SEGURANÇA E AUDITORIA DE SISTEMAS DE INFORMAÇÃO

Prof. Cesar Amaral

prof.cesar.amaral@gmail.com

Aula 3 - Análise de Riscos

- Como vimos anteriormente, devido ao fato de a informação ser o principal ativo das empresas diversos controles passaram a ser implementados a fim de protegê-la de pessoas mal intencionadas.

- A primeira coisa que temos que ter em mente quando o assunto é segurança da informação é que não existe segurança 100%. Novas **ameaças** surgem a todo instante e é impossível se proteger contra todas elas. O que podemos (e DEVEMOS) fazer é minimizar seus impactos na empresa.

- Outra coisa que torna o “sonho” da segurança 100% um mito é que o cenário de TI muda constantemente, e constantemente os **ativos** também mudam.

- Mas o que são os ativos da minha empresa???

- O ativo de uma empresa é qualquer coisa que tenha valor para ela, tudo aquilo que ela necessita para realizar suas atividades, como:

- Equipamentos
- Equipamentos de comunicação
- Mídias
- Servidores
- Móveis
- Serviços de rede
- Celulares
- Senhas
- Relatórios
- Dados de contrato, etc.

Classificação dos ativos

- Os ativos podem ser classificados em Tangíveis e Intangíveis:

  - **Tangíveis:** Aplicações, equipamentos, informações, a organização e os usuários.

  - **Intangíveis:** Imagem, reputação, credibilidade, habilidade de desenvolvimento de alguma atividade.

- Cada empresa terá seus ativos específicos e saberá qual a importância de cada um desses ativos.

- Os ativos são necessários nas atividades da empresa, nos processos empresariais de cada uma das áreas.

- Após essa etapa de identificação dos ativos, devemos definir qual a importância deles para o negócio da empresa, verificando os pontos fracos deles e identificando quais medidas de segurança podem ser implementadas a fim de melhorar isso.

- Para proteger os ativos, principalmente o ativo informação, é preciso conhecer os riscos, as ameaças e as vulnerabilidades que os colocam em perigo. Assim podemos planejar políticas e procedimentos para eliminar, ou pelo menos diminuir os possíveis problemas.

- Esse processo é conhecido como **análise de riscos**, e tem a função de indicar em que ocasião certo contexto pode ou não ser aceito por uma organização.

Só se deve aceitar um risco quando o custo de controle do mesmo for maior que os danos que ele pode causar

- Quando não sabemos o que temos que proteger, contra o que temos que proteger, implementar os controles de segurança torna-se uma tarefa quase impossível, pois acabamos implementando medidas de segurança inadequadas.

- Após realizar a análise de todo seu cenário, a empresa poderá tomar medidas que visem diminuir seu grau de exposição diante de um determinado problema.

