# 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:**

- Ativo: 1.1.3 Correio Eletrônico
  - Vulnerabilidade:
    - 1.1.3.1 Comunicação insegura nos protocolos SMTP e IMAP.
    - 1.1.3.2 Armazenamento dos e-mails nas caixas de entrada dos usuários e nas pastas de mensagens sem proteção de integridade, autenticidade e sigilo.
    - 1.1.3.3 Autenticação fraca com uso de credencial apenas com login e senha.
    - 1.1.3.4 Infraestrutura de correio eletrônico operando com servidor único, sem unidade sobressalente para substituir um equipamento em pane.

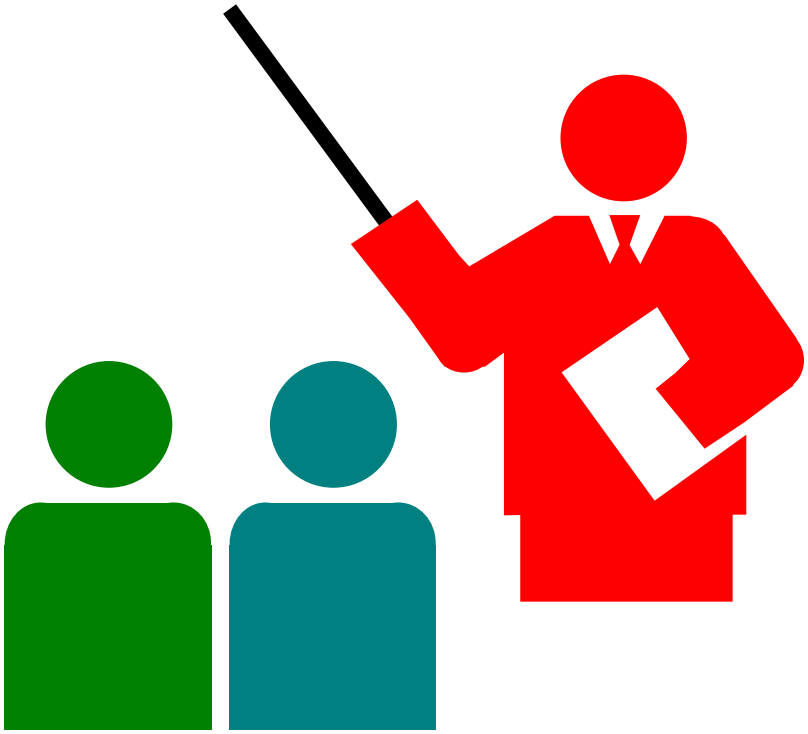
# Ementa

**Processo de Avaliação de Riscos e Tratamento de Riscos:**

- Ativo: 1.1.10 Ar-Condicionado
  - Vulnerabilidade:
    - 1.1.10.1 Sistema de refrigeração configurado com equipamento único, sem redundância para suprir falha.
    - 1.1.10.2 Serviço de manutenção do ar-condicionado prestado sem definição contratual de níveis de serviço (SLA).
    - 1.1.10.3 Sistema de refrigeração do Data Center operando sem fonte alternativa de energia dedicada.

# Processo de Avaliação de Riscos





# 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.<br><br>(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.<br><br>(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.<br><br>(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

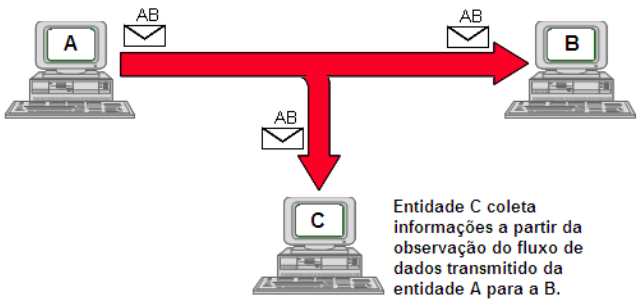
**Critério para avaliação de riscos e tratamento de riscos:**

| 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) |

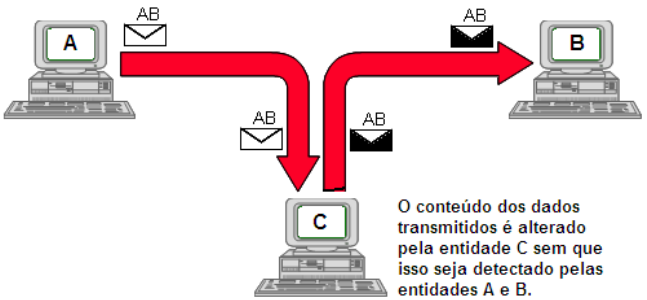
# Processo de Avaliação de Riscos – Identificação de Riscos

**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 Interceptação 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

**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)**<br><br>Probabilidade:<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## 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)**<br><br>Probabilidade: os protocolos SMTP/IMAP operam sem TLS (canal seguro de comunicação); qualquer nó de rede pode realizar captura.<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## 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)**<br><br>Probabilidade: os protocolos SMTP/IMAP operam sem TLS (canal seguro de comunicação); qualquer nó de rede pode realizar captura.<br><br>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.<br><br>(67% a 100% de chance de acontecer) |

# Processo de Avaliação de Riscos – Análise de Riscos

## 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)**<br><br>Probabilidade: os protocolos SMTP/IMAP operam sem TLS (canal seguro de comunicação); qualquer nó de rede pode realizar captura.<br><br>Consequência: vazamento de dados sensíveis e roubo de credenciais. | Alta | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## 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)**<br><br>Probabilidade: os protocolos SMTP/IMAP operam sem TLS (canal seguro de comunicação); qualquer nó de rede pode realizar captura.<br><br>Consequência: vazamento de dados sensíveis e roubo de credenciais. | 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

