SEGURANÇA E AUDITORIA DE SISTEMAS DE INFORMAÇÃO

Prof. Cesar Amaral

prof.cesar.amaral@gmail.com

Aula 2 - Principais Padrões, Normas de Segurança da Informação e LGPD

- Devido a toda a preocupação com segurança que se tem atualmente nas empresas, percebeu-se a necessidade de se criar regras para se lidar com ela.

- Até pouco tempo atrás, quase não existiam normas e padrões de segurança para orientar as empresas sobre como agir, mas isso mudou!!!

- Os padrões e normas surgiram para proteger a informação...

- Anterior ao 11 de setembro de 2001, até existiam algumas preocupações com segurança, mas ela era mais voltada para a parte física.

- Isso vem mudando gradativamente e as empresas começam a ter uma preocupação maior com seu bem mais precioso: a INFORMAÇÃO.

- O rápido crescimento das redes de computadores e da comunicação on-line fez as empresas perceberem sua dependência da informação e de seus sistemas.

NORMAS

- **Norma:** documento criado por uma autoridade reconhecida, feita em consenso por uma equipe com alta capacidade técnica sobre o assunto, que permite que seja tirada uma certificação.

- Usada para definir regras e padrões que servirão como meio de controle na realização de determinada atividade.

- As normas de segurança da informação foram criadas para fornecer as melhores práticas, diretrizes e princípios gerais para a implementação de sua gestão para qualquer organização.

Órgãos Padronizadores

- Existem alguns órgãos nacionais e internacionais reconhecidos e idôneos que elaboram padrões, editam, publicam e revisam normas técnicas.

- Os mais conhecidos são:

  - ISO – International Standardization Organization

  - IEC – International Electrotechnical Comission

  - IEEE – Institute of Electrical and Electronics Engineers

  - ABNT – Associação Brasileira de Normas Técnicas

Primeiras Normas Brasileiras

- NBR1333 (1990): controle de acesso físico ao CPD
- NBR1334 (1990): critérios de segurança física para o armazenamento das informações
- NBR1335 (1991): segurança física dos terminais dos usuários
- NBR10842 (1989): segurança para os equipamentos de TI

Evolução das Normas de Segurança

- 1970 – criação de uma força tarefa no departamento de defesa americano que criou o documento Security Control for Computer System.

- 1983 – criado um conjunto de regras para classificação dos sistemas operacionais como seguros ou não, chamado de Orange Book; usado para avaliar e classificar o grau de proteção que os SOs ofereciam ao hardware, software e informações armazenados.

- 1987 – criada uma adaptação do orange book, voltado para a segurança de equipamentos de redes, chamado de Red Book.

  - http://en.wikipedia.org/wiki/Rainbow_Series

- 1995 – foi criada no Reino Unido a **BS7799**, um padrão de segurança muito bem elaborado e complexo, que foi dividido em 2 partes:
  - **BS7799-1**: documento de referência para implementar "Boas Práticas" para a segurança da informação.
  - **BS7799-2**: proporcionar a base para a criação de um sistema de Gestão da Segurança da Informação (SGSI) dentro das empresas.
- Por ter sido uma norma muito bem elaborada e inédita, ela passou a ser usada no mundo todo.
- Porém, ela tinha diversos itens específicos do mercado britânico. Com isso, ela foi adaptada para ser usada internacionalmente.

- 2000 – criada a **ISO/IEC 17799**, a versão internacional da BS7799-1.

- 2001 – criada a **NBR ISO/IEC 17799**, a versão brasileira da norma internacional, que foi revisada em 2005.

Série ISO 27000

- Série composta por diversas normas de segurança, cada uma tratando temas específicos. As principais são:
  - ISO 27001
  - ISO 27002
  - ISO 27003
  - ISO 27004
  - ISO 27005
  - ISO 27006

- **ISO 27001** (2005)
  - BS7799-2 revisada e melhorada
  - Sistema de Gestão da Segurança da Informação (SGSI)
  - Contempla o ciclo de melhoria contínua.

