Processo de Avaliação de Riscos e Tratamento de Riscos

Anderson Oliveira da Silva

Ph. D. Ciências em Informática

Engenheiro de Computação

anderson@inf.puc-rio.br

Pós-graduação em Compliance de Cibersegurança

Departamento de Informática

Coordenação Central de Educação Continuada

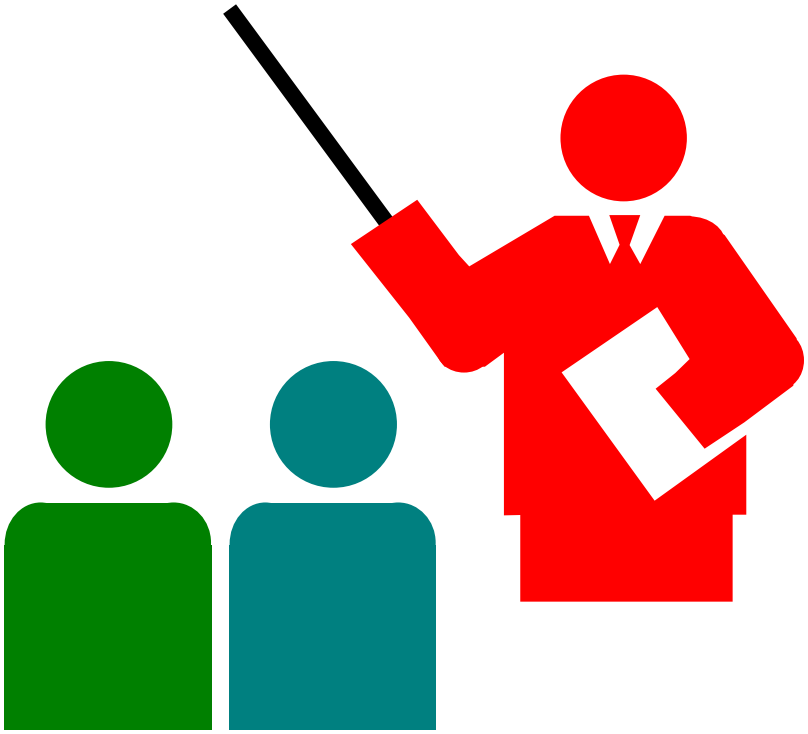
PUC-Rio

Ementa

Processo de Avaliação de Riscos e Tratamento de Riscos:

- Etapas do Processo de Avaliação de Riscos
- Tipos de Vulnerabilidades
- Classificação de Ameaças
- Agente de Ameaça
- Fatores Motivantes vs Probabilidade Inerente
- Processo de Avaliação de Riscos Aplicado
- Tratamento de Riscos Aplicado

Processo de Avaliação de Riscos



Processo de Avaliação de Riscos

O processo de avaliação de riscos é dividido em três etapas. (ISO27005, 2023, p.19)

- **Identificação de riscos:**
  - **Determinar o que pode causar uma perda potencial (vulnerabilidades e ameaças) e deixar claro como, onde e por que a perda pode acontecer.**
- **Análise de riscos:**
  - **Fazer uma avaliação da gravidade das consequências das ameaças e uma avaliação da probabilidade das ameaças se concretizarem, e determinar o nível de risco estimado a partir da combinação da probabilidade das ameaças com as suas consequências (impactos).**
- **Avaliação de riscos:**
  - **Fazer a comparação dos resultados da análise de riscos com critérios de risco para determinar se o risco é aceitável e priorizar os riscos analisados para o tratamento de riscos.**

Processo de Avaliação de Riscos – Identificação dos Riscos

Conceitos básicos: Vulnerabilidade

- **Qualquer fraqueza que possa ser explorada para violar um sistema ou a informação contida nele.**

- **Tipos de vulnerabilidades:**
  - ***vulnerabilidade no design ou na especificação*;**
  - ***vulnerabilidade na implantação*; e**
  - ***vulnerabilidade na operação e no gerenciamento*.**

- **Muitos sistemas possuem uma ou mais vulnerabilidades, mas isso não significa necessariamente que eles são demasiadamente falhos a ponto de não poderem ser usados.**

Processo de Avaliação de Riscos – Identificação dos Riscos

Conceitos básicos: Identificação de vulnerabilidades de cibersegurança

- **Identificação das fragilidades presentes nos sistemas de informação e na infraestrutura de TIC.**
- **Vulnerabilidades no design ou na especificação:**
  - **Verificar os requisitos de segurança da informação que não são atendidos no design ou na especificação dos sistemas de informação ou da infraestrutura de TIC.**
    - **Exemplo: revisar os projetos dos sistemas para identificar a ausência de requisitos de segurança para:**
      - **Autenticação de usuários;**
      - **Autorização de acesso aos recursos;**
      - **Trânsito seguro de dados na rede (data in-transit);**
      - **Armazenamento seguro de dados (data at-rest);**
      - **Alta disponibilidade de recursos.**

