UNI
METRO
CAMP
wyden

Introdução à Segurança da Informação - ARA0064

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

2.1 Tipos de Ameaças e Vulnerabilidade

UNI METRO CAMP wyden

Temas da Aula

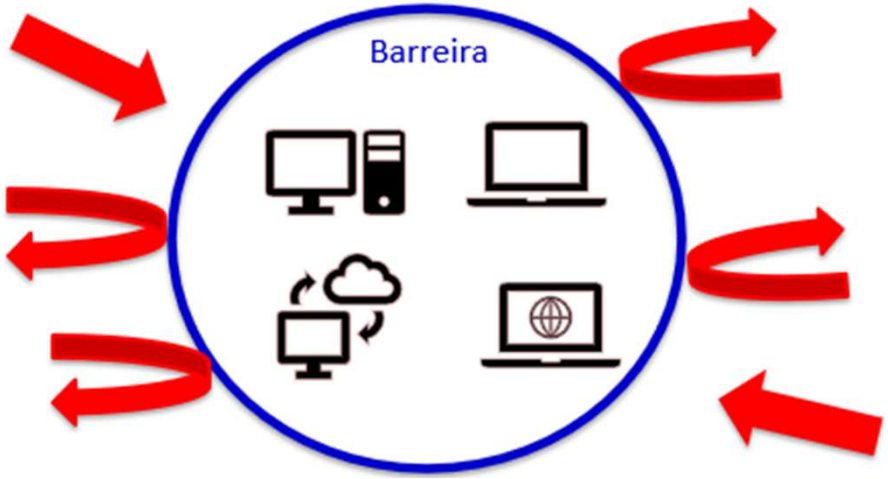
- Ameaça
- Vulnerabilidade
- Mitigação de Riscos
- Motivação
- Tipos de Ameaças
- Tipos de Vulnerabilidade
- Gestão de Risco
- Prepare-se para próxima aula

Melhores Momentos

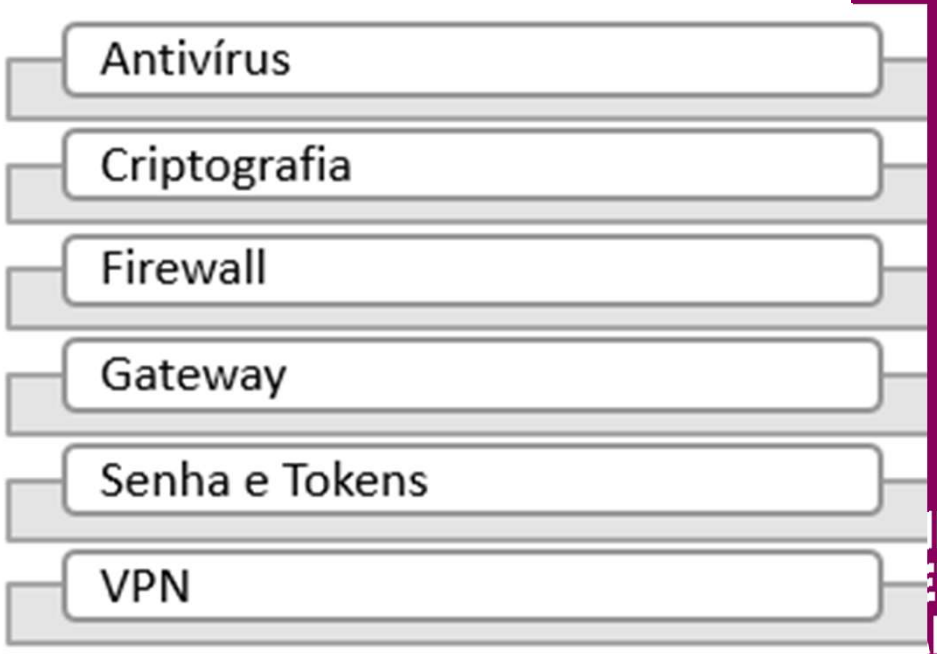
NBR ISO/IEC 17799

Norma Segurança da Informação

Controle Físico



Perímetro de Segurança



Controle Lógico

Imagem: Autor

Atividade Aula 2

1. Você foi contratado para avaliar a segurança da informação da XPTO Serviços de Informática.

   Identifique 3 pontos que você avaliaria e justifique a escolha.

