**Dia 1**

**Lesson 1**

**Due Care:** (devido cuidado) é um termo legal utilizado para descrever o cuidado que “uma pessoa razoável” tomaria sob determinadas circunstâncias. Não colocar senhas em post-it, por exemplo.

**Due Dilligence:** (diligência devida)um termo legal que significa que as pessoas responsáveis não foram negligentes no cumprimento de seus deveres.

**Benchmarks/Configuration Guides:**

* [CIS Critical Security Controls](https://www.cisecurity.org/controls/cis-controls-self-assessment-tool-cis-csat) / [CSAT Ransomware Business Impact Analysis Tool](https://www.cisecurity.org/insights/blog/connecting-cyber-risk-to-business-risk)
* [CIS-RAM (Risk Assessment Method)](https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method)
* [CIS Benchmarks](https://www.cisecurity.org/cis-benchmarks)
* [NIST National Checklist Program (NCP)](https://ncp.nist.gov/repository)
* [OWASP](https://owasp.org/)
* Vendor guides (Cisco, Fortinet, etc)

**Frameworks:**

* [NIST CSF](https://www.nist.gov/cyberframework)
* [MITRE ATT&CK](https://attack.mitre.org/) - Minhas contribuições: [LAPSUS$](https://attack.mitre.org/groups/G1004/) (group), [AvosLocker](https://attack.mitre.org/software/S1053/) (software), [C0018](https://attack.mitre.org/campaigns/C0018/) (campaign)

**Standards:**

* **International Organization for Standardization (ISO)** é uma organização internacional responsável por desenvolver padrões para várias áreas, incluindo tecnologia, saúde, meio ambiente, etc.
* **Cloud Security Alliance (CSA)** é uma organização que desenvolve padrões e práticas recomendadas para segurança em nuvem, ajudando empresas a entender e gerenciar riscos de segurança em ambientes de computação em nuvem.
* **SSAE** é um conjunto de padrões desenvolvidos pelo American Institute of Certified Public Accountants (AICPA) para avaliar a eficácia de controles internos de uma empresa.
* **SOC (Service Organization Control)** é um conjunto de relatórios que descrevem as medidas de segurança e privacidade adotadas por uma organização que presta serviços para outras empresas.
* **SOC2 Type I e Type I**I são relatórios de conformidade que descrevem as medidas de segurança e privacidade adotadas por uma organização que presta serviços para outras empresas.
  + O SOC2 Type I avalia os controles da empresa em um ponto no tempo.
  + SOC2 Type II avalia a efetividade dos controles ao longo de um período de tempo.
* **SOC3** é um resumo do relatório SOC2, que pode ser compartilhado publicamente. Ele fornece uma visão geral das medidas de segurança e privacidade adotadas pela organização, sem fornecer detalhes específicos dos controles implementados.
* **Sherwood Applied Business Security Architecture (SABSA)** é uma metodologia para fornecer garantia de informação alinhada às necessidades de negócios e impulsionada pela análise de riscos.

**Regulations, Standards and Legislation:** regulamentações, normas e legislações são regras e diretrizes que governam diferentes áreas da sociedade, como tecnologia, saúde, finanças, etc.

* **O Sarbanes-Oxley Act (SOX)** é uma lei dos Estados Unidos que define requisitos de relatórios financeiros para empresas que negociam suas ações em bolsas de valores dos EUA.
* **O Computer Security Act (1987)** é uma lei dos EUA que estabelece requisitos de segurança para as informações processadas por agências federais.
* **O Federal Information Security Management Act (FISMA)** é uma lei dos EUA que estabelece requisitos de segurança para agências federais e fornecedores de serviços que trabalham com o governo dos EUA.

**National, territory/state laws:**

* As leis nacionais ou estaduais incluem o **Gramm-Leach-Bliley Act (GLBA)**, que regula a privacidade e segurança financeira nos EUA.
* **California Consumer Privacy Act (CCPA)**, que regula a privacidade de informações pessoais de residentes da Califórnia.
* **General Data Protection Regulation (GDPR)** é uma regulamentação da União Europeia que define regras para a proteção de dados pessoais de indivíduos na UE.

O **Payment Card Industry Data Security Standard (PCI DSS)** é um conjunto de requisitos de segurança para empresas que processam, armazenam ou transmitem informações de cartão de crédito.

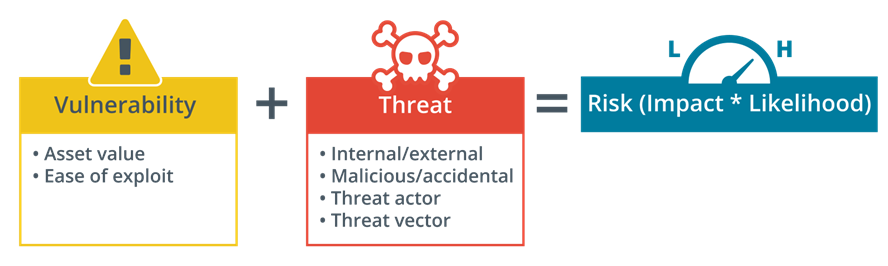
**Health Insurance Portability and Accountability Act (HIPAA)**, que regula a privacidade de informações médicas nos EUA.

**Lesson 2**

**Vulnerabilidade:** uma fraqueza que pode ser acionada acidentalmente ou explorada intencionalmente para causar uma violação de segurança. (bugs de software, erro humano, falha de hw, processos interrompidos).

**Ameaça:** o potencial de uma entidade exercer uma vulnerabilidade (ou seja, violar a segurança) (funcionários furiosos, criminosos, natureza).

**Risco:** a probabilidade e o impacto de um ator de ameaça explorar uma vulnerabilidade (interrupção de negócios; perda de vidas).



Uma **ameaça** causa danos a um **ativo**,  
explorando uma **vulnerabilidade**através de um **vetor**,  
que não possui contramedidas  
para mitigar os **riscos**.

**Hackers:** não utilizamos mais as terminologias black hat, white hat e gray hat, por não serem inclusivas. Os termos corretos são não autorizados, autorizados e semi autorizados, respectivamente.

**Questões pendentes em aula:** N/A