2018, de dezembro de 2018 Altera a Lei Nº 13.709 para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências.

Abrangência:

Sobre o que?

Artigo 1º - Está Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais.

A quem se aplica?

Art. 3º Esta lei aplica-se a qualquer operação de tratamento realizada por pessoas natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

1. A operação de tratamento seja realizada no território nacional;
2. ...
3. Os dados pessoais objeto do tratamento tenha sido coletados no território nacional.

Tratamento de Dados Pessoais

Art. 5º Para os fins desta Lei, considera-se:

X – Tratamento: toda operação realizada com dados pessoais,

* Coleta
* Produção
* Recepção
* Classificação
* Utilização
* Acesso
* Reprodução
* Transmissão
* Distribuição
* Processamento
* Arquivamento
* Armazenamento
* Eliminação
* Avaliação
* Modificação
* Comunicação
* Transferência
* Extração

Dados Pessoais

Art. 5º para os fins desta lei, considera-se:

* Dado pessoal: Informação relacionada a pessoa natural identificada ou identificável;
* Dado pessoal sensível:
  + Origem racial ou ética
  + Convicção religiosa
  + Opinião política
  + Filiação a sindicato ou organização de caráter religioso, filosófico ou político
  + Dado referente à saúde ou à vida sexual
  + Dado genético ou biométrico

Finalidade do uso

Art. 7º o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

* Consentimento
* Obrigação Legal
* Administração Publica
* Estudos por órgão de pesquisa
* Contratos
* Proteção da vida

Os responsáveis – Agentes de tratamento

Art. 5º os fins desta Lei, considera-se:

* VI – Controlador: Pessoa natural ou jurídica, de direto público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
* VII – Operador: Pessoa natural ou jurídica, de direito pública ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
* VII – Encarregado: Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;
* IX – agentes de tratamento: O controlador e o operador;

ANPD

Art. 58-A. Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

* Composto por vinte e três representantes:
  + I – seis do Poder Executivo Federal;
  + II – um do Senado Federal;
  + II - Um da Câmara dos Deputados;
  + IV – um do Conselho Nacional de Justiça;
  + V – um do Conselho Nacional do Ministério Público;
  + VI – um do Comitê Gestor da Internet no Brasil;
  + VII – quatro de entidades da sociedade civil com atuação comprovada em proteção dados pessoais;
  + VII – quatro de instituições científicas, tecnológicas e de inovação;
  + IX – quatro de entidades representativas do setor empresarial relacionada à área de tratamento de dados pessoais. (Incluído pela Medida Provisória nº 869, de 2018)

Sanções Administrativas

* Advertência, com indicação de prazo para adoção de medidas corretivas;
* Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

Consentimento

Art. 5º Para os fins desta Lei, considera-se:

XII – consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

A coleta dos dados para uso é somente para fins específicos, explícitos e legítimos, deixando claro ao cliente.

Tem que deixar bem claro, como vai coletar, armazenar, compartilhar...

Requisitos para o Tratamento e Dados Pessoais

* CAPÍTULO II
* Seção I – Dos Requisitos para o Tratamento de Dados Pessoais
  + Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
  + mediante o fornecimento de consentimento pelo titular;
  + II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
  + III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
  + IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
  + V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
  + VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da [Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)](http://www.planalto.gov.br/ccivil_03/LEIS/L9307.htm);
  + VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
  + VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;      [(Redação dada pela Lei nº 13.853, de 2019)](http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2)      [Vigência](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm#art65..)
  + IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
  + X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
  + Art 8º O consentimento previsto no inciso do art. 7º desta Lei deverá ser fornecido por escrito ou por outro que demonstre a manifestação de vontade do titular.
  + § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta lei.

Considerações

* O consentimento deverá ser obtido por manifestação livre.
  + Pode ser utilizar o checkBox, mas não pode está pré marcada, o cliente que deverá marcar.
* A aceitação não pode ser passiva, de forma que o silêncio do usuário não pode ser considerado consentimento.
* A aceitação do usuário, como ato jurídico, sujeita-se ainda aos chamados vícios de consentimento (erro, dolo, coação, etc.), os quais, quando verificados, importam na ineficácia da manifestação de vontade e consequente nulidade do vínculo contratual.

Obs.: Deixe bem claro possível o motivo de está coletando e tratando essas informações.

