

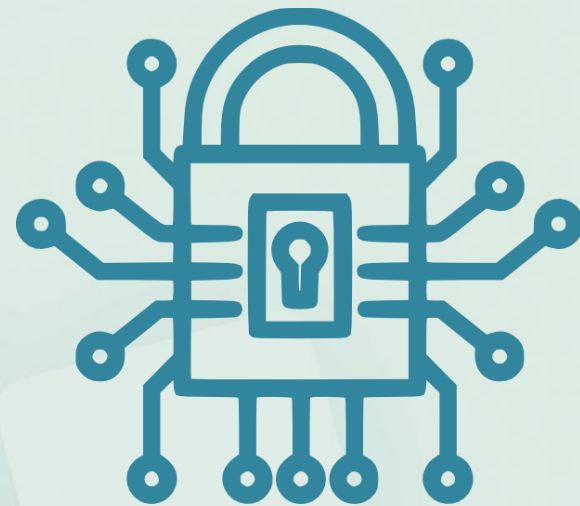


INSTITUTO FEDERAL

Sertão Pernambucano

Segurança da Informação

Leis e Normas



Prof. Heraldo Gonçalves Lima Junior

1. SOX (Sarbanes-Oxley)

1. SOX

- A Sarbanes-Oxley, ou simplesmente Sox, é uma lei criada nos Estados Unidos para aperfeiçoar os controles financeiros das empresas que possuem capital na Bolsa de Nova York.



1. SOX

- Esta lei veio em decorrência dos escândalos financeiros das empresas Enron, Worldcom e outras que pulverizaram as economias pessoais de muitos americanos. A lei foi promulgada em 30/07/2002 e prevê multas que variam de 1 milhão e 5 milhões de dólares e penas de reclusão entre 10 e 20 anos para os CEOs e CFOs das empresas.

1. SOX

- A SOX se estende além das empresas americanas, ou seja, se aplica a todas as empresas e suas respectivas subsidiárias registradas na SEC (Securities and Exchange Commission), as quais negociam suas ações nas bolsas de valores de NY.

NETSHOES



PagSeguro

1. SOX

- A seção mais importante da SOX em relação à Segurança da Informação é a 404 (Management Assessment of Internal Controls) que requer **conformidade com controles internos.**

2. Bacen 3380

2. Bacen 3380

- Em função de diversos escândalos envolvendo aspectos de ordem financeira (exemplo: fraudes em balanços) o Banco Central publica a resolução que trata da **implementação de controles voltados à Segurança e Tecnologia da Informação e Gestão de Riscos.**

2. Bacen 3380

- A resolução Bacen 3380 determina às instituições financeiras autorizadas a operar pelo Banco Central do Brasil a **implementação de estrutura de ger. do risco operacional.**



2. Bacen 3380

- Risco Operacional inclui: fraudes internas e externas, eventos que acarretam a interrupção das atividades, falhas em sistemas de tecnologia, falhas na execução, cumprimento de prazos e gerenciamento das atividades da instituição.

2. Bacen 3380

- Pontos Críticos:
 - Estrutura de Gestão de Riscos;
 - Documentação e Armazenamento das Informações;
 - Política de Gerenciamento de Riscos;
 - Contingência e Estratégias de Continuidade de Negócios;

2. Bacen 3380

- Treinamento, Monitoramento das ações e desenvolvimento da cultura de gestão de riscos.

3. CVM (Comissão de Valores Mobiliários)

3. CVM (Comissão de Valores Mobiliários)

- 12/03/07: movimento atípico com ações do grupo ipiranga negociadas na bovespa;
- 16/03/07: as ações da distribuidora sobem 33,33% e a semana termina com um volume inexplicável de investimentos em ações do grupo;

3. CVM (Comissão de Valores Mobiliários)

- 19/03/07: Petrobras, Ultra e Brasken oficializam o anúncio de compra do Grupo Ipiranga.
- 26/03/07: Um gerente da Petrobras está sob suspeita de ter lucrado mais de R\$ 900 mil com uso de informação privilegiada.

3. CVM (Comissão de Valores Mobiliários)

- **Instrução CVM 380/2002:**
 - Estabelece normas e procedimentos a serem observados nas operações realizadas em bolsas e mercados de balcão organizado por meio de rede mundial de computadores ...

3. CVM (Comissão de Valores Mobiliários)

- **Instrução CVM 380/2002:**
 - Art. 7: Compete às corretoras eletrônicas garantir a segurança e sigilo de toda a informação sobre seus clientes.

3. CVM (Comissão de Valores Mobiliários)

- **Instrução CVM 380/2002:**
 - Art. 8: As corretoras são responsáveis pela operação de seus sistemas, ainda que os esses sejam mantidos por terceiros..