Processo de Avaliação de Riscos – Identificação dos Riscos

Conceitos básicos: Identificação de vulnerabilidades de cibersegurança

- **Identificação das fragilidades presentes nos sistemas de informação e na infraestrutura de TIC.**
- **Vulnerabilidades na implantação:**
  - **Verificar quais são as falhas de segurança na implementação dos sistemas de informação ou da infraestrutura de TIC.**
    - **Exemplo: executar testes para verificar falhas de codificação dos sistemas de aplicação, serviços e sistemas operacionais relacionadas à:**
      - **Autenticação de usuários;**
      - **Autorização de acesso aos recursos;**
      - **Trânsito seguro de dados na rede (data in-transit);**
      - **Armazenamento seguro de dados (data at-rest);**
      - **Alta disponibilidade de recursos.**
  - **Base de conhecimento:**
    - **Common Weakness Enumeration (CWE)**
    - **Open Web Application Security (OWASP)**

Processo de Avaliação de Riscos – Identificação dos Riscos

Conceitos básicos: Identificação de vulnerabilidades de cibersegurança

- **Identificação das fragilidades presentes nos sistemas de informação e na infraestrutura de TIC.**
- **Vulnerabilidades na operação e no gerenciamento:**
  - **Verificar quais são as falhas de segurança na operação e na gestão dos sistemas de informação ou da infraestrutura de TIC.**
    - **Exemplo: executar testes de penetração nos sistemas de aplicação, serviços e sistemas operacionais para detectar falhas de:**
      - **Autenticação de usuários;**
      - **Autorização de acesso aos recursos;**
      - **Trânsito seguro de dados na rede (data in-transit);**
      - **Armazenamento seguro de dados (data at-rest);**
      - **Alta disponibilidade de recursos.**
  - **Base de conhecimento:**
    - **Common Vulnerability and Exposures (CVE)**
    - **National Vulnerability Database (NVD)**

Processo de Avaliação de Riscos – Identificação dos Riscos

Conceitos básicos: Ameaça

- **Potencial para violação da segurança**
  - **Quando há uma entidade, circunstância, capacidade, ação ou evento que pode causar mal ao sistema.**
- ***Ameaças Acidentais***
  - **Quando não há intenção premeditada para sua ocorrência.**
    - **Ex: o mau funcionamento do sistema, os erros operacionais graves, os erros em software (bugs) ou os desastres naturais (incêndio, inundação, terremoto, etc).**
- ***Ameaças Intencionais***
  - **Quando envolvem a possibilidade de se realizar uma ação maliciosa contra um alvo específico.**
    - **Ex: uma simples inspeção de conteúdo com ferramentas de monitoramento ou uso malicioso de conhecimentos especiais do sistema para prejudica-lo.**

Processo de Avaliação de Riscos – Identificação dos Riscos

Conceitos básicos: Agente de Ameaça

- **Fonte que pode causar um incidente de segurança da informação por meio da exploração de uma vulnerabilidade.**

Tipo de Agente	Descrição	Exemplos
Interno (insider)	Atua dentro da organização com acesso legítimo.	Funcionário desonesto, técnico negligente, prestador de serviço terceirizado.
Externo (outsider)	Atua fora do perímetro da organização.	Hacker, grupo de cibercriminisos, concorrente.
Parceiro/Fornecedor	Atua por meio de relações de negócio.	Empresa terceirizada com acesso à rede corporativa.
Ambiental/Natural	Ameaça física ou ambiental.	Tempestades, incêndios, inundações, falha de energia.
Tecnológico/Acidental	Ação não intencional de sistemas ou pessoas.	Erro humano, falha de software, mau funcionamento de equipamento.

Processo de Avaliação de Riscos – Identificação dos Riscos

Conceitos básicos: Agente de Ameaça

- **Características do agente de ameaça analisadas para se estimar a probabilidade e a consequência de uma ação maliciosa:**
  - **Motivação:**
    - **Por que agir – é a força condutora (ganho financeiro, vingança, ideologia).**
  - **Intenção:**
    - **Para que agir – é o propósito específico da ação (espionar, sabotar, roubar).**
  - **Capacidade:**
    - **Se é capaz de agir – grau de conhecimento técnico ou de poder para explorar a vulnerabilidade.**
  - **Oportunidade:**
    - **Quando e onde pode agir – se há acesso, tempo ou contexto favorável para a exploração.**

Processo de Avaliação de Riscos – Identificação dos Riscos

Exemplo: Fatores que motivam a exploração de vulnerabilidades por agentes de ameaça.

- **Vulnerabilidade:**
  - **Cabos de rede de dados expostos em área comum no prédio da organização.**
- **Tipos de Agente de Ameaça:**
  - **Funcionário mal-intencionado**
  - **Prestador de serviço terceirizado**
  - **Visitante ocasional ou curioso**
  - **Invasor externo (intruso físico)**
  - **Agente ambiental ou acidental**

Processo de Avaliação de Riscos – Identificação dos Riscos

Exemplo: Fatores que motivam a exploração de vulnerabilidades por agentes de ameaça.

