



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

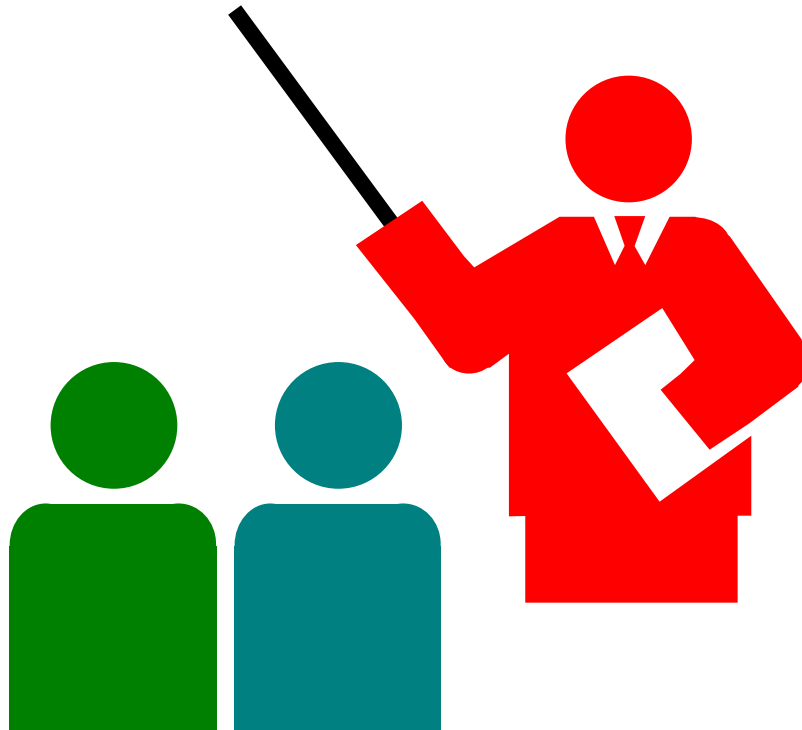
PUC-Rio

Processo de Avaliação de Riscos e Tratamento de Riscos:

- **Ativo: 1.1.2 Rede de Dados Sem Fio**
 - **Vulnerabilidades:**
 - 1.1.2.1 Rede sem fio extrapola o limite físico da organização.
 - 1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.
 - 1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.
 - 1.1.2.4 Rede de dados sem fio equipada apenas com dispositivos principais, sem disponibilidade imediata de unidade reserva para substituição em caso de pane.
- **Ativo: 1.1.3 Correio Eletrônico**
 - **Vulnerabilidade:**
 - 1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

Processo de Avaliação de Riscos

3



Processo de Avaliação de Riscos – Identificação dos Riscos

4

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 cibercrimininos, 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

5

Conceitos básicos: Agente de Ameaça

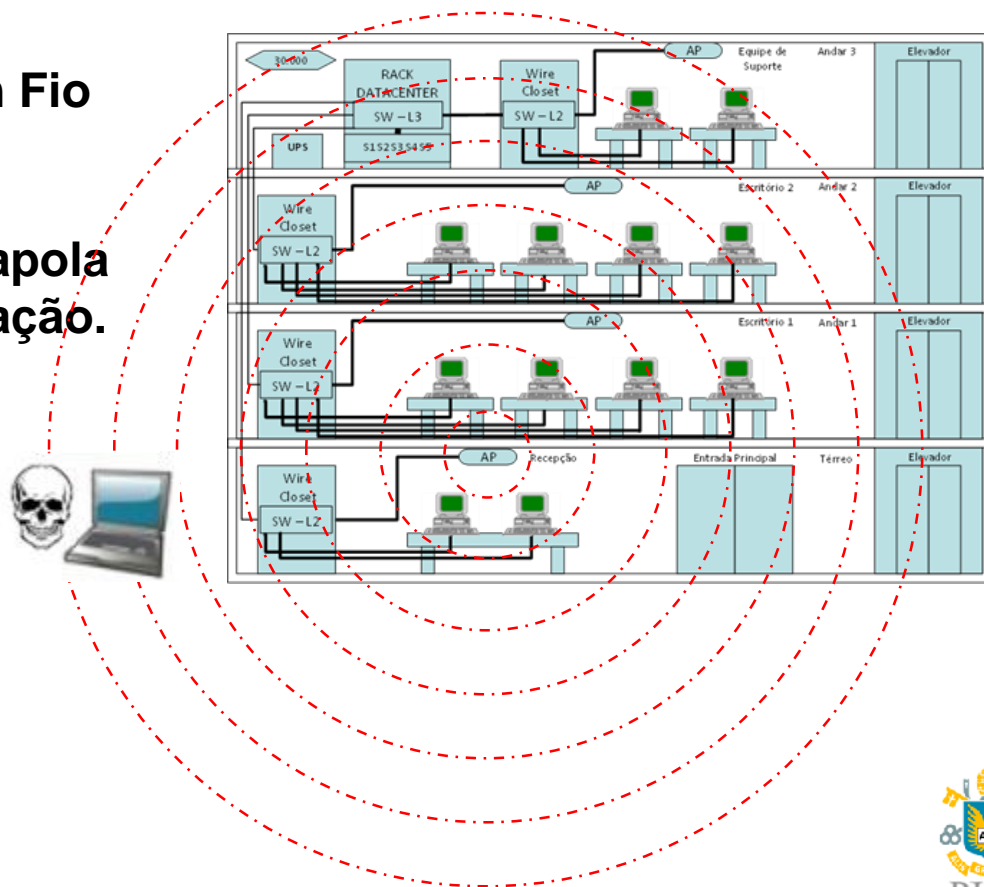
- **Características do agente de ameaça analisadas para se estimar a probabilidade e a consequência de uma ação maliciosa:**
 - **Motivação:**
 - Por que agir – é a força condutora (ganho financeiro, vingança, ideologia).
 - **Intenção:**
 - Para que agir – é o propósito específico da ação (espionar, 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

6

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

- **Ativo:**
 - 1.1.2 Rede de Dados Sem Fio
- **Vulnerabilidade:**
 - 1.1.2.1 Rede sem fio extrapola o limite físico da organização.