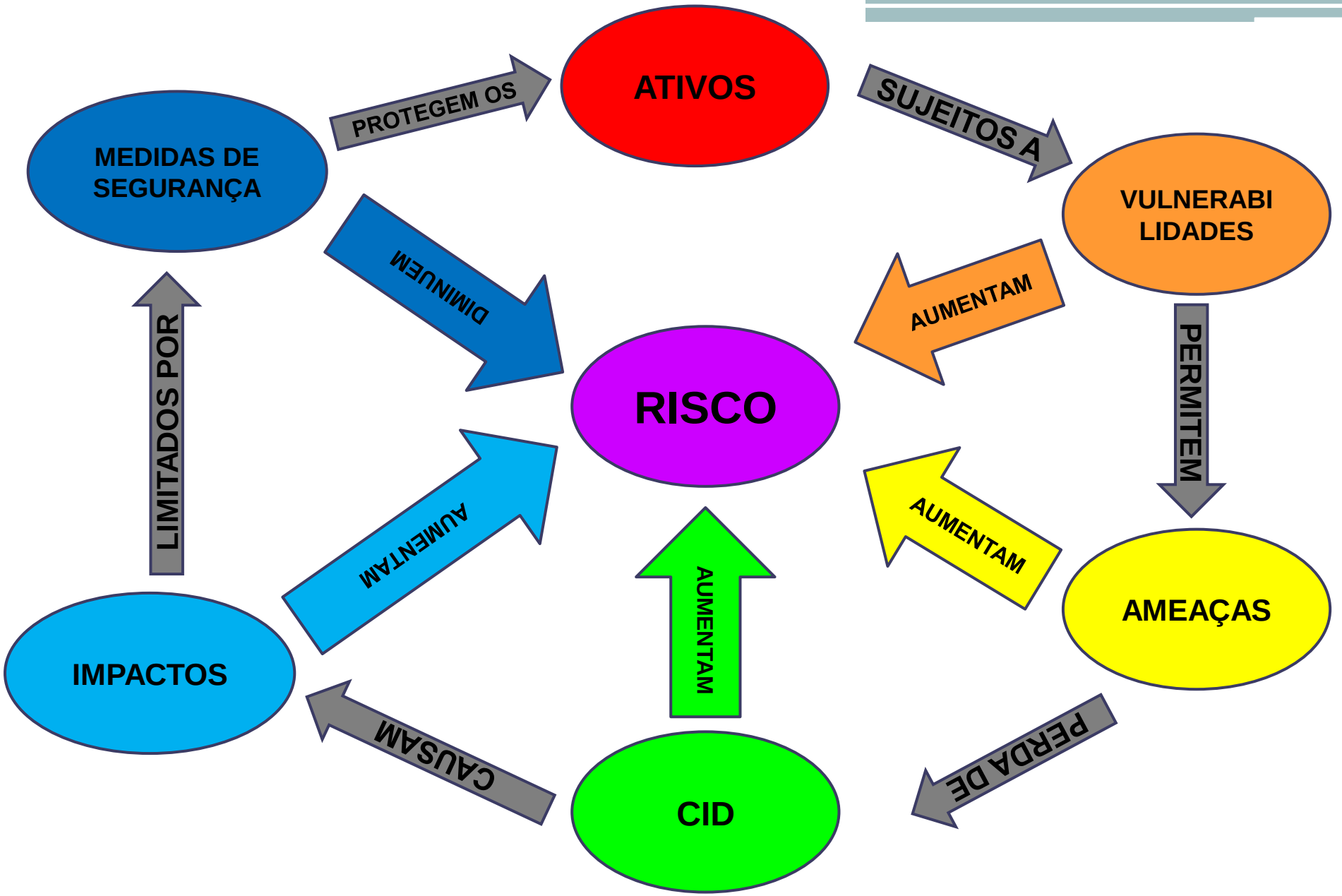
- Uma característica sobre a análise de riscos é que cada pessoa a realiza da sua maneira, então divergências podem ocorrer. Por isso é recomendável que mais de uma pessoa esteja envolvida nesse processo, a fim de trocar ideias e se chegar à melhor decisão possível, visando sempre proteger a informação da melhor maneira.

- Cada empresa deve avaliar os riscos do cenário de uma maneira.

- Mas o que é um **RISCO**?

  - Perigo ou possibilidade de perigo (chance de um problema relativo a segurança acontecer) pela exploração das vulnerabilidades (pontos fracos), expondo o ativo a perdas (de confidencialidade, integridade e disponibilidade), provocando perdas / impactos. Impactos esses que serão limitados pelas medidas de segurança que forem implementadas.

RISCO = probabilidade de uma ameaça explorar uma ou mais vulnerabilidades dos ativos, causando perdas.


ATIVOS
PROTEGEM OS
SUJEITOS A
MEDIDAS DE SEGURANÇA
VULNERABILIDADES
DIMINUEM
AUMENTAM
PERMITEM
LIMITADOS POR
RISCO
AUMENTAM
AUMENTAM
AMEAÇAS
IMPACTOS
AUMENTAM
CAUSAM
PERDA DE
CID

- Devemos fazer a análise de riscos para evitarmos as medidas **corretivas** de segurança. Quando fazemos a análise de riscos podemos agir de maneira **preventiva**.

- Para a realização da análise de riscos é essencial que se conheça muito bem o negócio da empresa e todo seu funcionamento.

- Além do conceito de risco, mais alguns conceitos são primordiais quando tratamos de análise de riscos:

- **Vulnerabilidades**: fraquezas associadas aos ativos, ponto suscetível a ataque ou ser explorado por uma ameaça. Todo ativo possui uma ou mais vulnerabilidades a serem protegidas.
- **Ameaças**: algo que pode resultar em um incidente inesperado; eventos que exploram as vulnerabilidades, causando prejuízos.
- **Impactos**: efeitos que uma determinada ação pode causar. Podem ser positivos ou negativos, mas no caso de ameaças à segurança da informação eles sempre são negativos.