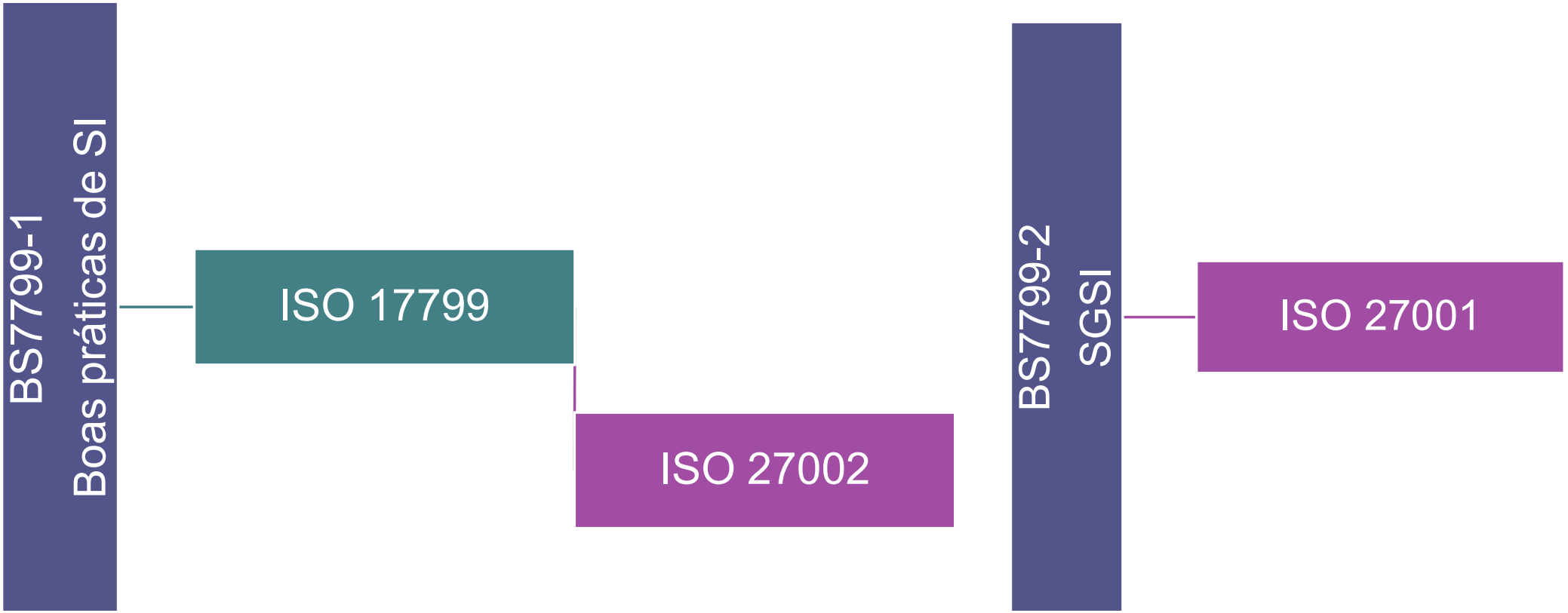
- **ISO 27002** (2005)
  - Voltada para a gestão da segurança da informação
  - Princípios gerais de concepção, implementação, manutenção e melhoria da segurança
  - Guia de boas práticas
  - Substitui a ISO 17799.

- **ISO 27003 (2010)**
  - Orientação sobre a implementação de SGSI, incluindo técnicas de segurança
  - Fornece instruções de como realizar um planejamento de um projeto SGSI em organizações de todos os tamanhos.

- **ISO 27004 (2009)**
  - Padrão referente aos mecanismos de medição e relatórios para um SGSI.

- **ISO 27005 (2008)**
  - Gestão de riscos: fornece diretrizes para o gerenciamento de informações de riscos.

- **ISO 27006 (2011)**
  - Requisitos para auditorias externas em um SGSI e certificação de sistemas de informação de gestão de segurança.


BS7799-1
Boas práticas de SI
ISO 17799
ISO 27002
BS7799-2
SGSI
ISO 27001

Outras Normas

- Algumas outras normas, de assuntos não tão voltados a segurança, surgiram, abrangendo um pouco essa área.

- **2002 - Sarbanes Oxley (SARBOX ou SOX):**
  - Criada nos EUA depois da crise financeira criada por causa de escândalos financeiros. Objetivo: dar transparência na divulgação das informações e assegurar a prestação de contas.

  - Responsabiliza diretores, auditores e pessoal de TI por informações falsas apresentadas aos investidores

- **BASEL III ACCORD (BASILEIA III):** tem o objetivo de manter estabilidade financeira pela implementação de controles que diminuam os riscos dos bancos. Realiza cálculo de riscos (de crédito, do mercado e operacionais).

- **PCI (Payment Card Industry):** criada pelas grandes bandeiras de cartão de crédito (AMEX, Discover Financial Services, Japan Credit Bureau, MasterCard e Visa), define um padrão para o manuseio de dados de pagamentos para todos os comerciantes que lidam com armazenamento, transmissão ou processamento de dados de cartões de crédito.

- **ITIL (Information Technology Infrastructure Library):** modelo de referência para gerenciamento de processos de TI, possui itens específicos que abordam o assunto da Segurança da Informação, principalmente em planos de continuidade de negócios.

- **COBIT (Control Objectives for Information and Related Technology):** conjunto de ferramentas de implementação e guia com técnicas de gerenciamento.

- **ISO 15408:** criada em 2005, estabelece critérios de segurança para o desenvolvimento de aplicações seguras.

- **BS 2599-2:** criada em 2007, é uma norma britânica com foco em gestão de continuidade de negócios.

- **ISO 31000:** norma criada em 2009 e voltada para a gestão de riscos.

- Como podemos ver, temos uma constante evolução das normas de segurança. Isso se deve ao fato de as TI evoluir muito rapidamente, e com ela as ameaças às quais estamos sujeitos. Todos os dias temos novas ameaças e vulnerabilidade, precisando de novos procedimentos e mecanismos para evitá-los.

Importância da Certificação

- Apesar de não garantir total e completamente a segurança da informação, a certificação mostra aos clientes de uma empresa que a mesma se preocupa com suas informações, o que pode ser um diferencial de mercado.

Vídeos

- **ISO 27000**
  https://www.youtube.com/watch?v=8kJp1ijbnvM&index=7&list=UUFFzm2qUHce7Gua4tGb6dvQ

Para saber mais

- https://www.portalgsti.com.br/2013/12/as-normas-da-familia-iso-27000.html
- https://www.portalgsti.com.br/2012/11/ebook-gratuito-gestao-da-seguranca-da-informacao.html

LGPD

FUNDAMENTOS

- O que é? É a lei geral de proteção de dados pessoais brasileira (Lei 13.709 de 2018);

- Dados pessoais estão relacionados com privacidade e direitos humanos e constitucionais como liberdade, direito de escolha e de pensamento;

- Dados pessoais, segundo a lei, são as informações relacionadas a pessoa natural identificada ou identificável;

- Informações como seu nome, CPF e RG, e também outros dados complexos como a informação geo- referenciada fornecida pelo serviço de localização do seu telefone móvel;

- Conflito? Era da Informação x Privacidade;

- Informação é poder! Informação é dinheiro! Informação é controle!