Fundamento legal para tratamento de dados pessoais

Princípios no tratamento de Dados Pessoais:

1. Finalidade (Bem claro ao cliente o porquê do recolhimento dos dados)
2. Adequação
3. Necessidade
4. Livre Acesso (Ciente pode consultar aos dados e se estão corretos)
5. Qualidade dos Dados
6. Transparência
7. Segurança
8. Prevenção
9. Não discriminação
10. Responsabilização e prestação de contas

Hipóteses pra o Tratamento de Dados Pessoais

* Art. 7ª O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
  1. Mediante o fornecimento de consentimento pelo o titular.
  2. Para o cumprimento de obrigação legal ou regulatório pelo o titular.
  3. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.
  4. Para a realização de estudos por órgão de pesquisa como por exemplo o IBGE.
  5. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionadas a contrato do qual seja parte o titular, a pedido do titular dos dados.
  6. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral
  7. Para a proteção da vida ou da incolumidade física do titular ou de terceiros.
  8. Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.
  9. Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
  10. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
* Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
  1. Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
  2. Realizado para fins exclusivamente:
     1. Jornalístico e artísticos; ou
     2. Acadêmicos;
     3. Acadêmicos, aplicando-se a esta hipótese arts. 7º e 11 desta Lei;
  3. Realizado para fins exclusivos de:
     1. Segurança pública;
     2. Defesa nacional;
     3. Segurança do Estado; ou
     4. Atividades de investigação e repressão de infrações penais; ou
  4. Provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Palestra com advogado

É necessária uma pessoa responsável pela a proteção de dados pela a empresa?  
Sim! Lei obriga ter uma pessoa responsável, chamando Data Protection Officer (DPO) ou Encarregado de Dados, responsável por cuidar das questões referentes à proteção de dados de uma empresa e seus clientes.  
Mas pode ser constituído uma comissão responsável, porém com o DPO responsável, que é um profissional da área de Informática ou advogado, não necessariamente presencial na empresa, mas será o responsável, que irá dialogar com ANPD (Autoridade Nacional de Proteção de Dados), Ministério Público, Tribunal de Justiça...

Em caso de notificação e não tenha concluído todas as normais de adequação a LGPD. Deve realizar um workshop de palestra para conscientização de como os funcionários irão trabalhar

Com a mudança da lei. O que precisa:

* Lista de presença;
* Certificados;
* Fotos para registro;
* Apostilas sobre o conteúdo;

Juta todos os documentos acima listados e coloque dentro de uma pasta, pós em caso de notificação, fica registrado que já iniciou adequação.

Em caso de invasão ou perda de dados dentro da LGPD:

1. A empresa realizou medidas para evitar invasão ou perda dos dados?
2. Que medidas essa empresa fez após a invasão ou a perda dos dados?

Por onde devo começar?

1. Criar um comitê (Governança) para análise e tomadas de decisão.
2. Designar um DPO (Oficial de proteção de dados).
3. Mapear e entender o ciclo de vida dos dados.
4. Analise de Risco.
5. Criar um relatório de impacto à proteção de dados pessoais.
6. Adotar regulamentações / padrões de segurança da informação.
7. Proteção em Camadas.
8. Auditar e monitorar o ambiente.
9. Treinar pessoal
10. Plano de ação para situações de emergência.

Comitê:

Aonde será constituído um DPO, advogado especialista na área da segurança da informação...