9 Respostas no Forms

Respostas

15 - Segurança Lógica

12 - Segurança Física

Atividade Aula 2

- Tipo de item a ser avaliado
- Identifique qual o ponto a ser avaliado
  - Acesso restrito ao local
  - Segurança dos equipamentos
  - Níveis de Acesso, perfis, senhas
  - Identificar ativo de maior valor
  - Rede
  - VPN, Software, criptografia

Atividade Aula 2

Considerações sobre avaliação de segurança

Avaliação	Levantamento e Análise	Detecção Vulnerabilidade	Ações
• Planejar • Executar a Avaliação preliminar	• Revisar resultados da fase anterior • Ampliar a análise • Identificar de ações corretivas	• Explorar vulnerabilidade • Testes	• Documentar falhas e ações • Corrigir falhas • Documentar situações não tratadas

Situação Problema

- Onde começa a segurança física?

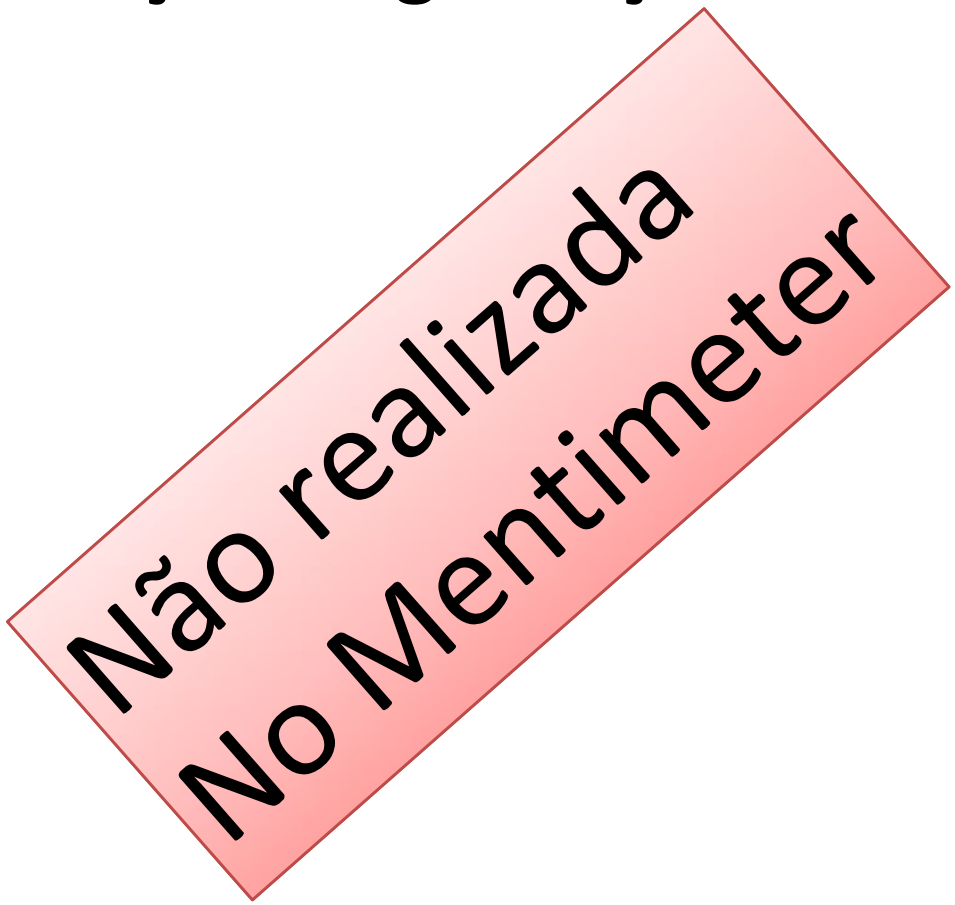


Imagem: Mentimeter resultado

UNI METRO CAMP wyden

Situação Problema

- Onde começa a segurança Lógica

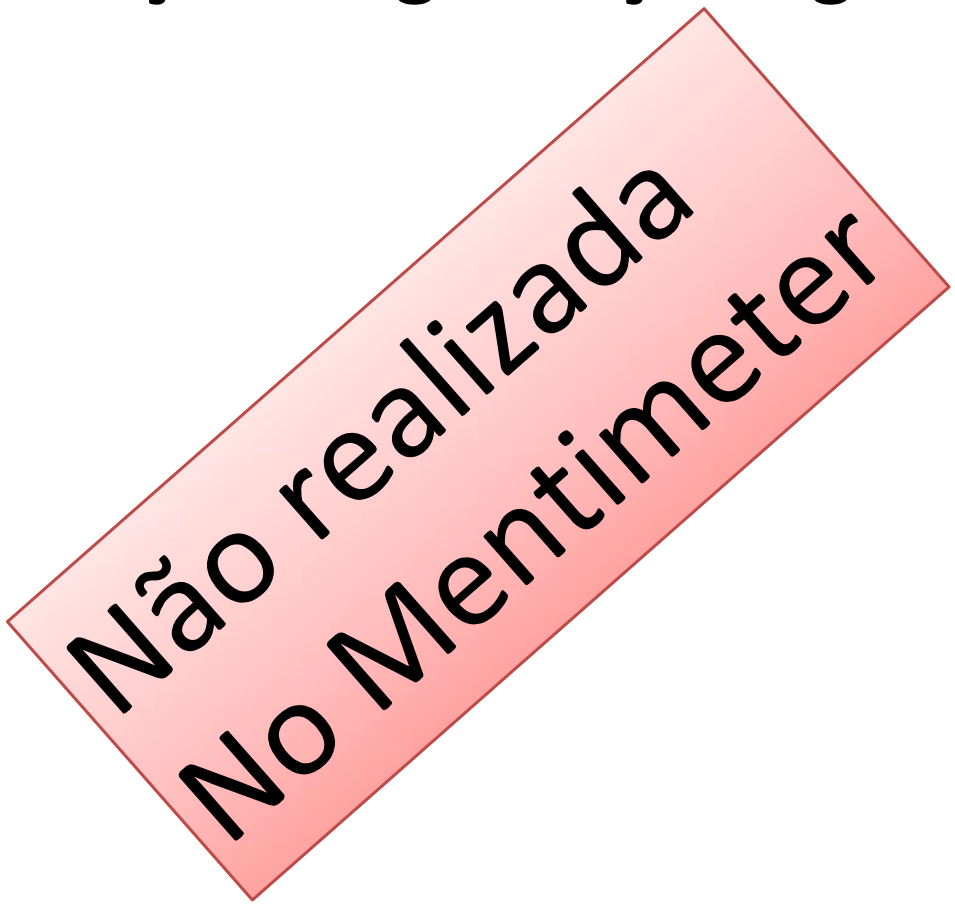


Imagem: Mentimeter resultado

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

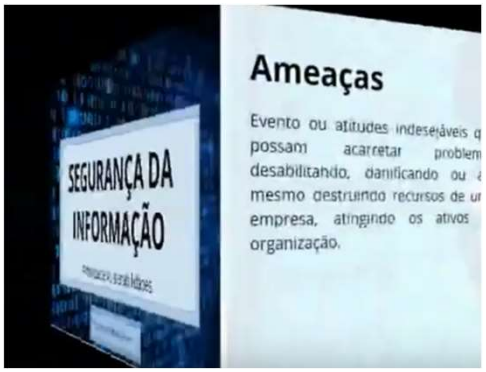
Objetivo da Aula

- Identificar os conceitos e os tipos de ameaças e vulnerabilidades de segurança da informação

Imagem: Autor wordart

UNI METRO CAMP wyden

Você se Preparou para Aula?



Segurança da Informação
Ameaças e Vulnerabilidades

Análise de Riscos,
Vulnerabilidade e Ameaças

Ameaças e Vulnerabilidades CCNA
200 301

Quais tipos de Ameaças/vulnerabilidade você conhece ?

