UNI
METRO
CAMP

wyden

Introdução à Segurança da Informação - ARA0064

Prof. José Luiz Alonso Silva, MsC
E-mail: jose.lsilva@unimetrocamp.edu.br

3.1 Finalidades e Benefícios das Normas

UNI METRO CAMP wyden

Temas da Aula

- Normas
- SGSI – Sistema de Gestão Segurança da Informação
- Prepare-se para próxima aula

Atividade Aula 4

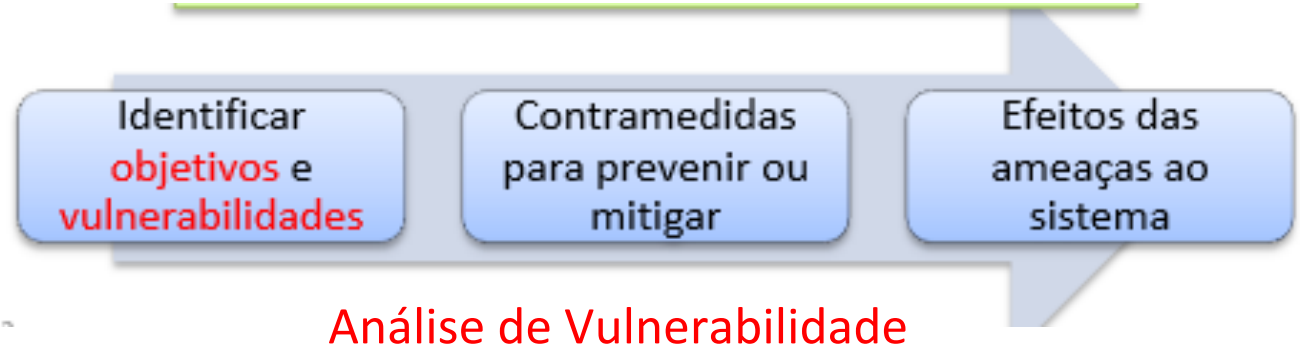
- Vulnerabilidade de senha
- Pentest
- Vírus, malwares, sites falsos
- Redes, portas
- Verificar as contas de usuários inativas

Atividade Aula 4
O que apredemos

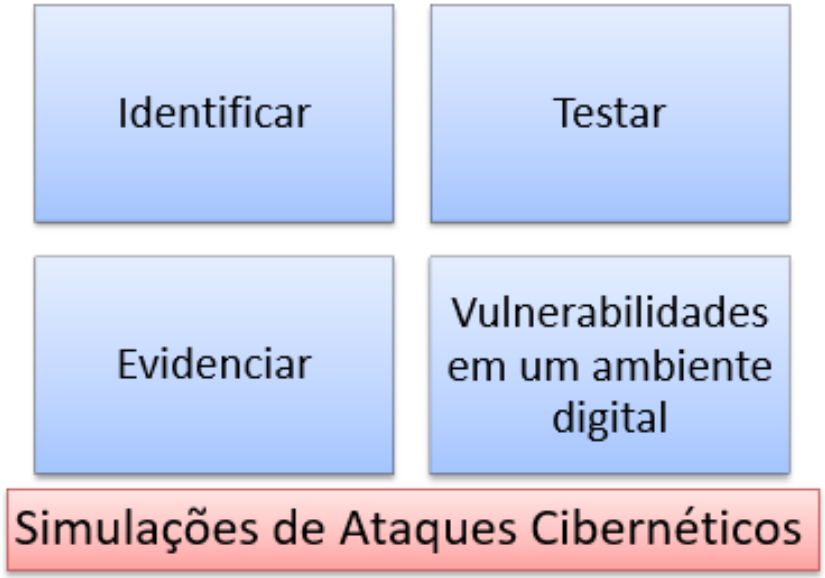
- Para reforçar segurança da senha de no mínimo
- Importância do teste de invasão (pentest), uso de ferramentas adequadas e conhecer o ambiente/infraestrutura
- Ações proativas de melhoria da segurança
- Identificar as vulnerabilidades, conscientização sobre os riscos de segurança e a importância de boas práticas de segurança cibernética
- Uso de Antivírus, teste de confiabilidade dos funcionários e capacitação
- Importância de conhecer as vulnerabilidade da empresa
- Planejar e ter estratégias para poder evitar ou máximo possíveis vulnerabilidades e utilizar as ferramentas adequadas
- Nunca que estamos 100% seguros

