



André Amorim
Finanças Corporativas

Auditoria

• contato@andreamorim.com.br
• www.andreamorim.com.br

Anhanguera

1

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**



André Amorim
Finanças Corporativas

Anhanguera

2

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

A avaliação prévia de riscos, em auditoria interna, mede e prioriza os riscos para possibilitar o foco da auditoria nas áreas auditáveis mais significativas.

André Amorim
Finanças Corporativas

Anhanguera

3

2ª Aula - Auditoria Baseada em Riscos – ABR

Auditoria

• Auditoria Baseada em Riscos

Para que a Auditoria baseada em Riscos seja efetiva, recomenda-se:

- 1) Que os conceitos de risco sejam compreendidos com clareza e
- 2) Que exista tempo para o planejamento.

4

2ª Aula - Auditoria Baseada em Riscos – ABR

Auditoria

• Auditoria Baseada em Riscos

Adicionalmente, os fundamentos da auditoria devem ser o norte:

“...os auditores internos auxiliam a organização a realizar seus objetivos....avaliando e melhorando a eficácia dos processos de gerenciamento de (1) governança, (2) riscos e (3) controle”

5

2ª Aula - Auditoria Baseada em Riscos – ABR

Auditoria

• Auditoria Baseada em Riscos

Fundamentos

“...os auditores internos auxiliam a organização a realizar seus objetivos.... avaliando e melhorando a eficácia dos processos de gerenciamento de:

- 1) Governança
- 2) Riscos
- 3) Controle

6

2ª Aula - Auditoria Baseada em Riscos – ABR

Auditoria

• Auditoria Baseada em Riscos

Governança Corporativa

"...os auditores internos auxiliam a organização a realizar seus objetivos.... avaliando e melhorando a eficácia dos processos de gerenciamento de (1) governança (2) riscos e (3) controle."



7

2ª Aula - Auditoria Baseada em Riscos – ABR

Auditoria

• Auditoria Baseada em Riscos

Governança de T.I

Podemos definir Governança de T.I como uma estrutura de relacionamentos e processos para dirigir e controlar a organização no atingimento de seus objetivos, adicionando valor ao mesmo tempo que equilibra os riscos em relação ao retorno da TI e seus processos.



8

2ª Aula - Auditoria Baseada em Riscos – ABR

Auditoria

• Auditoria Baseada em Riscos

Governança Corporativa

Podemos definir a Governança Corporativa como o conjunto de práticas, políticas de controle e processo de gestão baseado numa correta identificação dos riscos inerentes às operações e a consequente ação para garantir o máximo de eficiência em gestão.

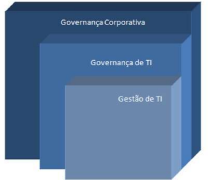


9

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Governança de T.I



- Garantir que a TI suporte e maximize os objetivos e estratégias da organização.
- Permitir controlar a execução e a qualidade dos serviços.
- Viabilizar o acompanhamento de contratos internos e externos.
- Definir condições para o exercício eficaz da gestão com base em conceitos consolidados de qualidade.

André Amorim
Instituto Corporativo

Anhanguera

10

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Riscos

“...os auditores internos auxiliam a organização a realizar seus objetivos.... avaliando e melhorando a eficácia dos processos de gerenciamento de (1) governança, (2) riscos e (3) controles.”

André Amorim
Instituto Corporativo

Anhanguera

11

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Riscos

Risco é a possibilidade de que um evento irá ocorrer tendo um impacto positivo ou negativo no cumprimento dos objetivos.

André Amorim
Instituto Corporativo

Anhanguera

12

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Riscos

Existem diversas categorias de riscos (dependendo do negócio), porém listamos abaixo os principais:

- 1) Risco Estratégico
- 2) Risco Financeiro
- 3) Risco Operacional

13

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Riscos

Identificar e mitigar riscos são atividades vitais para a manutenção da operação e para a garantia que os objetivos da organização serão atingidos.

- 1) O que significa mitigar riscos?
- 2) Quais riscos a Organização deve mitigar?
- 3) Qual a relação positiva entre a auditoria e a gestão de riscos?

14

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Riscos

Na análise de riscos, consideram-se (1) probabilidade e (2) o impacto de sua ocorrência.

15

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Riscos

		PROBABILIDADE		
		ALTO	MÉDIA	BAIXA
IMPACTO	ALTO	Alto	Alto	Médio
	MÉDIO	Alto	Médio	Baixo
	BAIXO	Médio	Baixo	Baixo

André Amorim
Parque Cooperativo

Anhanguera

16

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Avaliação de Riscos de T.I

Gerenciar os riscos de TI e da Segurança da Informação significa reconhecer as vulnerabilidades do ambiente, avaliá-las e recomendar controles (soluções e ferramentas) que mitiguem estes riscos à níveis aceitáveis.

André Amorim
Parque Cooperativo

Anhanguera

17

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Avaliação de Riscos de T.I

As principais áreas de risco em TI são:

- Aplicações
- Serviços Compartilhados (gerenciamento de database, etc)
- Infraestrutura humana (conhecimento, habilidades, etc)
- Componentes de TI (hardware e software)

André Amorim
Parque Cooperativo

Anhanguera

18

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Avaliação de Riscos de T.I

As principais ameaças em TI são:

- Acesso lógico não autorizado.
- Software malicioso.
- Falhas de software básico.

