

---

# Auditoria de Sistemas de Informação

Aula 3 - Auditoria de sistemas em produção

Prof. Mário Akita

---



# Agenda do dia

## → Pontos de Controle

Definições e exemplos

## → Análise de Risco

Veremos o que é e como este processo é realizado

## → Metodologia de Auditoria de sistemas em Produção

Veremos com mais detalhes a metodologia básica de ASI aplicada em um sistema em produção.

—

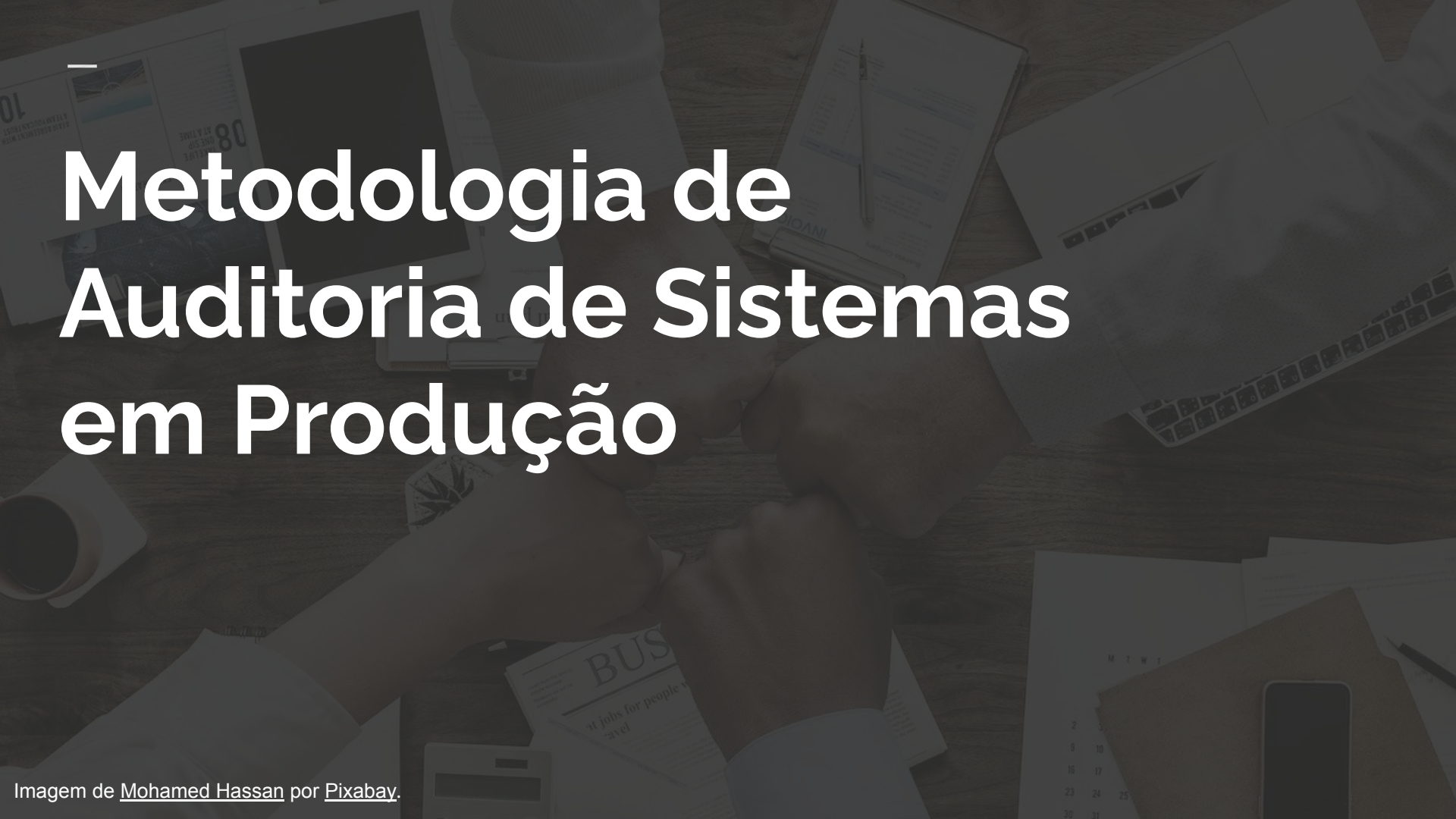
junho de 2023						
D	S	T	Q	Q	S	S
18	19 ✓	20 ✓	21	22	23	24
25	26	27	28	29	30	
julho de 2023						
D	S	T	Q	Q	S	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

