Sistemas de Informação

PUC Minas

Segurança de Sistemas de Informação

Aula 4: Normas para Gestão da Segurança da Informação

Prof. Fábio Leandro Rodrigues Cordeiro, Me.

Objetivos

1) Apresentar a evolução e o objetivo de cada uma das principais normas que fazem parte da ISO 27000;
2) Discutir os objetivos de controle do Código de Prática para Gestão da Segurança da Informação;
3) Descrever a relação entre normas, leis e recomendações.

Sumário

Introdução

O que são e para que servem as normas?

É aquilo que se estabelece como medida para a realização de uma atividade.

Uma norma tem como propósito definir regras e instrumentos de controle para assegurar a conformidade de um processo, produto ou serviço.

Conceitos

Objetivo da Normalização

Conforme definido pela Associação Brasileira de Normas Técnicas (ABNT), os objetivos da normalização são:

Comunicação: proporcionar meios mais eficientes na troca de informação entre o fabricante e o cliente, melhorando a confiabilidade das relações comerciais e de serviços;

Segurança: proteger a vida humana e a saúde;

Conceitos

Objetivo da Normalização

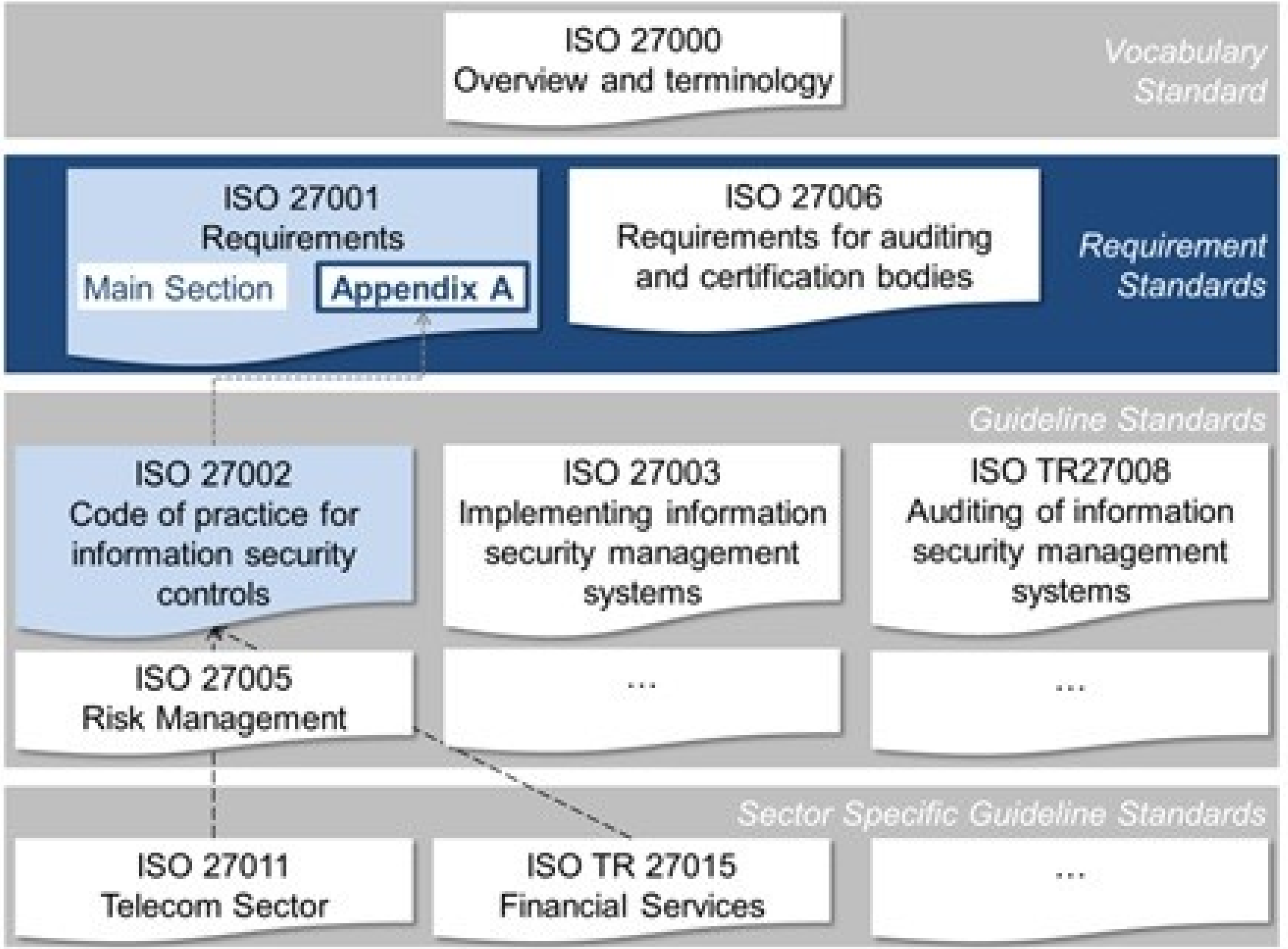
Conforme definido pela Associação Brasileira de Normas Técnicas (ABNT), os objetivos da normalização são:

