SÃO PAULO
GOVERNO DO ESTADO

Centro Paula Souza

Fatec Mauá

CST Desenvolvimento de Software Multiplataforma (DSM)

Disciplina: ISG-022 – SEGURANÇA NO DESENVOLVIMENTO DE APLICAÇÕES (SDA)

Tópico 02: CONFORMIDADE E OS ASPECTOS LEGAIS DA SI

SUMÁRIO

Fatec Mauá

1. Objetivo da Aula – Tópico da Ementa
2. Função de Conformidade
3. Regulamentação Internacional
4. Regulamentação Nacional de SI
5. Normas ABNT, ISO e IEC e SI
6. Modelos de Segurança da Informação (SI)

1. OBJETIVO E EMENTA

Fatec Mauá

- **Objetivo da Aula**

  Apresentar visões gerais sobre segurança da informação, os conceitos e a estrutura do sistema de gestão de segurança da informação (SI)

- **Tópico da Ementa**

  Conceitos fundamentais do pilar de segurança.

2. FUNÇÃO DE CONFORMIDADE

Fatec Mauá

❖ DEFINIÇÃO DE COMPLIANCE

➢ **Compliance** é um processo de negócio com o objetivo de **garantir** que uma organização esteja em **conformidade** ou em **aderência** com as políticas, diretrizes, regulamentos, legislações, procedimentos, normas e padrões estabelecidos para a realização das suas atividades, **cumprindo** e **fazendo cumprir** todas as **regras internas** e **externas** do **negócio**.

2. FUNÇÃO DE CONFORMIDADE

❖ FUNÇÃO DE COMPLIANCE

- A **função de compliance** é um grupo de **atividades** e **competências** especializadas para gerenciar o cumprimento das **regras de negócio** de uma instituição.
- Deve ser **compatível** com a natureza, o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio.
  E, pode estar sob a responsabilidade de uma **unidade de compliance**.

2. FUNÇÃO DE CONFORMIDADE

Fatec Mauá

❖ ORGANIZAÇÃO DE COMPLIANCE

- Uma **unidade de compliance** específica deve estar subordinada ao conselho de administração ou à diretoria, **segregada** das áreas de negócio e da auditoria interna.
- A **função de compliance** depende do comprometimento da alta administração e de todos os funcionários para estar integrada aos pilares da **governança corporativa** e à cultura organizacional.

2. FUNÇÃO DE CONFORMIDADE

Fatec Mauá

❖ RISCOS DE COMPLIANCE

Os **risco de conformidade** são as **ameaças**, resultantes de descumprimento das regras do negócio, que **podem afetar** uma instituição:

- **sanções legais ou regulamentares:** ações judiciais, multas, indenizações ...
- **perdas financeiras:** custos de litígio, interrupção dos negócios ...
- **perdas materiais:** adaptações às exigências, suspensão de operações ...

2. FUNÇÃO DE CONFORMIDADE

Fatec Mauá

❖ RISCOS DE COMPLIANCE

- **perdas de reputação:** percepção pública negativa, redução da confiança e fidelidade..
- **limitações estratégicas:** incapacidade de adaptação, perdas de novos mercados ...
- **falhas de gestão:** tomadas de decisão ruins, governança corporativa ineficaz ...
- **danos de terceiros:** fornecedores, parceiros e outros em não conformidade ...

2. FUNÇÃO DE CONFORMIDADE

Fatec Mauá

❖ PROGRAMA DE COMPLIANCE

Um **conjunto de elementos-chave** em uma organização para prevenir, detectar e corrigir as violações ao **cumprimento das regras de negócio**, minimizando os riscos de compliance:

1. **Políticas e Procedimentos:** condutas e operações de compliance, com apoio e compromisso da alta administração.
2. **Oficial e/ou Comitê de Compliance:** responsável c/ autoridade e independência.

2. FUNÇÃO DE CONFORMIDADE

Fatec Mauá

❖ PROGRAMA DE COMPLIANCE

3. **Práticas e Mecanismos:** inventário de normas e riscos e medidas de proteção.
4. **Respostas às Violações de Compliance:** investigações, correções e prevenções.
5. **Melhoria Contínua:** monitoração, revisão e atualização regulares do programa.
6. **Cultura de Compliance:** comunicação, treinamento e educação, valorizando integridade e ética.