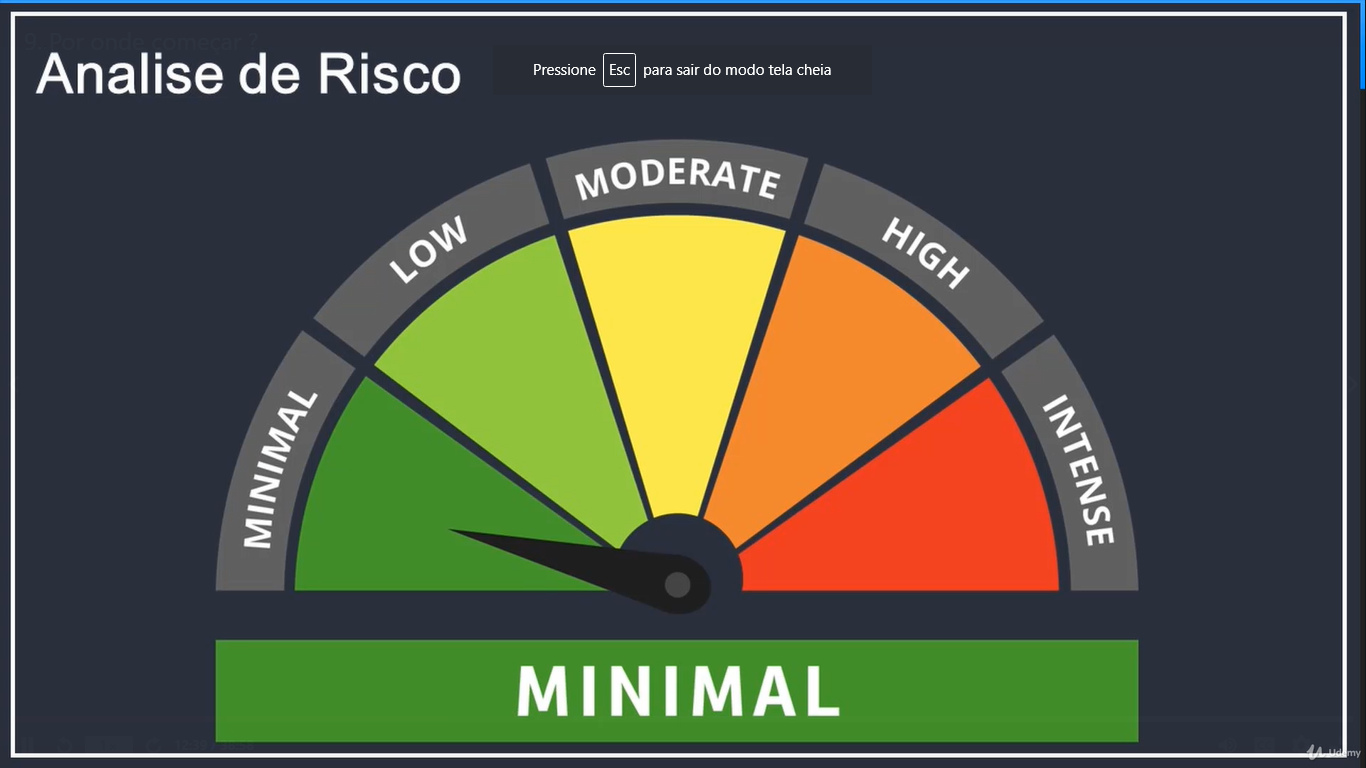
DPO:

responsável pelas diretrizes de todas as tomadas, procedimentos e segurança da informação conforme a LGPD. Que ficará responsável de dialogar com a ANPD, Tribunal de Justiça, Ministério Público...

Mapear e entender o ciclo de vida dos dados:

O artigo 5° considera tratamento as operações como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Analise de Risco:



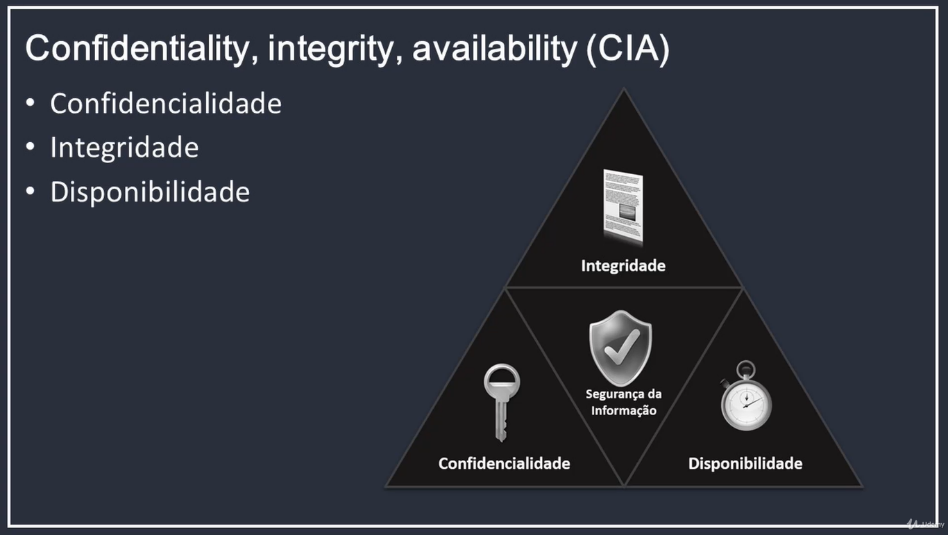
Após o mapeamento dos dados, identificar aonde estão localizados, verificar se existe o risco, identificas as possíveis vulnerabilidades e determinar a probabilidade de uma determinada ameaça e explorar uma vulnerabilidade existente aonde estiver essa informação.