Agente de Ameaça	Motivação	Intenção	Capacidade	Oportunidade
Funcionário mal-intencio-nado (interno)	Obter ganho financeiro, reconhecimento ou vingança.	Espionar sistemas internos ou causar prejuízo deliberado.	**Média/Alta** – conhece a infraestrutura local.	**Alta** – circula livremente pelas áreas comuns.
Prestador de serviço terceirizado	Vingança ou lucro vendendo acesso à rede ou dados.	Parar a rede, inserir backdoor, coletar dados e revende-los	**Alta** – experiência técnica em redes corporativas.	**Média** – acesso temporário e pouco monitorado.
Visitante ocasional ou curioso	Satisfazer curiosidade ou testar limites.	Conectar dispositivo pessoal à rede.	**Baixa** – pouco conhecimento técnico.	**Alta** – livre acesso visual e físico.
Invasor externo (intruso físico)	Ganhar dinheiro ou reputação no submundo cibernético.	Obter acesso à rede interna ou causar sabotagem.	**Alta** – domínio de técnicas de intrusão.	**Média** – depende de falhas físicas de segurança.
Agente ambiental/ acidental	Nenhuma – evento não deliberado (erro, desgaste ou ação natural).	Nenhuma – não há intenção consciente.	N/A	**Alta** – exposição física dos cabos.

Processo de Avaliação de Riscos – Identificação dos Riscos

Exemplo: Fatores que motivam a exploração de vulnerabilidades por agentes de ameaça.

- **Os quatro fatores, quando combinados, permitem avaliar com mais precisão a Probabilidade Inerente (Pi).**

  Probabilidade Inerente (Pi) ∝ f(Motivação, Intenção, Capacidade, Oportunidade)

- **A probabilidade de exploração cresce substancialmente quando três fatores coincidem:**
  1. **Alta motivação: agentes com incentivos claros (como lucro financeiro, vingança ou prestígio) tendem a procurar vulnerabilidades de baixo esforço e alto retorno, como pontos físicos desprotegidos.**
  2. **Alta capacidade: técnicos de manutenção, funcionários com conhecimento em redes ou invasores experientes têm plena habilidade para identificar cabos ativos, testar portas e conectar dispositivos de captura (sniffers, rogue access points).**
  3. **Alta oportunidade: a presença de trechos expostos em áreas comuns (corredores, recepções, dutos abertos, áreas compartilhadas) oferece acesso frequente, muitas vezes sem supervisão nem monitoramento com CFTV.**

Processo de Avaliação de Riscos – Identificação de Riscos

Exemplo: Listagem de ameaças para a vulnerabilidade.

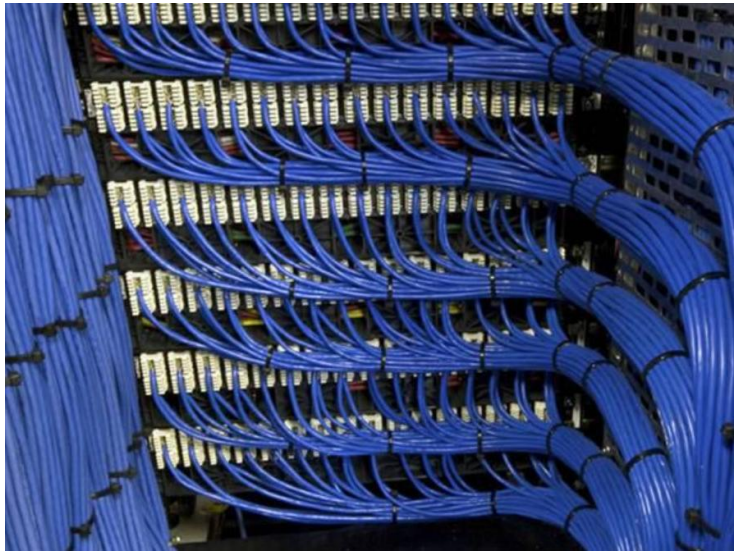
- **Vulnerabilidade:**
  - **Cabos de rede de dados expostos em área comum no prédio da organização.**
- **Ameaças:**

Acesso físico não autorizado (grampeamento)

Interceptação de tráfego (sniffing)

Injeção de tráfego malicioso

Infecção com código malicioso



Interrupção física ou sabotagem (corte do cabo)

Instalação de dispositivo clandestino (rogue device)

Perda de desempenho por interferência de fatores ambientais (umidade, calor, luz solar)

Fonte: https://www.tecnoims.com.br/imagens/informacoes/rede-logica-eletrica-01.jpg

Processo de Avaliação de Riscos – Análise de Riscos

Critério para análise de riscos: Probabilidade.