Proteção ao consumidor: prover a sociedade mecanismos eficazes para aferir qualidade de produtos;

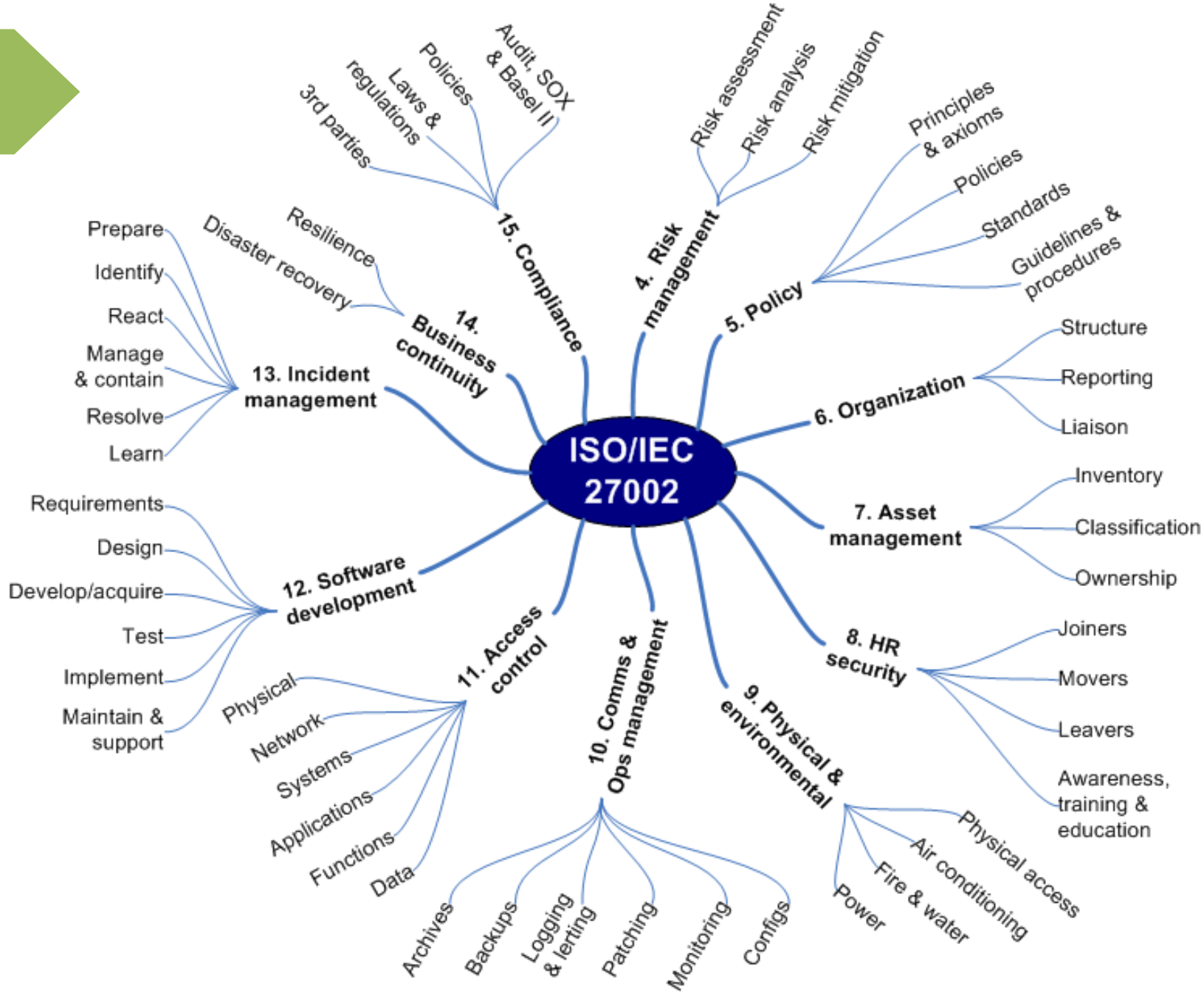
Eliminação de barreiras comerciais: evitar a existência de regulamentos conflitantes sobre produtos e serviços em diferentes países, facilitando assim, o intercâmbio comercial.