Relatório de impacto:

O relatório de impacto à proteção de dados pessoais é uma exigência legal.

Art. 5º Para os fins desta Lei, considera-se:

XVII – 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 mecanismo de mitigação de risco;



**Confidentiality, Integrity, Availability (CIA)**

* **Confidencialidade:** Garantir que meus dados são seguros e que nem todos terão acessos a ele, somente aqueles que eu confio.
* **Integridade:** Garantir que a informação não foi alterada, e quando for acessada, ter certeza que aquilo foi realmente criado original, que ninguém alterou.
* **Disponibilidade:** Ataques que venha ocorrer e garantir que os usuários não irão parar de trabalhar. É ideal ter planos de contra desastre e ataque para recuperação.

**ABNT NBR IO/IEC 27000**

* ISSO/IEC 27001:2013 – Esta Norma especifica os requisitos para estabelecer, implementar, manter melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.
* ISSO/IEC 27002:2013 – Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento controles, levando em consideração os ambientes de risco da segurança da informação da organização.
* ISSO/IEC27701:2019 – Este documento especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da informação (SGPI) na forma de uma extensão das ABNT NBR ISSO/IEC 27001 e ABNT NBR ISSO/IEC 27002 para a gestão da privacidade dentro do contexto da organização.

**Auditar e monitorar o ambiente**

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.



Treinar pessoal

Comitê precisa ajudar a elaborar o treinamento para o DPO a realizar o treinamento, onde as pessoas saibam como estão sendo tratados os dados, porém os treinamentos precisam ser realizados de acordo com a função de cada função.

Plano de ação para situação de emergência

Plano de recuperação dos dados, em caso de desastre naturais, hackers ou exclusão, onde precisamos tomar medidas urgente para prevenir qualquer eventualidade.

Minimizar o período que fica interrupto o tempo das operações, prazo para entrega de serviços e garantir que sistema estejam sempre confiáveis.

Considerações:

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1° A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

1. A descrição da natureza dos dados pessoais afetados;
2. As informações sobre os titulares envolvidos;
3. A indicação das medidas técnicas e de segurança utilizadas para proteção dos dados, observados os segredos comercial e industrial;
4. Os riscos relacionados ao incidente;
5. Os motivos da demora, no caso de a comunicação não ter sido imediata; e
6. As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

**JCA Contadores na condição de controlador, encarregado e operador.**

* Na situação do departamento de contabilidade a JCA se enquadra como **controlador**, pós irá tratar dos dados das empresas (titulares) para tratamento dos seus dados e informações com as entidades de fiscalização.
* Na situação do Departamento Pessoal e Fiscal a JCA se enquadra como **encarregado**, pós irá tratar das informações dos clientes das empresas contratantes, e a empresa passar a ser **controlador**, pós ela que tomará medidas a respeitos dos dados dos clientes, mas a JCA poderá também se encaixar como **controlador**, pós também irá tratar de dados pessoais da empresa e de seus titulares.
* Os colaboradores são colocados como **operador**, pós são responsáveis pelo o tratamento dos dados.
* Na situação da JCA contratar um servidor em nuvem, serviço de backup, captura de notas... passa a ser **controlador** e a empresa contratada a ser o **encarregado**, pós ela irá toma algumas decisões para o tratamento dos dados dos clientes da JCA.