3. REGULAMENTAÇÃO INTERNACIONAL

Fatec Mauá

- **General Data Protection Regulation (GDPR)** – UE: regula a proteção de dados e privacidade para todos os indivíduos dentro da União Européia e do Espaço Econômico Europeu. Base para LGPD.
- **United Nations Convention Against Corruption (UNCAC)** – um tratado anticorrupção universal, que cobre muitos aspectos da luta contra a corrupção, incluindo prevenção, criminalização, cooperação internacional e recuperação de ativos.

3. REGULAMENTAÇÃO INTERNACIONAL

Fatec Mauá

- **Sarbanes-Oxley Act (SOX)** – EUA: exige a conformidade com a prática de governança corporativa e divulgação financeira. Tem implicações internacionais para empresas estrangeiras com ações em bolsas dos EUA.

- **Public Company Accounting Oversight Board (PCAOB)** – EUA: entidade privada sem fins lucrativos estabelecida pelo Congresso dos EUA como parte da Lei SOX para a auditoria de empresas com ações em bolsas de valores.

3. REGULAMENTAÇÃO INTERNACIONAL

Fatec Mauá

❖ NORMAS ISO E IEC

- **ISO – International Organization for Standardization**

  Federação mundial de Organismos Nacionais de Normalização, tendo somente um representante por país. No Brasil **ABNT**.

- **IEC – International Electrotechnical Commision**

  Organização mundial líder que prepara e publica Normas Internacionais para as áreas elétrica, eletrônica e tecnologias relacionadas.

3. REGULAMENTAÇÃO INTERNACIONAL

Fatec Mauá

❖ FRAMEWORKS INTERNACIONAIS

- **Modelos de Referência** baseados em processo, vigentes e reconhecidos pelo mercado profissional.
- Um **framework** normalmente é composto por uma grande e abrangente base de conhecimento (**body of knowledge**).

- Exemplos:
  - **ITIL** - Information Technology Infrastructure Library
  - **COBIT** - Control Objectives For Information And Related Technology
  - **PMBOK** - Project Management Body of Knowledge

4. REGULAMENTAÇÃO NACIONAL DE SI

Fatec Mauá

1) **2023 - PR - Decreto nº 11.856** – Política e Comitê Nacionais de Cibersegurança
2) **2020 – PR – Decreto nº 10.222** – Estratégia Nacional de Segurança Cibernética
3) **2019 – PR – Lei nº 13.853 – Autoridade Nacional de Proteção de Dados (ANPD)**
4) **2018 – PR – Lei nº 13.709 – Lei Geral de Proteção de Dados (LGPD).** Baseada na GDPR.
5) **2018 – PR – Instrução Normativa nº 1 da GSI** – Política de Segurança da Informação
6) **2016 – PR – Decreto nº 8.771** – Regulamenta o Marco Civil da Internet

4. REGULAMENTAÇÃO NACIONAL DE SI

Fatec Mauá

7) **2014 – PR – Lei nº 12.965** – Marco Civil da Internet – "Constituição da Internet" no Brasil
8) **2013 – PR – Lei nº 12.846** – Lei Anticorrupção contra Adm. Pública Nacional ou Estrangeira
9) **2012 – PR – Lei nº 12.737** – Lei de Crime Cibernéticos – "Lei Carolina Dieckmann"
10) **2011 – PR – Lei nº 12.529** – Lei Antitruste – Aplicada pelo CADE (Cons. Adm. Def. Econômica)
11) **2011 – PR – Lei nº 12.525** – Lei de Acesso à Informação (LAI)
12) **1998 – PR – Lei nº 9.613** – Lei de Lavagem de Dinheiro – Ocultação de Bens, Direitos e Valores

4. REGULAMENTAÇÃO NACIONAL DE SI

Fatec Mauá

13) 1998 – PR – Lei nº 9.605 – Lei de Crimes Ambientais – Condutas e Atividades Lesivas

14) 1990 – PR – Lei nº 8.078 – Código de Defesa do Consumidor (CDC)

15) 1943 – PR – Decreto-Lei nº 5.452 – Consolidação das Leis do Trabalho (CLT)

16) 1940 – PR – Decreto-Lei nº 2.848 – Código Penal Brasileiro

Mais, inúmeras **Resoluções** e **Instruções** do **CMN** (Conselho Monetário Nacional), **BCB** (Banco Central do Brasil) e **CVM** (Comissão de Valores Mobiliários)