UNI METRO CAMP wyden

Melhores Momentos



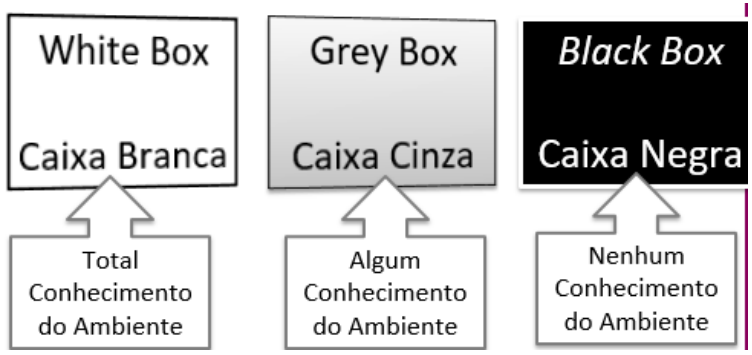
Análise de Vulnerabilidade



Segurança Cibernética

Teste realizado em uma rede, ou sistema de computadores, para descobrir vulnerabilidades e riscos de segurança

PENTEST



Estratégia PENTEST

UNI METRO CAMP wyden

Temas de Aprendizagem

1. PRINCÍPIOS DA SEGURANÇA E O CICLO DE VIDA DA INFORMAÇÃO
1.1 SEGURANÇA DA INFORMAÇÃO
1.2 SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO

2. AMEAÇAS E VULNERABILIDADES À SEGURANÇA DE INFORMAÇÃO
2.1 TIPOS DE AMEAÇAS E VULNERABILIDADES
2.2 ATAQUES CIBERNÉTICOS

3. NORMAS DE SEGURANÇA DA INFORMAÇÃO
3.1 FINALIDADES E BENEFÍCIOS DAS NORMAS 3.2 APLICAÇÃO DAS NORMAS

4. BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO
4.1 SENHAS, TREINAMENTO E PROTEÇÃO
4.2 CONTROLE DE ACESSO, VÍRUS E BACKUPS
4.3 CRIPTOGRAFIA DE DADOS E CERTIFICADO DIGITAL

5. GESTÃO DE RISCO
5.1 PRESERVAÇÃO DA CONFIDENCIALIDADE, INTEGRIDADE E DISPONILIDADE (CID)
5.2 ETAPAS DA GESTÃO DE RISCOS

6. GESTÃO DE CONTINUIDADE DO NEGÓCIO (ATIVIDADE PRÁTICA SUPERVISIONADA)
6.1 PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN) 6.2 ETAPAS DO PCN
6.3 PGCN E BIBLIOTECA ITIL

Objetivo da Aula

- Reconhecer as finalidades e os benefícios da adoção das normas ISO/IEC 27001 e 27002

Imagem: Autor wordart

UNI METRO CAMP wyden

Você se Preparou para Aula?

ISO 27002 | Uma visão geral no contexto da LGPD:
https://www.youtube.com/watch?v=Gp8WjPv0kj8

Qual certificação fazer? ISO27001 vs. Security+:
https://www.youtube.com/watch?v=jWHtwvbjDKc

UNI METRO CAMP wyden

Situação Problema

- Como posso implantar uma norma de segurança de informação na empresa que eu trabalho?