Probabilidade	Descrição
BAIXA	É esperado que a ameaça não se concretize na maioria dos casos. A vulnerabilidade é difícil de ser identificada e explorada por uma entidade hostil ou por um usuário mal-intencionado. (1% a 33% de chance de acontecer)
MÉDIA	Existe uma possibilidade razoável de que a ameaça se concretize. A vulnerabilidade exige um esforço significativo para ser identificada e explorada por uma entidade hostil ou por um usuário mal-intencionado. (34% a 66% de chance de acontecer)
ALTA	É esperado que a ameaça se concretize na maioria dos casos. A vulnerabilidade é fácil de ser identificada e explorada por uma entidade hostil ou por um usuário mal-intencionado. (67% a 100% de chance de acontecer)

Processo de Avaliação de Riscos – Análise de Riscos

Critério para análise de riscos: Consequência.

Consequência	Descrição
Baixo	Se explorada, a ameaça **não compromete** a confidencialidade, a integridade ou a disponibilidade do sistema. O funcionamento **permanece normal** e **não há risco** de vazamento de dados.
Médio	A ameaça pode **afetar parcialmente** a confidencialidade, a integridade ou a disponibilidade. Embora **não comprometa** diretamente dados sensíveis, pode executar ações não autorizadas que **degradem o desempenho**, provoquem **indisponibilidade temporária** ou causem **exposição limitada** de informações.
Alto	A ameaça pode **comprometer de forma significativa** a confidencialidade, a integridade e/ou a disponibilidade. Pode resultar em **vazamento de dados sensíveis**, **alteração indevida de informações** ou **interrupção total** do funcionamento do sistema.

Processo de Avaliação de Riscos – Análise de Riscos

Critério para análise de riscos: Matriz de Risco (Mapa de Calor).

Matriz de Risco			
	Probabilidade		
Consequência	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Avaliação de Riscos

Critério para avaliação de riscos e tratamento de riscos:

Risco	Descrição	Tratamento
Baixo	**Risco tolerável**, sem necessidade de acompanhamento especial.	Aceitar
Médio	**Risco tolerável**, porém, com chances razoáveis de causar um impacto moderado. Neste caso, deve ser monitorado, sem urgência para a implementação de controles.	Aceitar
Alto	**Risco não tolerável,** pois o impacto e sua probabilidade ultrapassam os critérios definidos. Deve ser monitorado continuamente e os controles devem ser implementados imediatamente.	Tratar (modificar, evitar, compartilhar)

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.1	**Acesso físico não autorizado (grampeamento)** Probabilidade: Consequência:			

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.1	**Acesso físico não autorizado (grampeamento)** Probabilidade: o acesso físico é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência:	Alta		

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.1	**Acesso físico não autorizado (grampeamento)** Probabilidade: o acesso físico é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência: permite invasão da rede interna, acesso indevido a sistemas e vazamento de informações.	Alta	Alta	

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.1	**Acesso físico não autorizado (grampeamento)** Probabilidade: o acesso físico é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência: permite invasão da rede interna, acesso indevido a sistemas e vazamento de informações.	Alta	Alta	**Alto**

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.1	**Acesso físico não autorizado (grampeamento)** Probabilidade: o acesso físico é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência: permite invasão da rede interna, acesso indevido a sistemas e vazamento de informações.	Alta	Alta	**Alto**
A3.3.1.1.2	**Interceptação de tráfego (sniffing)** Probabilidade: Consequência:			

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.1	**Acesso físico não autorizado (grampeamento)** Probabilidade: o acesso físico é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência: permite invasão da rede interna, acesso indevido a sistemas e vazamento de informações.	Alta	Alta	**Alto**
A3.3.1.1.2	**Interceptação de tráfego (sniffing)** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para captura de dados em trânsito. Consequência:.	Média		

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.1	**Acesso físico não autorizado (grampeamento)** Probabilidade: o acesso físico é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência: permite invasão da rede interna, acesso indevido a sistemas e vazamento de informações.	Alta	Alta	**Alto**
A3.3.1.1.2	**Interceptação de tráfego (sniffing)** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para captura de dados em trânsito. Consequência: pode resultar em roubo de credenciais e informações sensíveis.	Média	Alta	

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.1	**Acesso físico não autorizado (grampeamento)** Probabilidade: o acesso físico é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência: permite invasão da rede interna, acesso indevido a sistemas e vazamento de informações.	Alta	Alta	**Alto**
A3.3.1.1.2	**Interceptação de tráfego (sniffing)** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para captura de dados em trânsito. Consequência: pode resultar em roubo de credenciais e informações sensíveis.	Média	Alta	**Alto**

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.3	**Injeção de tráfego malicioso** Probabilidade: Consequência:			

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.3	**Injeção de tráfego malicioso** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para execução de ARP spoofing ou DHCP rogue. Consequência:	Média		

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.3	**Injeção de tráfego malicioso** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para execução de ARP spoofing ou DHCP rogue. Consequência: pode resultar em comprometimento da integridade das comunicações, redirecionamento de tráfego e eventual sequestro de sessão.	Média	Alta	

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.3	**Injeção de tráfego malicioso** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para execução de ARP spoofing ou DHCP rogue. Consequência: pode resultar em comprometimento da integridade das comunicações, redirecionamento de tráfego e eventual sequestro de sessão.	Média	Alta	**Alto**