UNI METRO CAMP wyden

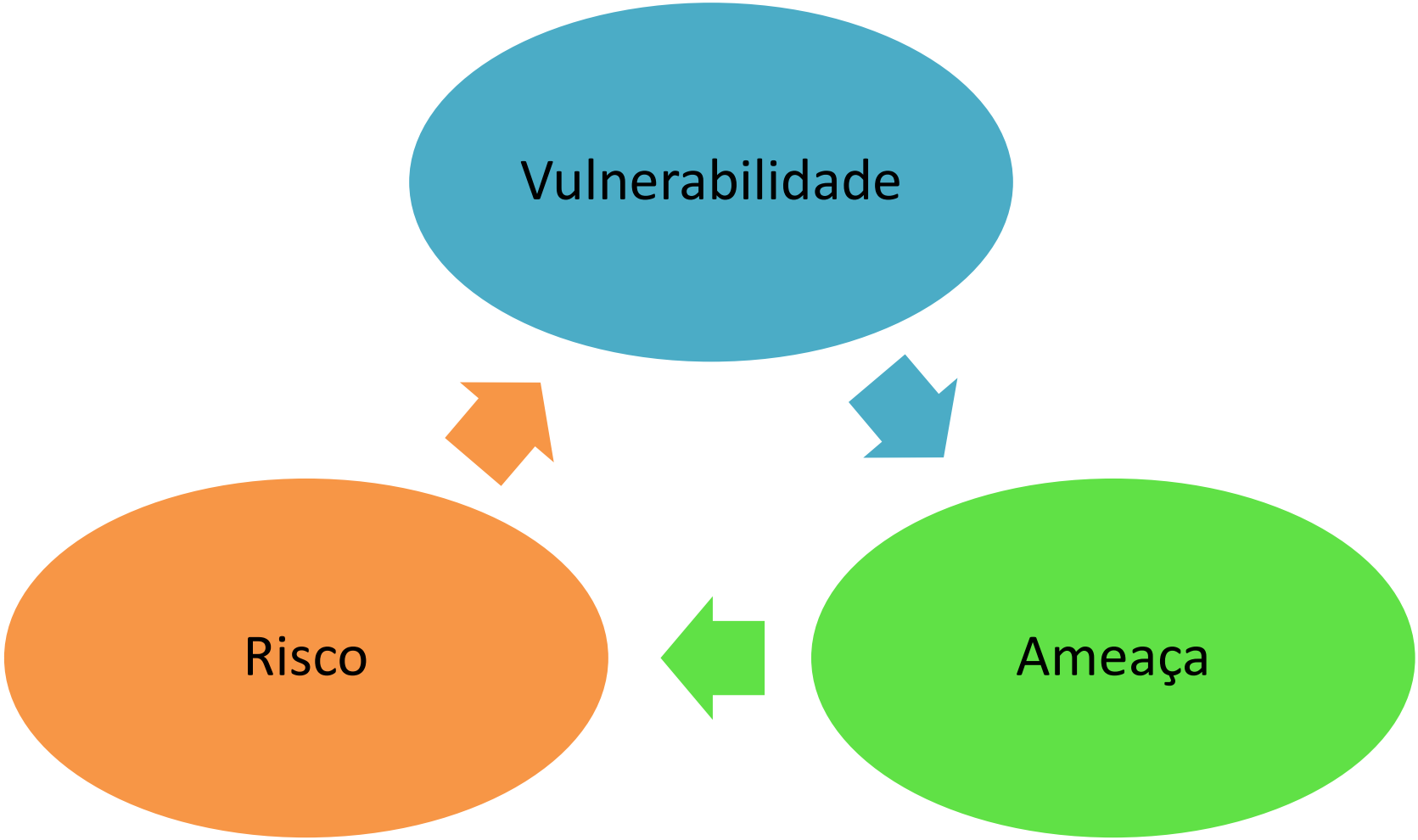
Situação Problema

- Devemos implementar mitigação para todas as vulnerabilidades?
- Porque?

Imagem: https://images.app.goo.gl/UpKYYWYBB9h2Nrv2A

UNI METRO CAMP wyden

Temas Abordados



UNI METRO CAMP wyden

Contexto

MIT Technology Review

Tópicos P

Custo de incidentes de segurança aumentam 10% em 2021 e alcançam o maior valor em 17 anos

Os incidentes com dados pessoais geram novas manchetes a cada dia, mesmo que o controlador, agindo de boa-fé, tenha tomado todas as medidas para evitá-los.

