# Segurança da informação

Leis e regulamentações

# 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

# O que são e para que servem as normas?

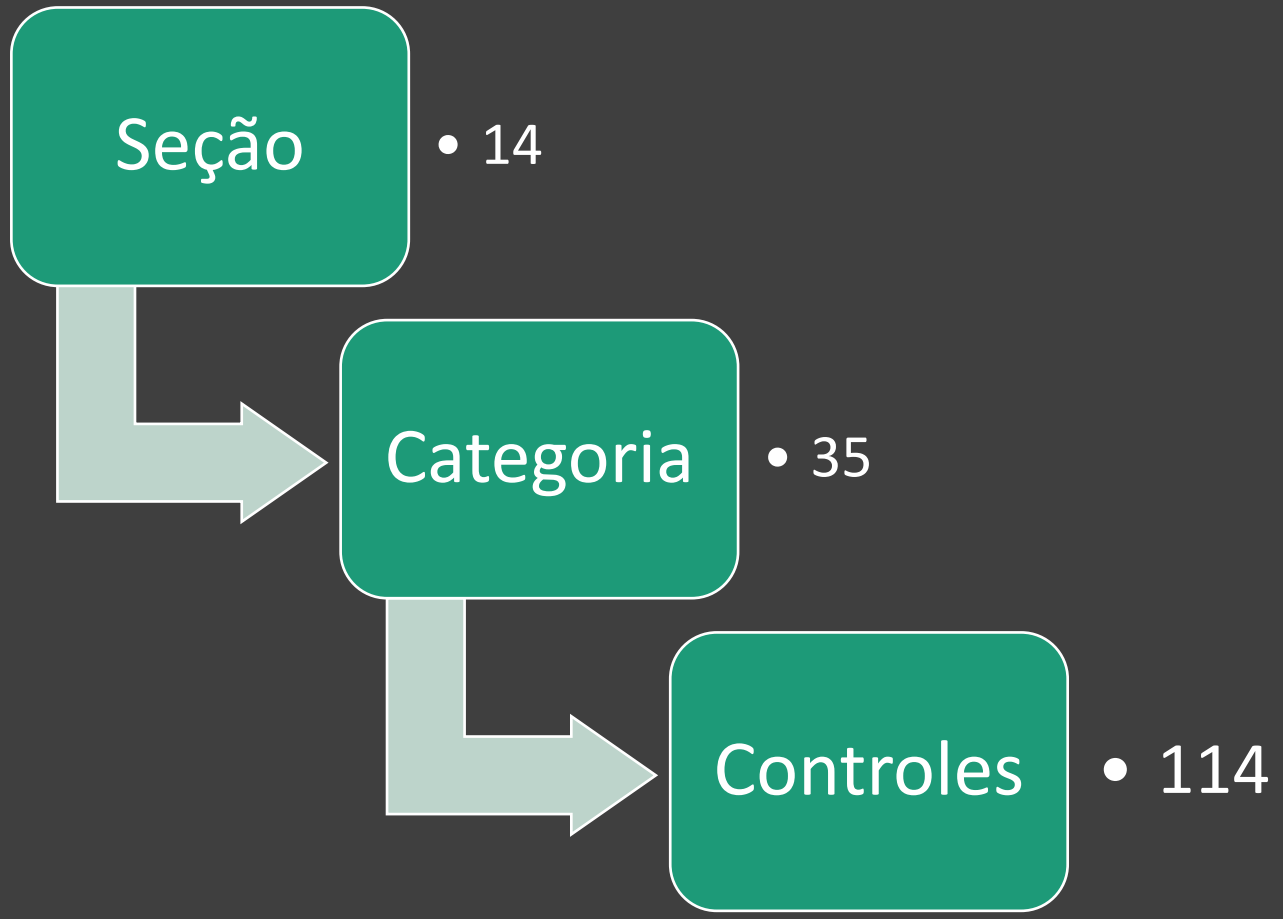
Conforme definido pela Associação Brasileira de Normas Técnicas (ABNT), os objetivos da normalização são:

- Comunicação
- Segurança
- Proteção do computador
- Eliminação de barreiras técnicas e comerciais

# ISO 27002 – Códigos de práticas

- Seções (categorias)
- Política de segurança da informação
- Organizando a segurança da informação
- Gestão de ativos
- Segurança em recursos humanos
- Segurança física e do ambiente
- Gestão de operações e Comunicações
- Controle de acesso
- Aquisição, desenvolvimento e manutenção de SI
- Gestão de incidentes de SI
- Gestão de continuidade de negócio
- Conformidade

# ISSO 27002 - estrutura



# ISO 27002 - Estrutura

5. Política de Segurança da informação

5.1 Política de segurança da informação

# ISO 27002 - Estrutura

6. Organizando a Segurança da Informação

6.1 Infraestrutura da Segurança da informação

6.2 Partes externas

# ISO 27002 - Estrutura

7. Gestão de ativos

7.1 Responsabilidade pelos Ativos

7.2 Classificação da Informação

# ISO 27002 - Estrutura

8. Segurança em Recursos Humanos

8.1 Antes da contratação

8.2 Durante a Contratação

8.3 Encerramento ou mudança de Contratação

# ISO 27002 - Estrutura

9. Segurança Física e do ambiente

9.1 Áreas Segura

9.2 Segurança de equipamentos

# ISO 27002 - Estrutura

10. Gestão de Operações e Comunicações
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 Trocas de informações
10.9 Serviços de comércio eletrônico
10.10 Monitoramento

# ISO 27002 - Estrutura

11. Controle de Acesso

11.1 Requisitos de negócios 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 - Estrutura

12. Aquisição, desenvolvimento e manutenção de SI

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 - Estrutura

13. Gestão de incidentes

13.1 Notificação de fragilidades e eventos de Seginfo

13.2 Gestão de incidentes de Seginfo e Melhorias

# ISO 27002 - Estrutura

14. Gestão da continuidade do negócio

14.1 Aspectos de gestão da continuidade do negócio, relativo à segurança da informação

# ISO 27002 - Estrutura

15. Conformidade

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 Regulamentações

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

# Leis e regulamentações

- Lei: é uma 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 regulamentações

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

- **SOX** (Sarbanes-Oxley)
- **Bacen** 3380 (Banco central)
- **CVM** (Comissão de Valores Imobiliários)
- **CFM** (Conselho Federal de Medicina)
- **GDPR** (General Data Protection Regulation)
- **LGPD** ( Lei Geral de Proteção de Dados)

# Atividade

Pesquisar sobre as leis e regulamentações descritas anteriormente e documentar sobre o histórico de cada uma e sua relação com a Segurança da informação.