**Boas práticas e governança de Dados Pessoais**

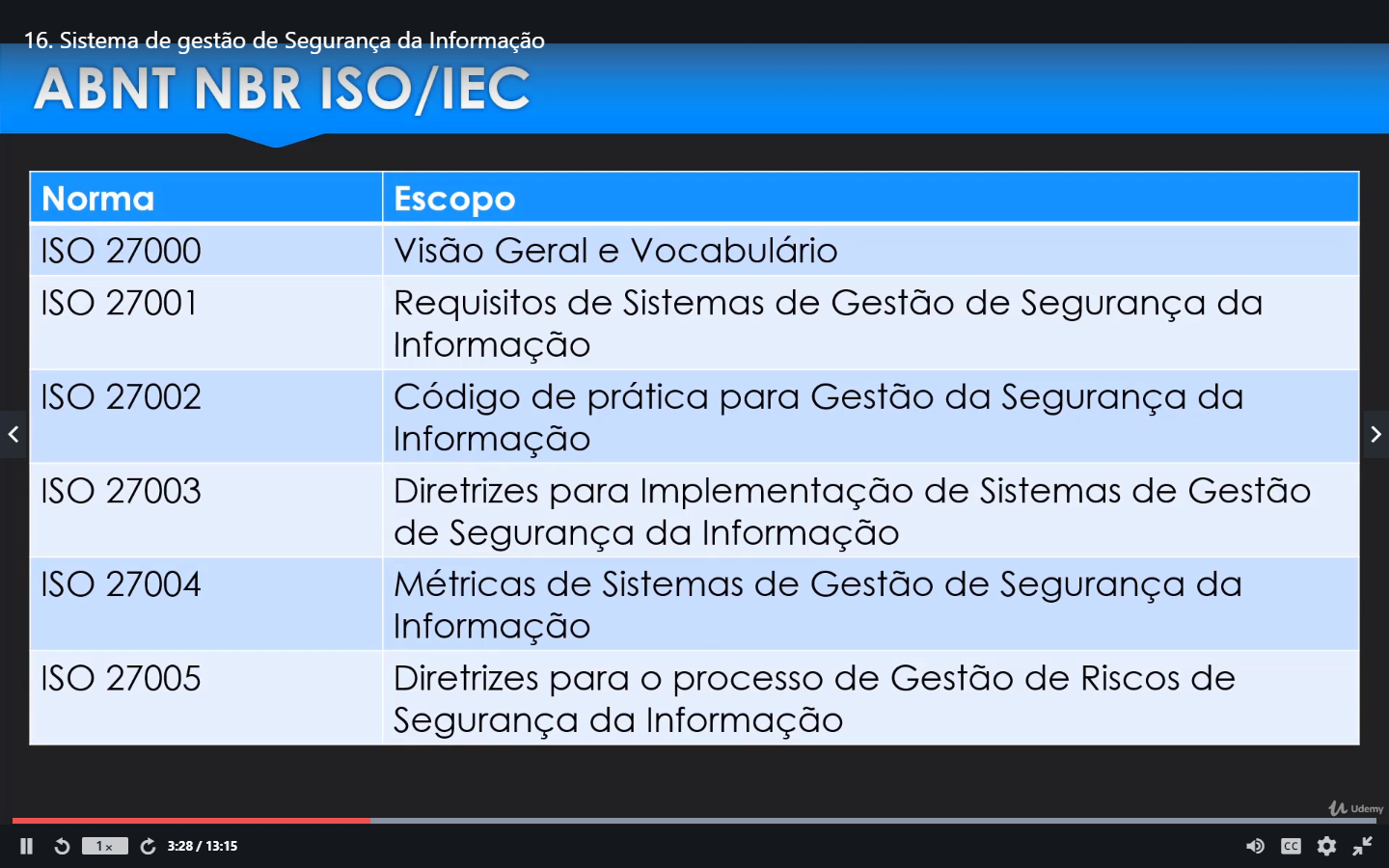
Agentes de tratamento