by **Fabio Correa Xavier** Dezembro 27, 2021

Gastos globais com segurança em TI crescerão 14% em 2024

No montante dos gastos das empresas, estão incluídos também os gastos com gerenciamento de risco. Em instituições financeiras, o treinamento de profissionais em segurança cibernética foi uma das prioridades deste ano. Nesse sentido, especialista defende a inclusão de equipes multidisciplinares no desenvolvimento de soluções para segurança de dados

Terra

3 nov 2023 - 13h45 (atualizado em 21/11/2023 às 14h06)

LONDON, U.K., September 28, 2023

Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024

Public Cloud Services Growth to Bolster Cloud Security Spending

Worldwide end-user spending on security and risk management is projected to total $215 billion in 2024, an increase of 14.3% from 2023, according to new forecast from Gartner, Inc. In 2023, global security and risk management end-user spending is estimated to reach $188.1 billion.

Gartner

UNI METRO CAMP wyden

Contexto

- *Security and Risk Management End-User Spending for All Segments, Worldwide, 2022-2024 (Millions of U.S. Dollars)*

Segment	2022 Spending	2022 Growth (%)	2023 Spending	2023 Growth (%)	2024 Spending	2024 Growth (%)
Application Security	5,047.6	10.9	5,765.2	14.2	6,670.3	15.7
Cloud Security	4,487.4	24.0	5,616.7	25.2	7,002.6	24.7
Data Privacy	1,129.2	9.9	1,338.7	18.5	1,667.3	24.6
Data Security	3,072.9	21.4	3,692.1	20.1	4,333.3	17.4
Identity Access Management	13,944.1	13.6	16,169.1	16.0	18,556.5	14.8
Infrastructure Protection	24,089.0	19.9	28,359.6	17.7	33,319.6	17.5
Integrated Risk Management	5,157.3	9.6	5,687.1	10.3	6,277.7	10.4
Network Security Equipment	18,932.5	11.9	21,383.6	12.9	24,360.1	13.9
Security Services	73,394.7	3.9	80,835.7	10.1	89,996.7	11.3
Consumer Security Software	7,443.4	2.9	7,901.7	6.2	8,406.7	6.4
Others	8,029.8	50.1	11,365.4	41.5	14,362.8	26.4
Total	**164,728.0**	**10.6**	**188,114.8**	**14.2**	**214,953.7**	**14.3**

Imagem: https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024

Vulnerabilidade

Vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança

Qualquer fator capaz de facilitar a atuação de cibercriminosos ou qualquer outro tipo de ameaça externa no que diz respeito a invasões, roubos de dados ou acessos não autorizados a recursos

Imagem: https://images.app.goo.gl/K8p3iJq9fEhkiL1r9

Vulnerabilidade

Fraquezas ou brechas na segurança da TIC de uma empresa

podem
ser usadas
por *hackers* para
um ataque na rede

Imagem: Autor

Tipos de Vulnerabilidade

S	Física
E	Hardware (projetado com falhas)
	Humana
R	Rede
Á	Processos
	Código e Criptografia - (Software mal desenvolvido e configurado)
?	Comunicação- Transmissão de dados

Imagem: autor

Como Pode Ocorrer

- Engenharia social
- Software e hardware sem atualizações
- Ataques de navegador
- Ataques de senha
- Eavesdropping – Monitoramento sem autorização
- Zero-Day - Falhas de segurança em programas de computador
- Ataques físicos

Imagem: autor

Ameaça

- Qualquer fator ou ação capaz de interferir e causar danos à:

- de dados e informações sobre a empresa

Ameaça

Confidencialidade:

- Garantia de que pessoas sem autorização não terão acesso aos dados institucionais.

Integridade:

- A informação uma vez armazenada não poderá sofrer quaisquer tipos de alteração

Disponibilidade:

- Dados devem estar disponíveis de acordo com a necessidade

Autenticidade:

- Assegurar que informação é verdadeira

Motivadores

Porque Segurança Informação?