ISO 27000

Visão Geral da ISO 27000



ISO 27002


ISO/IEC 27002
15. Compliance
Audit, SOX & Basel II
Policies
Laws & regulations
3rd parties
4. Risk management
Risk assessment
Risk analysis
Risk mitigation
5. Policy
Principles & axioms
Policies
Standards
Guidelines & procedures
6. Organization
Structure
Reporting
Liaison
7. Asset management
Inventory
Classification
Ownership
8. HR security
Joiners
Movers
Leavers
Awareness, training & education
9. Physical & environmental
Physical access
Air conditioning
Fire & water
Power
10. Comms & Ops management
Archives
Backups
Logging & lerting
Patching
Monitoring
Configs
11. Access control
Physical
Network
Systems
Applications
Functions
Data
12. Software development
Requirements
Design
Develop/acquire
Test
Implement
Maintain & support
13. Incident management
Prepare
Identify
React
Manage & contain
Resolve
Learn
14. Business continuity
Resilience
Disaster recovery

ISO 27002 – Código de Prática

Seções, Categorias e Controles

- Política de Segurança da Informação (1)
- Organizando a Segurança da Informação (2)
- Gestão de Ativos (2)
- Segurança em Recursos Humanos (3)
- Segurança Física e do Ambiente (2)
- Gestão de Operações e Comunicações (10)
- Controle de Acesso (7)
- Aquisição, Desenvolvimento e Manutenção de SI (6)
- Gestão de Incidentes de SI (2)
- Gestão da Continuidade do Negócio (1)
- Conformidade (3)

ISO 27002 – Código de Prática

Estrutura da Norma

5. Política de Segurança da Informação (1) **--> Seção**

5.1 Política de Segurança da Informação **--> Categoria**

Objetivo: “Prover uma orientação de apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes”

[--- Controles ---]

5.1.1 Documentos da Política de Segurança da Informação

“Convém que um documento da política de SI seja aprovado pela direção ...”

5.1.2 Análise Crítica da Política de SI

“Convém que a politica de SI seja analisada criticamente a intervalos planejados ou quando mudanças...