## 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)**<br><br>Probabilidade: os protocolos SMTP/IMAP operam sem TLS (canal seguro de comunicação); qualquer nó de rede pode realizar captura.<br><br>Consequência: vazamento de dados sensíveis e roubo de credenciais. | Alta | Alta | **Alto** |

| Matriz de Risco | | | |
|---|---|---|---|
| | **Probabilidade** | | |
| **Consequência** | **Baixo** | **Médio** | **Alto** |
| **Alto** | | | |
| **Médio** | | | |
| **Baixo** | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

**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** |
| **A1.1.3.1.2** | **Manipulação ou injeção de mensagens (ataque ativo)**<br><br>Probabilidade:<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

**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** |
| **A1.1.3.1.2** | **Manipulação ou injeção de mensagens (ataque ativo)**<br><br>Probabilidade: depende de ataque ativo com acesso man-in-the-middle.<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## 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** |
| **A1.1.3.1.2** | **Manipulação ou injeção de mensagens (ataque ativo)**<br><br>Probabilidade: depende de ataque ativo com acesso man-in-the-middle.<br><br>Consequência: | 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.<br><br>(34% a 66% de chance de acontecer) |

# Processo de Avaliação de Riscos – Análise de Riscos

## 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** |
| **A1.1.3.1.2** | **Manipulação ou injeção de mensagens (ataque ativo)**<br><br>Probabilidade: depende de ataque ativo com acesso man-in-the-middle.<br><br>Consequência: possível disseminação de phishing interno ou malware. | Média | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## 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** |
| **A1.1.3.1.2** | **Manipulação ou injeção de mensagens (ataque ativo)**<br><br>Probabilidade: depende de ataque ativo com acesso man-in-the-middle.<br><br>Consequência: possível disseminação de phishing interno ou malware. | Média | 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

## 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** |
| **A1.1.3.1.2** | **Manipulação ou injeção de mensagens (ataque ativo)**<br><br>Probabilidade: depende de ataque ativo com acesso man-in-the-middle.<br><br>Consequência: possível disseminação de phishing interno ou malware. | Média | Alta | **Alto** |

| Matriz de Risco | | | |
|---|---|---|---|
| | **Probabilidade** | | |
| **Consequência** | **Baixo** | **Médio** | **Alto** |
| **Alto** | | | |
| **Médio** | | | |
| **Baixo** | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## 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

**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

**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

**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

**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 | | | |
|---|---|---|---|
| | Probabilidade | | |
| Consequência | Baixo | Médio | Alto |
| Alto | | | |
| Médio | | | |
| Baixo | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

## 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

**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

**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

**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

**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 | | | |
|---|---|---|---|
| | Probabilidade | | |
| **Consequência** | **Baixo** | **Médio** | **Alto** |
| **Alto** | | | |
| **Médio** | | | |
| **Baixo** | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

**Ativo: 1.1.3 Servidor de Correio**

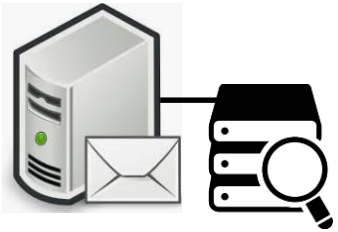
| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| **T1.1.3.1.2** | Implementar assinatura digital de mensagens (S/MIME ou PGP); validação de integridade no cliente; filtro antimalware no servidor de e-mail. | A1.1.3.1.2 | Modificar | Baixa | Alta | **Médio** |

| 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) |

# Processo de Avaliação de Riscos – Identificação de Riscos

**Exemplo: Listagem de ameaças para a vulnerabilidade.**

- **Ativo:**
  - **1.1.3 Servidor de Correio.**
- **Vulnerabilidade:**
  - **1.1.3.2 Armazenamento dos e-mails nas caixas de entrada dos usuários e nas pastas de mensagens sem proteção de integridade, autenticidade e sigilo.**
- **Ameaças:**



**1.1.3.2.1 Exposição ou modificação não autorizada dos arquivos de correio**

# Processo de Avaliação de Riscos – Análise de Riscos

**Ativo: 1.1.3 Servidor de Correio**

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.2 Armazenamento dos e-mails nas caixas de entrada dos usuários e nas pastas de mensagens sem proteção de integridade, autenticidade e sigilo.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.2.1** | **Exposição ou modificação não autorizada dos arquivos de correio**<br><br>Probabilidade:<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.2 Armazenamento dos e-mails nas caixas de entrada dos usuários e nas pastas de mensagens sem proteção de integridade, autenticidade e sigilo.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.2.1** | **Exposição ou modificação não autorizada dos arquivos de correio**<br><br>Probabilidade: acesso não autorizado aos arquivos da área de armazenamento do servidor de correio.<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.2 Armazenamento dos e-mails nas caixas de entrada dos usuários e nas pastas de mensagens sem proteção de integridade, autenticidade e sigilo.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.2.1** | **Exposição ou modificação não autorizada dos arquivos de correio**<br><br>Probabilidade: acesso não autorizado aos arquivos da área de armazenamento do servidor de correio.<br><br>Consequência: | 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.<br><br>(34% a 66% de chance de acontecer) |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.2 Armazenamento dos e-mails nas caixas de entrada dos usuários e nas pastas de mensagens sem proteção de integridade, autenticidade e sigilo.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.2.1** | **Exposição ou modificação não autorizada dos arquivos de correio**<br><br>Probabilidade: acesso não autorizado aos arquivos da área de armazenamento do servidor de correio.<br><br>Consequência: exposição de dados confidenciais e comunicações corporativas. | Média | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.2 Armazenamento dos e-mails nas caixas de entrada dos usuários e nas pastas de mensagens sem proteção de integridade, autenticidade e sigilo.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.2.1** | **Exposição ou modificação não autorizada dos arquivos de correio**<br><br>Probabilidade: acesso não autorizado aos arquivos da área de armazenamento do servidor de correio.<br><br>Consequência: exposição de dados confidenciais e comunicações corporativas. | Média | 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