4. CFM (Conselho Federal Medicina)

4. CFM (Conselho Federal Medicina)

- O CFM manifesta como uma das suas maiores preocupações a preservação do sigilo das informações existentes no prontuário, em qualquer formato (eletrônico e impresso).



4. CFM (Conselho Federal Medicina)

- Para proteger as informações sensíveis, o CFM tem editado resoluções que tratam da **disponibilidade do prontuário** (CFM 1605/2000), da **sua privacidade** (CFM 1638/2002 e CFM 1639/2002 – essa sobre **guarda e manuseio do prontuário...**



5. Lei Geral de Proteção de Dados Pessoais (LGPD)

5. LGPD

- A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece **diretrizes importantes e obrigatórias para a coleta, processamento e armazenamento de dados pessoais**. Ela foi inspirada na GDPR (General Data Protection Regulation), que entrou em vigência em 2018 na União Europeia, trazendo grandes impactos para empresas e consumidores.

5. LGPD

- Diante dos atuais casos de uso indevido, comercialização e vazamento de dados, as novas regras garantem a privacidade dos brasileiros, além de evitar entraves comerciais com outros países.



5.1. LGPD: Quem fiscaliza?

- Com a sua criação veio também a criação da Autoridade Nacional de Proteção de Dados (ANPD), que será a agência responsável pela fiscalização, administração e cumprimento da (LGPD).



5.2. LGPD: Objetivos

- Assegurar o **direito à privacidade e à proteção de dados pessoais** dos usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais.
- Estabelecer **regras claras sobre o tratamento de dados** pessoais.

5.2. LGPD: Objetivos

- Fortalecer a **segurança das relações jurídicas e a confiança do titular** no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo.
- Promover a concorrência e a livre atividade econômica, inclusive com **portabilidade de dados**.

5.3. LGPD: Dados

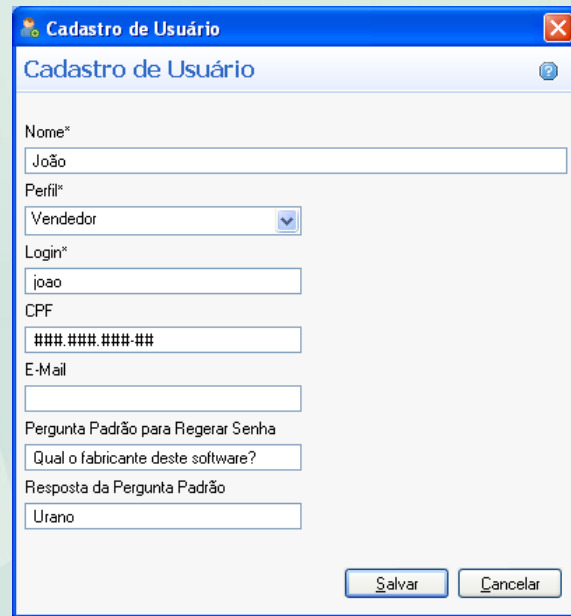
- **Dados pessoais:** informação relacionada a pessoa natural identificada ou identificável;
- **Dados pessoais sensíveis:** origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

5.3. LGPD: Dados

- **dados jurídicos:** CNPJ, razão social, endereço, entre outros identificáveis.

5.4. LGPD: Agentes

- **O titular:** que é toda pessoa física ou jurídica detentora dos dados.
- **O controlador:** a empresa ou pessoa física que faz a coleta destes dados.



Cadastro de Usuário

Cadastro de Usuário

Nome*
João

Perfil*
Vendedor

Login*
joao

CPF
###.###.###-##

E-Mail

Pergunta Padrão para Regerar Senha
Qual o fabricante deste software?

Resposta da Pergunta Padrão
Urano

Salvar Cancelar

5.4. LGPD: Agentes

- **O operador:** o operador é que realiza o tratamento e processamento destes dados e podendo ser a empresa ou pessoa física também.
- **O encarregado:** a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares e a ANPD.

5.5. LGPD: Consentimento

- Na LGPD, o consentimento do titular dos dados é considerado elemento essencial.
- **A lei traz várias garantias ao cidadão, como: poder solicitar que os seus dados pessoais sejam excluídos; revogar o consentimento; transferir dados para outro fornecedor de serviços, entre outras ações.**

5.6. LGPD: O que muda para as empresas?

- Qualquer empresa que lide com dados de clientes e ou outras empresas, precisa se adequar a LGPD.
- Essa adequação significa **adotar novos procedimentos que garantam um maior transparência, controle e segurança da informação que gerencia.**

5.7. LGPD: Quais sanções são aplicadas por não cumprimento?

- As sanções podem variar entre uma simples advertência, com indicação de prazo para adoção de medidas corretivas, até mesmo multas que podem chegar a 50 milhões de reais, por infração.

Obrigado!
Vlw! Flw!



INSTITUTO FEDERAL
Sertão Pernambucano