Processo de Avaliação de Riscos – Identificação dos Riscos

7

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

Agente de Ameaça	Motivação	Intenção	Capacidade	Oportunidade
Funcionário mal-intencionado (interno)	Obter ganho financeiro, retaliação, insatisfação profissional ou vingança.	Acesso não autorizado fora do perímetro físico; exfiltração de dados; uso indevido da infraestrutura.	Alta – conhece a infraestrutura local, políticas internas, SSIDs, métodos de autenticação e credenciais válidas	Alta – extrapolação do sinal permite acesso fora do horário de trabalho ou fora das áreas controladas.
Prestador de serviço terceirizado	Vingança ou lucro vendendo acesso à rede ou dados.	Reutilizar acesso após o término do contrato; coletar informações internas.	Média/Alta – pode ter experiência técnica relevante e acesso prévio autorizado..	Alta – extrapolação do sinal permite acesso fora do horário de trabalho ou fora das áreas controladas.
Visitante ocasional ou curioso	Satisfazer curiosidade ou obter acesso gratuito à Internet.	Conectar dispositivo pessoal à rede.	Baixa – pouco conhecimento técnico.	Média – Depende de redes abertas ou com senha fraca..
Invasor externo (intruso físico)	Ganhar dinheiro com espionagem corporativa, preparar ataques cibernéticos mais sofisticados..	Obter acesso à rede interna, capturar tráfego, explorar sistemas internos ou causar sabotagem.	Alta – domínio de técnicas de intrusão (sniffing, cracking, evil twin, deauthentication)	Alta – extrapolação do sinal permite acesso em locais públicos próximos à organização.
Agente ambiental/acidental	Nenhuma – não há motivação.	Nenhuma – não há intenção consciente.	N/A	Média – extrapolação do sinal por erro na configuração de potência ou posição do AP..

Processo de Avaliação de Riscos – Identificação dos Riscos

8

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) \propto 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 a extrapolação do sinal da rede sem fio da organização.
 2. **Alta capacidade:** técnicos de manutenção, funcionários com conhecimento em redes ou invasores experientes têm plena habilidade para explorar a vulnerabilidade (por exemplo, com técnicas de sniffing, cracking, evil twin, deauthentication).
 3. **Alta oportunidade:** extrapolação do sinal permite acesso em locais públicos próximos à organização, ou seja, fora das áreas controladas e fora do horário de trabalho.

Processo de Avaliação de Riscos – Análise de Riscos

9

Critério para análise de riscos: Probabilidade.

Probabilidade	Descrição
BAIXA	<p>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.</p> <p>(1% a 33% de chance de acontecer)</p>
MÉDIA	<p>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.</p> <p>(34% a 66% de chance de acontecer)</p>
ALTA	<p>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.</p> <p>(67% a 100% de chance de acontecer)</p>

Processo de Avaliação de Riscos – Análise de Riscos

10

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

11

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

12

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 – Identificação de Riscos

13

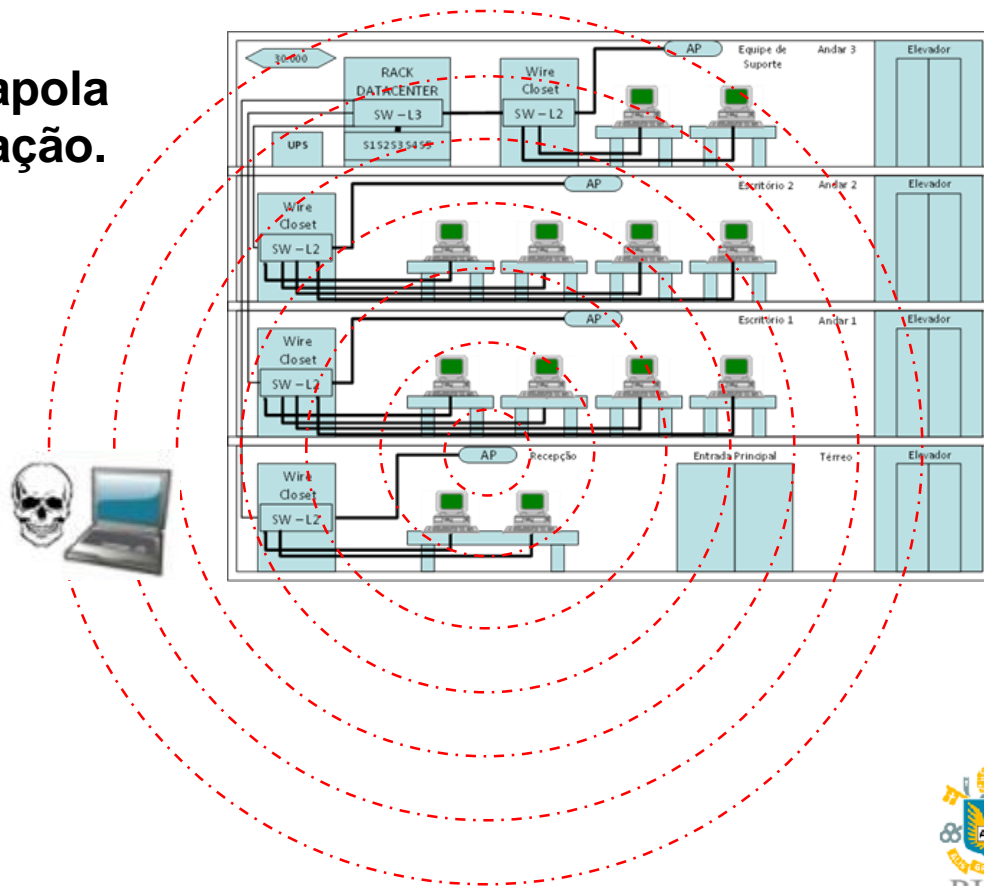
Exemplo: Listagem de ameaças para a vulnerabilidade.

- **Vulnerabilidade:**
 - **1.1.2.1 Rede sem fio extrapola o limite físico da organização.**

- **Ameaças:**

1.1.2.1.1 Captura de sinal fora das dependências da organização

1.1.2.1.2 Jamming do sinal originado fora das dependências da organização



Processo de Avaliação de Riscos – Análise de Riscos

14

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.1 Rede sem fio extrapola o limite físico da organização.

A1.1.2.1.1

Captura de sinal fora das dependências da organização

Probabilidade:

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

15

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.1 Rede sem fio extrapola o limite físico da organização.

A1.1.2.1.1

Captura de sinal fora das dependências da organização

Probabilidade: o sinal 802.11n vaza para áreas externas; não há controle de potência nem política de cobertura.

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

16

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.1 Rede sem fio extrapola o limite físico da organização.

A1.1.2.1.1

Captura de sinal fora das dependências da organização

Probabilidade: o sinal 802.11n vaza para áreas externas; não há controle de potência nem política de cobertura.

Consequência:

Pi**Ci****Ri**

Alta

Probabilidade	Descrição
ALTA	<p>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.</p> <p>(67% a 100% de chance de acontecer)</p>

Processo de Avaliação de Riscos – Análise de Riscos

17

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.1 Rede sem fio extrapola o limite físico da organização.

A1.1.2.1.1

Captura de sinal fora das dependências da organização

Probabilidade: o sinal 802.11n vaza para áreas externas; não há controle de potência nem política de cobertura.