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.2 Armazenamento dos e-mails nas caixas de entrada dos usuários e nas pastas de mensagens sem proteção de integridade, autenticidade e sigilo.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.2.1** | **Exposição ou modificação não autorizada dos arquivos de correio**<br><br>Probabilidade: acesso não autorizado aos arquivos da área de armazenamento do servidor de correio.<br><br>Consequência: exposição de dados confidenciais e comunicações corporativas. | Média | Alta | **Alto** |

| Matriz de Risco | | | |
|---|---|---|---|
| | **Probabilidade** | | |
| **Consequência** | **Baixo** | **Médio** | **Alto** |
| **Alto** | | | |
| **Médio** | | | |
| **Baixo** | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.2 Armazenamento dos e-mails nas caixas de entrada dos usuários e nas pastas de mensagens sem proteção de integridade, autenticidade e sigilo.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.2.1** | **Exposição ou modificação não autorizada dos arquivos de correio** | 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

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.3.2.1 | | A1.1.3.2.1 | Modificar | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.3.2.1 | Implementar criptografia em repouso (AES-256); controle de acesso RBAC/ABAC; monitoramento de acesso privilegiado; segregação do storage. | A1.1.3.2.1 | 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

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.3.2.1 | Implementar criptografia em repouso (AES-256); controle de acesso RBAC/ABAC; monitoramento de acesso privilegiado; segregação do storage. | A1.1.3.2.1 | 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

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| **T1.1.3.2.1** | Implementar criptografia em repouso (AES-256); controle de acesso RBAC/ABAC; monitoramento de acesso privilegiado; segregação do storage. | A1.1.3.2.1 | Modificar | Baixa | Média | **Baixo** |

| Matriz de Risco | | | |
|---|---|---|---|
| | Probabilidade | | |
| Consequência | Baixo | Médio | Alto |
| Alto | | | |
| Médio | | | |
| Baixo | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

## Ativo: 1.1.3 Servidor de Correio

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| **T1.1.3.2.1** | Implementar criptografia em repouso (AES-256); controle de acesso RBAC/ABAC; monitoramento de acesso privilegiado; segregação do storage. | A1.1.3.2.1 | Modificar | Baixa | Média | **Baixo** |

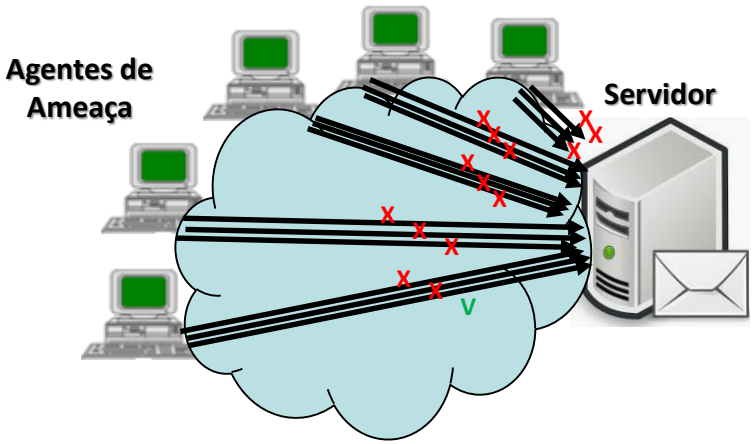
| Risco | Descrição | Tratamento |
|---|---|---|
| **Baixo** | **Risco tolerável**, sem necessidade de acompanhamento especial. | Aceitar |
| **Médio** | **Risco tolerável**, porém, com chances razoáveis de causar um impacto moderado. Neste caso, deve ser monitorado, sem urgência para a implementação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

**Exemplo: Listagem de ameaças para a vulnerabilidade.**

- **Ativo:**
  - **1.1.3 Servidor de Correio.**
- **Vulnerabilidade:**
  - **1.1.3.3 Autenticação fraca com uso de credencial apenas com login e senha.**
- **Ameaças:**

