Requisitos de *Software*

Prof.ª Ma. Jessica Oliveira

Católica
Universidade Católica de Brasília

Aula 10 – 26/05/2025

Requisitos de Segurança e Privacidade.

Universidade Católica de Brasília

Conceituação de Requisitos de Segurança e de Privacidade.

Requisitos de Segurança.

- São definidos como os atributos, restrições e funcionalidades do sistema que asseguram a proteção dos ativos da informação contra ameaças, ataques, falhas e acessos não autorizados.
- Segundo Sommerville (2019), esses requisitos são cruciais para assegurar que o sistema se comporte corretamente mesmo quando sujeito a atividades maliciosas ou acidentais que possam comprometer sua operação.

Requisitos de Segurança.

- A segurança da informação, conforme definido na **ISO/IEC 27001:2013**, tem três pilares fundamentais:
  - **Confidencialidade:** assegura que a informação seja acessível apenas a pessoas autorizadas.
  - **Integridade:** garante a exatidão e completude da informação e dos métodos de processamento.
  - **Disponibilidade:** garante que os usuários autorizados tenham acesso à informação e aos ativos correspondentes sempre que necessário.

Requisitos de Segurança.

- Adicionalmente, são reconhecidos outros atributos relevantes (**ISO/IEC 27002:2022**):
  - **Autenticidade:** garantia da veracidade da origem da informação.
  - **Não repúdio:** assegura que um indivíduo não possa negar a autoria de uma ação executada.
- A ausência de requisitos bem definidos relacionados à segurança pode resultar em falhas graves, como vazamentos de dados, acessos não autorizados, perda de informações, entre outros (Pressman; Maxim, 2016).

Requisitos de Privacidade.

- São aqueles que tratam da proteção dos dados pessoais, considerando aspectos legais, éticos e técnicos.
- Eles visam assegurar que o tratamento de dados esteja alinhado aos princípios de privacidade e proteção de dados estabelecidos por legislações como a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), no Brasil, e o Regulamento Geral sobre a Proteção de Dados (GDPR - *General Data Protection Regulation*, Regulamento UE 2016/679), na União Europeia.
- A ISO/IEC 29100:2011, que estabelece um framework de privacidade, define privacidade como a preservação dos dados pessoais, garantindo que as informações que identificam direta ou indiretamente uma pessoa estejam protegidas contra uso indevido.

Requisitos de Privacidade.

- Os principais princípios que regem a privacidade, segundo a LGPD (Art. 6º) e a ISO/IEC 29100:2011, incluem:
  - **Finalidade:** tratamento realizado para propósitos legítimos e específicos.
  - **Adequação:** compatibilidade do tratamento com as finalidades informadas.
  - **Necessidade (Minimização de dados):** limitação do tratamento ao mínimo necessário.
  - **Livre acesso:** garantia de consulta facilitada e gratuita sobre os dados tratados.
  - **Qualidade dos dados:** exatidão, clareza e atualidade dos dados.

Requisitos de Privacidade.

- **Transparência:** informação clara e acessível sobre o tratamento dos dados.
- **Segurança:** adoção de medidas para proteger os dados.
- **Prevenção:** adoção de medidas para prevenir danos.
- **Não discriminação:** proibição do uso dos dados para atos ilícitos ou discriminatórios.
- **Responsabilização e prestação de contas:** demonstração da adoção de medidas eficazes para garantir a proteção de dados.

- Além disso, os conceitos de *Privacy by Design* e *Privacy by Default*, presentes tanto no GDPR (Art. 25) quanto na LGPD (Art. 46), reforçam a necessidade de incorporar requisitos de privacidade desde a concepção do software e garantir que a configuração padrão proteja os dados dos titulares.

Normas, Legislações e Frameworks Aplicáveis.

LGPD (Lei nº 13.709/2018 - Brasil).

- Estabelece diretrizes sobre o tratamento de dados pessoais, tanto no meio físico quanto no digital, com foco na proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural.
  - Enfoque na responsabilização dos agentes de tratamento (Controlador e Operador).
  - Obriga a implementação de medidas de segurança, técnicas e administrativas capazes de proteger os dados pessoais (Art. 46).
  - Garante aos titulares direitos como: acesso, correção, anonimização, portabilidade, eliminação e revogação do consentimento (Art. 18).

GDPR (*General Data Protection Regulation* - União Europeia).

- Regulamentação europeia que inspirou a LGPD. É considerada uma das legislações mais rigorosas do mundo em termos de proteção de dados.
- Estabelece princípios como:
  - Privacy by Design e Privacy by Default (Art. 25);
  - Accountability (responsabilização ativa);
  - Definição clara dos direitos dos titulares, incluindo o direito ao esquecimento (Art. 17).

ISO/IEC 27001:2013.

- Padrão internacional para Sistema de Gestão da Segurança da Informação (SGSI).
- Define requisitos para implementação de um sistema robusto de segurança.
  - Baseia-se no ciclo PDCA (Plan-Do-Check-Act).
  - Exige avaliação e tratamento sistemático de riscos de segurança da informação.