ISO 27002 – Código de Prática

Estrutura da Norma

5. Política de Segurança da Informação (1)

5.1 Política de Segurança da Informação

ISO 27002 – Código de Prática

Estrutura da Norma

6. Organizando a Segurança da Informação (2)

6.1 Infraestrutura da Segurança da Informação

6.2 Partes Externas

ISO 27002 – Código de Prática

Estrutura da Norma

7. Gestão de Ativos (2)

7.1 Responsabilidade pelos Ativos

7.2 Classificação da Informação

ISO 27002 – Código de Prática

Estrutura da Norma

8. Segurança em Recursos Humanos (3)

8.1 Antes da Contratação

8.2 Durante a Contratação

8.3 Encerramento ou mudança da Contratação

ISO 27002 – Código de Prática

Estrutura da Norma

9. Segurança Física e do Ambiente (2)

9.1 Áreas Segura

9.2 Segurança de Equipamentos

ISO 27002 – Código de Prática

Estrutura da Norma

10. Gestão de Operações e Comunicações (10)

10.1 Procedimentos e Responsabilidades Operacionais

10.2 Gerenciamento de Serviços Terceirizados

10.3 Planejamento e Aceitação dos Sistemas

10.4 Proteção contra Códigos Maliciosos e Códigos Móveis

10.5 Cópias de Segurança

10.6 Gerenciamento de Segurança em Redes

10.7 Manuseio de Mídias

10.8 Troca de Informações

10.9 Serviços de Comércio Eletrônico

10.10 Monitoramento

ISO 27002 – Código de Prática

Estrutura da Norma

11. Controle de Acesso (7)

11.1 Requisitos de Negócio para Controle de Acesso

11.2 Gerenciamento de Acesso do Usuário

11.3 Responsabilidades dos Usuários

11.4 Controle de Acesso à Rede

11.5 Controle de Acesso ao SO

11.6 Controle de Acesso à Aplicação e à Informação

11.7 Computação Móvel e Trabalho Remoto

ISO 27002 – Código de Prática

Estrutura da Norma

12. Aquisição, Desenvolvimento e Manutenção de SI (6)

12.1 Requisitos de Segurança de Sistemas de Informação

12.2 Processamento Correto nas Aplicações

12.3 Controles Criptográficos

12.4 Segurança dos Arquivos do Sistema

12.5 Segurança em Processos de Desenvolvimento e de Suporte

12.6 Gestão de Vulnerabilidades Técnicas

ISO 27002 – Código de Prática

Estrutura da Norma

13. Gestão de Incidentes de SI (2)

13.1 Notificação de Fragilidades e Eventos de SegInfo

13.2 Gestão de Incidentes de SegInfo e Melhorias

Estrutura da Norma

14. Gestão da Continuidade do Negócio (1)

14.1 Aspectos da Gestão da Continuidade do Negócio, relativo à Segurança da Informação

Estrutura da Norma

15. Conformidade (3)

15.1 Conformidade com os Requisitos Legais

15.2 Conformidade com Normas e Políticas de SI e Técnicas

15.3 Considerações quanto à Auditoria

Leis e Regulamentos

Objetivo

A seguir serão apresentadas algumas informações básicas sobre leis e regulamentações que possuem relação (impacto) direto na segurança da informação de instituições que estão posicionadas em diferentes mercados.

O atendimento dessas leis e regulamentações são amparadas pelos controles mencionados anteriormente.

Leis e Regulamentos

Definições

Lei: é a regra jurídica escrita emanada do poder competente;

Resolução: espécie de norma utilizada pelo poder público ou autoridade para regulamentar alguma situação que guarde relação com as suas atribuições.