Consequência: possibilidade de acesso não autorizado a partir do exterior (fora das dependências da organização).

Pi

Alta

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

18

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.1 Rede sem fio extrapola o limite físico da organização.

A1.1.2.1.1

Captura de sinal fora das dependências da organização

Probabilidade: o sinal 802.11n vaza para áreas externas; não há controle de potência nem política de cobertura.

Consequência: possibilidade de acesso não autorizado a partir do exterior (fora das dependências da organização).

Pi

Alta

Ci

Alta

Ri**Consequência****Alto****Descrição**

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

19

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.1 Rede sem fio extrapola o limite físico da organização.

A1.1.2.1.1

Captura de sinal fora das dependências da organização

Probabilidade: o sinal 802.11n vaza para áreas externas; não há controle de potência nem política de cobertura.

Consequência: possibilidade de acesso não autorizado a partir do exterior (fora das dependências da organização).

Pi**Ci****Ri**

Alta

Alta

Alto

Matriz de Risco

	Probabilidade		
	Baixo	Médio	Alto
Consequência			
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Análise de Riscos

20

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.1 Rede sem fio extrapola o limite físico da organização.

A1.1.2.1.2

Jamming do sinal originado fora das dependências da organização

Probabilidade:

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

21

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.1 Rede sem fio extrapola o limite físico da organização.

A1.1.2.1.2

Jamming do sinal originado fora das dependências da organização

Probabilidade: o sinal 802.11n está sujeito à jamming no canal do serviço da rede Wi-Fi.

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

22

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.1 Rede sem fio extrapola o limite físico da organização.

A1.1.2.1.2

Jamming do sinal originado fora das dependências da organização

Probabilidade: o sinal 802.11n está sujeito à jamming no canal do serviço da rede Wi-Fi.

Consequência:

Pi**Ci****Ri**

Alta

Probabilidade	Descrição
ALTA	<p>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.</p> <p>(67% a 100% de chance de acontecer)</p>

Processo de Avaliação de Riscos – Análise de Riscos

23

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.1 Rede sem fio extrapola o limite físico da organização.

A1.1.2.1.2

Jamming do sinal originado fora das dependências da organização

Probabilidade: o sinal 802.11n está sujeito à jamming no canal do serviço da rede Wi-Fi.

Consequência: possibilidade de indisponibilidade pelo aumento anormal de ruído ou ocupação do espectro.

Pi

Alta

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

24

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.1 Rede sem fio extrapola o limite físico da organização.

A1.1.2.1.2

Jamming do sinal originado fora das dependências da organização

Probabilidade: o sinal 802.11n está sujeito à jamming no canal do serviço da rede Wi-Fi.

Consequência: possibilidade de indisponibilidade pelo aumento anormal de ruído ou ocupação do espectro.

Pi

Ci

Ri

Alta

Alta

Consequência	Descrição
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

25

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.1 Rede sem fio extrapola o limite físico da organização.

A1.1.2.1.2

Jamming do sinal originado fora das dependências da organização

Probabilidade: o sinal 802.11n está sujeito à jamming no canal do serviço da rede Wi-Fi.

Consequência: possibilidade de indisponibilidade pelo aumento anormal de ruído ou ocupação do espectro.

Pi

Alta

Ci

Alta

Ri**Alto**

Matriz de Risco

	Probabilidade		
	Baixo	Médio	Alto
Consequência			
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Análise de Riscos

26

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.1 Rede sem fio extrapola o limite físico da organização.

		Pi	Ci	Ri
A1.1.2.1.1	Captura de sinal fora das dependências da organização	Alta	Alta	Alto
A1.1.2.1.2	Jamming do sinal originado fora das dependências da organização	Alta	Alta	Alto

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 – Tratamento de Riscos

27

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.1.1		A1.1.2.1.1	Modificar			

Processo de Avaliação de Riscos – Tratamento de Riscos

28

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.1.1	Planejamento de RF com limitação de potência; criptografia forte (AES).	A1.1.2.1.1	Modificar			

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria 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

29

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.1.1	Planejamento de RF com limitação de potência; criptografia forte (AES).	A1.1.2.1.1	Modificar			

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

30

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.1.1	Planejamento de RF com limitação de potência; criptografia forte (AES).	A1.1.2.1.1	Modificar	Baixa	Alta	

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

31

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.1.1	Planejamento de RF com limitação de potência; criptografia forte (AES).	A1.1.2.1.1	Modificar	Baixa	Alta	Médio

Matriz de Risco			
Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Tratamento de Riscos

32

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.1.1	Planejamento de RF com limitação de potência; criptografia forte (AES).	A1.1.2.1.1	Modificar	Baixa	Alta	Médio

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 – Tratamento de Riscos

33

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.1.2	Configurar a troca dinâmica de canal (Adaptive Channel Switching); planejamento multi-banda (2,4 / 5 GHz) e MIMO (Multiple-Input and Multiple-Output).	A1.1.2.1.2	Modificar			

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

34

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.1.2	Configurar a troca dinâmica de canal (Adaptive Channel Switching); planejamento multi-banda (2,4 / 5 GHz) e MIMO (Multiple-Input and Multiple-Output).	A1.1.2.1.2	Modificar	Baixa	Alta	

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

35

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.1.2	Configurar a troca dinâmica de canal (Adaptive Channel Switching); planejamento multi-banda (2,4 / 5 GHz) e MIMO (Multiple-Input and Multiple-Output).	A1.1.2.1.2	Modificar	Baixa	Alta	Médio

Matriz de Risco			
Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Tratamento de Riscos

36

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.1.2	Configurar a troca dinâmica de canal (Adaptive Channel Switching); planejamento multi-banda (2,4 / 5 GHz) e MIMO (Multiple-Input and Multiple-Output).	A1.1.2.1.2	Modificar	Baixa	Alta	Médio