**1.1.3.3.1 Quebra de senhas fracas por força bruta ou pulverização de senhas (password spray)**



# Processo de Avaliação de Riscos – Análise de Riscos

**Ativo: 1.1.3 Servidor de Correio**

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.3 Autenticação fraca com uso de credencial apenas com login e senha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.3.1** | **Quebra de senhas fracas por força bruta ou pulverização de senhas (password spray)**<br><br>Probabilidade:<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.3 Autenticação fraca com uso de credencial apenas com login e senha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.3.1** | **Quebra de senhas fracas por força bruta ou pulverização de senhas (password spray)**<br><br>Probabilidade: serviço usa apenas login/senha para autenticação de usuários; e permite o cadastro de senhas curtas ou reutilizadas.<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.3 Autenticação fraca com uso de credencial apenas com login e senha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.3.1** | **Quebra de senhas fracas por força bruta ou pulverização de senhas (password spray)**<br><br>Probabilidade: serviço usa apenas login/senha para autenticação de usuários; e permite o cadastro de senhas curtas ou reutilizadas.<br><br>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.<br><br>(67% a 100% de chance de acontecer) |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.3 Autenticação fraca com uso de credencial apenas com login e senha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.3.1** | **Quebra de senhas fracas por força bruta ou pulverização de senhas (password spray)**<br><br>Probabilidade: serviço usa apenas login/senha para autenticação de usuários; e permite o cadastro de senhas curtas ou reutilizadas.<br><br>Consequência: acesso não autorizado e escalação de privilégios | Alta | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.3 Autenticação fraca com uso de credencial apenas com login e senha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.3.1** | **Quebra de senhas fracas por força bruta ou pulverização de senhas (password spray)**<br><br>Probabilidade: serviço usa apenas login/senha para autenticação de usuários; e permite o cadastro de senhas curtas ou reutilizadas.<br><br>Consequência: acesso não autorizado e escalação de privilégios | 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

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.3 Autenticação fraca com uso de credencial apenas com login e senha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.3.1** | **Quebra de senhas fracas por força bruta ou pulverização de senhas (password spray)**<br><br>Probabilidade: serviço usa apenas login/senha para autenticação de usuários; e permite o cadastro de senhas curtas ou reutilizadas.<br><br>Consequência: acesso não autorizado e escalação de privilégios | Alta | Alta | **Alto** |

| Matriz de Risco | | | |
|---|---|---|---|
| | **Probabilidade** | | |
| **Consequência** | **Baixo** | **Médio** | **Alto** |
| **Alto** | | | |
| **Médio** | | | |
| **Baixo** | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.3 Autenticação fraca com uso de credencial apenas com login e senha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.3.1** | **Quebra de senhas fracas por força bruta ou pulverização de senhas (password spray)** | 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

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.3.3.1 | | A1.1.3.3.1 | Modificar | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.3.3.1 | Implantação de MFA (Multifactor Authentication) com TOTP (Time-based One Time Password); política de senhas fortes; bloqueio por tentativas excedidas. | A1.1.3.3.1 | 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

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.3.3.1 | Implantação de MFA (Multifactor Authentication) com TOTP (Time-based One Time Password); política de senhas fortes; bloqueio por tentativas excedidas. | A1.1.3.3.1 | 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

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| **T1.1.3.3.1** | Implantação de MFA (Multifactor Authentication) com TOTP (Time-based One Time Password); política de senhas fortes; bloqueio por tentativas excedidas. | A1.1.3.3.1 | Modificar | Baixa | Média | **Baixo** |

| Matriz de Risco | | | |
|---|---|---|---|
| | Probabilidade | | |
| **Consequência** | **Baixo** | **Médio** | **Alto** |
| **Alto** | | | |
| **Médio** | | | |
| **Baixo** | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| **T1.1.3.3.1** | Implantação de MFA (Multifactor Authentication) com TOTP (Time-based One Time Password); política de senhas fortes; bloqueio por tentativas excedidas. | A1.1.3.3.1 | Modificar | Baixa | Média | **Baixo** |

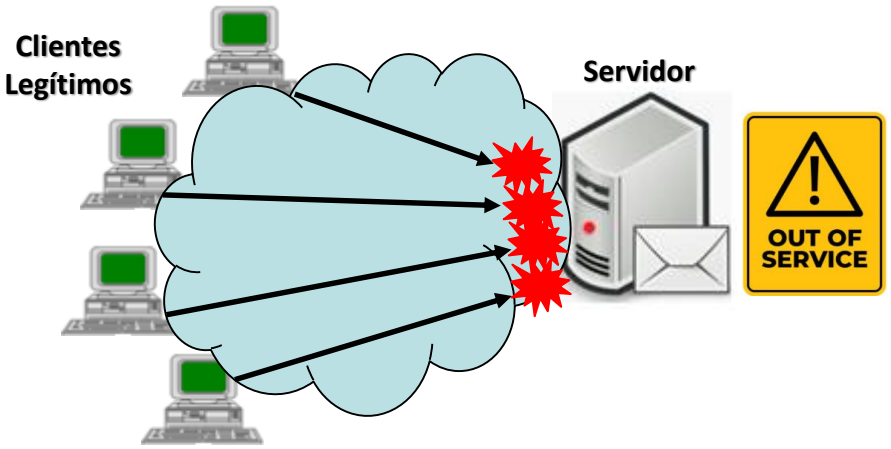
| Risco | Descrição | Tratamento |
|---|---|---|
| **Baixo** | **Risco tolerável**, sem necessidade de acompanhamento especial. | Aceitar |
| **Médio** | **Risco tolerável**, porém, com chances razoáveis de causar um impacto moderado. Neste caso, deve ser monitorado, sem urgência para a implementação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

**Exemplo: Listagem de ameaças para a vulnerabilidade.**

- **Ativo:**
  - **1.1.3 Servidor de Correio.**
- **Vulnerabilidade:**
  - **1.1.3.4 Infraestrutura de correio eletrônico operando com servidor único, sem unidade sobressalente para substituir um equipamento em pane.**
- **Ameaças:**