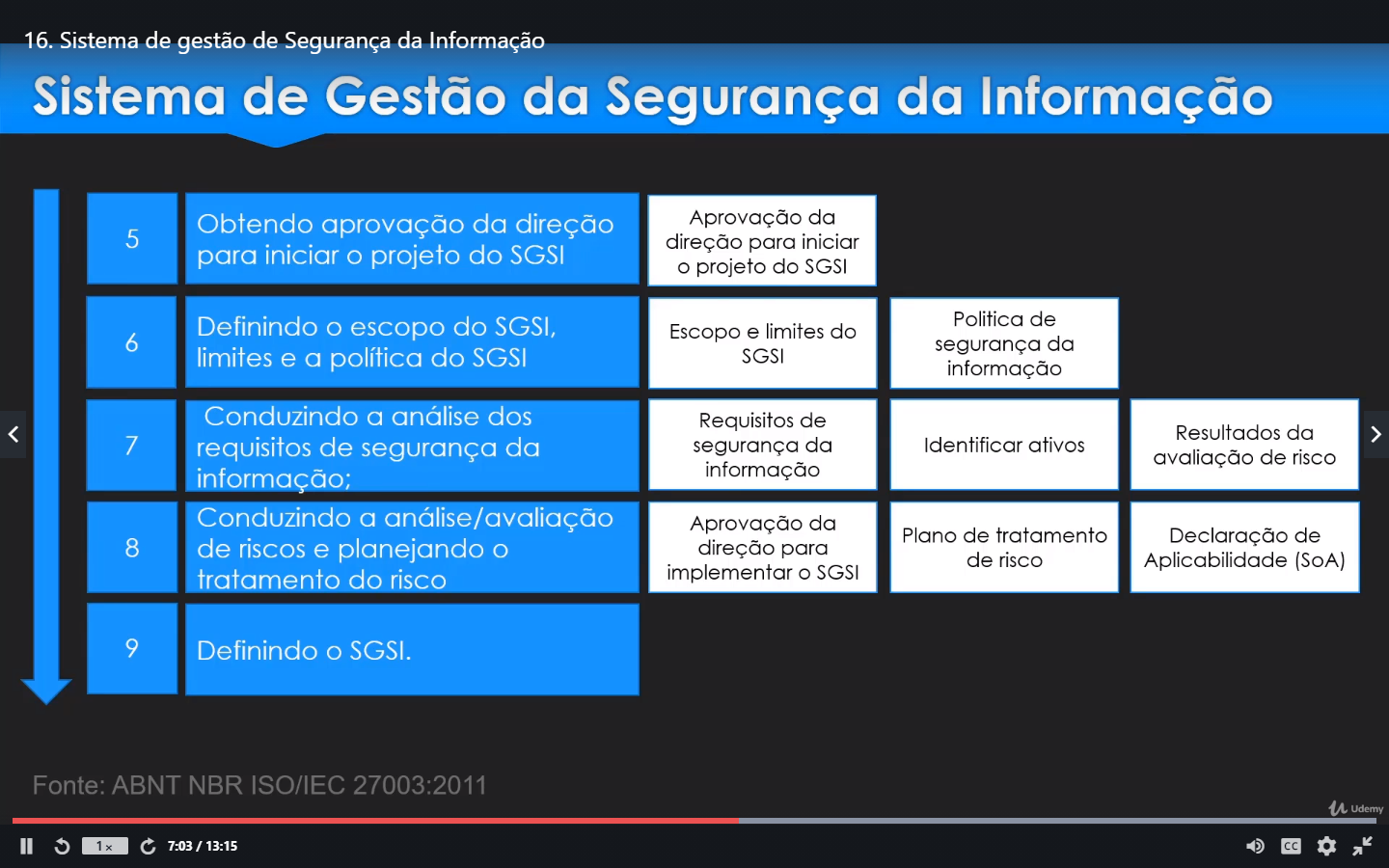
* Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
* Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