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 – Identificação de Riscos

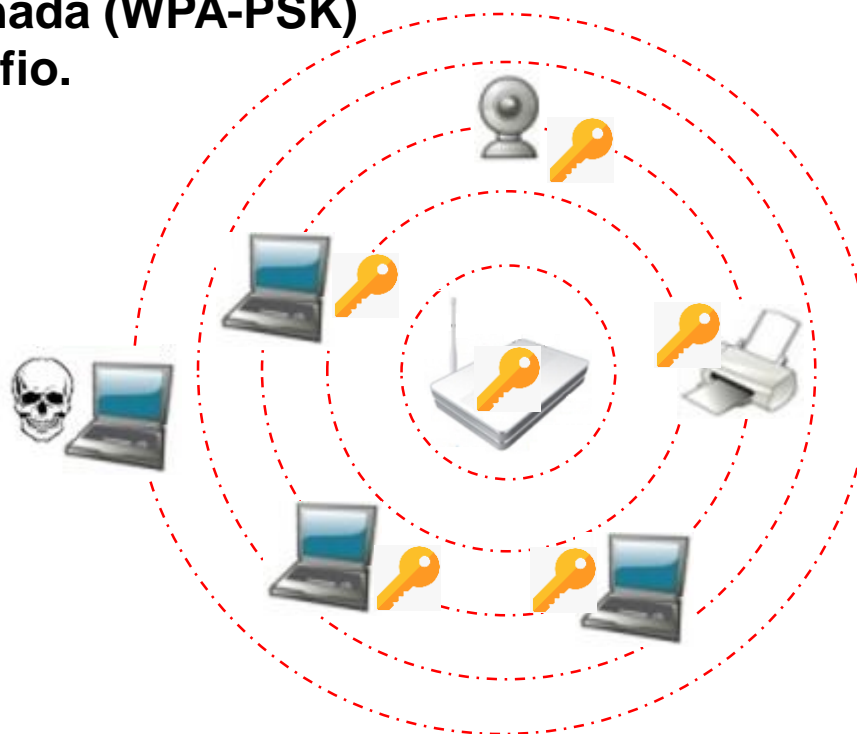
37

Exemplo: Listagem de ameaças para a vulnerabilidade.

- **Vulnerabilidade:**
 - **1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.**
- **Ameaças:**

1.1.2.2.1 Vazamento ou força bruta da chave PSK

1.1.2.2.2 Acesso não autorizado por dispositivos desconhecidos



Processo de Avaliação de Riscos – Análise de Riscos

38

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.

A1.1.2.2.1

Vazamento ou força bruta da chave PSK

Probabilidade:

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

39

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.

A1.1.2.2.1

Vazamento ou força bruta da chave PSK

Probabilidade: uso de PSK é estático e compartilhado; há risco de divulgação entre usuários ou fornecedores; ou quebra por força bruta por um invasor.

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

40

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.

		Pi	Ci	Ri
A1.1.2.2.1	Vazamento ou força bruta da chave PSK Probabilidade: uso de PSK é estático e compartilhado; há risco de divulgação entre usuários ou fornecedores; ou quebra por força bruta por um invasor. Consequência:	Alta		

Probabilidade	Descrição
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

41

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.

A1.1.2.2.1

Vazamento ou força bruta da chave PSK

Probabilidade: uso de PSK é estático e compartilhado; há risco de divulgação entre usuários ou fornecedores; ou quebra por força bruta por um invasor.

Consequência: acesso pleno à rede interna, possibilitando monitoramento e exfiltração.

Pi

Alta

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

42

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.

A1.1.2.2.1

Vazamento ou força bruta da chave PSK

Probabilidade: uso de PSK é estático e compartilhado; há risco de divulgação entre usuários ou fornecedores; ou quebra por força bruta por um invasor.

Consequência: acesso pleno à rede interna, possibilitando monitoramento e exfiltração.

Pi

Alta

Ci

Alta

Ri**Consequência****Alto****Descrição**

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

43

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.

A1.1.2.2.1

Vazamento ou força bruta da chave PSK

Probabilidade: uso de PSK é estático e compartilhado; há risco de divulgação entre usuários ou fornecedores; ou quebra por força bruta por um invasor.

Consequência: acesso pleno à rede interna, possibilitando monitoramento e exfiltração.

Pi

Alta

Ci

Alta

Ri

Alto

Matriz de Risco

Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Análise de Riscos

44

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.

A1.1.2.2.2

Acesso não autorizado por dispositivos desconhecidos

Probabilidade:

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

45

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.

A1.1.2.2.2

Acesso não autorizado por dispositivos desconhecidos

Probabilidade: qualquer equipamento com a chave pode se conectar; não há NAC (Network Access Control) robusto.

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

46

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.

A1.1.2.2.2

Acesso não autorizado por dispositivos desconhecidos

Probabilidade: qualquer equipamento com a chave pode se conectar; não há NAC (Network Access Control) robusto.

Consequência:

Pi

Alta

Ci**Ri**

Probabilidade	Descrição
ALTA	<p>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.</p> <p>(67% a 100% de chance de acontecer)</p>

Processo de Avaliação de Riscos – Análise de Riscos

47

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.

		Pi	Ci	Ri
A1.1.2.2.2	<p>Acesso não autorizado por dispositivos desconhecidos</p> <p>Probabilidade: qualquer equipamento com a chave pode se conectar; não há NAC (Network Access Control) robusto.</p> <p>Consequência: compromete confidencialidade, integridade e disponibilidade.</p>	Alta		

Processo de Avaliação de Riscos – Análise de Riscos

48

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.

A1.1.2.2.2	Acesso não autorizado por dispositivos desconhecidos			
	Probabilidade: qualquer equipamento com a chave pode se conectar; não há NAC (Network Access Control) robusto.	Alta	Alta	
	Consequência: compromete confidencialidade, integridade e disponibilidade.			

Consequência	Descrição
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

49

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.

		Pi	Ci	Ri
A1.1.2.2.2	<p>Acesso não autorizado por dispositivos desconhecidos</p> <p>Probabilidade: qualquer equipamento com a chave pode se conectar; não há NAC (Network Access Control) robusto.</p> <p>Consequência: compromete confidencialidade, integridade e disponibilidade.</p>	Alta	Alta	Alto

Matriz de Risco			
Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Análise de Riscos

50

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.2 Chave compartilhada (WPA-PSK) para acesso à rede sem fio.

		Pi	Ci	Ri
A1.1.2.2.1	Vazamento ou força bruta da chave PSK	Alta	Alta	Alto
A1.1.2.2.2	Acesso não autorizado por dispositivos desconhecidos	Alta	Alta	Alto

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 – Tratamento de Riscos

51

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.2.1		A1.1.2.2.1	Modificar			

Processo de Avaliação de Riscos – Tratamento de Riscos

52

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.2.1	Migrar para WPA2/3-Enterprise com autenticação 802.1X (RADIUS); atribuição individual de credenciais.	A1.1.2.2.1	Modificar			

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

53

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.2.1	Migrar para WPA2/3-Enterprise com autenticação 802.1X (RADIUS); atribuição individual de credenciais.	A1.1.2.2.1	Modificar	Baixa	Alta	

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

54

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.2.1	Migrar para WPA2/3-Enterprise com autenticação 802.1X (RADIUS); atribuição individual de credenciais.	A1.1.2.2.1	Modificar	Baixa	Alta	Médio

Matriz de Risco			
Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Tratamento de Riscos

55

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.2.1	Migrar para WPA2/3-Enterprise com autenticação 802.1X (RADIUS); atribuição individual de credenciais.	A1.1.2.2.1	Modificar	Baixa	Alta	Médio