# Calendário

- SEG 19/6 - aula presencial ✓
- TER 20/6 - reposição presencial

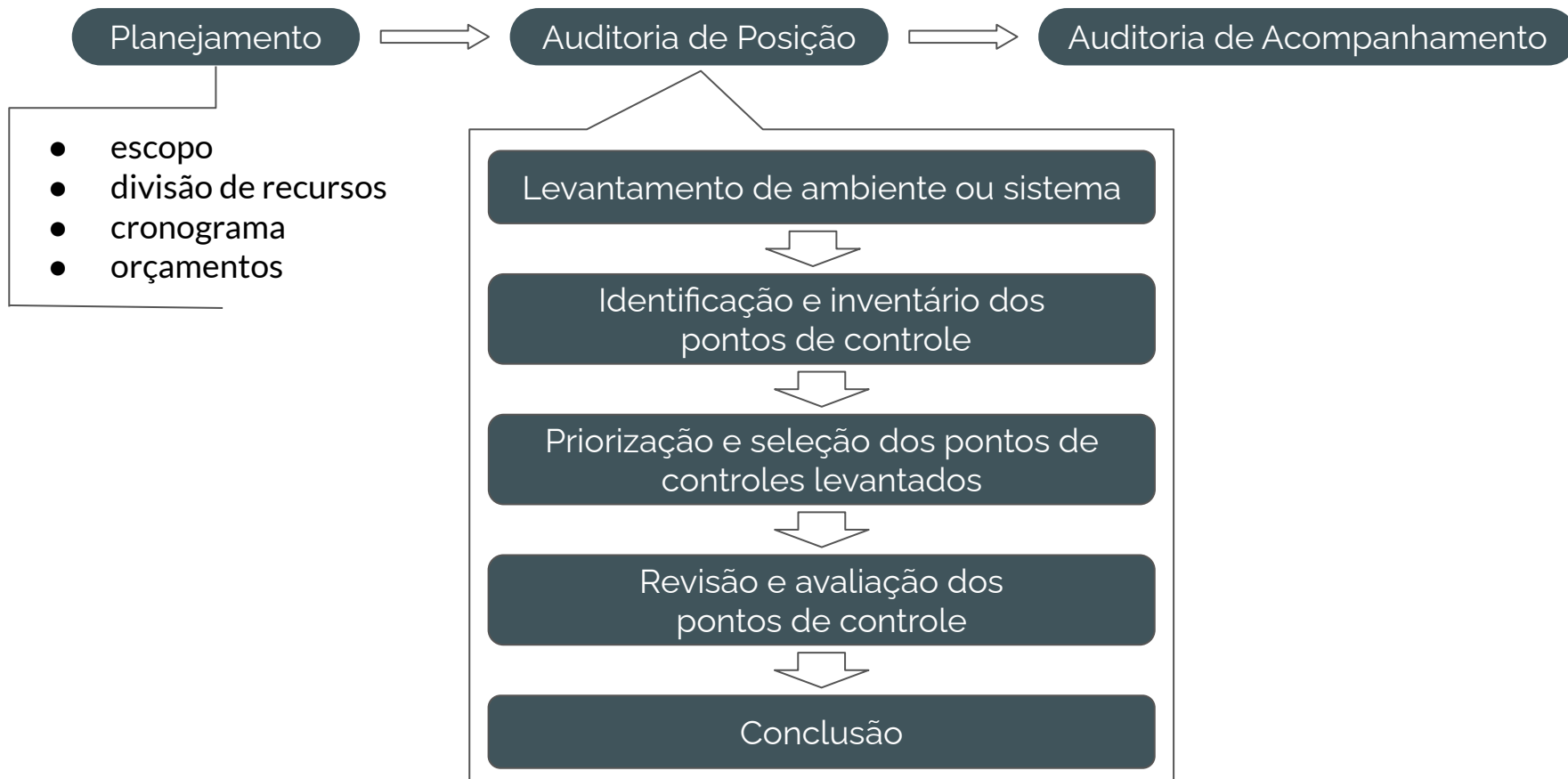


- SEX 23/6 - reposição presencial
- SAB 24/6 - reposição remota
- SEG 26/6 - aula presencial (P2)
- TER 27/6 - reposição presencial
- SEX 30/6 - reposição presencial
- SAB 1/7 - reposição remota
- SEG 3/7 - reposição presencial
- TER 4/7 - reposição remota
- QUA 5/7 - reposição remota
- QUI 6/7 - reposição remota
- SEX 7/7 - reposição remota



# Metodologia de Auditoria de Sistemas em Produção

## – Da aula anterior...



# – Na auditoria de sistema em produção



## → Identificação do tipo de auditoria

- ◆ Verificação de conformidade com padrões
- ◆ Melhoria processos sistematizados
- ◆ Compliance (conformidade)
  - Sistema bancário com normas do BACEN
  - Sistema de gerenciamento com regulamentos internos
  - Sistema de saúde com LGPD
- ◆ Certificação
  - Normas ISO, IEEE
- ◆ “Auditoria CSI”