4. REGULAMENTAÇÃO NACIONAL DE SI

Fatec Mauá

❖ NORMAS ABNT - NBR

- **ABNT - Associação Brasileira de Normas Técnicas**
  Órgão responsável pela normalização técnica no Brasil, fornecendo insumos ao desenvolvimento tecnológico brasileiro.
  NBR – Normas Técnicas Brasileiras

- Representante oficial no Brasil das entidades **ISO** e **IEC**

4. REGULAMENTAÇÃO NACIONAL DE SI

Fatec Mauá

❖ **Tratamento de Dados Pessoais**
(Adequação e Monitoração)

❖ **Conformidade às Leis e Regulamentos**
(Função de Compliance)

❖ **Lei Geral de Proteção de Dados Pessoais**
LGPD (Lei nº 13.709/2018)

❖ **Encarregado de Proteção de Dados**
DPO (Cargo ou Função)

4. REGULAMENTAÇÃO NACIONAL DE SI

Fatec Mauá

❖ DPO – DATA PROTECTION OFFICER
Encarregado de Proteção de Dados

Trata-se de um **agente**, pessoa física ou jurídica, **designado** por uma organização para um **cargo** ou uma **função** **responsável** pela **monitoração** das atividades de **tratamento de dados pessoais**, visando a **adequação** da **proteção dos dados** e a sua **conformidade** com a **Lei** e os **regulamentos** aplicáveis.

4. REGULAMENTAÇÃO NACIONAL DE SI

Fatec Mauá

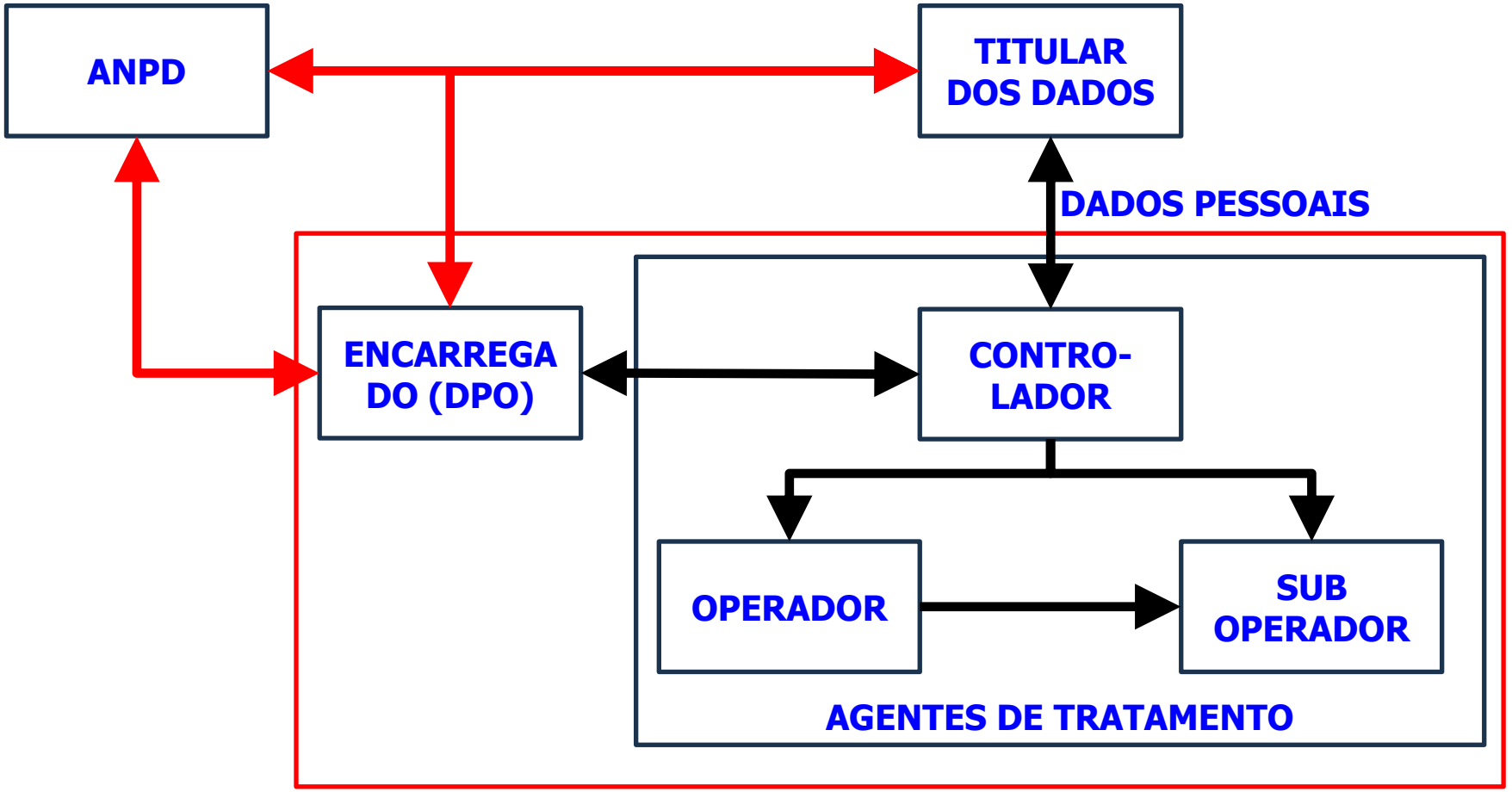
❖ LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