- Evitar Perdas Financeiras
- Guerra cibernética
- Espionagem corporativa
- Hackivistas
- Roubo de recursos

Tipos de Ameaças

- Adware
- Backdoor
- Bootnet (controlar computadores e smarphone)
- Keylogger (captura teclas digitadas)
- Macros
- Phishing
- Ransomware (sequestro dados)
- Rootkit (instalados camadas do Sistemas Operacionais, controla computador)
- Spyware
- Trojan - Cavalo de Tróia

Imagem: autor Wordart

UNI METRO CAMP wyden

Tipos de Ameaças

- Adware (sem a permissão do usuário)
  - Programa que executa automaticamente e exibe uma grande quantidade de anúncios sem a permissão do usuário.
  - (ad = anúncio, software = programa)
- Backdoor (Porta dos Fundos)
  - Recurso utilizado por diversos malwares para garantir acesso remoto ao sistema ou à rede infectada, explorando falhas críticas não documentadas existentes em programas instalados, softwares desatualizados e do firewall para abrir portas do roteador.
- Browser Hijacker (sequestro do navegador)
  - Tipo de vírus que tem por objetivo a alteração das principais configurações do navegador
  - Altera a homepage e mecanismos de busca
  - Exibem anúncios em sites legítimos e redirecionam a vítima para sites maliciosos que podem conter outras pragas digitais

Tipos de Ameaças

- Cavalo de Troia (Trojan Horse)
  - Objetivo manter-se ocultos enquanto baixam e instalam ameaças mais robustas em computadores
  - Pode vir em arquivos de música, mensagens de e-mail, downloads e sites maliciosos
  - Se aproveitam de vulnerabilidades do navegador utilizado para instalar a praga no computador.
- Rogue Security Software
  - Busca informações confidenciais para roubar dinheiro
  - Passam por programas de segurança (como antivírus ou antispywares) e de otimização
- Rootkit
  - Rootkit são trojans que utilizam métodos avançados de programação para serem instalados em camadas profundas ou não documentadas do sistema operacional
  - Capacidade de se autorrecuperar, reinstalando-se mesmo após limpeza do computador e sua rápida disseminação

Tipos de Ameaças

- Spyware
  - Programas espiões utilizados para captar informações sobre os costumes dos usuários na internet, com o propósito de distribuir propaganda “customizada”.
- Time Bomb
  - É um malware de contagem regressiva
  - Ameaça programada para ser executada em um determinado momento no sistema operacional
- Worm (verme)
  - Podem se autorreplicar sem a necessidade de infectar arquivos legítimos,
  - Cria cópias funcionais de si mesmos
  - Se espalhem por redes de computadores e drives USB, mensagens de e-mail

Tipos de Ameaças

- Greyware
  - Situa-se na chamada zona cinzenta, entre o software normal e um vírus, causando mais irritação que problemas, como programas de piada e adware
  - Programas que são instalados sem o consentimento do usuário
- Joke Program
  - Programas desenvolvidos para causar danos temporários ao sistema operacional,
  - Travamentos e mudanças inesperadas de comportamento
- Keylogger
  - Programas de computador capazes de monitorar, armazenar e enviar todas as teclas digitadas
  - Roubo de logins ou dados bancários.

Tipos de Ameaças

- Macros
  - Comandos automatizados que podem ser configurados em softwares como Word e Excel
  - Documentos com instruções maliciosas podem ser criados, infectando outros arquivos ou executando ações prejudiciais toda vez que eles forem executados
- Ransonware
  - São códigos maliciosos que sequestram arquivos ou todo o sistema da vítima por meio de técnicas de criptografia
  - Após o “sequestro”, o malware exibe mensagens exigindo o depósito de uma quantia em dinheiro para liberar os arquivos