# Formação das equipes de auditoria

- Grupo de coordenação

- Gerente de auditoria (coordenador dos trabalhos)
- Todos os gerentes que trabalham diretamente com o sistema a ser auditado
  - Gerente de Requisitos
  - Gerente de Desenvolvimento
  - Gerente de Testes
  - Gerente de Operações
  - Gerente de Suporte ao Produto
- (Desejável) Todos os coordenadores que trabalham em áreas diretamente afetadas ou afins
  - Coordenador de produto
  - Coordenador de RH (sistema de RH)
  - Coordenador de vendas (sistema de comércio online)
  - Coordenador de suprimentos (sistema de compras)
- (Desejável) Alta Gerência (representante)
  - Diretor de TI
  - CIO



# Formação das equipes de auditoria

- Grupo de trabalho
  - Auditores
  - Alguns representantes que trabalham diretamente com o sistema a ser auditado
    - Analista de Requisitos
    - Analista de Desenvolvimento
    - Analista de Testes
    - Analista de Operações
    - Analista de Suporte ao Produto
  - Algum representante de áreas diretamente afetadas ou afins
    - Analista de RH (sistema de RH)
    - Analista de vendas (sistema de comércio online)
    - Analista de suprimentos (sistema de compras)



# Tarefas de cada grupo

- Grupo de coordenação
  - Verificar se os trabalhos se alinham com os objetivos geral da empresa e do processo
  - Definição do objetivo
  - Definir o escopo
  - Aprovar orçamentos e cronogramas
  - Aprovar relatório final ou parecer de auditoria
- Grupo de trabalho
  - Elaborar os orçamentos e cronogramas
  - levantar recursos necessários para realização da auditoria
  - Realizar as análises e coletas de evidências
  - Escrever o relatório final ou parecer

Planejamento

Auditoria de Posição

Auditoria de Acompanhamento

Levantamento de  
ambiente ou sistema

### Objetivos:

- Entender o sistema a nível macro.
- Entender os conceitos envolvidos em sua concepção, modelos, arquitetura e componentes.

Identificação e  
inventário dos  
pontos de controle

### → Análise de documentação

Priorização e  
seleção dos pontos  
de controles  
levantados

- ◆ Diagrama de fluxo de dados (DFD)
- ◆ Dicionário de dados
- ◆ Modelo Entidade-Relacionamento

Revisão e avaliação  
dos pontos de  
controle

### → Entrevistas com analistas/responsáveis

### → Conversa com os operadores do sistema

Conclusão

Planejamento



Auditoria de Posição

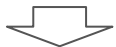


Auditoria de Acompanhamento

Levantamento de  
sistema



Identificação e  
inventário dos  
pontos de controle



Priorização e  
seleção dos pontos  
de controles  
levantados



Revisão e avaliação  
dos pontos de  
controle



Conclusão

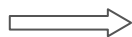
## Objetivos:

- Identificar elementos que estão no escopo delimitado no planejamento e merecem ser levantados e validados pela auditoria.

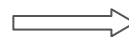
## → Identificação dos pontos de controle

- ◆ rotinas
- ◆ arquivos gerados e consumidos
- ◆ informações

Planejamento



Auditoria de Posição



Auditoria de Acompanhamento

Levantamento de  
sistema



Identificação e  
inventário dos  
pontos de controle



Priorização e  
seleção dos pontos  
de controles  
levantados



Revisão e avaliação  
dos pontos de  
controle

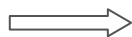


Conclusão

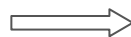
## → Ciclo de vida de dado em um sistema de informação

- ◆ captação de dados
- ◆ codificação e entrada de dados
- ◆ transmissão
- ◆ processamento
- ◆ armazenamento
- ◆ recuperação da informação
- ◆ apresentação/divulgação de informação

Planejamento



Auditoria de Posição

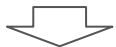


Auditoria de Acompanhamento

Levantamento de  
sistema



Identificação e  
inventário dos  
pontos de controle



Priorização e  
seleção dos pontos  
de controles  
levantados



Revisão e avaliação  
dos pontos de  
controle



Conclusão

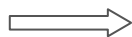
## Sistemas de processamento em lotes (*batch*)

São sistemas que processam de uma só vez uma grande quantidade de arquivos acumulados durante certo período de tempo, geralmente com pouca ou nenhuma interação humana.