Leis e Regulamentos

Definições

Common Law e **Civil Law**: os países que adotam o sistema common law utilizam-se dos costumes para julgar os conflitos que surgem entre as pessoas (Inglaterra). Já os países que adotam o civil law têm a lei como principal fonte para julgamento dos conflitos (América latina);

Leis e Regulamentos

Definições

Nos últimos anos observou-se a publicação de muitas leis e regulamentações (em âmbito nacional e internacional) cujo escopo contempla aspectos de Segurança da Informação. Por exemplo:

- SOX (Sarbanes-Oxley)
- Bacen 3380 (Banco Central)
- CFM (Conselho Federal de Medicina)
- LGPD (Lei Geral de Proteção de Dados Pessoais - Lei 13.709/18

Leis e Regulamentos

SOX (Sarbanes-Oxley)

Em 30 de julho de 2002, George W. Bush, então presidente dos Estados Unidos da América, assinou a lei Sarbanes-Oxley (Sarbanes-Oxley Act 2002), também conhecida como SOX ou Sarbox. Esta lei foi criada por dois congressistas americanos, Paul Sarbanes e Michael Oxley.

Leis e Regulamentos

SOX (Sarbanes-Oxley)

Eles foram motivados pela onda de escândalos de fraudes em empresas como Enron, WorldCom e Tyco, os quais fizeram com que houvesse uma diminuição da confiança pública nas práticas financeiras e contábeis das empresas.

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.

Leis e Regulamentos

SOX (Sarbanes-Oxley)

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

A seção 404 da SOX tem um impacto significativo na segurança da informação, pois exige que as empresas avaliem e reportem a eficácia de seus controles financeiros e de segurança da informação, ajudando a garantir a integridade e a proteção das informações financeiras e a prevenir fraudes.

Leis e Regulamentos

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.**

Leis e Regulamentos

Bacen 3380

A resolução Bacen 3380 determina as instituições financeiras autorizadas a operar pelo Banco Central do Brasil a implementação de estrutura de gerenciamento do risco operacional.

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.

Leis e Regulamentos

Bacen 3380

Pontos de Responsabilidade: **Due Dilligence** (demonstra que a empresa está realizando as atividades de Segurança de maneira constante).
Aqui é importante observar a necessidade de um processo de investigação que as Ifs devem realizar antes contratar fornecedores e terceirizados relacionados a S.I.

Due Care (demostra que a alta direção tomou as ações necessárias para proteger a empresa). O foco em implementar mecanismo de proteção às informações financeiras dos clientes garantindo integridade dos sistemas de informação.

Leis e Regulamentos

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

Leis e Regulamentos

CFM (Conselho Federal de 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).

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...

Leis e Regulamentos

CFM (Conselho Federal de Medicina)

- Manutenção do sigilo das informações médicas dos pacientes, divulgadas apenas com consentimento do paciente ou determinação legal.
- Obrigatoriedade de manter o prontuário atualizado e completo e em local seguro.
- Prontuário deve ser arquivado por no mínimo 20 a partir do último lançamento.

Não trata diretamente de dados pessoais, no entanto estabelece diretrizes importantes para o sigilo e a privacidade dos pacientes que são consideradas informações sensíveis.

Leis e Regulamentos

Marco Civil da Internet

- O Marco Civil da Internet é uma lei brasileira que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
- Foi criado para garantir a liberdade de expressão, a privacidade dos usuários e a neutralidade da rede, entre outros aspectos.
- Estabelece que o provedor de acesso à Internet não pode monitorar ou filtrar o conteúdo acessado pelos usuários, exceto em casos de ordem judicial.
- Os ISPs ou provedores de aplicação (sites, redes sociais, etc.) devem respeitar a privacidade dos usuários e manter a segurança dos dados pessoais coletados.