Vulnerabilidades

- Fraquezas associadas aos ativos da organização que caso exploradas por uma ameaça representam riscos concretos a organização. É o ponto onde o sistema poderá ser suscetível a ataque.

- Exemplo:
  - A localização física dos prédios deverá ser observada conforme:
    - Linhas de comunicação podem ser escutadas ou interrompidas?

- Mesmo que as ameaças pareçam insignificantes, todas as possíveis vulnerabilidades devem ser identificadas.

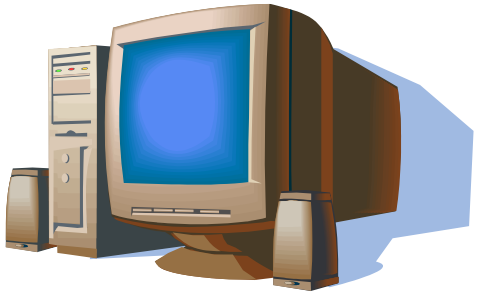
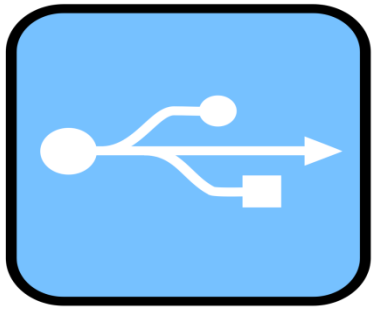
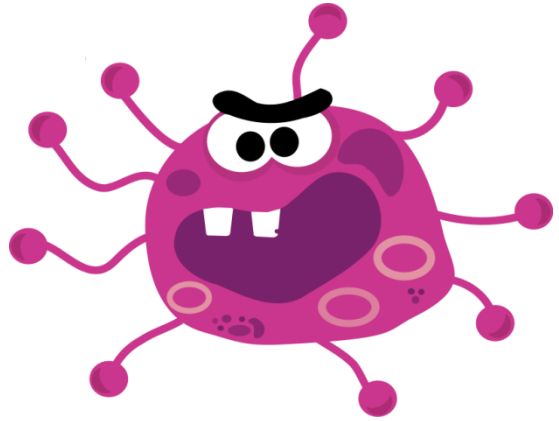
Ameaças

- Independente do que façamos, as ameaças irão existir... Mas temos que nos precaver contra sua ocorrência o máximo possível.
- As ameaças podem ser classificadas em:
  - **Naturais**: envolvem fenômenos da natureza;
  - **Físicas**: envolvem a ação de um agente externo:
    - **Não intencionais**: ocorre sem intenção de causar danos;
    - **Propositais:** o agente causador desse tipo de ameaça tem essa intenção... A ideia é prejudicar o próximo.

Impacto

- É o conceito utilizado para medir os efeitos positivos ou negativos que uma determinada atividade pode causar.

- Como impactos podemos citar:
  - Perda financeira; Abalo na imagem; Multas ou sanções; Perda de investidores; Prejuízo operacional; Aumento no custo operacional; Parada no negócio da empresa; Perda de ativos; Alteração na quantidade de pessoas para a execução do processo; Redução da margem de lucro. etc..

ATIVO	VULNERABILIDADE	AMEAÇA
		
Computador	Portas USB desbloqueadas	Infecção por vírus de computador

QUAIS OUTRAS AMEAÇAS PODEM SER UM PROBLEMA PARA ESSA VULNERABILIDADE?

RISCO = probabilidade de uma ameaça explorar uma ou mais vulnerabilidades dos ativos, causando perdas

- **Principais etapas do processo de análise de riscos:**
  - Entender o negócio da empresa;
  - Mapear os processos;
  - Identificar os ativos que suportam os processos;
  - Identificar as vulnerabilidades dos ativos;
  - Identificar quais ameaças podem explorar essas vulnerabilidade;
  - Identificar quais são os possíveis impactos que essas ameaças podem causar;
  - Determinar a probabilidade dessas ameaças se tornarem realidade;
  - Tomar medidas preventivas quanto a essas vulnerabilidades.

MAPEAMENTO DE PROCESSOS

- Um processo empresarial é o conjunto de atividades que uma determinada área da empresa tem que executar para atender ou produzir algum serviço.