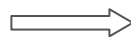
Exemplos:

- processamento de agendamento de pagamento
- fechamento de fatura do cartão de crédito

Planejamento



Auditoria de Posição

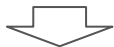


Auditoria de Acompanhamento

Levantamento de  
sistema



Identificação e  
inventário dos  
pontos de controle



Priorização e  
seleção dos pontos  
de controles  
levantados



Revisão e avaliação  
dos pontos de  
controle

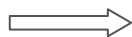


Conclusão

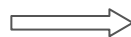
## Pontos de controle em Sistemas de processamento em lotes (*batch*)

- documentos de entrada
- rotina de preparação de dados
- rotina de conversão de dados
- rotina de consistência de dados
- rotina de cálculo e atualização de arquivos
- arquivo mestre
- arquivo de transação
- emissão de relatório
- controle de qualidade
- saída de dados

Planejamento



Auditoria de Posição

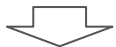


Auditoria de Acompanhamento

Levantamento de  
sistema



Identificação e  
inventário dos  
pontos de controle



Priorização e  
seleção dos pontos  
de controles  
levantados



Revisão e avaliação  
dos pontos de  
controle



Conclusão

## Sistemas de processamento em tempo real (online)

São sistemas que interagem com usuários (ou outros sistemas) em tempo real. As informações não são acumuladas e processadas à medida em que são recebidas pelos serviços.

Exemplos:

- rede social
- sistema de controle



Planejamento



Auditoria de Posição

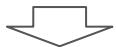


Auditoria de Acompanhamento

Levantamento de  
sistema



Identificação e  
inventário dos  
pontos de controle



Priorização e  
seleção dos pontos  
de controles  
levantados



Revisão e avaliação  
dos pontos de  
controle



Conclusão

## Sistemas de processamento em tempo real (online)

- autorização e acesso ao banco de dados
- transação e atualização de registros em banco de dados
- rotinas de manutenção em banco de dados
- leitura de banco de dados
- escrita de log
- consulta e emissão de relatórios
- conteúdo de telas
- conteúdo de relatórios

Planejamento



Auditoria de Posição



Auditoria de Acompanhamento

Levantamento de  
sistema



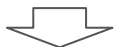
Identificação e  
inventário dos  
pontos de controle



Priorização e  
seleção dos pontos  
de controles  
levantados



Revisão e avaliação  
dos pontos de  
controle



Conclusão

### Objetivos:

- Identificar elementos que estão no escopo delimitado no planejamento e merecem ser levantados e validados pela auditoria.

### Saída:

- Listagem com os pontos de controle identificados assim como os riscos associados a cada um deles para que sejam analisados pela equipe de coordenação.

Planejamento

Auditoria de Posição

Auditoria de Acompanhamento

Levantamento de  
sistema

Identificação e  
inventário dos  
pontos de controle

Priorização e  
seleção dos pontos  
de controles  
levantados

Revisão e avaliação  
dos pontos de  
controle

Conclusão

### Objetivos:

- Priorizar os pontos de controle encontrados e selecionar aqueles que serão efetivamente auditados.

### → Análise de risco

Cálculo do risco que cada fraqueza representa para a empresa ponderado pela chance (probabilidade) de que ela efetivamente se materialize (em algumas ferramentas, pode ser ponderada pelo custo também).

Planejamento

Auditoria de Posição

Auditoria de Acompanhamento

Levantamento de  
sistema

Identificação e  
inventário dos  
pontos de controle

Priorização e  
seleção dos pontos  
de controles  
levantados

Revisão e avaliação  
dos pontos de  
controle

Conclusão

## Matriz de risco

Cálculo do risco que cada ponto representa para a empresa ponderado pela chance (probabilidade) de que ela efetivamente se materialize (em algumas ferramentas, pode ser ponderada pelo custo também).

---

## Exemplo de análise de risco:

<https://www.linkedin.com/embed/feed/update/urn:li:ugcPost:7072531444610269185?compact=1>