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.3	**Injeção de tráfego malicioso** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para execução de ARP spoofing ou DHCP rogue. Consequência: pode resultar em comprometimento da integridade das comunicações, redirecionamento de tráfego e eventual sequestro de sessão.	Média	Alta	**Alto**
A3.3.1.1.4	**Infecção com código malicioso** Probabilidade: Consequência:			

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.3	**Injeção de tráfego malicioso** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para execução de ARP spoofing ou DHCP rogue. Consequência: pode resultar em comprometimento da integridade das comunicações, redirecionamento de tráfego e eventual sequestro de sessão.	Média	Alta	**Alto**
A3.3.1.1.4	**Infecção com código malicioso** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para disseminar código malicioso na rede. Consequência:	Média		

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.3	**Injeção de tráfego malicioso** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para execução de ARP spoofing ou DHCP rogue. Consequência: pode resultar em comprometimento da integridade das comunicações, redirecionamento de tráfego e eventual sequestro de sessão.	Média	Alta	**Alto**
A3.3.1.1.4	**Infecção com código malicioso** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para disseminar código malicioso na rede. Consequência: pode resultar na infecção de outros dispositivos presentes na rede.	Média	Alta	

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.3	**Injeção de tráfego malicioso** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para execução de ARP spoofing ou DHCP rogue. Consequência: pode resultar em comprometimento da integridade das comunicações, redirecionamento de tráfego e eventual sequestro de sessão.	Média	Alta	**Alto**
A3.3.1.1.4	**Infecção com código malicioso** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para disseminar código malicioso na rede. Consequência: pode resultar na infecção de outros dispositivos presentes na rede.	Média	Alta	**Alto**

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.5	**Interrupção física ou sabotagem (corte do cabo)** Probabilidade: Consequência:			

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.5	**Interrupção física ou sabotagem (corte do cabo)** Probabilidade: corte do cabo é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência:	Alta		

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.5	**Interrupção física ou sabotagem (corte do cabo)** Probabilidade: corte do cabo é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência: dispositivos que usam o cabo ficam inoperantes e prejudicam o trabalho dos colaboradores da organização (perda de disponibilidade).	Alta	Alta	

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.5	**Interrupção física ou sabotagem (corte do cabo)** Probabilidade: corte do cabo é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência: dispositivos que usam o cabo ficam inoperantes e prejudicam o trabalho dos colaboradores da organização (perda de disponibilidade).	Alta	Alta	**Alto**

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.5	**Interrupção física ou sabotagem (corte do cabo)** Probabilidade: corte do cabo é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência: dispositivos que usam o cabo ficam inoperantes e prejudicam o trabalho dos colaboradores da organização (perda de disponibilidade).	Alta	Alta	**Alto**
A3.3.1.1.6	**Instalação de dispositivo clandestino (rogue device)** Probabilidade: Consequência:			

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.5	**Interrupção física ou sabotagem (corte do cabo)** Probabilidade: corte do cabo é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência: dispositivos que usam o cabo ficam inoperantes e prejudicam o trabalho dos colaboradores da organização (perda de disponibilidade).	Alta	Alta	**Alto**
A3.3.1.1.6	**Instalação de dispositivo clandestino (rogue device)** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para instalar um rogue AP. Consequência:	Média		

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.5	**Interrupção física ou sabotagem (corte do cabo)** Probabilidade: corte do cabo é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência: dispositivos que usam o cabo ficam inoperantes e prejudicam o trabalho dos colaboradores da organização (perda de disponibilidade).	Alta	Alta	**Alto**
A3.3.1.1.6	**Instalação de dispositivo clandestino (rogue device)** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para instalar um rogue AP. Consequência: ponto de acesso não autorizado ligado na rede, evasão de perímetro e exposição da rede da organização.	Média	Alta	

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.5	**Interrupção física ou sabotagem (corte do cabo)** Probabilidade: corte do cabo é fácil, a vulnerabilidade é evidente e não requer conhecimento técnico. Consequência: dispositivos que usam o cabo ficam inoperantes e prejudicam o trabalho dos colaboradores da organização (perda de disponibilidade).	Alta	Alta	**Alto**
A3.3.1.1.6	**Instalação de dispositivo clandestino (rogue device)** Probabilidade: exige algum conhecimento técnico e acesso físico ao cabeamento para instalar um rogue AP. Consequência: ponto de acesso não autorizado ligado na rede, evasão de perímetro e exposição da rede da organização.	Média	Alta	**Alto**

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		Pi	Ci	Ri
A3.3.1.1.7	**Perda de desempenho por interferência de fatores ambientais (umidade, calor, luz solar)** Probabilidade:. Consequência:			

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.7	**Perda de desempenho por interferência de fatores ambientais (umidade, calor, luz solar)** Probabilidade: o ambiente fechado do prédio reduz a chance de fatores ambientais interferirem no desempenho. Consequência:	Baixa		