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 – Tratamento de Riscos

56

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.2.2		A1.1.2.2.2	Modificar			

Processo de Avaliação de Riscos – Tratamento de Riscos

57

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.2.2	Implantar NAC ou controle de identidade na WLAN; segregar SSID de convidados; monitoramento de endereços MAC; política de cadastro de dispositivos.	A1.1.2.2.2	Modificar			

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

58

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.2.2	Implantar NAC ou controle de identidade na WLAN; segregar SSID de convidados; monitoramento de endereços MAC; política de cadastro de dispositivos.	A1.1.2.2.2	Modificar	Baixa	Média	

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

59

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.2.2	Implantar NAC ou controle de identidade na WLAN; segregar SSID de convidados; monitoramento de endereços MAC; política de cadastro de dispositivos.	A1.1.2.2.2	Modificar	Baixa	Média	Baixo

Matriz de Risco			
Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Tratamento de Riscos

60

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.2.2	Implantar NAC ou controle de identidade na WLAN; segregar SSID de convidados; monitoramento de endereços MAC; política de cadastro de dispositivos.	A1.1.2.2.2	Modificar	Baixa	Média	Baixo

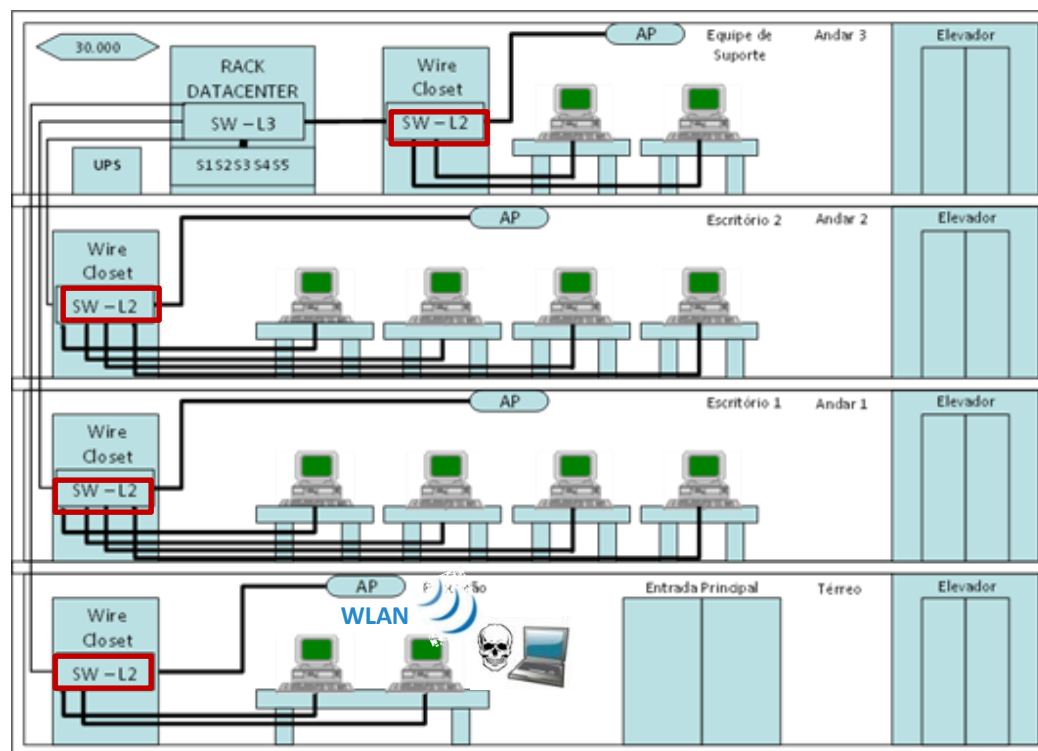
Risco	Descrição	Tratamento
Baixo	Risco tolerável, sem necessidade de acompanhamento especial.	Aceitar
Médio	Risco tolerável, porém, com chances razoáveis de causar um impacto moderado. Neste caso, deve ser monitorado, sem urgência para a implementação de controles.	Aceitar
Alto	Risco não tolerável, pois 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 – Identificação de Riscos

61

Exemplo: Listagem de ameaças para a vulnerabilidade.

- **Vulnerabilidade:**
 - 1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.
- **Ameaças:**
 - 1.1.2.3.1 Ação maliciosa na camada 2 (ARP spoofing, sniffing local)
 - 1.1.2.3.2 Infecção cruzada entre dispositivos



Processo de Avaliação de Riscos – Análise de Riscos

62

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.

A1.1.2.3.1

Ação maliciosa na camada 2 (ARP spoofing, sniffing local)

Probabilidade:

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

63

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.

A1.1.2.3.1

Ação maliciosa na camada 2 (ARP spoofing, sniffing local)

Probabilidade: topologia plana (flat) sem isolamento entre WLAN e estações.

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

64

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.

		Pi	Ci	Ri
A1.1.2.3.1	Ação maliciosa na camada 2 (ARP spoofing, sniffing local) Probabilidade: topologia plana (flat) sem isolamento entre WLAN e estações. Consequência:	Alta		

Probabilidade	Descrição
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

65

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.

A1.1.2.3.1

Ação maliciosa na camada 2 (ARP spoofing, sniffing local)

Probabilidade: topologia plana (flat) sem isolamento entre WLAN e estações.

Consequência: facilita captura de tráfego e comprometimento de ativos internos.

Pi

Alta

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

66

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.

A1.1.2.3.1

Ação maliciosa na camada 2 (ARP spoofing, sniffing local)

Probabilidade: topologia plana (flat) sem isolamento entre WLAN e estações.

Consequência: facilita captura de tráfego e comprometimento de ativos internos.

Pi

Alta

Ci

Alta

Ri**Consequência****Alto****Descrição**

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

67

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.

		Pi	Ci	Ri
A1.1.2.3.1	<p>Ação maliciosa na camada 2 (ARP spoofing, sniffing local)</p> <p>Probabilidade: topologia plana (flat) sem isolamento entre WLAN e estações.</p> <p>Consequência: facilita captura de tráfego e comprometimento de ativos internos.</p>	Alta	Alta	Alto

Matriz de Risco			
Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Análise de Riscos

68

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.

A1.1.2.3.2

Infecção cruzada entre dispositivos

Probabilidade:

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

69

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.

A1.1.2.3.2

Infecção cruzada entre dispositivos

Probabilidade: depende de malware ativo ou estação infectada.

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

70

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.

A1.1.2.3.2

Infecção cruzada entre dispositivos

Probabilidade: depende de malware ativo ou estação infectada.

Consequência:

Alta

Probabilidade	Descrição
ALTA	<p>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.</p> <p>(67% a 100% de chance de acontecer)</p>

Processo de Avaliação de Riscos – Análise de Riscos

71

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.