- **E quando a LGPD não é aplicável?**
  - Pessoa física quando não há interesse econômico;
  - Para fins jornalísticos, artísticos e acadêmicos;
  - Pelo poder público no caso de segurança pública, defesa nacional, segurança do estado e atividades de investigação e repressão penal.

ORIGEM

- Inspirada na GDPR (Lei europeia de proteção a dados);
- Construção da GDPR se deu durante algumas décadas;
- Primeiro artigo sobre privacidade data de 1890!!
- “O Direito da Privacidade” foi publicado na Harvard Law Review por Samuel D. Warren;

- Esse artigo foi escrito em resposta aos avanços tecnológicos da época como a fotografia e a imprensa (sensacionalista);

- Artigo 12º da Declaração Universal dos Direitos Humanos:

"Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação."

LGPD - O PORQUÊ DA EXISTÊNCIA

- Será que fazemos alguma ideia por onde nossas informações pessoais se encontram espalhadas e que tipo de uso empresas e governo fazem delas?
- Apenas dados que explicitamente forneci foram capturados?
- Podem ter sido repassados sem o meu conhecimento e consentimento?
- Quando eu forneço um dado pessoal ele deixa de ser privado e passa a ser público?

O PORQUÊ DA EXISTÊNCIA

- A LGPD visa regular o ambiente do uso das informações pessoais que tramitam no território brasileiro;
- Abrange inclusive empresas que apesar de não estarem localizadas fisicamente no Brasil oferecem serviços em nosso território;
- Seu objetivo é disciplinar e regular o uso dos dados pessoais mantidos por organizações públicas e privadas, a fim de que se evitem abusos contra aqueles que confiaram as suas informações à sua guarda;

O PORQUÊ DA EXISTÊNCIA

- Todas as organizações, públicas ou privadas, que detém sob sua guarda dados de pessoas naturais com o objetivo de oferecer e prestar serviços estão sujeitos ao regramento da LGPD;
- Caso não cumpram o dever de resguardar, proteger e utilizar esses dados apenas para as atividades autorizadas ou necessárias na prestação do serviço, poderão se sujeitar as penalidades da lei, inclusive, multas e suspensão de atividades.

LGPD

OS ATORES

CASO REAL 01

1. Uma pessoa deseja fazer a compra de um celular através de uma empresa de e-commerce.

2. Esta empresa, por sua vez, precisa ter acesso ao nome e endereço do comprador para a entrega do produto adquirido e, provavelmente, ao telefone de contato, numero de CPF, cartão de crédito, etc..

3. Por sua vez, uma empresa de entrega, contratada pela empresa de e-commerce, também vai precisar ter acesso ao nome completo, endereço e telefone do comprador, tanto para executar a entrega propriamente dita, quanto para contatá-lo, caso haja algum problema urgente a ser resolvido durante a mesma.

OS ATORES

- TITULAR DE DADOS
  - Pessoa natural (física) que fornece seus dados a uma organização ou tem seus dados pessoais obtidos através de uma organização terceira de forma legal.
- CONTROLADOR DE DADOS
  - O controlador nada mais é que a própria organização que obtém dados pessoais diretamente dos titulares ou através de uma organização terceira, no objetivo de prestar algum tipo de serviço.

OS ATORES

- OPERADOR DE DADOS
  - Organização que, sob autorização do controlador, recebe dados pessoais de seus titulares para efetuar algum tipo de prestação de serviço ao próprio controlador.
- TRATAMENTO DE DADOS“
  - Toda e qualquer operação executada nos dados pessoais dos titulares, como, acessar, classificar, armazenar, apagar, distribuir, imprimir, transmitir, etc. necessários à prestação de serviço por controladores e operadores.

OS ATORES

- TITULAR : CLIENTE
- CONTROLADOR: EMPRESA DE E-COMMERCE
- OPERADOR: TRANSPORTADORA
- TRATAMENTO DE DADOS: CADASTRO, ACESSO, ENVIO, ETC.
- HOUVE TRANSFERÊNCIA DE DADOS: SIM!

CASO REAL 2

1. Estudantes concluintes do 2º grau e outros inscritos que já possuem esse nível de escolaridade participam do ENEM como parte do processo de ingresso no ensino superior de várias instituições, notadamente as públicas.

2. Os inscritos vão ao site do INEP, uma autarquia do governo federal ligada ao ministério da educação(MEC), a fim de proceder a sua inscrição fornecendo os seus dados.

3. Após a publicação do resultado do ENEM, os estudantes que tiverem interesse de ingressar em uma instituição pública federal, devem recorrer ao site do MEC para proceder a inscrição no SISU.

CASO REAL 2 (CONTINUAÇÃO)

4. Inscrição no SISU. Os dados já fornecidos para a participação no ENEM e a sua nota final já são de conhecimento do mec. O candidato deve fazer as opções relativas as instituições e cursos que deseja fazer indicando, inclusive, se fará a opção de participar de ações afirmativas (cotas) e como deverá comprovar informações como origem racial, baixa renda, formação em escola pública, etc.