---

## → Matriz de risco



## → Matriz de risco





## → Matriz de risco

chance do risco acontecer

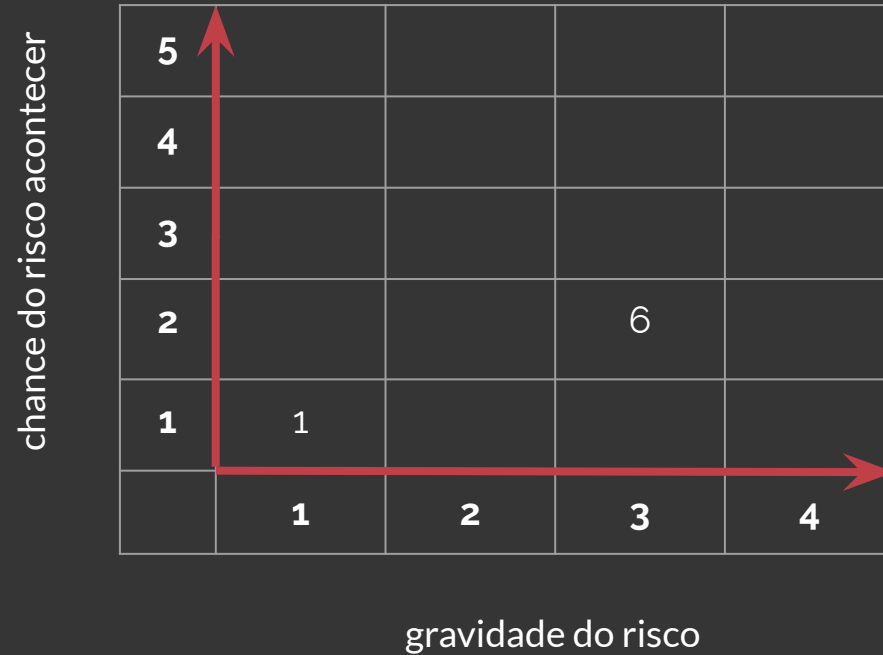
5	<b>Frequente:</b> Ocorre continuamente.
4	<b>Provável:</b> Ocorre muitas vezes durante o ciclo de vida de um produto
3	<b>Ocasional:</b> Pode ocorrer alguma vez durante o ciclo de vida de um produto
2	<b>Remoto:</b> Dificilmente ocorrerá
1	<b>Improvável:</b> Muito improvável de acontecer, mas possível.

## → Matriz de risco

	Insignificante	Marginal	Crítico	Catastrófico
Vida	Escoriações	Pequenos ferimentos	Incapacidade severa	Morte
Sistemas	Perda ou indisponibilidade pontual de sistema	Perda ou indisponibilidade restrita de sistema	Perda ou indisponibilidade considerável de sistema	Perda permanente de sistema
Perda de dados	Sem perda ou indisponibilidade considerável de dados	Breve indisponibilidade de dados	Perda temporária de dados	Perda permanente de dados
Atividades empresariais	Desempenho de atividades afetado pontualmente	Desempenho de atividades levemente afetado	Desempenho de atividades seriamente afetado	Grande perda de faturamento ou paralisia das atividades
Físico/ambiental	Dano causal	Pequenos danos	Dano de grande monta	Destruição completa
Impacto atividades	Impacto altamente contido	Impacto local	Impacto de médio prazo	Impacto de Longo prazo
Legal	Sem risco de punição	Punição questionável	Risco de punição importante	Risco de punição severa
	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>

gravidade do risco

## → Matriz de risco



## → Matriz de risco

chance do risco acontecer

<b>5</b>	5	10	15	20
<b>4</b>	4	8	12	16
<b>3</b>	3	6	9	12
<b>2</b>	2	4	6	8
<b>1</b>	1	2	3	4
	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>

gravidade do risco

## → Matriz de risco

chance do risco acontecer	5	5	10	15	20
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
gravidade do risco					

$r \leq 3$	aceitável
$4 \leq r \leq 7$	aceitável com plano de gerenciamento
$8 \leq r \leq 10$	indesejável
$r > 10$	inaceitável