A1.1.2.3.2

Infecção cruzada entre dispositivos

Probabilidade: depende de malware ativo ou estação infectada.

Consequência: propagação em rede sem segmentação.

Alta

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

72

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.

A1.1.2.3.2

Infecção cruzada entre dispositivos

Probabilidade: depende de malware ativo ou estação infectada.

Consequência: propagação em rede sem segmentação.

Alta

Alta

Alta

Consequência	Descrição
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

73

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.

A1.1.2.3.2

Infecção cruzada entre dispositivos

Probabilidade: depende de malware ativo ou estação infectada.

Consequência: propagação em rede sem segmentação.

Alta

Alta

Alto

Matriz de Risco

	Probabilidade		
	Baixo	Médio	Alto
Consequência			
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Análise de Riscos

74

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.3 Ponto de acesso ligado na mesma rede das estações da organização.

		Pi	Ci	Ri
A1.1.2.3.1	Ação maliciosa na camada 2 (ARP spoofing, sniffing local)	Alta	Alta	Alto
A1.1.2.3.2	Infecção cruzada entre dispositivos	Alta	Alta	Alto

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 – Tratamento de Riscos

75

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.3.1		A1.1.2.3.1	Modificar			

Processo de Avaliação de Riscos – Tratamento de Riscos

76

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.3.1	Isolamento da WLAN em VLAN própria; firewall entre redes; APs com isolamento de cliente e controle de broadcast.	A1.1.2.3.1	Modificar			

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

77

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.3.1	Isolamento da WLAN em VLAN própria; firewall entre redes; APs com isolamento de cliente e controle de broadcast.	A1.1.2.3.1	Modificar	Baixa	Alta	

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

78

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.3.1	Isolamento da WLAN em VLAN própria; firewall entre redes; APs com isolamento de cliente e controle de broadcast.	A1.1.2.3.1	Modificar	Baixa	Alta	Médio

Matriz de Risco			
Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Tratamento de Riscos

79

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.3.1	Isolamento da WLAN em VLAN própria; firewall entre redes; APs com isolamento de cliente e controle de broadcast.	A1.1.2.3.1	Modificar	Baixa	Alta	Médio

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 – Tratamento de Riscos

80

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.3.2		A1.1.2.3.2	Modificar			

Processo de Avaliação de Riscos – Tratamento de Riscos

81

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.3.2	Antimalware corporativo; IDS/IPS wireless.	A1.1.2.3.2	Modificar			

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

82

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.3.2	Antimalware corporativo; IDS/IPS wireless.	A1.1.2.3.2	Modificar	Baixa	Média	

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

83

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.3.2	Antimalware corporativo; IDS/IPS wireless.	A1.1.2.3.2	Modificar	Baixa	Média	Baixo

Matriz de Risco			
Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Tratamento de Riscos

84

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.3.2	Antimalware corporativo; IDS/IPS wireless.	A1.1.2.3.2	Modificar	Baixa	Média	Baixo

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 – Identificação de Riscos

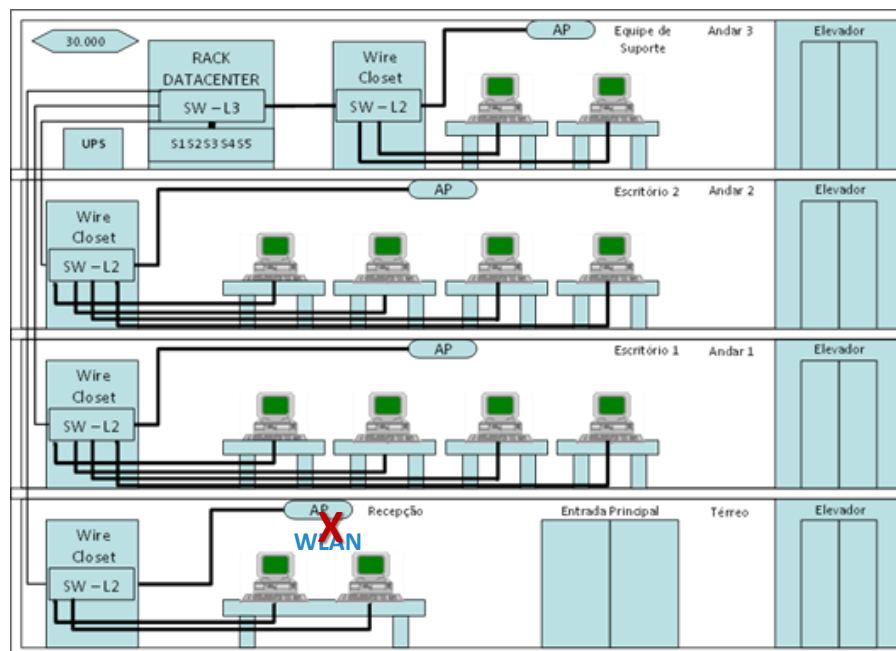
85

Exemplo: Listagem de ameaças para a vulnerabilidade.

- **Vulnerabilidade:**
 - **1.1.2.4 Rede de dados sem fio equipada apenas com dispositivos principais, sem disponibilidade imediata de unidade reserva para substituição em caso de pane.**

- **Ameaças:**

1.1.2.4.1 Parada da rede Wi-Fi
por falha de AP único



Processo de Avaliação de Riscos – Análise de Riscos

86

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.4 Rede de dados sem fio equipada apenas com dispositivos principais, sem disponibilidade imediata de unidade reserva para substituição em caso de pane.

Pi

Ci

Ri

A1.1.2.4.1

Parada da rede Wi-Fi por falha de AP único

Probabilidade:

Consequência:

Processo de Avaliação de Riscos – Análise de Riscos

87

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.4 Rede de dados sem fio equipada apenas com dispositivos principais, sem disponibilidade imediata de unidade reserva para substituição em caso de pane.

Pi

Ci

Ri

A1.1.2.4.1

Parada da rede Wi-Fi por falha de AP único

Probabilidade: sem equipamento sobressalente; depende do suporte interno limitado.

Consequência:

Processo de Avaliação de Riscos – Análise de Riscos

88

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.4 Rede de dados sem fio equipada apenas com dispositivos principais, sem disponibilidade imediata de unidade reserva para substituição em caso de pane.

A1.1.2.4.1

Parada da rede Wi-Fi por falha de AP único

Probabilidade: sem equipamento sobressalente; depende do suporte interno limitado.

Consequência:

Alta

Probabilidade

Descrição

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

89

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.4 Rede de dados sem fio equipada apenas com dispositivos principais, sem disponibilidade imediata de unidade reserva para substituição em caso de pane.

A1.1.2.4.1

Parada da rede Wi-Fi por falha de AP único

Probabilidade: sem equipamento sobressalente; depende do suporte interno limitado.