Imagem: Desconhecido

Normas

Normas "segurança da informação"

- Fornecer as melhores práticas, diretrizes
- Princípios gerais para a implantação de sua gestão
- Instituições padronizadoras reconhecidas nacionais e internacionais

Normas

- Organizações

https://www.iso.org/home.html

https://iec.ch/homepage

https://www.abnt.org.br/

UNI METRO CAMP wyden

Normas

- Anos 70 o Departamento de Defesa (DoD – *Department of Defense*)
- Criou o documento "*Security Control for Computer System*"
- Conjunto de regras ficou conhecido como "*The Orange Book*"
- Evolução
  - "Rainbow Series" ou "Rainbow Books"

Imagem: https://en.wikipedia.org/wiki/Rainbow_Series#/media/File:Rainbow_series_documents.jpg

Normas

BS - *British Standard*

- **BS7799-1** – Primeira parte
  - Referência para implementar "Boas Práticas" para a segurança da informação
- **BS7799-2** – Segunda parte
  - Base para a criação de um sistema de Gestão da Segurança da Informação
- **BS7799 Parte 3** - Terceira parte
  - Cobre gerenciamento e análise de riscos

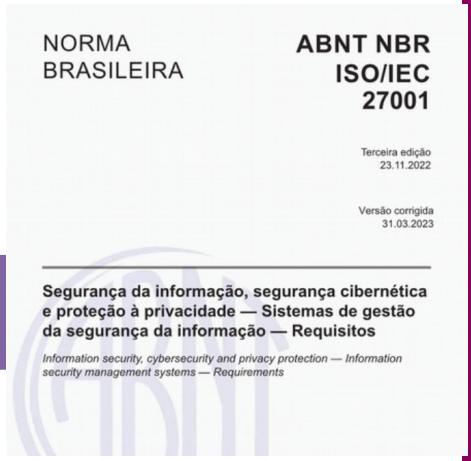
ISO - *International Standardization Organization*

- **A ISO/IEC 17799:2000**
  - Versão internacional da BS7799, homologada pela ISO

ABNT

- **A NBR ISO/IEC 17799:2001**
  - Versão brasileira "tradução" da norma ISO, homologada pela ABNT

Normas


NORMA BRASILEIRA

ABNT NBR ISO/IEC 27001

Terceira edição 23.11.2022

Versão corrigida 31.03.2023

Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

ISO 15408

- Segurança lógica das aplicações
- Foco principal no desenvolvimento de aplicações seguras

NBRISO/IEC27001

- Segurança da informação, segurança cibernética e proteção à privacidade
- Sistemas de gestão da segurança da informação
- Requisitos

NBRISO/IEC27002

- Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação

ABNT

- **A NBR ISO/IEC 17799:2001**
- Versão brasileira “tradução” da norma ISO, homologada pela ABNT

Imagem: https://www.normas.com.br/visualizar/abnt-nbr-nm/25074/nbriso-iec27001-seguranca-da-informacao-seguranca-cibernetica-e-protecao-a-privacidade-sistemas-de-gestao-da-seguranca-da-informacao-requisitos

Normas

ISO 27000 - Série

- Vocabulário de Gestão da Segurança da Informação
- Reuni as diversas normas existentes de segurança da informação

ISO 27001

- Sistema de Gestão da Segurança da Informação – Única passível de certificação

ISO 27002

- Tecnologia da informação - Técnicas de segurança - Guia de Boas prática para controles de segurança da informação

ISO 27003

- Implementação de Sistemas de Informação de Gestão de Segurança - SGSI

Normas

ISO 27004

- Monitorização, medição, análise e avaliação.

ISO 27005

- Gestão de Riscos de Segurança da Informação
- Diretrizes para o gerenciamento de informações de risco de segurança da informação

ISO 27006

- Requisitos para auditorias externas em um SGSI
- Certificação de sistemas de informação de gestão de segurança