—

# Dúvidas?



---

---

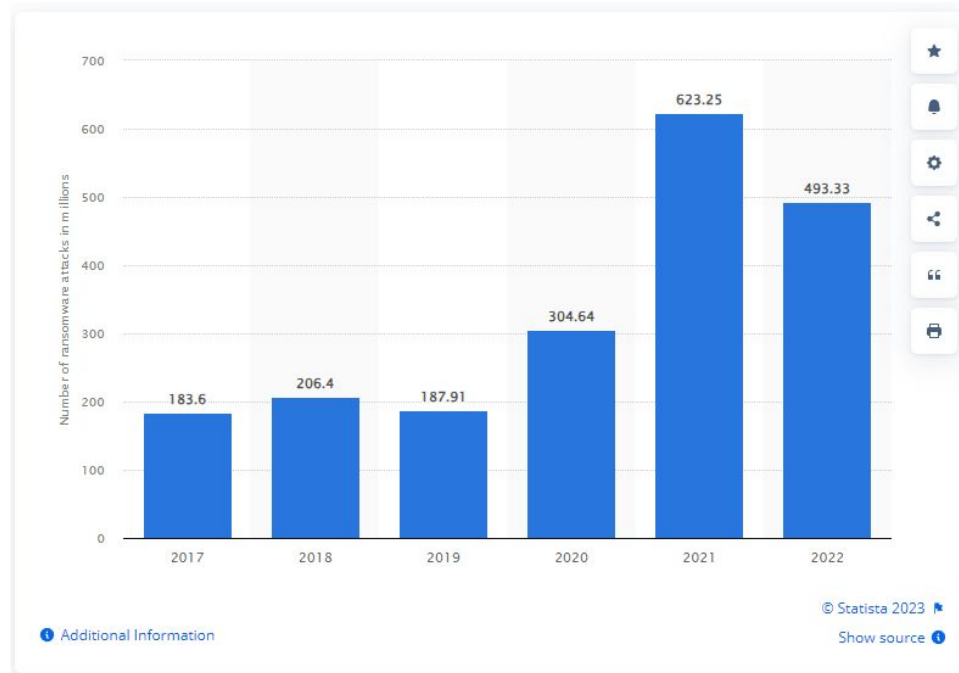
**Exemplo:**

Ataque de *ransomware*


---



# Ataque de *ransomware*



## Ataque de *ransomware*

- 
- |   |   |
|---|---|
| 5 | <b>Frequente:</b> Ocorre continuamente.   |
| 4 | <b>Provável:</b> Ocorre muitas vezes durante o ciclo de vida de um produto      |
| 3 | <b>Ocasional:</b> Pode ocorrer alguma vez durante o ciclo de vida de um produto |
| 2 | <b>Remoto:</b> Dificilmente ocorrerá  |
| 1 | <b>Improvável:</b> Muito improvável de acontecer, mas possível.                 |

## Ataque de *ransomware*

5 **Frequente:** Ocorre continuamente.

4 **Provável:** Ocorre muitas vezes durante o ciclo de vida de um produto


3 **Ocasional:** Pode ocorrer alguma vez durante o ciclo de vida de um produto

2 **Remoto:** Dificilmente ocorrerá

1 **Improvável:** Muito improvável de acontecer, mas possível.

## Ataque de *ransomware*

Insignificante	Marginal	Crítico	Catastrófico
Escoriações	Pequenos ferimentos	Incapacidade severa	Morte
Perda ou indisponibilidade pontual de sistema	Perda ou indisponibilidade restrita de sistema	Perda ou indisponibilidade considerável de sistema	Perda permanente de sistema
Sem perda ou indisponibilidade considerável de dados	Breve indisponibilidade de dados	Perda temporária de dados	Perda permanente de dados
Desempenho de atividades afetado pontualmente	Desempenho de atividades levemente afetado	Desempenho de atividades seriamente afetado	Grande perda de faturamento ou paralisia das atividades
Dano causal	Pequenos danos	Dano de grande monta	Destruição completa
Impacto altamente contido	Impacto local	Impacto de médio prazo	Impacto de Longo prazo
Sem risco de punição	Punição questionável	Risco de punição importante	Risco de punição severa
1	2	3	4



## Ataque de *ransomware*

Insignificante	Marginal	Crítico	Catastrófico
Escoriações	Pequenos ferimentos	Incapacidade severa	Morte
Perda ou indisponibilidade pontual de sistema	Perda ou indisponibilidade restrita de sistema	Perda ou indisponibilidade considerável de sistema	Perda permanente de sistema
Sem perda ou indisponibilidade considerável de dados	Breve indisponibilidade de dados	Perda temporária de dados	Perda permanente de dados
Desempenho de atividades afetado pontualmente	Desempenho de atividades levemente afetado	Desempenho de atividades seriamente afetado	Grande perda de faturamento ou paralisia das atividades
Dano causal	Pequenos danos	Dano de grande monta	Destruição completa
Impacto altamente contido	Impacto local	Impacto de médio prazo	Impacto de Longo prazo
Sem risco de punição	Punição questionável	Risco de punição importante	Risco de punição severa
1	2	3	4

## Ataque de *ransomware*

chance do risco acontecer	5	5	10	15	20
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		gravidade do risco			

$r \leq 3$	aceitável
$4 \leq r \leq 7$	aceitável com plano de gerenciamento
$8 \leq r \leq 10$	indesejável
$r > 10$	inaceitável

---

---

## Exemplo:

Conversão de separador decimal incorreto no relatório gerencial interno

---



## Conversão de separador decimal incorreto no relatório gerencial interno

5	<b>Frequente:</b> Ocorre continuamente.
4	<b>Provável:</b> Ocorre muitas vezes durante o ciclo de vida de um produto
3	<b>Ocasional:</b> Pode ocorrer alguma vez durante o ciclo de vida de um produto
2	<b>Remoto:</b> Dificilmente ocorrerá
1	<b>Improvável:</b> Muito improvável de acontecer, mas possível.

## Conversão de separador decimal incorreto no relatório gerencial interno

5	<b>Frequente:</b> Ocorre continuamente.
4	<b>Provável:</b> Ocorre muitas vezes durante o ciclo de vida de um produto
3	<b>Ocasional:</b> Pode ocorrer alguma vez durante o ciclo de vida de um produto
2	<b>Remoto:</b> Dificilmente ocorrerá
1	<b>Improvável:</b> Muito improvável de acontecer, mas possível.