Consequência: indisponibilidade imediata da rede para os usuários e impacto na produtividade.

Pi

Ci

Ri

Alta

Processo de Avaliação de Riscos – Análise de Riscos

90

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.4 Rede de dados sem fio equipada apenas com dispositivos principais, sem disponibilidade imediata de unidade reserva para substituição em caso de pane.

A1.1.2.4.1

Parada da rede Wi-Fi por falha de AP único

Probabilidade: sem equipamento sobressalente; depende do suporte interno limitado.

Consequência: indisponibilidade imediata da rede para os usuários e impacto na produtividade.

Pi

Ci

Ri

Alta

Alta

Consequência

Descrição

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

91

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.4 Rede de dados sem fio equipada apenas com dispositivos principais, sem disponibilidade imediata de unidade reserva para substituição em caso de pane.

A1.1.2.4.1

Parada da rede Wi-Fi por falha de AP único

Probabilidade: sem equipamento sobressalente; depende do suporte interno limitado.

Consequência: indisponibilidade imediata da rede para os usuários e impacto na produtividade.

Pi

Ci

Ri

Alta

Alta

Alto

Matriz de Risco

Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Análise de Riscos

92

Ativo: 1.1.2 Rede de Dados Sem Fio

1.1.2 Rede de Dados Sem Fio

V1.1.2.4 Rede de dados sem fio equipada apenas com dispositivos principais, sem disponibilidade imediata de unidade reserva para substituição em caso de pane.

A1.1.2.4.1

Parada da rede Wi-Fi por falha de AP único

Pi

Ci

Ri

Alta

Alta

Alto

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 – Tratamento de Riscos

93

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.4.1		A1.1.2.4.1	Modificar			

Processo de Avaliação de Riscos – Tratamento de Riscos

94

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.4.1	Aquisição de AP sobressalente ou hot-spare; contrato de suporte com SLA de reposições; testes de troca de equipamento.	A1.1.2.4.1	Modificar			

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

95

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.4.1	Aquisição de AP sobressalente ou hot-spare; contrato de suporte com SLA de reposições; testes de troca de equipamento.	A1.1.2.4.1	Modificar	Alta	Baixa	

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

96

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.4.1	Aquisição de AP sobressalente ou hot-spare; contrato de suporte com SLA de reposições; testes de troca de equipamento.	A1.1.2.4.1	Modificar	Alta	Baixa	Médio

Matriz de Risco			
Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Tratamento de Riscos

97

Ativo: 1.1.2 Rede de Dados Sem Fio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.2.4.1	Aquisição de AP sobressalente ou hot-spares; contrato de suporte com SLA de reposições; testes de troca de equipamento.	A1.1.2.4.1	Modificar	Alta	Baixa	Médio

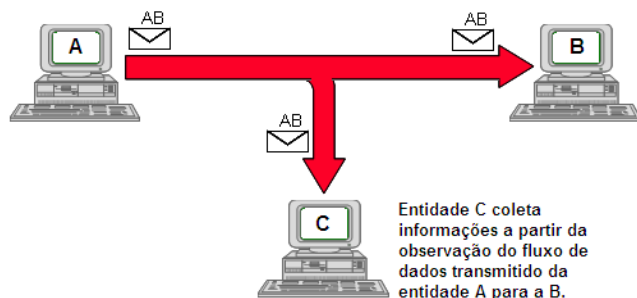
Risco	Descrição	Tratamento
Baixo	Risco tolerável, sem necessidade de acompanhamento especial.	Aceitar
Médio	Risco tolerável, porém, com chances razoáveis de causar um impacto moderado. Neste caso, deve ser monitorado, sem urgência para a implementação de controles.	Aceitar
Alto	Risco não tolerável, pois 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 – Identificação de Riscos

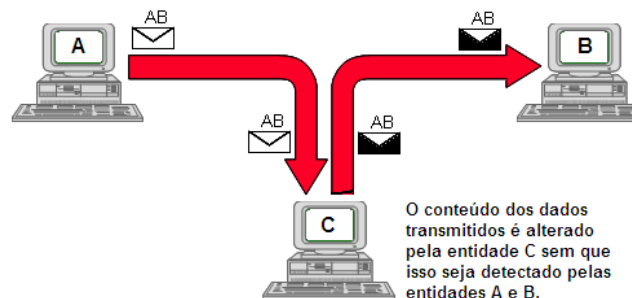
98

Exemplo: Listagem de ameaças para a vulnerabilidade.

- **Ativo:**
 - 1.1.3 Servidor de Correio.
- **Vulnerabilidade:**
 - 1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.
- **Ameaças:**



1.1.3.1.1 Intercepção de
credenciais ou mensagens
(ataque passivo)



1.1.3.1.2 Manipulação ou injeção
de mensagens (ataque ativo)

Processo de Avaliação de Riscos – Análise de Riscos

99

Ativo: 1.1.3 Servidor de Correio

1.1.3 Servidor de Correio

V1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

A1.1.3.1.1

Interceptação de credenciais ou mensagens (ataque passivo)

Probabilidade:

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

100

Ativo: 1.1.3 Servidor de Correio

1.1.3 Servidor de Correio

V1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

A1.1.3.1.1

Interceptação de credenciais ou mensagens (ataque passivo)

Probabilidade: os protocolos SMTP/IMAP operam sem TLS (canal seguro de comunicação); qualquer nó de rede pode realizar captura.

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

101

Ativo: 1.1.3 Servidor de Correio

1.1.3 Servidor de Correio

V1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

A1.1.3.1.1

Interceptação de credenciais ou mensagens (ataque passivo)

Probabilidade: os protocolos SMTP/IMAP operam sem TLS (canal seguro de comunicação); qualquer nó de rede pode realizar captura.

Consequência:

Pi**Ci****Ri**

Alta

Probabilidade	Descrição
ALTA	<p>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.</p> <p>(67% a 100% de chance de acontecer)</p>

Processo de Avaliação de Riscos – Análise de Riscos

102

Ativo: 1.1.3 Servidor de Correio

1.1.3 Servidor de Correio

V1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

A1.1.3.1.1

Interceptação de credenciais ou mensagens (ataque passivo)

Probabilidade: os protocolos SMTP/IMAP operam sem TLS (canal seguro de comunicação); qualquer nó de rede pode realizar captura.

Consequência: vazamento de dados sensíveis e roubo de credenciais.

Pi

Ci

Ri

Alta

Processo de Avaliação de Riscos – Análise de Riscos

103

Ativo: 1.1.3 Servidor de Correio

1.1.3 Servidor de Correio

V1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

A1.1.3.1.1

Interceptação de credenciais ou mensagens (ataque passivo)

Probabilidade: os protocolos SMTP/IMAP operam sem TLS (canal seguro de comunicação); qualquer nó de rede pode realizar captura.