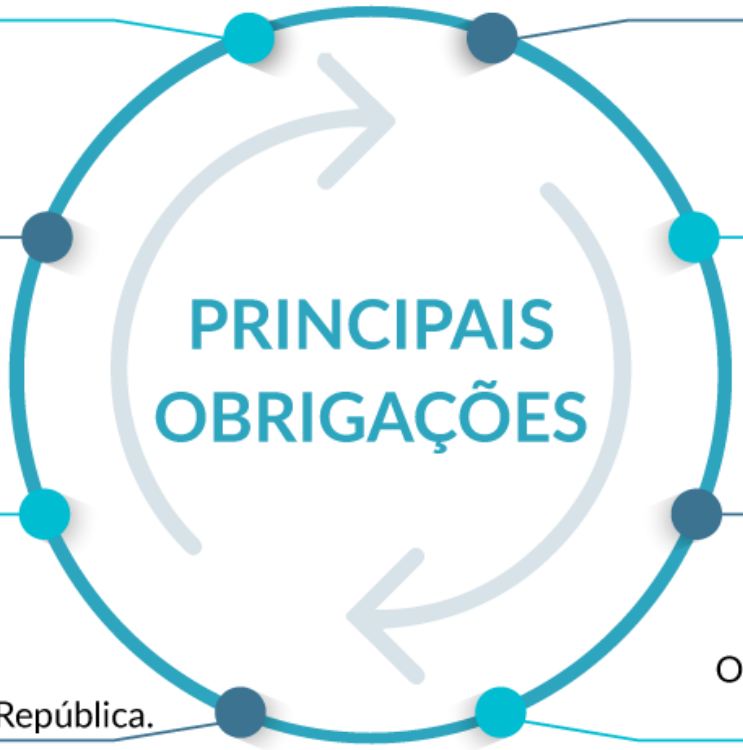
Leis e Regulamentos

Marco Civil da Internet

- O Marco Civil da Internet estabelece que os ISPs devem armazenar os dados pessoais por um período de no mínimo 6 meses para eventuais investigações de âmbito legal.
- As politicas de privacidade dos ISPs devem ser informadas aos usuários de maneira clara e objetiva através de termos de uso.
- A lei estabelece que o acesso à Internet é um direito fundamental, e que o Estado deve promover a inclusão digital e a universalização do acesso à rede.
- Existem regras em relação ao armazenamento de dados de usuários em servidores fora do pais com previsões de sanções para descumprimento de normas estabelecidadas.

Leis e Regulamentos

Lei Geral de Proteção de Dados



Qualquer empresa ou órgão público deve ser **responsabilizado em caso de violação à lei.**

Órgãos públicos devem organizar dados de forma **interoperáveis e estruturados.**

Multa diária de **até 2% do faturamento**, com limite de R$ 50 milhões.

MP 869/18 Cria a **Autoridade Nacional de Proteção de Dados**, vinculada à Presidência da República.

Conceitua dado pessoal, **dado sensível, dado pseudonimizado e dado anonimizado.**

Tratamento de dados pessoais no Brasil **em meios digitais ou não.**

Empresa ou órgão público só poderá fazê-lo se tiver **consentimento do titular.**

O titular pode retirar seu **consentimento, pedir a exclusão ou a portabilidade** de seus dados.

Leis e Regulamentos

Lei Geral de Proteção de Dados

A **LGPD** cobri operações de tratamento realizadas no Brasil, ou a partir de da coleta de dados feita no país por empresas brasileiras ou estrangeiras.

Abrange também empresas ou entes que ofertem bens e serviços ou tratem informações de pessoas que estão no Brasil.

Possui cobertura em relação a transferência de dados internacional, desde que o país envolvido na troca de dados tenha níveis equiparados às exigências pela LGPD.

São mais de 100 países que possuem lei sobre o assunto que rege o cotidiano dos usuários, empresas e Poder Público.

Referências

Notas de Aula: Prof. Prof. Leonardo Lemes Fagundes.

ISO 27001 Security. Information Security Compliance. 2011.

ABNT NBR ISO/IEC 27002:2006. Código de Prática para a Gestão da Segurança da Informação, 2006.

Kpmg. Seção 404 da Lei Sarbanes-Oxley: Certificação dos Controles Internos pela Administração Respostas às perguntas mais frequentes.

PROTIVIT. LGPD – Abordagem para adequação. 2019. https://www.protiviti.com/BR-por/protecao-de-dados-pessoais