  **1.1.3.4.1 Indisponibilidade total por falha de hardware**



# Processo de Avaliação de Riscos – Análise de Riscos

**Ativo: 1.1.3 Servidor de Correio**

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.4 Infraestrutura de correio eletrônico operando com servidor único, sem unidade sobressalente para substituir um equipamento em pane.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.4.1** | **Indisponibilidade total por falha de hardware**<br><br>Probabilidade:<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.4 Infraestrutura de correio eletrônico operando com servidor único, sem unidade sobressalente para substituir um equipamento em pane.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.4.1** | **Indisponibilidade total por falha de hardware**<br><br>Probabilidade: sem equipamento sobressalente; depende do suporte interno limitado.<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.4 Infraestrutura de correio eletrônico operando com servidor único, sem unidade sobressalente para substituir um equipamento em pane.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.4.1** | **Indisponibilidade total por falha de hardware**<br><br>Probabilidade: sem equipamento sobressalente; depende do suporte interno limitado.<br><br>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.<br><br>(67% a 100% de chance de acontecer) |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.4 Infraestrutura de correio eletrônico operando com servidor único, sem unidade sobressalente para substituir um equipamento em pane.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.4.1** | **Indisponibilidade total por falha de hardware**<br><br>Probabilidade: sem equipamento sobressalente; depende do suporte interno limitado.<br><br>Consequência: paralisação de serviços críticos e impacto operacional. | Alta | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.4 Infraestrutura de correio eletrônico operando com servidor único, sem unidade sobressalente para substituir um equipamento em pane.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.4.1** | **Indisponibilidade total por falha de hardware**<br><br>Probabilidade: sem equipamento sobressalente; depende do suporte interno limitado.<br><br>Consequência: paralisação de serviços críticos e impacto operacional. | 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

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| **V1.1.3.4 Infraestrutura de correio eletrônico operando com servidor único, sem unidade sobressalente para substituir um equipamento em pane.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.3.4.1** | **Indisponibilidade total por falha de hardware**<br><br>Probabilidade: sem equipamento sobressalente; depende do suporte interno limitado.<br><br>Consequência: paralisação de serviços críticos e impacto operacional. | Alta | Alta | **Alto** |

| Matriz de Risco | | | |
|---|---|---|---|
| | **Probabilidade** | | |
| **Consequência** | **Baixo** | **Médio** | **Alto** |
| **Alto** | | | |
| **Médio** | | | |
| **Baixo** | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.3 Servidor de Correio

| 1.1.3 Servidor de Correio | | | | |
|---|---|---|---|---|
| V1.1.3.4 Infraestrutura de correio eletrônico operando com servidor único, sem unidade sobressalente para substituir um equipamento em pane. | | Pi | Ci | Ri |
| A1.1.3.4.1 | Indisponibilidade total por falha de hardware | 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

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.3.4.1 | | A1.1.3.4.1 | Modificar | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.3.4.1 | Implementação de redundância (cluster de alta disponibilidade); replicação em tempo real; monitoramento proativo de falhas. | A1.1.3.4.1 | 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

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.3.4.1 | Implementação de redundância (cluster de alta disponibilidade); replicação em tempo real; monitoramento proativo de falhas. | A1.1.3.4.1 | Modificar | Média | 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

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.3.4.1 | Implementação de redundância (cluster de alta disponibilidade); replicação em tempo real; monitoramento proativo de falhas. | A1.1.3.4.1 | Modificar | Média | Baixa | Baixo |

| Matriz de Risco | | | |
|---|---|---|---|
| | Probabilidade | | |
| Consequência | Baixo | Médio | Alto |
| Alto | | | |
| Médio | | | |
| Baixo | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

## Ativo: 1.1.3 Servidor de Correio

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.3.4.1 | Implementação de redundância (cluster de alta disponibilidade); replicação em tempo real; monitoramento proativo de falhas. | A1.1.3.4.1 | Modificar | Média | Baixa | Baixo |

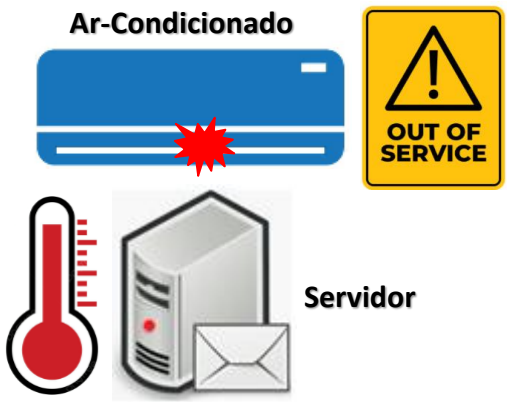
| Risco | Descrição | Tratamento |
|---|---|---|
| Baixo | **Risco tolerável**, sem necessidade de acompanhamento especial. | Aceitar |
| Médio | **Risco tolerável**, porém, com chances razoáveis de causar um impacto moderado. Neste caso, deve ser monitorado, sem urgência para a implementação de controles. | 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

**Exemplo: Listagem de ameaças para a vulnerabilidade.**

- **Ativo:**
  - **1.1.10 Ar-Condicionado.**
- **Vulnerabilidade:**
  - **1.1.10.1 Sistema de refrigeração configurado com equipamento único, sem redundância para suprir falha.**
- **Ameaças:**