## Conversão de separador decimal incorreto no relatório gerencial interno

<b>Insignificante</b>	<b>Marginal</b>	<b>Crítico</b>	<b>Catastrófico</b>
Escoriações	Pequenos ferimentos	Incapacidade severa	Morte
Perda ou indisponibilidade pontual de sistema	Perda ou indisponibilidade restrita de sistema	Perda ou indisponibilidade considerável de sistema	Perda permanente de sistema
Sem perda ou indisponibilidade considerável de dados	Breve indisponibilidade de dados	Perda temporária de dados	Perda permanente de dados
Desempenho de atividades afetado pontualmente	Desempenho de atividades levemente afetado	Desempenho de atividades seriamente afetado	Grande perda de faturamento ou paralisia das atividades
Dano causal	Pequenos danos	Dano de grande monta	Destruição completa
Impacto altamente contido	Impacto local	Impacto de médio prazo	Impacto de Longo prazo
Sem risco de punição	Punição questionável	Risco de punição importante	Risco de punição severa
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>

# Conversão de separador decimal incorreto no relatório gerencial interno

Insignificante	Marginal	Crítico	Catastrófico
Escoriações	Pequenos ferimentos	Incapacidade severa	Morte
Perda ou indisponibilidade pontual de sistema	Perda ou indisponibilidade restrita de sistema	Perda ou indisponibilidade considerável de sistema	Perda permanente de sistema
Sem perda ou indisponibilidade considerável de dados	Breve indisponibilidade de dados	Perda temporária de dados	Perda permanente de dados
Desempenho de atividades afetado pontualmente	Desempenho de atividades levemente afetado	Desempenho de atividades seriamente afetado	Grande perda de faturamento ou paralisia das atividades
Dano causal	Pequenos danos	Dano de grande monta	Destruição completa
Impacto altamente contido	Impacto local	Impacto de médio prazo	Impacto de Longo prazo
Sem risco de punição	Punição questionável	Risco de punição importante	Risco de punição severa
1	2	3	4

# Conversão de separador decimal incorreto no relatório gerencial interno

chance do risco acontecer	5	5	10	15	20
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		gravidade do risco			

$r \leq 3$	aceitável
$4 \leq r \leq 7$	aceitável com plano de gerenciamento
$8 \leq r \leq 10$	indesejável
$r > 10$	inaceitável

## Ataque de *ransomware*

chance do risco acontecer

5	5	10	15	20
4	4	8	12	16
3	3	6	9	12
2	2	4	6	8
1	1	2	3	4
	1	2	3	4

gravidade do risco

$r \leq 3$	aceitável
$4 \leq r \leq 7$	aceitável com plano de gerenciamento
$8 \leq r \leq 10$	indesejável
$r > 10$	inaceitável

Planejamento

Auditoria de Posição

Auditoria de Acompanhamento

Levantamento de  
**sistema**

Identificação e  
inventário dos  
pontos de controle

Priorização e  
seleção dos pontos  
de controles  
levantados

Revisão e avaliação  
dos pontos de  
controle

Conclusão

### Objetivos:

- Priorizar os pontos de controle encontrados e selecionar aqueles que serão efetivamente auditados.

### Saída:

- Listagem com os pontos de controle priorizados e eleitos.

Planejamento

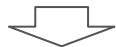
Auditoria de Posição

Auditoria de Acompanhamento

Levantamento de  
sistema



Identificação e  
inventário dos  
pontos de controle



Priorização e  
seleção dos pontos  
de controles  
levantados



Revisão e avaliação  
dos pontos de  
controle



Conclusão

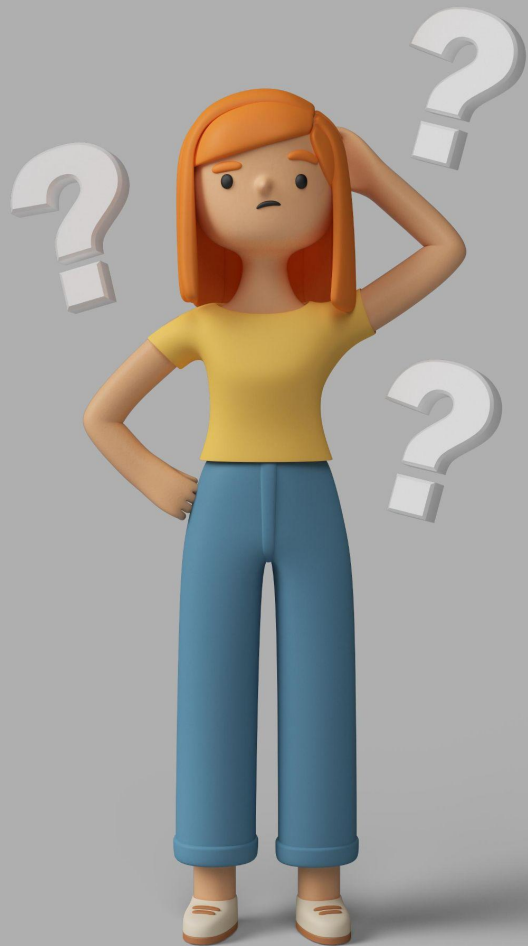
### Objetivos:

- Examinar os pontos priorizados validando-os ou detectando suas fraquezas.