Alguns Riscos

Roubo de dados

Hackers de senhas

Funcionários não especializados / erros humanos

Softwares vulneráveis

Espionagem industrial

Imagem: autor

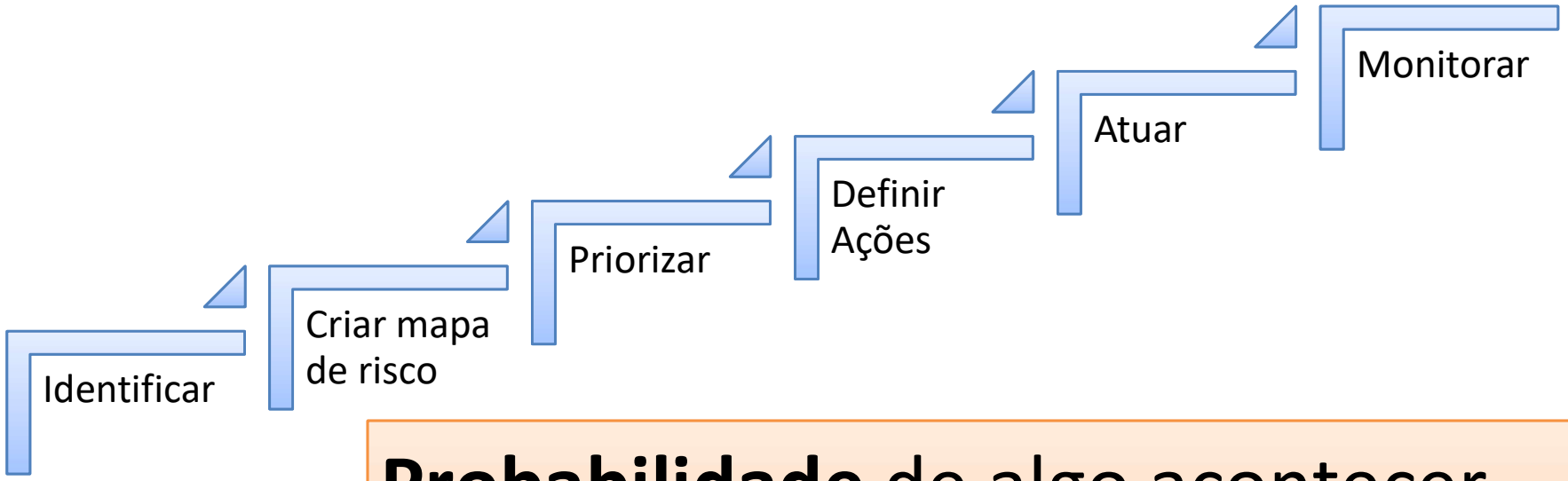
Mitigação de Riscos

- Mitigar significa reduzir ou aliviar o efeito de algo

Estratégias adotadas pela empresa para identificar potenciais fraquezas e ameaças

Atuar de forma a minimizar impactos nas operações do negócio

Gestão de Risco



Probabilidade de algo acontecer

Qualificado (Existe ou não o Risco)

Baixo, Médio ou Alto

Severidade

Baixo, Médio ou Alto

Imagem: autor

Gestão de Risco

- Ver planilha Plano de Risco

Nome do Risco	Descrição do Risco	Probabilidade de Ocorrer	Impacto	Severidade	Descrição da ação mitigação	Responsável pela Ação