**1.1.10.1.1 Indisponibilidade total por falha de hardware**



# Processo de Avaliação de Riscos – Análise de Riscos

**Ativo: 1.1.10 Ar-Condicionado**

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.1 Sistema de refrigeração configurado com equipamento único, sem redundância para suprir falha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.1.1** | **Interrupção total do resfriamento por falha do único equipamento**<br><br>Probabilidade:<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.1 Sistema de refrigeração configurado com equipamento único, sem redundância para suprir falha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.1.1** | **Interrupção total do resfriamento por falha do único equipamento**<br><br>Probabilidade: há apenas um aparelho split; falha inevitável paralisa o resfriamento do Data Center.<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.1 Sistema de refrigeração configurado com equipamento único, sem redundância para suprir falha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.1.1** | **Interrupção total do resfriamento por falha do único equipamento**<br><br>Probabilidade: há apenas um aparelho split; falha inevitável paralisa o resfriamento do Data Center.<br><br>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.<br><br>(67% a 100% de chance de acontecer) |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.1 Sistema de refrigeração configurado com equipamento único, sem redundância para suprir falha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.1.1** | **Interrupção total do resfriamento por falha do único equipamento**<br><br>Probabilidade: há apenas um aparelho split; falha inevitável paralisa o resfriamento do Data Center.<br><br>Consequência: superaquecimento rápido de servidores, desligamentos e possível perda de hardware. | Alta | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.1 Sistema de refrigeração configurado com equipamento único, sem redundância para suprir falha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.1.1** | **Interrupção total do resfriamento por falha do único equipamento**<br><br>Probabilidade: há apenas um aparelho split; falha inevitável paralisa o resfriamento do Data Center.<br><br>Consequência: superaquecimento rápido de servidores, desligamentos e possível perda de hardware. | 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

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.1 Sistema de refrigeração configurado com equipamento único, sem redundância para suprir falha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.1.1** | **Interrupção total do resfriamento por falha do único equipamento**<br><br>Probabilidade: há apenas um aparelho split; falha inevitável paralisa o resfriamento do Data Center.<br><br>Consequência: superaquecimento rápido de servidores, desligamentos e possível perda de hardware. | Alta | Alta | **Alto** |

| Matriz de Risco | | | |
|---|---|---|---|
| | **Probabilidade** | | |
| **Consequência** | **Baixo** | **Médio** | **Alto** |
| **Alto** | | | |
| **Médio** | | | |
| **Baixo** | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.1 Sistema de refrigeração configurado com equipamento único, sem redundância para suprir falha.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.1.1** | **Interrupção total do resfriamento por falha do único equipamento** | 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

**Ativo: 1.1.10 Ar-Condicionado**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.10.1.1 | | A1.1.10.1.1 | Modificar | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

**Ativo: 1.1.10 Ar-Condicionado**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.10.1.1 | Implantar redundância; instalar sensores de temperatura com alarme; plano de contingência com ventilação emergencial ou desligamento gradual dos servidores. | A1.1.10.1.1 | 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

**Ativo: 1.1.10 Ar-Condicionado**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.10.1.1 | Implantar redundância; instalar sensores de temperatura com alarme; plano de contingência com ventilação emergencial ou desligamento gradual dos servidores. | A1.1.10.1.1 | Modificar | Média | 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

**Ativo: 1.1.10 Ar-Condicionado**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| **T1.1.10.1.1** | Implantar redundância; instalar sensores de temperatura com alarme; plano de contingência com ventilação emergencial ou desligamento gradual dos servidores. | A1.1.10.1.1 | Modificar | Média | Baixa | **Baixo** |

| Matriz de Risco | | | |
|---|---|---|---|
| | Probabilidade | | |
| Consequência | Baixo | Médio | Alto |
| Alto | | | |
| Médio | | | |
| Baixo | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| **T1.1.10.1.1** | Implantar redundância; instalar sensores de temperatura com alarme; plano de contingência com ventilação emergencial ou desligamento gradual dos servidores. | A1.1.10.1.1 | Modificar | Média | Baixa | **Baixo** |

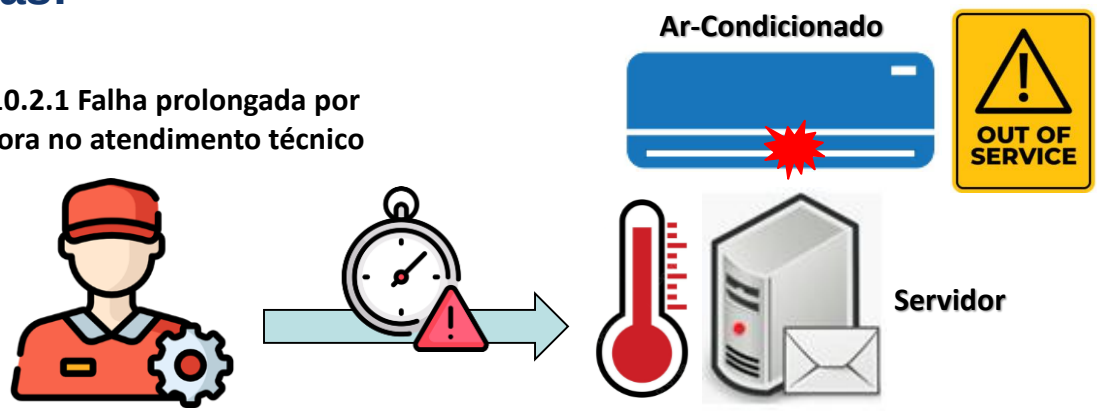
| Risco | Descrição | Tratamento |
|---|---|---|
| **Baixo** | **Risco tolerável**, sem necessidade de acompanhamento especial. | Aceitar |
| **Médio** | **Risco tolerável**, porém, com chances razoáveis de causar um impacto moderado. Neste caso, deve ser monitorado, sem urgência para a implementação 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