### → Coleta das evidências

Através da utilização de alguns métodos, o auditor deverá juntar materiais como documentos e mídias para validar os pontos de controles ou evidenciar suas fraquezas ou falhas e recomendar a adoção de novos controles para endereçá-las.





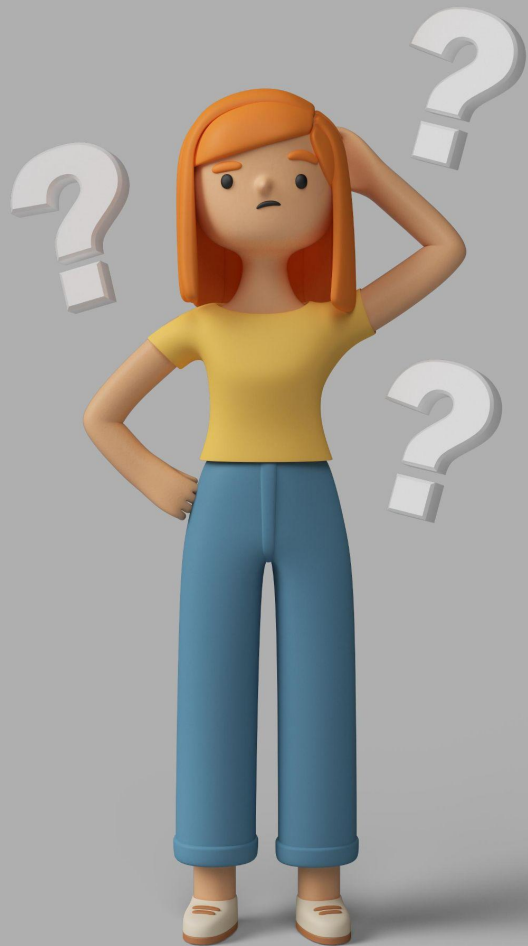
## Estamos coletando evidências **do quê,** afinal?

De que as ameaças em potencial foram devidamente tratadas ou precisam de tratamentos.

# E como, coletar essas evidências?

Através de alguns métodos tais como:

- Verificação *in loco*
- Questionários
- Entrevistas
- *Test-deck*
- *Tracing, mapping* e *snapshot*
- Análise de *log*
- Desenvolvimento de script/uso de *software* específico
- Simulação paralela
- Teste de recuperação
- Teste de desempenho
- Teste de segurança / suites de segurança
- Testes de caixa preta / caixa branca



## Verificação *in loco*

Consiste em uma visita ao local de trabalho para observar as atividades, layout do local, interações entre pessoas e equipamentos, como os procedimentos são executados, dentre outros aspectos.

### O que pode ser coletado?

- descrição dos procedimentos
- situações ou acontecimentos dignos de nota
- relatos
- fotografias de layouts, postos de trabalhos
- fluxo da rotina local

### Limitações

- presença do auditor pode mudar a rotina □ fator surpresa
- janela temporal limitada
- pode não observar períodos de picos, sazonalidade

# Questionários

Consiste em um conjunto de perguntas aplicado a pessoas estrategicamente selecionadas para avaliar se determinado ponto de controle é efetivo e eficaz em evitar determinados riscos.

Serve como um bom ponto de partida para selecionar pontos a serem avaliados com mais profundidade posteriormente.

## O que pode ser coletado?

- respostas de questionários
- relatos

## Limitações

- produz evidências circunstanciais
- limitada pela percepção do respondente
- qualidade das respostas pode ser baixa
- sujeito a subjetividade

# Entrevistas

Consiste em reuniões entre o auditor e pessoas envolvidas com o ponto de controle a ser auditado.

Tem como objetivo avaliar o grau de controle existente.

## O que pode ser coletado?

- testemunhos
- relatos
- esclarecimentos

## Limitações

- limitada pela percepção do entrevistado
- sujeito a subjetividade

—

# Dúvidas?



# Referências

SCHMIDT, Paulo. SANTOS, José Luiz. ARIMA, Carlos Hideo. **Introdução à Auditoria de Sistemas de Informação**. 2006.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA (ENAP). **Técnicas de Auditoria Interna Governamental**.

UNIVERSIDADE ESTÁCIO DE SÁ. **Auditoria e controles de seg. e classificação da informação**

UNIVERSIDADE DE CIÊNCIA E TECNOLOGIA DE HONG KONG. **Information Systems Auditing, Controls and Assurance**. 2023. In: coursera.org

NAGATA, Hiromassa. GOMES, Estela Maria. **Fundamentos de Auditoria e Auditoria de Sistemas**.