5. Caso seja aprovado na instituição, o candidato deverá confirmar a sua opção a fim de efetivar a sua matrícula.

OS ATORES (FASE 1)

- TITULAR: INSCRITOS NO ENEM
- CONTROLADOR: INEP
- OPERADOR: (NÃO ESTÁ CLARO)
- TRATAMENTO DE DADOS: CADASTRO, ACESSO, ENVIO, ETC.
- HOUVE TRANSFERÊNCIA DE DADOS: NÃO!

OS ATORES (FASE 2)

- TITULAR: INSCRITOS NO SISU
- CONTROLADOR: MEC
- OPERADOR: (NÃO ESTÁ CLARO)
- TRATAMENTO DE DADOS: CADASTRO, ACESSO, ENVIO, ETC.
- HOUVE TRANSFERÊNCIA DE DADOS: SIM!

OS ATORES (FASE 3)

- TITULAR: APROVADO EM INSTITUIÇÃO DE ENSINO
- CONTROLADOR: INSTITUIÇÃO PÚBLICA DE ENSINO
- OPERADOR: (NÃO ESTÁ CLARO)
- TRATAMENTO DE DADOS: CADASTRO, ACESSO, ENVIO, ETC.
- HOUVE TRANSFERÊNCIA DE DADOS: SIM!

OS ATORES

- **CONCEITOS IMPORTANTES:**
  - Os dados pessoais fornecidos ou obtidos pelo controlador deverá ser apenas e tão somente os dados necessários a prestação de serviço (Para que se questionar origem racial se essa informação não fosse importante para implementação da política de cotas ou de outro uso relevante para um cumprimento legal ou de uma política pública?);
  - Todo tratamento de dados efetuado deve contribuir para as ações necessárias a prestação de serviços por parte do controlador ou naquilo que foi autorizado pelo próprio titular. Nem mais, nem menos;

OS ATORES

- **CONCEITOS IMPORTANTES (CONTINUAÇÃO):**
  - Se essa premissa não é respeitada, há uma forte possibilidade de o controlador estar cometendo algum tipo de abuso com os dados pessoais dos seus titulares;
  - Todo o tratamento de dados pessoais feito pelo operador na prestação de serviços deve ser feito sob a demanda e orientação do controlador;
  - Uma pessoa física pode ser um controlador desde que mantenha dados pessoais para prestação de serviços e seja remunerado por tal, como os profissionais liberais.

OS ATORES

- CONCEITOS IMPORTANTES (CONTINUAÇÃO):
  - Pode haver transferência de dados do setor público para o setor privado, mas apenas nas hipóteses:
    1. Os dados já se encontrarem públicos;
    2. Na atividade descentralizada de atividade pública que exija essa transferência e apenas para tal fim;
    3. Quando houver previsão legal mas, também, seja respaldado em convênios, contratos e acordos;
    4. Prevenção de fraudes e proteção dos titulares.
  - De maneira geral a transferência internacional de dados só deverá ser feita se o país destino tenha um nível de proteção igual ou superior aos previstos na lei brasileira.

LGPD

PRINCÍPIOS

PRINCÍPIOS

1. **FINALIDADE** – Propósitos específicos, legítimos e relevantes informados ao titular;
2. **ADEQUAÇÃO** – Tratamento compatível com a finalidade informada pelo agente controlador;
3. **NECESSIDADE** – Limitação do tratamento e abrangência dos dados ao mínimo necessário para atendimento a finalidade;
4. **LIVRE ACESSO** – Direito do titular a consulta facilitada e gratuita sobre a forma e duração do tratamento;
5. **QUALIDADE** – Direito a clareza, exatidão, relevância e atualização dos dados de acordo com a necessidade e cumprimento da finalidade;

PRINCÍPIOS

6. **TRANSPARÊNCIA** – Direito a informações claras, precisas e acessíveis sobre o tratamento de dados;
7. **SEGURANÇA** – Direito a segurança dos dados devendo os agentes de tratamento utilizar medidas adequadas a fim de alcança-la;
8. **PREVENÇÃO** – Direito a prevenção de danos devendo os agentes de tratamento utilizar medidas adequadas para tal fim;
9. **NÃO DISCRIMINAÇÃO** – Direito a anti-discriminação. Impossibilidade de tratamento abusivos ou ilícitos;
10. **RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS** – Direito de exigir a responsabilização e prestação de contas da adoção de medidas eficazes ao cumprimento das normas.

PRINCÍPIOS

- **APLICABILIDADE:**
  - Controladores só podem efetuar tratamento de dados de acordo com uma ou mais bases legais descritas na LGPD e, principalmente na hipótese do consentimento, os propósitos devem estar claros ao titular (Princípios 1 e 2);
  - Controladores não devem solicitar e nem capturar dados que não sejam necessários a necessidade e finalidade do serviço prestado (Princípio 3);
  - Titulares têm o direito de solicitar aos controladores informações sobre o tratamento de seus dados (Princípios 4 e 6)
  - Titulares têm o direito de solicitar a atualização e correção de seus dados (Princípio 5);