- Aprovada a **Lei nº 13.709** de 14/08/**2018**.
- Criação da Autoridade Nacional de Proteção de Dados (**ANPD**) pela Lei nº 13.853/**2019**.
- A partir de 03/05/**2021** entra em vigor a **LGPD** com a MP nº 959.

Regulamenta o uso, a proteção e a transferência de **dados pessoais** de pessoas naturais ou de pessoas físicas (PF)

4. REGULAMENTAÇÃO NACIONAL DE SI

❖ ESTRUTURA FUNCIONAL DA LGPD



5. NORMAS ABNT, ISO e IEC de SI

Fatec Mauá

- **Normas 27000:** Segurança da Informação

- **ABNT NBR ISO/IEC 17799:** 2001-2005-2006/10 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação.
- **ABNT NBR ISO/IEC 27002:** 2005-2013-**2022** ... Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação.
- **ABNT NBR ISO/IEC 27001:** 2006-2013-2022-**2023** ... - Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação - Requisitos.

5. NORMAS ABNT, ISO e IEC de SI

Fatec Mauá

- Baseadas na **27002:** Controles de SI

- ABNT NBR ISO/IEC **27017:** 2016 ...
  Controles de SI para serviços em nuvem.
- ABNT NBR ISO/IEC **27018:** 2021 ...
  Proteção de dados pessoais (DP) em nuvens públicas.

- Baseadas na **27001:** Sistemas de Gestão de SI

- ABNT NBR ISO/IEC **27003:** 2020 ...
  SGSI - Orientações.
- ABNT NBR ISO/IEC **27004:** 2017 ...
  SGSI - Avaliação.

5. NORMAS ABNT, ISO e IEC de SI

Fatec Mauá

➢ **Normas 27000:** Segurança da Informação

- ABNT NBR ISO/IEC **27005:** 2023 ...
  Segurança da informação, segurança cibernética e proteção à privacidade – Orientações para gestão de riscos de SI.
- ABNT NBR ISO/IEC **27007:** 2021 ...
  Segurança da informação, segurança cibernética e proteção à privacidade – Diretrizes para auditoria de sistemas de GSI.
- ABNT NBR ISO/IEC **27032:** 2015 ...
  Tecnologia da informação – Técnicas de segurança – Diretrizes para segurança cibernética.

5. NORMAS ABNT, ISO e IEC de SI

Fatec Mauá

- ABNT NBR ISO/IEC **27035:** 2023 ...
  Tecnologia da informação – Gestão de incidentes da SI – P1. Processo – P2.Planejar – P3.Respostas.

➢ Outras Normas, **não 27000**, para SI

- ABNT NBR ISO **16167:** 2020 ...
  Segurança da Informação – Diretrizes para classificação, rotulação, tratamento e gestão da informação.
- ABNT NBR ISO **31000:** 2018 - 2023 ...
  Gestão de riscos – Diretrizes e Handbook orientativo.