Consolidando

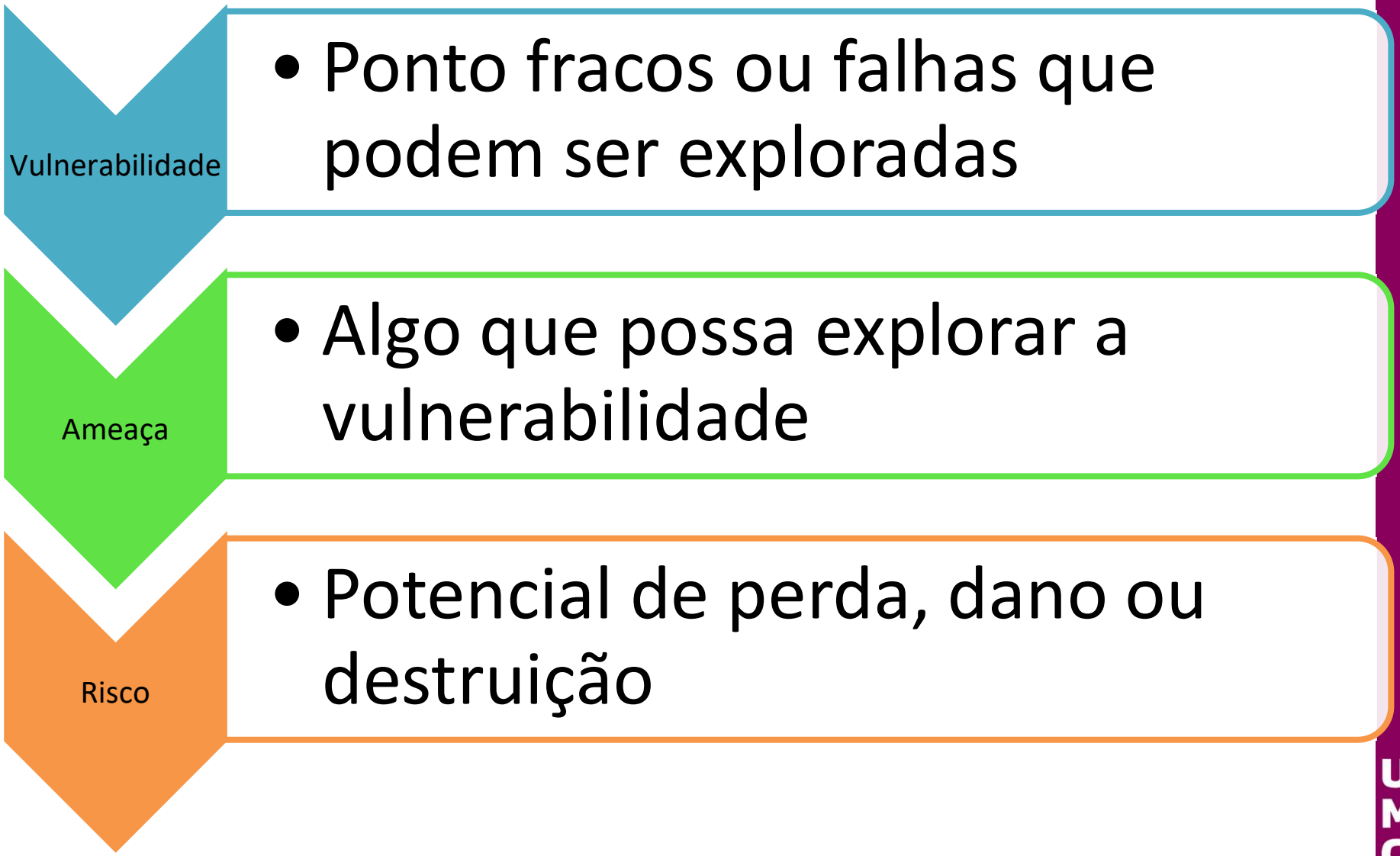


Imagem Ícones MS-Power Point

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 3. 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 3. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/26525

Referências

- Fabio Correa Xavier . **Custo de incidentes de segurança aumentam 10% em 2021 e alcançam o maior valor em 17 anos**. Disponível em: <https://mittechreview.com.br/custo-de-incidentes-de-seguranca-aumentam-10-em-2021-e-alcancam-o-maior-valor-em-17-anos/>. Acesso em 09/03/2024

Referências

- Segurity Report. **Investimentos em cibersegurança atingirão U$ 172 bilhões em 2022, diz estudo. Disponível: em** https://www.securityreport.com.br/overview/investimentos-em-cibersegurança-atingirao-u-172-bilhoes-em-2022-diz-estudo/#.ZBieFPbMLDc<>. Acesso em 09/03/2024

Referências

- TCU. **Lista de Alto Risco**. Disponível em: <https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_cibernetica.html>. Acesso em 09/03/2024
- **Gastos globais com seguranca em TI crescerão 14% em 2024**. <https://www.terra.com.br/noticias/gastos-globais-com-seguranca-em-ti-crescerao-14-em-2024,d0f49a1233bb40b8084366b9dfe2a0d2uclii4ao.html>. Acesso em 09/03/2024

UNI METRO CAMP wyden

Referências

- *Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024.* Disponível em: <https://gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024>. Acesso em 09/03/2024

Atividade Aula 3
Parte 1

1. Identifique uma vulnerabilidade
2. Explique qual ameaça para a vulnerabilidade identificada
3. Defina um plano de ação para o risco definido na ameaça.
   - Um integrante do grupo deverá explicar para sala
   - Tempo preparação 30 minutos
   - Explicação 5 minutos

Equipe de 3 até 6 pessoas

Resposta no Teams Até 07/04 – 22:00

https://forms.office.com/r/mw8ntYBJtj

UNI METRO CAMP wyden

Para Próxima Aula
Assista aos vídeos

- Vencendo um Desafio Hacker Pentest e Hacking: ttps://www.youtube.com/watch?v=XTdP8lWeuxs
- Como Estudar Hacking e Pentest montando um ambiente de estudo: https://www.youtube.com/watch?v=syXuqAKZfA0

UNI METRO CAMP

wyden