ISO 31000

- Assuntos relacionados a gestão de riscos

Normas

Proteção de um conjunto de Dados e Informações

Ativos Organizacionais

Preservar o valor que possuem

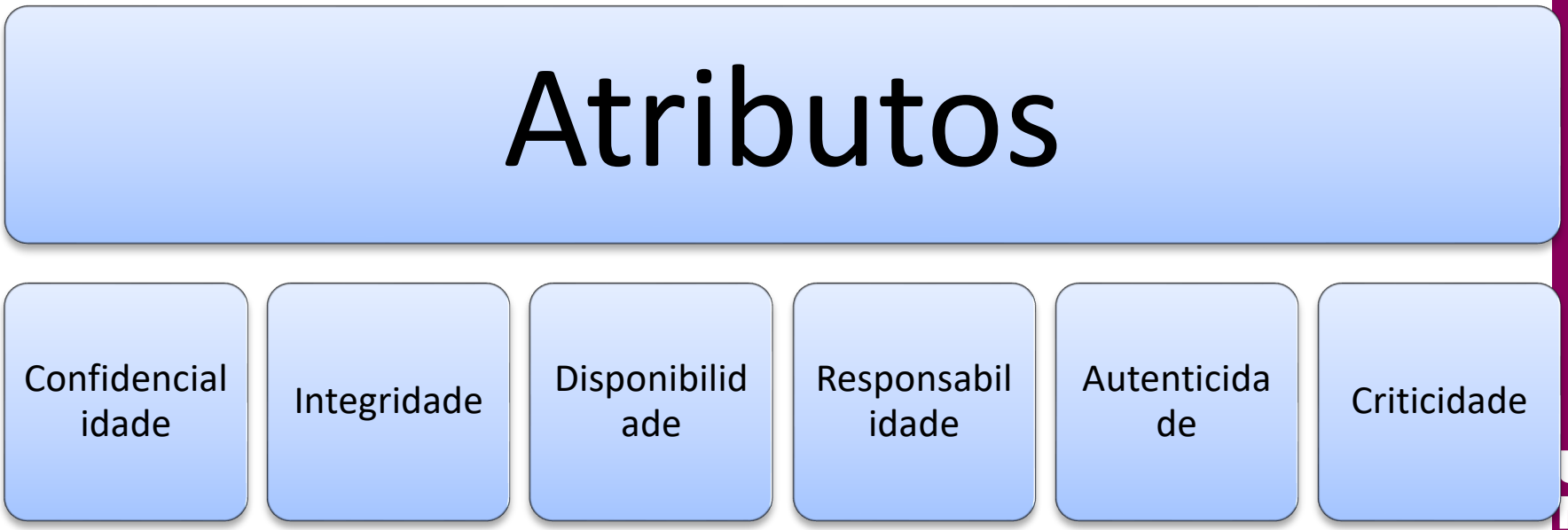
Indivíduo ou uma organização

CID

Confidencialidade
Integridade
Disponibilidade

SGSI

- A abordagem institucional usada para proteger a informação de acordo com seus princípios