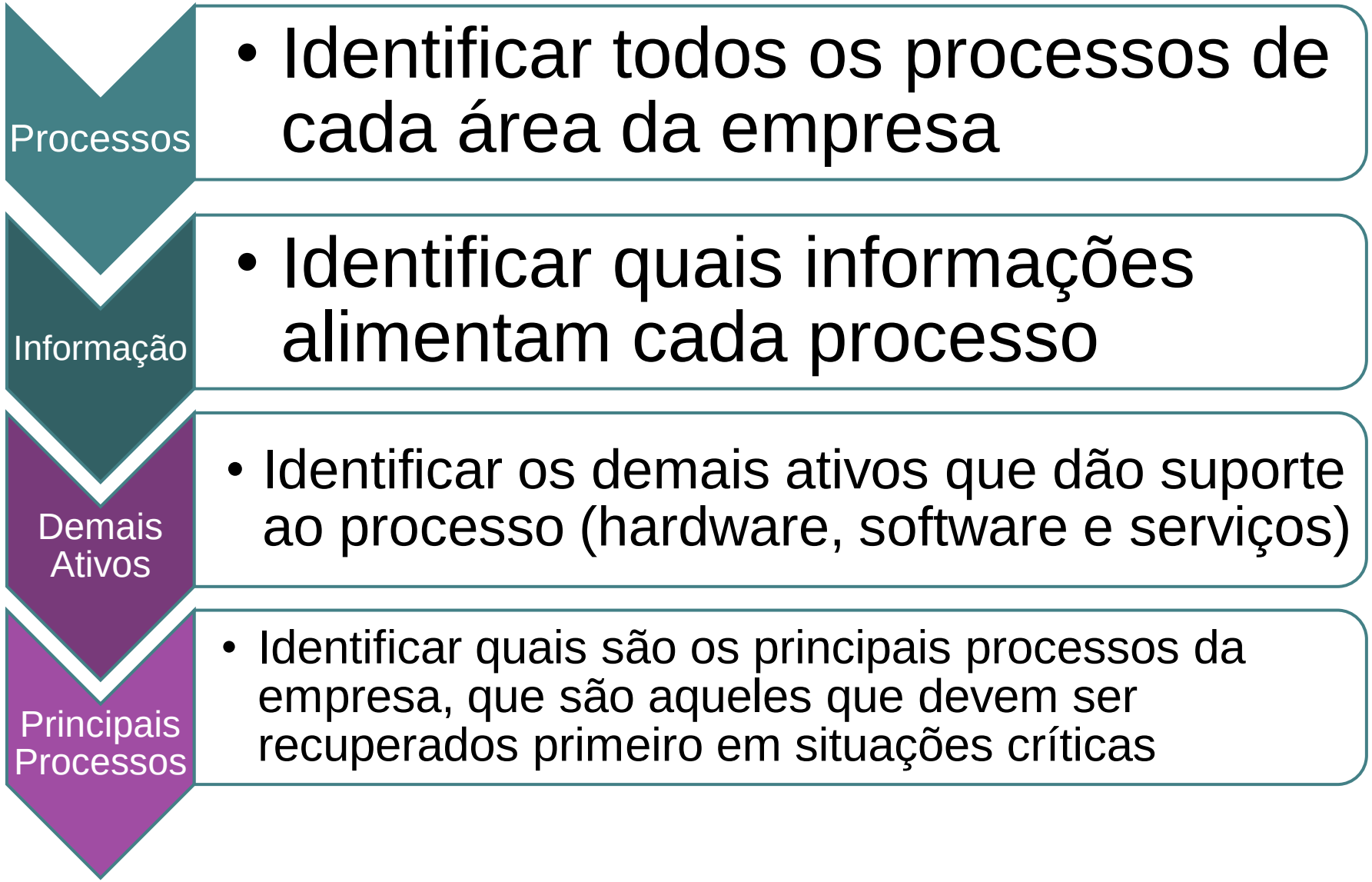
- Precisamos identificar TODOS os processos de cada área, em seguida identificar todos os ativos que alimentam esses processos, definir quais são os processos mais importantes para o negócio da empresa e, em seguida, começar a implementar controles de segurança.