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.7	**Perda de desempenho por interferência de fatores ambientais (umidade, calor, luz solar)** Probabilidade: o ambiente fechado do prédio reduz a chance de fatores ambientais interferirem no desempenho. Consequência: pode resultar em intermitência na operação da rede ou indisponibilidade temporária para alguns equipamentos.	Baixa	Média	

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		**Pi**	**Ci**	**Ri**
A3.3.1.1.7	**Perda de desempenho por interferência de fatores ambientais (umidade, calor, luz solar)** Probabilidade: o ambiente fechado do prédio reduz a chance de fatores ambientais interferirem no desempenho. Consequência: pode resultar em intermitência na operação da rede ou indisponibilidade temporária para alguns equipamentos.	Baixa	Média	**Baixo**

Processo de Avaliação de Riscos – Análise de Riscos

Ativo: Rede de Dados Cabeada

3.3.1 Rede de Dados Cabeada				
V3.3.1.1 Cabeamento de rede de dados exposto e de fácil acesso em áreas comuns.		Pi	Ci	Ri
A3.3.1.1.1	Acesso físico não autorizado (grampeamento)	Alta	Alta	**Alto**
A3.3.1.1.2	Interceptação de tráfego (sniffing)	Média	Alta	**Alto**
A3.3.1.1.3	Injeção de tráfego malicioso	Média	Alta	**Alto**
A3.3.1.1.4	Infecção com código malicioso	Média	Alta	**Alto**
A3.3.1.1.5	Interrupção física ou sabotagem (corte do cabo)	Alta	Alta	**Alto**
A3.3.1.1.6	Instalação de dispositivo clandestino (rogue device)	Média	Alta	**Alto**
A3.3.1.1.7	Perda de desempenho por interferência de fatores ambientais (umidade, calor, luz solar)	Baixa	Média	**Baixo**

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.1		A3.3.1.1.1	Modificar			

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.1	Proteger fisicamente os cabos e pontos de rede; implementar NAC e autenticação de portas.	A3.3.1.1.1	Modificar			

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.1	Proteger fisicamente os cabos e pontos de rede; implementar NAC e autenticação de portas.	A3.3.1.1.1	Modificar			

Para calcularmos a redução da probabilidade e da consequência, um método prático é associar a efetividade do controle a uma redução de nível...

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.1	Proteger fisicamente os cabos e pontos de rede; implementar NAC e autenticação de portas.	A3.3.1.1.1	Modificar			

Para calcularmos a redução da probabilidade e da consequência, um método prático é associar a efetividade do controle a uma redução de nível...

Critério	Pergunta-chave	Escala
Cobertura	O controle atua diretamente sobre a vulnerabilidade?	Alto / Médio / Baixo
Força	O controle é técnico, administrativo ou físico? (controles técnicos geralmente são mais eficazes)	Alto / Médio / Baixo
Confiabilidade	O controle é monitorado, auditado e testado periodicamente?	Alto / Médio / Baixo

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.1	Proteger fisicamente os cabos e pontos de rede; implementar NAC e autenticação de portas.	A3.3.1.1.1	Modificar			

Para calcularmos a redução da probabilidade e da consequência, um método prático é associar a efetividade do controle a uma redução de nível...

Efetividade do Controle	Redução na Probabilidade	Redução na Consequência
Alta	Reduz 2 níveis.	Reduz 1 nível.
Média	Reduz 1 nível.	Reduz 0 ou 1 nível.
Baixa	Reduz 0 ou 1 nível.	Normalmente, não altera.

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.1	Proteger fisicamente os cabos e pontos de rede; implementar NAC e autenticação de portas.	A3.3.1.1.1	Modificar			

ou verificar o tipo do controle...

- ***Preventivo***: atua antes que um incidente ocorra, para evita-lo (ex: controle de acesso à rede, firewall).
- ***Detectivo***: atua durante um incidente para identifica-lo (ex: IDS, monitoramento, auditoria).
- ***Corretivo***: atua após um incidente para minimizar seus impactos e restaurar a normalidade (ex: backup, redundância, planos de recuperação).

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.1	Proteger fisicamente os cabos e pontos de rede; implementar NAC e autenticação de portas.	A3.3.1.1.1	Modificar			

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.1	Proteger fisicamente os cabos e pontos de rede; implementar NAC e autenticação de portas.	A3.3.1.1.1	Modificar	Baixa	Alta	Médio

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.2		A3.3.1.1.2	Modificar			

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.2	Criptografar as comunicações (TLS), segmentar e monitorar com IDS/IPS.	A3.3.1.1.2	Modificar			

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.2	Criptografar as comunicações (TLS), segmentar e monitorar com IDS/IPS.	A3.3.1.1.2	Modificar	Baixa	Média	**Baixo**

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.3		A3.3.1.1.3	Modificar			

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.3	Implantar controles detectivos nos switches gerenciáveis (ARP inspection, DHCP snooping), monitorar com IDS/IPS.	A3.3.1.1.3	Modificar			