Consequência: vazamento de dados sensíveis e roubo de credenciais.

Pi

Alta

Ci

Alta

Ri**Consequência****Alto****Descrição**

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

104

Ativo: 1.1.3 Servidor de Correio

1.1.3 Servidor de Correio

V1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

A1.1.3.1.1

Interceptação de credenciais ou mensagens (ataque passivo)

Probabilidade: os protocolos SMTP/IMAP operam sem TLS (canal seguro de comunicação); qualquer nó de rede pode realizar captura.

Consequência: vazamento de dados sensíveis e roubo de credenciais.

Pi

Alta

Ci

Alta

Ri**Alto**

Matriz de Risco

	Probabilidade		
	Baixo	Médio	Alto
Consequência			
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Análise de Riscos

105

Ativo: 1.1.3 Servidor de Correio

1.1.3 Servidor de Correio

V1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

A1.1.3.1.2

Manipulação ou injeção de mensagens (ataque ativo)

Probabilidade:

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

106

Ativo: 1.1.3 Servidor de Correio

1.1.3 Servidor de Correio

V1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

A1.1.3.1.2

Manipulação ou injeção de mensagens (ataque ativo)

Probabilidade: depende de ataque ativo com acesso man-in-the-middle.

Consequência:

Pi

Ci

Ri

Processo de Avaliação de Riscos – Análise de Riscos

107

Ativo: 1.1.3 Servidor de Correio

1.1.3 Servidor de Correio

V1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

A1.1.3.1.2

Manipulação ou injeção de mensagens (ataque ativo)

Probabilidade: depende de ataque ativo com acesso man-in-the-middle.

Consequência:

Pi**Ci****Ri**

Média

Probabilidade	Descrição
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)

Processo de Avaliação de Riscos – Análise de Riscos

108

Ativo: 1.1.3 Servidor de Correio

1.1.3 Servidor de Correio

V1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

A1.1.3.1.2

Manipulação ou injeção de mensagens (ataque ativo)

Probabilidade: depende de ataque ativo com acesso man-in-the-middle.

Consequência: possível disseminação de phishing interno ou malware.

Pi

Ci

Ri

Média

Processo de Avaliação de Riscos – Análise de Riscos

109

Ativo: 1.1.3 Servidor de Correio

1.1.3 Servidor de Correio

V1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

A1.1.3.1.2

Manipulação ou injeção de mensagens (ataque ativo)

Probabilidade: depende de ataque ativo com acesso man-in-the-middle.

Consequência: possível disseminação de phishing interno ou malware.

Pi

Média

Ci

Alta

Ri

Consequência	Descrição
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

110

Ativo: 1.1.3 Servidor de Correio

1.1.3 Servidor de Correio

V1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

A1.1.3.1.2

Manipulação ou injeção de mensagens (ataque ativo)

Probabilidade: depende de ataque ativo com acesso man-in-the-middle.

Consequência: possível disseminação de phishing interno ou malware.

Pi
MédiaCi
AltaRi
Alto

Matriz de Risco

Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Análise de Riscos

111

Ativo: 1.1.3 Servidor de Correio

1.1.3 Servidor de Correio

V1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.

		Pi	Ci	Ri
A1.1.3.1.1	Interceptação de credenciais ou mensagens (ataque passivo)	Alta	Alta	Alto
A1.1.3.1.2	Manipulação ou injeção de mensagens (ataque ativo)	Média	Alta	Alto

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 – Tratamento de Riscos

112

Ativo: 1.1.3 Servidor de Correio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.3.1.1		A1.1.3.1.1	Modificar			

Processo de Avaliação de Riscos – Tratamento de Riscos

113

Ativo: 1.1.3 Servidor de Correio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.3.1.1	Configurar SMTPS/IMAPS com TLS 1.3 obrigatório; Configurar SPF/DKIM/DMARC; bloquear a porta 25 sem TLS; monitoramento de logs de autenticação.	A1.1.3.1.1	Modificar			

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

114

Ativo: 1.1.3 Servidor de Correio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.3.1.1	Configurar SMTPS/IMAPS com TLS 1.3 obrigatório; Configurar SPF/DKIM/DMARC; bloquear a porta 25 sem TLS; monitoramento de logs de autenticação.	A1.1.3.1.1	Modificar	Baixa	Média	

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

115

Ativo: 1.1.3 Servidor de Correio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.3.1.1	Configurar SMTPS/IMAPS com TLS 1.3 obrigatório; Configurar SPF/DKIM/DMARC; bloquear a porta 25 sem TLS; monitoramento de logs de autenticação.	A1.1.3.1.1	Modificar	Baixa	Média	Baixo

Matriz de Risco			
Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Tratamento de Riscos

116

Ativo: 1.1.3 Servidor de Correio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.3.1.1	Configurar SMTPS/IMAPS com TLS 1.3 obrigatório; Configurar SPF/DKIM/DMARC; bloquear a porta 25 sem TLS; monitoramento de logs de autenticação.	A1.1.3.1.1	Modificar	Baixa	Média	Baixo

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 – Tratamento de Riscos

117

Ativo: 1.1.3 Servidor de Correio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.3.1.2		A1.1.3.1.2	Modificar			

Processo de Avaliação de Riscos – Tratamento de Riscos

118

Ativo: 1.1.3 Servidor de Correio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.3.1.2	Implementar assinatura digital de mensagens (S/MIME ou PGP); validação de integridade no cliente; filtro antimalware no servidor de e-mail.	A1.1.3.1.2	Modificar			

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

119

Ativo: 1.1.3 Servidor de Correio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.3.1.2	Implementar assinatura digital de mensagens (S/MIME ou PGP); validação de integridade no cliente; filtro antimalware no servidor de e-mail.	A1.1.3.1.2	Modificar	Baixa	Alta	

Para calcularmos a redução da probabilidade e da consequência, um método prático é verificar a categoria do controle:

Categoria 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

120

Ativo: 1.1.3 Servidor de Correio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.3.1.2	Implementar assinatura digital de mensagens (S/MIME ou PGP); validação de integridade no cliente; filtro antimalware no servidor de e-mail.	A1.1.3.1.2	Modificar	Baixa	Alta	Médio

Matriz de Risco			
Consequência	Probabilidade		
	Baixo	Médio	Alto
Alto			
Médio			
Baixo			

Processo de Avaliação de Riscos – Tratamento de Riscos

121

Ativo: 1.1.3 Servidor de Correio

Tratamento dos riscos		Ameaça	Tipo	Pr	Cr	Rr
T1.1.3.1.2	Implementar assinatura digital de mensagens (S/MIME ou PGP); validação de integridade no cliente; filtro antimalware no servidor de e-mail.	A1.1.3.1.2	Modificar	Baixa	Alta	Médio

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)



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