6. MODELOS DE SEGURANÇA DA INFORMAÇÃO

Fatec Mauá

- **ISO/IEC 27001:** preparada para prover um modelo para estabelecer, implantar, operar, monitorar, rever, manter e melhorar um SGSI.

- **ISO/IEC 27002:** estabelece diretrizes e princípios gerais para iniciar, manter e melhorar a gestão da segurança da informação em uma organização, fornecendo direcionamentos sobre as metas geralmente aceitas para a gestão.

6. MODELOS DE SEGURANÇA DA INFORMAÇÃO

Fatec Mauá

- **Framework ITIL:** processos relacionados com segurança da informação.

  Desenho do Serviço:
  - Gerenciamento de disponibilidade
  - Gerenciamento de continuidade de serviço
  - Gerenciamento de segurança da informação

  Operação do Serviço:
  - Gerenciamento de incidente
  - Gerenciamento de problema
  - Gerenciamento de acesso

6. MODELOS DE SEGURANÇA DA INFORMAÇÃO

Fatec Mauá

- **Framework COBIT:** processos relacionados com segurança da informação.

  Domínio APO:
  - Gerenciar riscos
  - Gerenciar segurança
- **Domínio BAI:**
  - Gerenciar disponibilidade e capacidade
  - Gerenciar ativos
- **Domínio DSS:**
  - Gerenciar incidentes
  - Gerenciar problemas
  - Gerenciar serviços de continuidade
  - Gerenciar serviços de segurança

6. MODELOS DE SEGURANÇA DA INFORMAÇÃO

Fatec Mauá

- **Estrutura do Modelo ISO/IEC 27001:**
  a norma é dividida em 5 (cinco) grandes seções:

1. **O sistema de gestão da segurança da informação.**
   - O estabelecimento do SGSI;
   - A implementação e operação;
   - A monitoração e revisão;
   - A manutenção e melhoria, e
   - Os requisitos de documentação.

6. MODELOS DE SEGURANÇA DA INFORMAÇÃO

Fatec Mauá

2. A responsabilidade da administração.

- Deve haver evidência do compromisso da administração com o estabelecimento, a implementação, a operação, o monitoramento, a revisão, a manutenção e a melhoria do SGSI.

3. As auditorias internas do SGSI.

- A organização deve conduzir auditorias internas do SGSI em intervalos planejados, para determinar a conformidade das atividades de controle, dos controles, dos processos e dos procedimentos do sistema.

6. MODELOS DE SEGURANÇA DA INFORMAÇÃO

Fatec Mauá

4. A revisão do SGSI pela administração.

- A administração deve revisar o SGSI pelo menos uma vez por ano, para assegurar sua contínua adequação e eficácia.

5. A melhoria do SGSI.

- A organização deve melhorar continuamente a eficácia do SGSI por meio do uso da política e dos objetivos de segurança da informação, dos resultados de auditoria, da análise de eventos monitorados, das ações corretivas e preventivas e das revisões gerenciais.

6. MODELOS DE SEGURANÇA DA INFORMAÇÃO

Fatec Mauá

- **Estrutura do Modelo ISO/IEC 27002:** a norma é dividida em 11 (onze) seções, constituídas por **categorias de segurança** da informação, que correspondem a um total de **132 controles** descritos em detalhes.

6. MODELOS DE SEGURANÇA DA INFORMAÇÃO

Fatec Mauá

- **Seções do Modelo ISO/IEC 27002:**

1. Política de segurança da informação.
2. Organizando a segurança da informação.
3. Gestão de ativos.
4. Segurança em recursos humanos.
5. Segurança física do ambiente.
6. Gestão das operações e comunicações.

6. MODELOS DE SEGURANÇA DA INFORMAÇÃO

Fatec Mauá

- **Seções do Modelo ISO/IEC 27002:**

7. Controle de acesso.
8. Aquisição, desenvolvimento e manutenção de sistemas de informação.
9. Gestão de incidentes de segurança da informação.
10. Gestão da continuidade do negócio.
11. Conformidade.

SÃO PAULO
GOVERNO DO ESTADO

Centro Paula Souza

Fatec Mauá

CST Desenvolvimento de Software Multiplataforma (DSM)

Disciplina: ISG-022 – SEGURANÇA NO DESENVOLVIMENTO DE APLICAÇÕES (SDA)

Tópico 02: CONFORMIDADE E OS ASPECTOS LEGAIS DA SI