 André Amorim
Parque Cooperativa

 Anhanguera

19

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Avaliação de Riscos de T.I

As principais ameaças em TI são:

- Modificação não autorizada de dados e software.
- Engenharia social. (Email's falsos de entidades bancos, etc)
- Falsificação de endereço IP

 André Amorim
Parque Cooperativa

 Anhanguera

20

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Avaliação de Riscos de T.I

As principais ameaças em TI são:

- Captura de informações.
- Erro humano.
- Vírus

 André Amorim
Parque Cooperativa

 Anhanguera

21

2ª Aula - Auditoria Baseada em Riscos – ABR

Auditoria

• Auditoria Baseada em Riscos

Avaliação de Riscos de T.I

As principais vulnerabilidades em TI são:

- Administração negligente de perfis de acessos (senhas).
- Compartilhamento de conta/senha.
- Falta de "time out" em conexão.

22

2ª Aula - Auditoria Baseada em Riscos – ABR

Auditoria

• Auditoria Baseada em Riscos

Avaliação de Riscos de T.I

As principais vulnerabilidades em TI são:

- Ausência de notificação de tentativa de acesso.
- Ausência de criptografia e dados sensíveis.
- Ausência de segregação de ambientes (desenvolvimento, homologação e produção).

23

2ª Aula - Auditoria Baseada em Riscos – ABR

Auditoria

• Auditoria Baseada em Riscos

Avaliação de Riscos de T.I

As principais vulnerabilidades em TI são:

- Ausência de backup.
- Inexistência de controles de mudanças de software.

24

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**
Avaliação de Riscos de T.I
 NBR ISO/IEC 27001
A ABNT NBR ISO/IEC 27001 especifica requisitos para um Sistema de Gestão de Segurança da Informação (SGSI) baseado em uma abordagem de riscos do negócio.

 André Amorim
 Anhanguera 

25

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**
Avaliação de Riscos de T.I
 NBR ISO/IEC 27001
A ABNT NBR ISO/IEC 27001 adota o ciclo denominado PDCA (Plan, Do, Check, Act) para estruturar todos os processos envolvidos em um SGSI.

 André Amorim
 Anhanguera 

26

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**
Avaliação de Riscos de T.I
 NBR ISO/IEC 27001
O PDCA é uma ferramenta gerencial que possibilita a melhoria contínua de processos e a solução de problemas.

 André Amorim
 Anhanguera 

27

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**
Avaliação de Riscos de T.I
 NBR ISO/IEC 27001



André Amorim
Parque Corporativo

Anhanguera

28

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**
Avaliação de Riscos de T.I
 Estabelecimento do SGSI (Plan)



- Definir escopo e políticas do SGSI.
- Definir uma abordagem sistemática para avaliação do risco.
- Identificar os riscos.

André Amorim
Parque Corporativo

Anhanguera

29

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**
Avaliação de Riscos de T.I
 Estabelecimento do SGSI (Plan)



- Analisar e avaliar os riscos.
- Identificar e analisar opções para tratamento de riscos.
- Selecionar objetivos de controles para tratar esses riscos.

André Amorim
Parque Corporativo

Anhanguera

30

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Avaliação de Riscos de T.I

Estabelecimento do SGSI (Plan)

- Obter aprovação da direção dos riscos residuais propostos.
- Obter autorização da direção para implementar e operar o SGSI.
- Preparar uma declaração de aplicabilidade.

André Amorim
Parque Cooperativa

Anhanguera

31

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Avaliação de Riscos de T.I

Estabelecimento do SGSI (Do)

- Formular um plano de tratamento de riscos que identifique a ação de gestão apropriada, recursos, responsabilidades e prioridades para a gestão dos riscos de segurança.

André Amorim
Parque Cooperativa

Anhanguera

32

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Avaliação de Riscos de T.I

Estabelecimento do SGSI (Check)

- Executar procedimentos de monitoração e análise crítica e outros controles para detectar erros, identificar tentativas, violações e incidentes de segurança

André Amorim
Parque Cooperativa

Anhanguera

33

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Avaliação de Riscos de T.I

Estabelecimento do SGSI (Do)

- Implementar os controles selecionados para atender os objetivos
- Definir como medir a eficácia dos controles ou grupos de controles selecionados.



34

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Avaliação de Riscos de T.I

Estabelecimento do SGSI (Check)

- Realizar análises críticas regulares da eficácia do SGSI
- Medir a eficácia dos controles para verificar que os requisitos de segurança da informação foram atendidos.



35

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**

Avaliação de Riscos de T.I

Estabelecimento do SGSI (Act)

- Mensurar performance do SGSI.
- Identificar e implementar melhorias no SGSI.



36

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

• **Auditoria Baseada em Riscos**
Avaliação de Riscos de T.I
 Estabelecimento do SGSI (Act)

- Tomar ações corretivas e preventivas.
- Revisar o SGSI quando necessário.



37

2ª Aula - Auditoria Baseada em Riscos – ABR **Auditoria**

FIM



38