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.3	Implantar controles detectivos nos switches gerenciáveis (ARP inspection, DHCP snooping), monitorar com IDS/IPS.	A3.3.1.1.3	Modificar	Baixa	Baixo	**Baixo**

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.4		A3.3.1.1.4	Modificar			

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.4	Adotar solução antimalware nos dispositivos ligados na rede.	A3.3.1.1.4	Modificar			

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.4	Adotar solução antimalware nos dispositivos ligados na rede.	A3.3.1.1.4	Modificar	Baixa	Média	**Baixo**

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.5		A3.3.1.1.5	Modificar			

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.5	Proteger fisicamente os cabos e pontos de rede; monitoramento com CFTV.	A3.3.1.1.5	Modificar			

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.5	Proteger fisicamente os cabos e pontos de rede; monitoramento com CFTV.	A3.3.1.1.5	Modificar	Baixa	Média	**Baixo**

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.6		A3.3.1.1.6	Modificar			

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.6	Proteger fisicamente os cabos e pontos de rede; implementar NAC e autenticação de portas.	A3.3.1.1.6	Modificar			

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Tratamento de Riscos

Ativo: Rede de Dados Cabeada

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T3.3.1.6	Proteger fisicamente os cabos e pontos de rede; implementar NAC e autenticação de portas.	A3.3.1.1.6	Modificar	Baixa	Alta	**Médio**

ou verificar o tipo do controle...

Tipo do Controle	Redução na Probabilidade	Redução na Consequência
Preventivo (ex: firewall, controle de acesso)	X	-
Corretivo ou de Contingência (ex: backup, plano de recuperação, redundância)	-	X
Detectivo (ex: IDS, monitoramento, auditoria)	X	X

Processo de Avaliação de Riscos – Categoria de Controles da ISO/IEC 27002:2022

Categoria de Controles – ISO/IEC 27002:2022

Controle Organizacionais (Seção 5)

- Políticas de segurança da informação (5.1) - **Preventivo**
- Papéis e responsabilidades pela segurança da informação (5.2) - **Preventivo**
- Segregação de funções (5.3) - **Preventivo**
- Responsabilidades da direção (5.4) - **Preventivo**
- Contato com autoridades (5.5) - **Preventivo e Corretivo**
- Contato com grupos de interesse especial (5.6) - **Preventivo e Corretivo**
- Inteligência de ameaças (5.7) - **Preventivo, Detectivo e Corretivo**
- Segurança da informação no gerenciamento de projetos (5.8) - **Preventivo**
- Inventário de informações e outros ativos associados (5.9) - **Preventivo**
- Uso aceitável de informações e outros ativos associados (5.10) - **Preventivo**
- Devolução de ativos (5.11) - **Preventivo**
- Classificação das informações (5.12) - **Preventivo**
- Rotulagem de informações (5.13) - **Preventivo**
- Transferência de informações (5.14) - **Preventivo**
- Controle de acesso (5.15) - **Preventivo**
- Gestão de identidade (5.16) - **Preventivo**
- Informações de autenticação (5.17) - **Preventivo**

Processo de Avaliação de Riscos – Categoria de Controles da ISO/IEC 27002:2022

Categoria de Controles – ISO/IEC 27002:2022

Controle Organizacionais (Seção 5)

- Direitos de acesso (5.18) - **Preventivo**
- Segurança da informação nas relações com fornecedores (5.19) - **Preventivo**
- Abordagem da segurança da informação nos contratos de fornecedores (5.20) - **Preventivo**
- Gestão da segurança da informação na cadeia de fornecimento de TIC (5.21) - **Preventivo**
- Monitoramento, análise crítica e gestão de mudanças dos serviços de fornecedores (5.22) - **Preventivo**
- Segurança da informação para uso de serviços em nuvem (5.23) - **Preventivo**
- Planejamento e preparação da gestão de incidentes de segurança da informação (5.24) - **Corretivo**
- Avaliação e decisão sobre eventos de segurança da informação (5.25) - **Detectivo**
- Resposta a incidentes de segurança da informação (5.26) - **Corretivo**
- Aprendizado com incidentes de segurança da informação (5.27) - **Preventivo**
- Coleta de evidências (5.28) - **Corretivo**
- Segurança da informação durante a disrupção (5.29) - **Preventivo e Corretivo**
- Prontidão de TIC para continuidade de negócios (5.30) - **Corretivo**
- Requisitos legais, estatutários, regulamentares e contratuais (5.31) - **Preventivo**
- Direitos de propriedade intelectual (5.32) - **Preventivo**
- Proteção de registros (5.33) - **Preventivo**
- Privacidade e proteção de dados pessoais (5.34) - **Preventivo**

Processo de Avaliação de Riscos – Categoria de Controles da ISO/IEC 27002:2022

Categoria de Controles – ISO/IEC 27002:2022

Controle Organizacionais (Seção 5)

- Análise crítica independente da segurança da informação (5.35) - **Preventivo e Corretivo**
- Conformidade com políticas, regras e normas para segurança da informação (5.36) - **Preventivo**
- Documentação dos procedimentos de operação (5.37) - **Preventivo e Corretivo**