PRINCÍPIOS

- **APLICABILIDADE (CONTINUAÇÃO):**
  - Controladores tem o dever de resguardar os dados pessoais de seus titulares, tomando preventivamente medidas de segurança, fazendo os investimentos devidos, adotando medidas e procedimentos explícitos em uma política de segurança da informação para que sejam evitados incidentes como ataques e vazamentos de dados; (Princípios 7 e 8);
  - Especialmente dados pessoais sensíveis ligados ao pensamento político, orientação sexual, origem racial ou étnica, convicção religiosa ou filosófica e dados biométricos ou genéticos não podem ser levados em consideração para nenhuma ação discriminatória por parte dos controladores(Princípio 9);

PRINCÍPIOS

- **APLICABILIDADE (CONTINUAÇÃO):**
  - Controladores estão sujeitos a multas e sanções, como paralisação das atividades, principalmente em caso de vazamento de dados por negligência do regramento da LGPD (Princípio 10);

LGPD

OS FISCAIS

OS FISCAIS

- **QUESTIONAMENTOS:**
  - Mas quem pode fiscalizar o cumprimento da LGPD no âmbito das organizações??
  - E se algo não for feito da maneira correta??
  - E se houver um tratamento abusivo de dados por parte de um controlador??
  - Ou mesmo um vazamento de dados por conta de uma falha de segurança onde dados pessoais de titulares podem ter sido acessados, modificados ou destruídos??

OS FISCAIS

- **ENCARREGADO DE DADOS (ou DPO - Data Protection Officer)** : Responsável no âmbito de uma organização por monitorar e verificar se os tratamentos de dados estão em conformidade com as boas práticas exigidas pela LGPD e como canal de comunicação entre os titulares e controladores e também com a ANPD.

- **ANPD (Autoridade Nacional de Proteção de Dados)**: Agência governamental responsável por proteger e zelar os dados pessoais que estão sob a guarda das diversas organizações controladoras e punir também por eventuais descumprimentos à LGPD. É também missão da ANPD orientar e regulamentar a aplicação da lei, bem como, formar um elo para com a sociedade a fim de receber sugestões, dúvidas e, até mesmo, denúncias.

OS FISCAIS

- **CONCEITOS IMPORTANTES**:
  - O encarregado pode ser uma pessoa física ou jurídica;
  - Suas informações de contato devem ser amplamente divulgadas;
  - Além de atender titulares, o encarregado deve estar em contato constante com a área técnica a fim de verificar se as políticas de segurança e privacidade estão sendo rigorosamente cumpridas e os tratamentos de dados estão em conformidade com boas práticas e em consonância com a LGPD;

OS FISCAIS

- **CONCEITOS IMPORTANTES (CONTINUAÇÃO):**

  - Caso constate alguma “não conformidade” é dever do encarregado notificar a área responsável e solicitar a correção do procedimento a fim de não se tornar corresponsável de um eventual incidente;
  - Um incidente é um evento que leva a destruição, perda, alteração, divulgação ou acesso não autorizado, de forma acidental ou ilícita;
  - Um plano de resposta a incidentes serve para orientar acerca dos procedimentos mais adequados a serem executados quando da ocorrência de incidentes com dados pessoais;

OS FISCAIS

- **CONCEITOS IMPORTANTES (CONTINUAÇÃO):**
  - A ANPD é responsável por verificar se o controlador e encarregado agiram de forma diligente, tentando entender a origem do incidente, as medidas protetivas implementadas, o porquê da falha e as medidas corretivas e remediadoras feitas para diminuir o impacto dos prejuízos causados aos titulares;
  - Ao longo do processo de averiguação do incidente, se a ANPD constatar que a organização, no papel de controladora de dados, não se adequou à LGPD, se encontra com processos de segurança da informação falhos e/ou com tratamento de dados abusivos, a lei permite que sejam aplicadas multas e sanções.

OS FISCAIS

- **CONCEITOS IMPORTANTES (CONTINUAÇÃO):**
  - As sanções somente serão aplicadas após procedimento administrativo que deverá permitir a ampla defesa ao infrator.
  - Sanções:
    - Advertência - Virá com um prazo para que a empresa se adeque à legislação. Se não corrigir no prazo estipulado, haverá penalidade;
    - Multa simples - Pode ser de até 2% do faturamento da pessoa jurídica. O limite é de 50 milhões de reais por infração;
    - Multa diária - Limitada a 50 milhões de reais;

OS FISCAIS

CONCEITOS IMPORTANTES (CONTINUAÇÃO):

- Sanções (continuação):
  - Publicização da infração - Os prejuízos à imagem da organização poderão ser enormes;
  - Bloqueio de tratamento dos dados pessoais - Sanção administrativa que impedirá que as organizações utilizem os dados pessoais coletados até a situação se regularizar.
  - Eliminação dos dados pessoais - Obrigará a eliminação por completo dos dados coletados em seus serviços, causando danos à operação normal da organização.
  - A LGPD prevê apenas sanções administrativas o que não impede que sigam processos em outras esferas, inclusive a criminal.

OS FISCAIS

CONCEITOS IMPORTANTES (CONTINUAÇÃO):

- Em uma sanção serão levadas em consideração:
  - Gravidade;
  - Reincidência;
  - Natureza da infração e dos direitos dos titulates afetados;
  - Boa fé;
  - Ocorrência de vantagem auferida ou pretendida;
  - Condição econômica;
  - Cooperação;
  - Entre outros..

OS FISCAIS

CONCEITOS IMPORTANTES (CONTINUAÇÃO):

- Mas e os órgãos públicos? Podem estar sujeitos à multas? E a eventual negligência de gestores públicos e servidores será tratada de alguma forma?