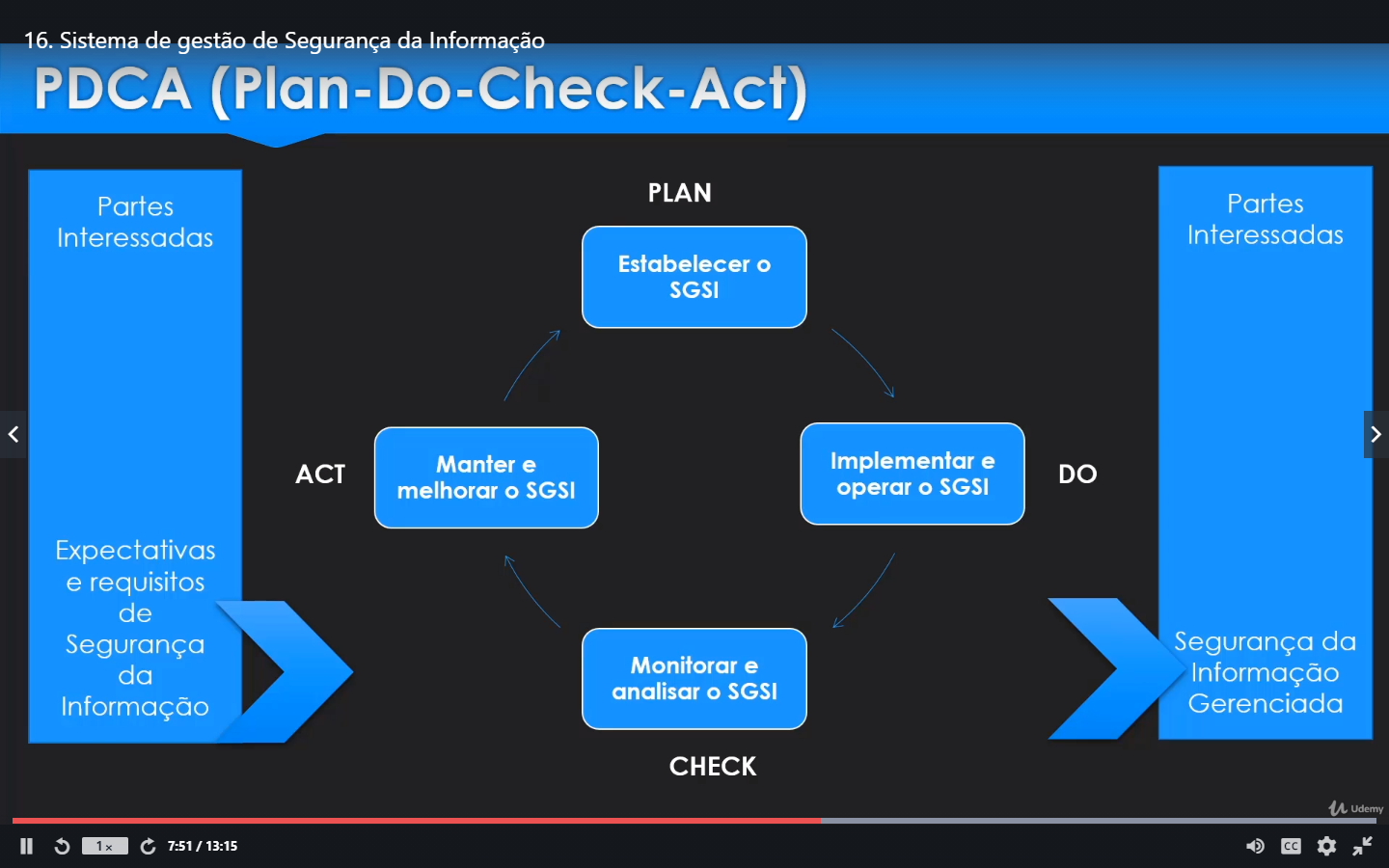
Término do tratamento de dados

* Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
  + Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (Excluir os dados)
  + Fim do período do tratamento;
  + Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5° do art. 8° desta Lei, resguardado o interesse público; ou
  + Determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Sistema de Gestão da Segurança da Informação







Mapeando os dados pessoais

Identificar dados pessoais

* Utilizando a planilha vamos analisar alguns recursos comuns de rede e identificar:
  + Tipo de Dados
  + Propósito
  + Segurança aplicada
  + Quem tem acesso
  + Qual a origem dos dados e outras informações relevantes.

Mapear Dados em Servidores de Arquivos

* Mapear os acessos aos arquivos e pastas
  + Usuários
  + Grupos
  + NFTS
  + Compartilhamento

Criptografia

O que é Encrypting File System?

* O EFS é um recurso que pode criptografar arquivos armazenados em uma partição NFTS.
* A criptografia EFS age com uma camada adicional de segurança.
* EFS pode ser usado sem configuração.

Como funciona o EFS?

* A criptografia simétrica é usada para proteger os dados do arquivo
  + Chave de Descriptografia do Arquivo (FEK).
* A criptografia de chave pública é usada para proteger a chave simétrica.
  + Certificado de usuário com chave pública e chave privada.
  + Além do certificado de agente de recuperação.

Recuperação de arquivos criptografados por EFS

* Para garantir que você possa recuperar arquivos com criptografia EFS:
  + Faça backup de certificados de usuários
  + Configure um agente de recuperação.

Observações:

* Cuidado ao tirar fotos (selfs) para não demostrar os dados do cliente.