**Exemplo: Listagem de ameaças para a vulnerabilidade.**

- **Ativo:**
  - **1.1.10 Ar-Condicionado.**
- **Vulnerabilidade:**
  - **1.1.10.2 Serviço de manutenção do ar-condicionado prestado sem definição contratual de níveis de serviço (SLA).**
- **Ameaças:**

**1.1.10.2.1 Falha prolongada por demora no atendimento técnico**



# Processo de Avaliação de Riscos – Análise de Riscos

**Ativo: 1.1.10 Ar-Condicionado**

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.2 Serviço de manutenção do ar-condicionado prestado sem definição contratual de níveis de serviço (SLA).** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.2.1** | **Falha prolongada por demora no atendimento técnico**<br><br>Probabilidade:<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

**Ativo: 1.1.10 Ar-Condicionado**

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.2 Serviço de manutenção do ar-condicionado prestado sem definição contratual de níveis de serviço (SLA).** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.2.1** | **Falha prolongada por demora no atendimento técnico**<br><br>Probabilidade: não há contrato com SLA; manutenção é reativa.<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.2 Serviço de manutenção do ar-condicionado prestado sem definição contratual de níveis de serviço (SLA).** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.2.1** | **Falha prolongada por demora no atendimento técnico**<br><br>Probabilidade: não há contrato com SLA; manutenção é reativa.<br><br>Consequência: | 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.<br><br>(34% a 66% de chance de acontecer) |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.2 Serviço de manutenção do ar-condicionado prestado sem definição contratual de níveis de serviço (SLA).** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.2.1** | **Falha prolongada por demora no atendimento técnico**<br><br>Probabilidade: não há contrato com SLA; manutenção é reativa.<br><br>Consequência: risco de indisponibilidade total dos serviços de TIC por aquecimento. | Média | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.2 Serviço de manutenção do ar-condicionado prestado sem definição contratual de níveis de serviço (SLA).** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.2.1** | **Falha prolongada por demora no atendimento técnico**<br><br>Probabilidade: não há contrato com SLA; manutenção é reativa.<br><br>Consequência: risco de indisponibilidade total dos serviços de TIC por aquecimento. | Média | 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

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.2 Serviço de manutenção do ar-condicionado prestado sem definição contratual de níveis de serviço (SLA).** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.2.1** | **Falha prolongada por demora no atendimento técnico**<br>Probabilidade: não há contrato com SLA; manutenção é reativa.<br>Consequência: risco de indisponibilidade total dos serviços de TIC por aquecimento. | Média | Alta | **Alto** |

| Matriz de Risco | | | |
|---|---|---|---|
| | **Probabilidade** | | |
| **Consequência** | **Baixo** | **Médio** | **Alto** |
| **Alto** | | | |
| **Médio** | | | |
| **Baixo** | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.2 Serviço de manutenção do ar-condicionado prestado sem definição contratual de níveis de serviço (SLA).** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.2.1** | **Falha prolongada por demora no atendimento técnico** | 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

**Ativo: 1.1.10 Ar-Condicionado**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.10.2.1 | | A1.1.10.2.1 | Modificar | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

**Ativo: 1.1.10 Ar-Condicionado**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.10.2.1 | Firmar contrato de manutenção com SLA definido (ex: 4 h on-site); criar checklist mensal de verificação técnica; monitorar a temperatura ambiente. | A1.1.10.2.1 | 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

**Ativo: 1.1.10 Ar-Condicionado**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.10.2.1 | Firmar contrato de manutenção com SLA definido (ex: 4 h on-site); criar checklist mensal de verificação técnica; monitorar a temperatura ambiente. | A1.1.10.2.1 | Modificar | Baixa | 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

**Ativo: 1.1.10 Ar-Condicionado**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| **T1.1.10.2.1** | Firmar contrato de manutenção com SLA definido (ex: 4 h on-site); criar checklist mensal de verificação técnica; monitorar a temperatura ambiente. | A1.1.10.2.1 | Modificar | Baixa | Baixa | **Baixo** |

| Matriz de Risco | | | |
|---|---|---|---|
| | Probabilidade | | |
| Consequência | Baixo | Médio | Alto |
| Alto | | | |
| Médio | | | |
| Baixo | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| **T1.1.10.2.1** | Firmar contrato de manutenção com SLA definido (ex: 4 h on-site); criar checklist mensal de verificação técnica; monitorar a temperatura ambiente. | A1.1.10.2.1 | Modificar | Baixa | Baixa | **Baixo** |

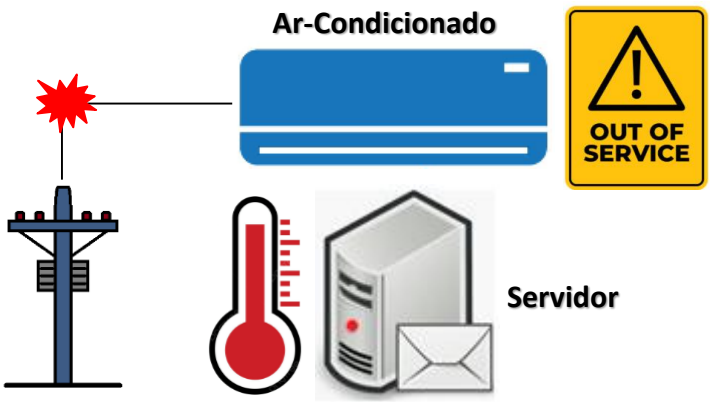
| Risco | Descrição | Tratamento |
|---|---|---|
| **Baixo** | **Risco tolerável**, sem necessidade de acompanhamento especial. | Aceitar |
| **Médio** | **Risco tolerável**, porém, com chances razoáveis de causar um impacto moderado. Neste caso, deve ser monitorado, sem urgência para a implementação 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