- Incidentes que envolvem entidades e órgãos públicos não estão sujeitos às sanções de multa, apenas advertência, publicização da infração, bloqueio e eliminação dos dados;

OS FISCAIS

CONCEITOS IMPORTANTES (CONTINUAÇÃO):

- Outras leis podem ser aplicadas em complementação a sanção administrativa, incluindo a própria responsabilização dos servidores públicos envolvidos:
  - Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal)
  - Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa)
  - Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)

LGPD

DADOS SENSÍVEIS

DADOS SENSÍVEIS

- Proteção a dados é fruto de antigas discussões e avanços sobre privacidade, direitos humanos e direitos constitucionais;

- Há determinados tipos de dados pessoais chamados de “sensíveis” que merecem uma atenção uma atenção redobrada;

- Dados sensíveis estão ligados ao pensamento político, orientação sexual, origem racial ou étnica, convicção religiosa e/ou filosófica e dados biométricos ou genéticos dos seus titulares.

DADOS SENSÍVEIS

- Para que uma organização possa tratar dados sensíveis, via de regra, deve haver o explicito consentimento do titular ou, então, hipóteses como cumprimento de lei, execução de política pública, estudos por órgãos de pesquisa, tutela de saúde, entre outros.

- Por que as instituições públicas precisam da informação da origem racial de seus alunos?

- O mau uso de dados sensíveis podem provocar, por exemplo, discriminação!

DADOS SENSÍVEIS

- A LGPD também determina que dados pessoais de crianças e de adolescentes deverão ter cuidados adicionais ao serem tomados e tratados em seu melhor interesse;

- Pelo Estatuto da Criança e do Adolescente (ECA), criança é a pessoa de até 12 anos de idade incompletos e adolescente aquela entre 12 e 18 anos;

- Para tratamento de dados de crianças até 12 anos de idade é necessário consentimento específico e em destaque, dado por pelo menos um dos pais ou responsável legal.

LGPD

DIREITOS DOS TITULARES

DIREITOS DOS TITULARES

- **CONSULTA AOS SEUS DADOS PESSOAIS**
  - Dados pessoais pertencem ao titular e como expressão do seu direito constitucional à privacidade e intimidade, o fornecimento destas informações deverão se dar no atendimento do seu interesse;

  - Há contudo casos em que a lei obriga o fornecimento dos dados pessoais como:
    - Compra de medicamentos de uso controlado;
    - Operações de Câmbio.

DIREITOS DOS TITULARES

- **CONSENTIMENTO PARA TRATAMENTO DE DADOS**
  - Afora as situações previstas em lei, dados pessoais somente poderão ser tratados com consentimento do titular, devendo este ser manifestado de forma expressa, informada e, preferencialmente, em destaque;

  - Importante ler o “aviso de privacidade”, pois é neste documento que será dito quais são os dados que serão capturados, como serão tratados e, ao final, se necessário for, será pedido a concordância com os termos apresentados.

DIREITOS DOS TITULARES

- **DIREITO DE INFORMAÇÃO**
  - A obrigação de informar a finalidade do tratamento não tem exceções na lei;
  - A operação dos dados ficará estritamente vinculada à finalidade informada;
  - Se a finalidade for modificada ao longo do tratamento, será necessário tomar novo consentimento quanto às alterações ocorridas;
  - Somente os dados estritamente pertinentes e necessários para a finalidade informada deverão ser tratados.

DIREITOS DOS TITULARES

- **DIREITO AO LIVRE ACESSO**
  - Livre acesso às informações sobre o tratamento dos dados que devem ser expressas de forma clara, precisa e de fácil acesso;
  - O titular poderá obter, a qualquer tempo e mediante requisição, a confirmação da existência de tratamento.
- **DIREITO A SEGURANÇA**
  - Os agentes de tratamento tem o dever de adotar medidas técnicas para garantir a proteção dos dados pessoais dos titulares contra brechas, acesso indevido, destruição, perda, alteração, comunicação ou difusão.

DIREITOS DOS TITULARES

- **DIREITO A NÃO-DISCRIMINAÇÃO**
  - A própria Constituição Federal proíbe a discriminação;
  - A LGPD reforça que o titular tem direito a não ser discriminado de forma ilícita ou abusiva com base nos dados pessoais.
- **REVISÃO DE DECISÕES AUTOMATIZADAS**
  - Dados pessoais podem servir de entrada para algoritmos que tipificam perfil pessoal, profissional, de consumo ou crédito;
  - Decisões de forma automatizada podem afetar os seus interesses e o titular tem direito a obter informações sobre os critérios e procedimentos utilizados no processo de decisão, além do direito de revisão dessas decisões.

DIREITOS DOS TITULARES

- **RESPONSABILIDADE DOS AGENTES DE TRATAMENTO**
  - Na ocorrência de danos à privacidade decorrentes do tratamento dos dados pessoais , a lei prevê a responsabilização dos agentes de tratamento e a correspondente indenização.

- **RETIFICAÇÃO, ANONIMIZAÇÃO, ELIMINAÇÃO OU BLOQUEIO DOS DADOS**
  - Sempre que possível, os dados devem ser anonimizados, ou seja, tratados de forma a não permitir a identificação do titular;
  - Dados desnecessários ou excessivos que não atendem a finalidade informada para o tratamento devem ser eliminados;

DIREITOS DOS TITULARES

- **RETIFICAÇÃO, ANONIMIZAÇÃO, ELIMINAÇÃO OU BLOQUEIO DOS DADOS (CONTINUAÇÃO)**

  - Retificação de dados incorretos ou incompletos;
  - Feita a solicitação pelo titular, o controlador deverá providenciar medida idêntica a todos os demais agentes com quem tenha realizado o uso compartilhado dos dados;
  - Dados não poderão ser eliminados quando a lei determinar sua conservação para cumprimento de obrigação legal ou regulatória pelo controlador.