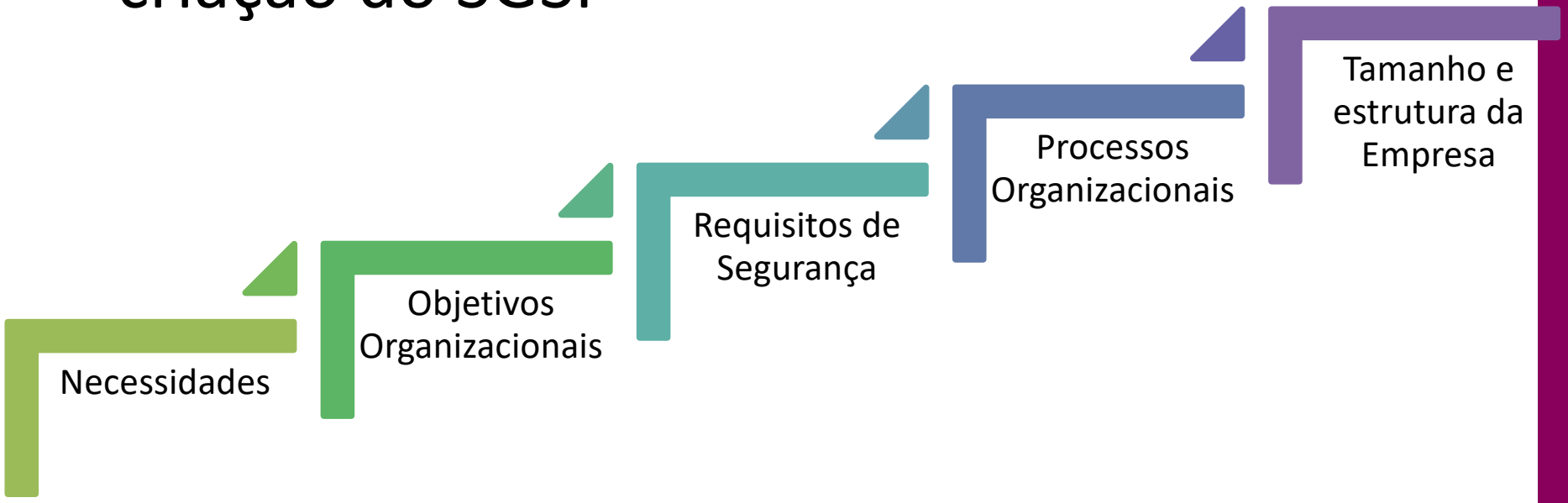
UNI METRO CAMP wyden

SGSI

UNI METRO CAMP wyden

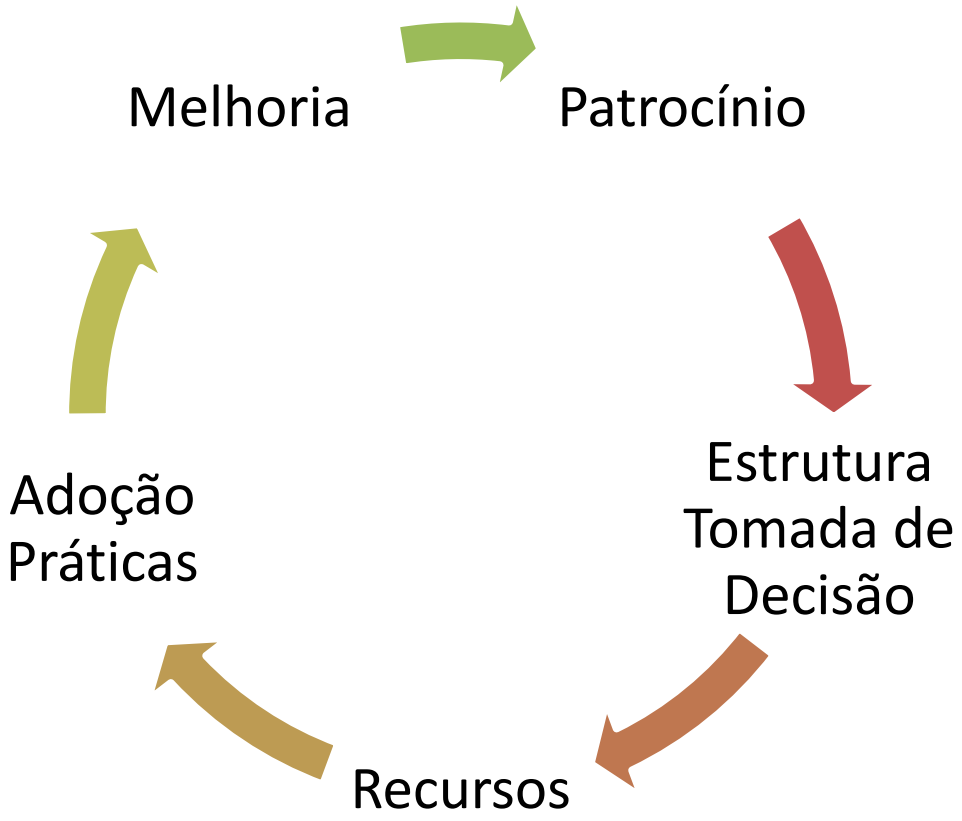
SGSI

- Fatores Motivacionais que influenciam na criação do SGSI



UNI METRO CAMP wyden

SGSI



UNI METRO CAMP wyden

Duvidas, considerações ...