ISO/IEC 27002:2022.

- Complementa a ISO/IEC 27001, oferecendo diretrizes práticas para implementação de controles de segurança, como:
  - Controle de acesso;
  - Gestão de ativos;
  - Segurança física e ambiental;
  - Segurança nas operações;
  - Segurança nas comunicações;
  - Aquisição, desenvolvimento e manutenção de sistemas seguros.

ISO/IEC 29100:2011.

- Fornece uma estrutura de alto nível para proteger informações pessoalmente identificáveis (PII) dentro dos sistemas de TI, definindo:
  - Princípios de privacidade;
  - Funções dos agentes de privacidade;
  - Controles aplicáveis a ambientes que processam dados pessoais.

Principais falhas e vulnerabilidades decorrentes da má definição dos requisitos.

Falhas de Segurança.

- **Ausência de controle de acesso:** permite que usuários não autorizados acessem dados ou funcionalidades sensíveis.
- **Armazenamento inseguro de credenciais:** senhas armazenadas em texto simples ou sem criptografia.
- **Interfaces expostas sem autenticação:** APIs ou endpoints abertos sem mecanismos de proteção.
- **Injeção de código:** ataques como SQL Injection ou Command Injection, decorrentes da falta de validação de entrada.
- **Ausência de logs e rastreabilidade:** dificulta a auditoria de eventos e detecção de acessos não autorizados.
- **Falta de backups ou planos de contingência:** afeta a disponibilidade e resiliência do sistema.

Falhas de Privacidade.

- **Coleta excessiva de dados:** desrespeito ao princípio da minimização de dados.
- **Ausência de consentimento adequado:** dados coletados sem informar corretamente o titular sobre a finalidade.
- **Compartilhamento indevido de dados:** com terceiros sem respaldo legal ou consentimento.
- **Falta de transparência:** usuários não sabem como, por que e por quem seus dados são tratados.
- **Dados sensíveis não tratados com medidas adicionais de segurança:** violação do Art. 11 da LGPD.

Técnicas de elicitação e especificação de requisitos de segurança e privacidade.

Threat Modeling (Modelagem de Ameaças).

- Metodologia utilizada para identificar, entender e priorizar ameaças contra o sistema. A técnica mais conhecida é o STRIDE (Microsoft):
  - S: *Spoofing* (Falsificação de identidade)
  - T: *Tampering* (Manipulação de dados)
  - R: *Repudiation* (Não repúdio)
  - I: *Information Disclosure* (Divulgação de informações)
  - D: *Denial of Service* (Negação de serviço)
  - E: *Elevation of Privilege* (Escalada de privilégios)

SQUARE (*Security Quality Requirements Engineering*).

- Metodologia desenvolvida pela *Carnegie Mellon University* para engenharia de requisitos de segurança, composta por nove etapas:

1. Acordo sobre os objetivos de segurança.
2. Desenvolvimento de artefatos.
3. Riscos de segurança identificados.
4. Seleção de técnicas de elicitação apropriadas.
5. Realização da elicitação dos requisitos.
6. Categorização dos requisitos.
7. Priorização dos requisitos.
8. Inspeção da qualidade dos requisitos.
9. Planejamento para mitigação de riscos.

Privacy Impact Assessment (PIA).

- Avaliação sistemática dos impactos que um sistema ou projeto pode gerar sobre a privacidade dos titulares de dados, obrigatória em muitos contextos pela LGPD e GDPR.

Checklists e Frameworks de Compliance.

- Utilização de listas de verificação baseadas em normas como ISO 27001, ISO 29100 ou nas diretrizes da Autoridade Nacional de Proteção de Dados (ANPD), que incluem:
  - Mapeamento de dados pessoais;
  - Avaliação de bases legais para o tratamento;
  - Análise de compartilhamento de dados;
  - Definição de medidas de segurança e governança.

Dúvidas?

jessica.oliveira@p.ucb.br

Católica
Universidade Católica de Brasília

Referências.

- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.
- UNIÃO EUROPEIA. Regulamento (UE) 2016/679 (GDPR). Disponível em: https://gdpr.eu/.
- ISO/IEC. 27001:2013. *Information technology - Security techniques - Information security management systems - Requirements*. Genebra: ISO, 2013.
- ISO/IEC. 27002:2022. *Information security, cybersecurity and privacy protection - Information security controls*. Genebra: ISO, 2022.
- ISO/IEC. 29100:2011. *Information technology - Security techniques - Privacy framework*. Genebra: ISO, 2011.
- SOMMERVILLE, Ian. Engenharia de Software. 10. ed. São Paulo: Pearson, 2019.
- PRESSMAN, Roger S.; MAXIM, Bruce R. Engenharia de Software: Uma Abordagem Profissional. 9. ed. Porto Alegre: AMGH, 2016.
- PELTZER, Daniel. Engenharia de Requisitos: Software Orientado ao Negócio. São Paulo: Érica, 2019.
- SHOSTACK, Adam. *Threat Modeling: Designing for Security*. 1. ed. Indianapolis: Wiley, 2014.