**Exemplo: Listagem de ameaças para a vulnerabilidade.**

- **Ativo:**
  - **1.1.10 Ar-Condicionado.**
- **Vulnerabilidade:**
  - **1.1.10.3 Sistema de refrigeração do Data Center operando sem fonte alternativa de energia dedicada.**
- **Ameaças:**

**1.1.10.3.1 Desligamento do ar-condicionado durante falhas de energia elétrica**



# Processo de Avaliação de Riscos – Análise de Riscos

**Ativo: 1.1.10 Ar-Condicionado**

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.3 Sistema de refrigeração do Data Center operando sem fonte alternativa de energia dedicada.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.3.1** | **Desligamento do ar-condicionado durante falhas de energia elétrica**<br><br>Probabilidade:<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.3 Sistema de refrigeração do Data Center operando sem fonte alternativa de energia dedicada.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.3.1** | **Desligamento do ar-condicionado durante falhas de energia elétrica**<br><br>Probabilidade: não há gerador nem alimentação independente para o sistema de refrigeração.<br><br>Consequência: | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.3 Sistema de refrigeração do Data Center operando sem fonte alternativa de energia dedicada.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.3.1** | **Desligamento do ar-condicionado durante falhas de energia elétrica**<br><br>Probabilidade: não há gerador nem alimentação independente para o sistema de refrigeração.<br><br>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.<br><br>(67% a 100% de chance de acontecer) |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.3 Sistema de refrigeração do Data Center operando sem fonte alternativa de energia dedicada.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.3.1** | **Desligamento do ar-condicionado durante falhas de energia elétrica**<br><br>Probabilidade: não há gerador nem alimentação independente para o sistema de refrigeração.<br><br>Consequência: risco de indisponibilidade total dos serviços de TIC por aquecimento. | Alta | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.3 Sistema de refrigeração do Data Center operando sem fonte alternativa de energia dedicada.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.3.1** | **Desligamento do ar-condicionado durante falhas de energia elétrica**<br><br>Probabilidade: não há gerador nem alimentação independente para o sistema de refrigeração.<br><br>Consequência: risco de indisponibilidade total dos serviços de TIC por aquecimento. | 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

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.3 Sistema de refrigeração do Data Center operando sem fonte alternativa de energia dedicada.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.3.1** | **Desligamento do ar-condicionado durante falhas de energia elétrica**<br><br>Probabilidade: não há gerador nem alimentação independente para o sistema de refrigeração.<br><br>Consequência: risco de indisponibilidade total dos serviços de TIC por aquecimento. | Alta | Alta | **Alto** |

| Matriz de Risco | | | |
|---|---|---|---|
| | **Probabilidade** | | |
| **Consequência** | **Baixo** | **Médio** | **Alto** |
| **Alto** | | | |
| **Médio** | | | |
| **Baixo** | | | |

# Processo de Avaliação de Riscos – Análise de Riscos

## Ativo: 1.1.10 Ar-Condicionado

| 1.1.10 Ar-Condicionado | | | | |
|---|---|---|---|---|
| **V1.1.10.3 Sistema de refrigeração do Data Center operando sem fonte alternativa de energia dedicada.** | | **Pi** | **Ci** | **Ri** |
| **A1.1.10.3.1** | **Desligamento do ar-condicionado durante falhas de energia elétrica** | 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

**Ativo: 1.1.10 Ar-Condicionado**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.10.3.1 | | A1.1.10.3.1 | Modificar | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

**Ativo: 1.1.10 Ar-Condicionado**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.10.3.1 | Implantar fonte alternativa de energia (gerador); instalar sistema automático de acionamento do backup energético; monitorar a temperatura ambiente. | A1.1.10.3.1 | 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

**Ativo: 1.1.10 Ar-Condicionado**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| T1.1.10.3.1 | Implantar fonte alternativa de energia (gerador); instalar sistema automático de acionamento do backup energético; monitorar a temperatura ambiente. | A1.1.10.3.1 | Modificar | Média | 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

**Ativo: 1.1.10 Ar-Condicionado**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| **T1.1.10.3.1** | Implantar fonte alternativa de energia (gerador); instalar sistema automático de acionamento do backup energético; monitorar a temperatura ambiente. | A1.1.10.3.1 | Modificar | Média | Baixa | **Baixo** |

| Matriz de Risco | | | |
|---|---|---|---|
| | Probabilidade | | |
| **Consequência** | **Baixo** | **Médio** | **Alto** |
| **Alto** | | | |
| **Médio** | | | |
| **Baixo** | | | |

# Processo de Avaliação de Riscos – Tratamento de Riscos

**Ativo: 1.1.3 Servidor de Correio**

| Tratamento dos riscos | | Ameaça | Tipo | Pr | Cr | Rr |
|---|---|---|---|---|---|---|
| **T1.1.10.3.1** | Implantar fonte alternativa de energia (gerador); instalar sistema automático de acionamento do backup energético; monitorar a temperatura ambiente. | A1.1.10.3.1 | Modificar | Média | Baixa | **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) |

# Dúvidas?


## 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

# 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


DEPARTAMENTO DE INFORMÁTICA PUC·RIO

PUC RIO