DIREITOS DOS TITULARES

- **PORTABILIDADE DOS DADOS**
  - Através de requisição expressa, o titular pode levar seus dados para outro fornecedor de serviço ou produto, observados os segredos comercial e industrial.
  - Pode ser inócuo se não for regulado padrões para a interoperabilidade dos dados.

LGPD

BASES LEGAIS PARA TRATAMENTO

BASES LEGAIS PARA TRATAMENTO

- A execução de tratamentos de dados pessoais exige do controlador uma base legal;
- Um tratamento não pode ser um ato de livre arbítrio do controlador. Se assim o fizer, provavelmente, estará incorrendo em alguma ilegalidade;
- As bases legais são hipóteses da LGPD que autorizam o tratamento de dados pessoais;
- As bases legais não têm dependência ou predominância entre si. Para todo caso de tratamento de dados, a organização deverá definir qual base legal é a mais apropriada.

BASES LEGAIS PARA TRATAMENTO

EXECUÇÃO DE POLÍTICAS PÚBLICAS

- Quando o tratamento de dados pessoais é resguardado pelo interesse público ou por necessidade de uma autoridade oficial exercendo o papel de controlador;
- Base legal extremamente relacionada a realidade das instituições públicas de ensino;
- Ao receber os dados dos ENEM/SISU, tanto as IES (instituições de educação superior) quanto o INEP (Instituto Nacional de Estudos e Pesquisas Educacionais) e MEC estão executando políticas públicas;
- Assim, não é necessário o consentimento dos titulares para executar os tratamentos necessários aos registros de ingresso do aluno, mas continua sendo necessário informar a finalidade e a forma como o dado será tratado.

BASES LEGAIS PARA TRATAMENTO

CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA

- Possibilita que a LGPD não entre em conflito com outras legislações vigentes em nosso país;
- Instituições de ensino superior devem enviar anualmente ao INEP dados pessoais do seu alunado junto a informações da vida escolar a fim de que seja feito o Censo da Educação Superior;
- Trata-se de obrigação legal, não pode haver recusa!

BASES LEGAIS PARA TRATAMENTO

CONSENTIMENTO

- Declaração clara e inequívoca da concordância do titular com o uso dos seus dados para as finalidades propostas pelo controlador;
- Geralmente é a base legal utilizada na contratação ou aquisição de serviços ou produtos e mais alguns procedimentos adicionais desejados pelo controlador;
- Os termos estão contidos no aviso de privacidade que, de maneira ainda mais destacada, deve exibir as condições que envolvam dados sensíveis, dados de menores de idade e transferência internacional de dados.

BASES LEGAIS PARA TRATAMENTO

LEGÍTIMO INTERESSE

- Base legal mais flexível mas aplicação não é simples;
- Permite o uso dos dados, sem a necessidade de obtenção de consentimento;
- Porém deve ser feita uma análise rigorosa para ponderar os interesses do controlador e os direitos do titular;
- Quando usar:
  - O consentimento do titular for muito difícil de ser obtido ou considerado desnecessário;
  - Houver um impacto mínimo no indivíduo ou uma justificativa convincente para a sua utilização.

BASES LEGAIS PARA TRATAMENTO

LEGÍTIMO INTERESSE (CONTINUAÇÃO)

- O uso do legítimo interesse não pode contrariar outras diretrizes estabelecidas pela lei ou os direitos fundamentais do titular dos dados;
- A utilização do legítimo interesse deve ser uma escolha residual, ou seja, quando não for possível o enquadramento das outras bases legais.

BASES LEGAIS PARA TRATAMENTO

EXECUÇÃO CONTRATUAL

- Cumprir uma obrigação prevista em contrato ou em uma fase pré-contratual onde será necessário um tratamento preliminar de dados para validar e iniciar o acordo onde o titular de dados figurará como integrante;

- O titular dos dados não poderá revogar o fornecimento de dados a qualquer momento como no consentimento. O controlador estará resguardado pela LGPD enquanto durar a vigência do contrato.

BASES LEGAIS PARA TRATAMENTO

EXERCÍCIO REGULAR DE DIREITOS

- Dados pessoais tratados para a execução processual em ações judiciais.

PROTEÇÃO DA VIDA

- Uso de dados quando são indispensáveis para a proteção da vida ou da incolumidade física do titular ou de terceiros.

TUTELA DA SAÚDE

- Tratamento de dados para a tutela da saúde, desde que realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

BASES LEGAIS PARA TRATAMENTO

ESTUDOS POR ORGÃO DE PESQUISA

- Para fins de estudos em órgãos oficialmente credenciados como de pesquisa;
- Sempre que possível os dados devem ser anonimizados garantindo ao máximo a privacidade dos titulares.

PROTEÇÃO DE CRÉDITO

- Para a aprovação de crédito, reduzindo os riscos da transação, e também evitar que titulares se utilizem de uma brecha legislativa para criarem mecanismos de fuga de cobranças por dívidas contraídas.

BASES LEGAIS PARA TRATAMENTO

E QUANDO É POSSÍVEL COMPARTILHAR DADOS?