Imagem Ícones MS-Power Point

UNI METRO CAMP wyden

Referência Bibliográfica

- BAARS, Hans. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002?** Rio de Janeiro ? RJ ? Editora Brasport, 2018. Capítulo 4 e 18. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/160044
- GALVÃO, Michele da Costa, Agnaldo Aragon. **Fundamentos em Segurança da Informação?** Rio de Janeiro ? RJ: Editora Pearson, 2015. Capítulo 4. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/26525

Referência

- **DoD Rainbow Series**. Disponível em: <https://csrc.nist.gov/publications/detail/white-paper/1985/12/26/dod-rainbow-series/final>. Acesso em 25/03/2024
- Macedo, Diego. **Sistemas de controle de acesso (*Rainbow Book*)**. Disponível em: <https://www.diegomacedo.com.br/sistemas-de-controle-de-acesso/>. Acesso em 25/03/2024

UNI METRO CAMP wyden

Referências

- NIST. **DoD Rainbow Series.** Disponível em: <https://csrc.nist.gov/pubs/other/1985/12/26/dod-rainbow-series/final>. Acesso em 25/03/2024
- Wikipedia. **ISO/IEC 27000-series.** Disponível em: <https://en.wikipedia.org/wiki/ISO/IEC_27000-series>. Acesso em 25/03/2024

UNI METRO CAMP wyden

Referências

- AWS. **Segurança na Nuvem AWS**. Disponível em: <https://aws.amazon.com/pt/security/?nc=sn&loc=0>. Acesso em 25/03/2024
- AWS. **ISO/IEC 27001:2022**. Disponível em: <https://aws.amazon.com/pt/compliance/iso-27001-faqs/>. Acesso em 25/03/2024

Referência

- Portal GSTI. **Sistema de Gestão de Segurança da Informação (SGSI)**. Disponível em: <portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html>. Acesso em 25/03/2024
- Embrapa. **Plano de Implantação de Segurança da Informação na Embrapa**. Disponível em: <https://www.infoteca.cnptia.embrapa.br/infoteca/bitstream/doc/1120124/1/Planodeimplantacaodesegurancadainformacao.pdf>. Acesso em 25/03/2024

Referência

- Passarin, Leonardo M. **Resumo da ISO 27001 – Sistema de Gestão de Segurança da Informação**. Disponível em: <https://www.estrategiaconcursos.com.br/blog/resumo-da-iso-27001/>. Acesso em 25/03/2024

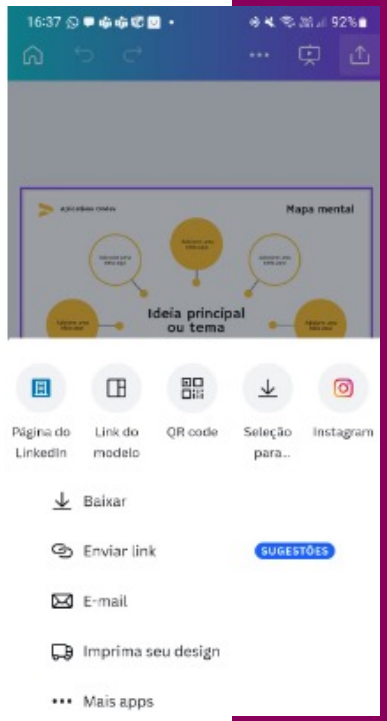
UNI METRO CAMP wyden

Atividade Aula 5

Elaborar Mapa Mental dos pontos chave da NBR-ISO-IEC-27001

Utilize o CANVA ou outro

1. Procure modelo “Mapa
2. Escolha um modelo Grátis
3. Após Conclusão enviar no SAVA
4. Data limite 13/04/24 – 22h Sabado



Apresentar na próxima aula

Equipe de 3 até 6 pessoas – 1 pessoa posta

Para Próxima Aula
Assista aos vídeos

- Webinar Auditando a ISO 27001 e a ISO 27701: https://www.youtube.com/watch?v=fpElceq1ncQ
- SOC 2 vs ISO 27001: https://www.youtube.com/watch?v=vPmbzEKAHmM

UNI METRO CAMP

wyden