Controles de Pessoas (Seção 6)

- Seleção (6.1) - **Preventivo**
- Termos e condições de contratação (6.2) - **Preventivo**
- Conscientização, educação e treinamento em segurança da informação (6.3) - **Preventivo**
- Processo disciplinar (6.4) - **Preventivo**
- Responsabilidades após encerramento ou mudança da contratação (6.5) - **Preventivo**
- Acordos de confidencialidade ou não divulgação (6.6) - **Preventivo**
- Trabalho remoto (6.7) - **Preventivo e Corretivo**
- Relato de eventos de segurança da informação (6.8) - **Detectivo**

Processo de Avaliação de Riscos – Categoria de Controles da ISO/IEC 27002:2022

Categoria de Controles – ISO/IEC 27002:2022

Controles Físicos (Seção 7)

- Perímetros de segurança física (7.1) - **Preventivo**
- Entrada física (7.2) - **Preventivo**
- Segurança de escritórios, salas e instalações (7.3) - **Preventivo**
- Monitoramento de segurança física (7.4) - **Preventivo e Detectivo**
- Proteção contra ameaças físicas e ambientais (7.5) - **Preventivo**
- Trabalho em áreas seguras (7.6) - **Preventivo**
- Mesa limpa e tela limpa (7.7) - **Preventivo**
- Localização e proteção de equipamentos (7.8) - **Preventivo**
- Segurança de ativos fora das instalações da organização (7.9) - **Preventivo**
- Mídia de armazenamento (7.10) - **Preventivo**
- Serviços de infraestrutura (7.11) - **Preventivo e Detectivo**
- Segurança do cabeamento (7.12) - **Preventivo**
- Manutenção de equipamentos (7.13) - **Preventivo**
- Descarte seguro ou reutilização de equipamentos (7.14) - **Preventivo**

Processo de Avaliação de Riscos – Categoria de Controles da ISO/IEC 27002:2022

Categoria de Controles – ISO/IEC 27002:2022

Controles Tecnológicos (Seção 8)

- Dispositivos endpoint do usuário (8.1) - **Preventivo**
- Direitos de acessos privilegiados (8.2) - **Preventivo**
- Restrição de acesso à informação (8.3) - **Preventivo**
- Acesso ao código-fonte (8.4) - **Preventivo**
- Autenticação segura (8.5) - **Preventivo**
- Gestão de capacidade (8.6) - **Preventivo e Detectivo**
- Proteção contra malware (8.7) - **Preventivo, Detectivo e Corretivo**
- Gestão de vulnerabilidades técnicas (8.8) - **Preventivo**
- Gestão de configuração (8.9) - **Preventivo**
- Exclusão de informações (8.10) - **Preventivo**
- Mascaramento de dados (8.11) - **Preventivo**
- Prevenção de vazamento de dados (8.12) - **Preventivo e Detectivo**
- Backup das informações (8.13) - **Corretivo**
- Redundância dos recursos de tratamento de informações (8.14) - **Preventivo**
- Log (8.15) - **Detectivo**
- Atividades de monitoramento (8.16) - **Detectivo e Corretivo**
- Sincronização do relógio (8.17) - **Detectivo**

Processo de Avaliação de Riscos – Categoria de Controles da ISO/IEC 27002:2022

Categoria de Controles – ISO/IEC 27002:2022

Controles Tecnológicos (Seção 8)

- Uso de programas utilitários privilegiados (8.18) - **Preventivo**
- Instalação de software em sistemas operacionais (8.19) - **Preventivo**
- Segurança de redes (8.20) - **Preventivo e Detectivo**
- Segurança dos serviços de rede (8.21) - **Preventivo**
- Segregação de redes (8.22) - **Preventivo**
- Filtragem da web (8.23) - **Preventivo**
- Uso de criptografia (8.24) - **Preventivo**
- Ciclo de vida de desenvolvimento seguro (8.25) - **Preventivo**
- Requisitos de segurança da aplicação (8.26) - **Preventivo**
- Princípios de arquitetura e engenharia de sistemas seguros (8.27) - **Preventivo**
- Codificação segura (8.28) - **Preventivo**
- Testes de segurança em desenvolvimento e aceitação (8.29) - **Preventivo**
- Desenvolvimento terceirizado (8.30) - **Preventivo e Detectivo**
- Separação dos ambientes de desenvolvimento, teste e produção (8.31) - **Preventivo**
- Gestão de mudanças (8.32) - **Preventivo**
- Informações de testes (8.33) - **Preventivo**
- Proteção de sistemas de informação durante os testes de auditoria (8.34) - **Preventivo**

Obrigado!

Anderson Oliveira da Silva
Ph. D. Ciências em Informática
Engenheiro de Computação
anderson@inf.puc-rio.br

Pós-graduação em Compliance de Cibersegurança

Departamento de Informática
Coordenação Central de Educação Continuada
PUC-Rio