- Quando os dados forem indispensáveis para o controlador cumprir obrigações legais ou regulatórias;
- Quando o tratamento compartilhado de dados for necessário para a execução de políticas públicas;
- Para que os órgãos de pesquisa possam realizar estudos, sempre observando a anonimização de dados pessoais sensíveis;
- Para o exercício regular de direitos, incluindo contrato e processo judicial, administrativo e arbitral;

BASES LEGAIS PARA TRATAMENTO

E QUANDO É POSSÍVEL COMPARTILHAR DADOS?

- Em caso de proteção da vida ou segurança física do titular dos dados ou de terceiros;
- Para tutela de saúde, em procedimentos que devem ser realizados por profissionais ou serviços de saúde/autoridade sanitária;
- Para garantir que o titular dos dados esteja seguro e prevenido de fraudes, sempre observando o direito à informação e transparência garantido pela lei (exceto em casos onde a proteção dos dados seja fundamental para garantir direitos e liberdades).

BASES LEGAIS PARA TRATAMENTO

O compartilhamento de uma organização pública para uma privada só é permitido quando:

- Os dados a serem compartilhados já são de conhecimento público;
- Ocorrer execução descentralizada de alguma atividade sendo ressalvado que os dados somente poderão ser usados para esse fim;
- Houver previsão legal e a transferência se basear em termos como contratos ou convênios;
- For necessário para a prevenção de fraudes e proteção ao titular de dados.

LGPD

ADEQUAÇÃO

ADEQUAÇÃO

- Adequar uma organização à LGPD é um desafio que necessita de uma equipe multidisciplinar;
- Necessário também grande envolvimento da alta gestão;
- Fundamental que seja desenvolvida uma cultura de boas práticas no tratamento de dados pessoais;
- Exige-se uma mudança de mentalidade organizacional.

ADEQUAÇÃO

- O ideal é seguir alguma metodologia de implantação.
- Um comitê deve ser formado refletindo as diversas áreas necessárias à implantação:
  - TI (Segurança da Informação: Diagnóstico, política de segurança,...);
  - Jurídica (Revisão contratuais, aviso de privacidade, base legais,...);
  - Processo (Mapeamento de dados, relatório de impacto,...);
  - Ouvidoria (Recepção e encaminhamento de demandas de titulares);
  - Comunicação (Divulgação interna e externa, redes sociais, vídeos,...);
  - RH (Conscientização e treinamentos);

ADEQUAÇÃO

- Essa multidisciplinaridade é bem refletida em documentos como o plano de resposta a incidentes que descreve os procedimentos a serem executados quando da ocorrência de Incidentes;

- Nele devem estar contidas orientações relativas a segurança da informação, procedimentos jurídicos e a comunicação a ser feita para ANPD e titulares entre outras orientações, como a indicação das pessoas que irão participar da resposta ao incidente e suas respectivas responsabilidades.

LGPD

ÉTICA E BOAS PRÁTICAS

ÉTICA E BOAS PRÁTICAS

- Algumas práticas estão enraizadas em nosso dia a dia;
- É bastante comum, por muitas vezes, ao se executar atividades serem utilizadas planilhas, envio de informações por e-mail ou uso de relatórios em que parte do conteúdo está relacionado a dados pessoais;
- Deve-se evitar:
  - Exibir relatórios contendo dados pessoais à consulta pública;
  - Enviar informações pessoais através de e-mails, principalmente se for anexado planilhas e relatórios contendo tais informações.
- Tais ações de prevenção podem evitar tanto uma exposição pública desnecessária de dados pessoais, bem como, um incidente em caso da invasão a uma caixa de e-mail, por exemplo.

ÉTICA E BOAS PRÁTICAS

- No desenvolvimento de sistemas há de se levar em consideração técnicas que podem deixar a aplicação mais segura, como a exigência de senhas reforçadas, a implementação de auditorias e criptografia de dados (pseudonimização);
- **Princípios do "Privacy by Design":**
    1. Prevenção: adotar ações preventivas de segurança de tratamento de dados pessoais;
    2. Privacidade por padrão: projetar a configuração padrão de qualquer produto ou serviço visando sempre a privacidade dos dados;

- **Princípios do “Privacy by Design” (continuação):**
  3. Privacidade incorporada ao design: Incorporar a preocupação com privacidade desde a fase do design;
  4. Funcionalidade total: Exceções não devem ser feitas para acomodar a privacidade e a funcionalidade. Não deve haver dilemas!
  5. Proteção de ponta a ponta: a proteção desde quando os dados pessoais entram no sistema, são retidas, processadas com segurança e destruídas adequadamente;
  6. Foco centrado no usuário: Tornar privacidade uma preocupação importante fazendo com que sistemas sejam adequados para atender todas as necessidades de privacidade;
  7. Visibilidade e transparência: permitir que um titular conheça como os dados se movem pelo sistema, o nível de segurança que ele fornece, etc.

Para saber mais

- https://www.gov.br/mds/pt-br/acesso-a-informacao/lgpd
- https://www.lgpdbrasil.com.br/
- https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd
- https://getprivacy.com.br/exemplos-praticos-e-reais-de-aplicacao-da-lgpd/

Atividade de Fixação

- Faça uma breve pesquisa na internet explorando casos de violações de dados e suas consequências sob a LGPD.

- Exemplo recente:
  - Especialistas debatem aplicativo do estado de São Paulo instalado sem permissão
  - Link: https://encurtador.com.br/rANP9