- Todo processo envolve 3 etapas:
  - Entrada
  - Processamento
  - Saída

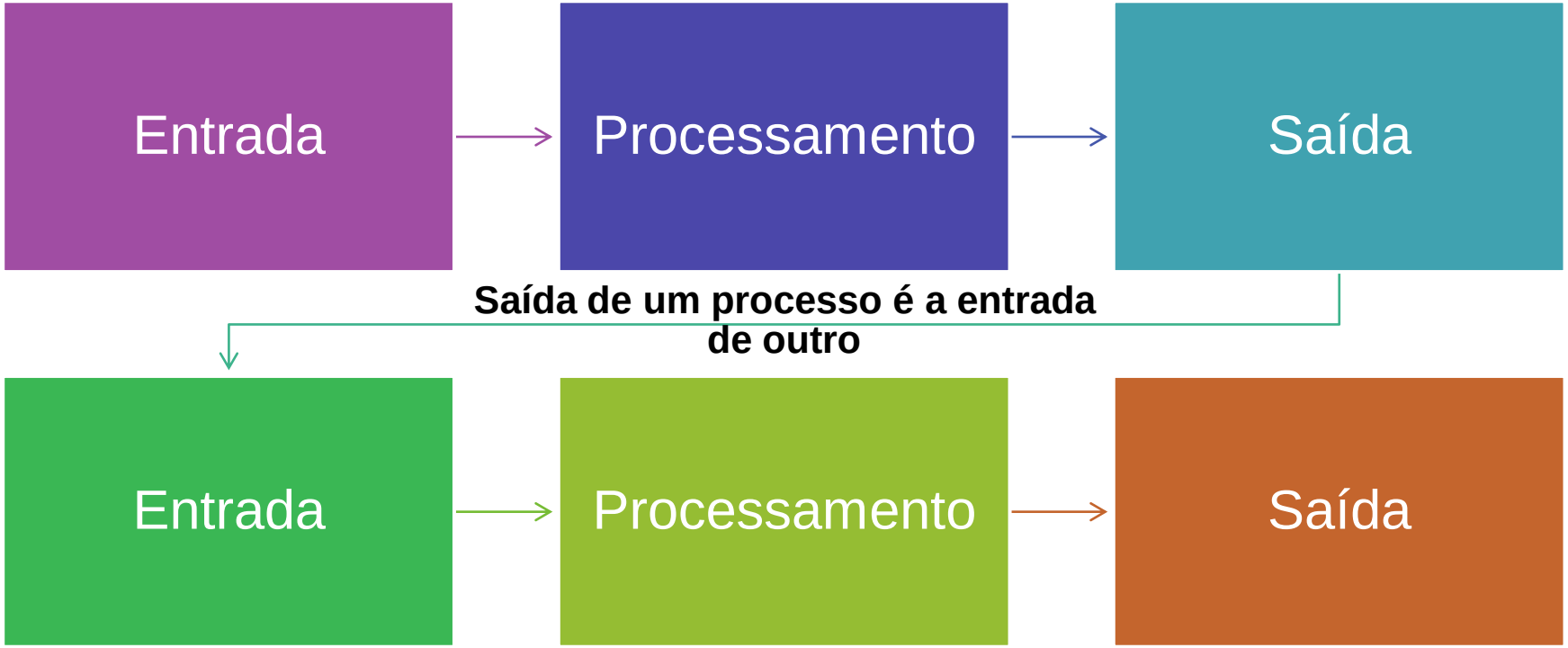
- Apesar da importância do conhecimento dos processos das empresas, na maioria das vezes eles são realizados no automático, de maneira informal e não documentada.

- O mapeamento dos processos não é importante apenas para segurança e continuidade, mas também para trazer maior eficiência empresarial.

- Quando os processos estão devidamente mapeados, conseguimos identificar quais são os mais importantes para a empresa, quais são as vulnerabilidades de cada um deles e quais controles devemos implementar.


Processos
• Identificar todos os processos de cada área da empresa
Informação
• Identificar quais informações alimentam cada processo
Demais Ativos
• Identificar os demais ativos que dão suporte ao processo (hardware, software e serviços)
Principais Processos
• Identificar quais são os principais processos da empresa, que são aqueles que devem ser recuperados primeiro em situações críticas

- Os processos se relacionam uns com os outros, e a saída de um processo, na maioria das vezes, é a entrada de outro.



Métodos de Análise de Riscos

- O objetivo da análise de riscos é identificar os possíveis riscos de um cenário de TI, respondendo perguntas como:
  - O que pode acontecer de errado?
  - Com que frequência isso pode acontecer?
  - Quais as suas possíveis consequências?
  - O que precisa ser feito para que se possa diminuir os riscos?
  - O que, como e onde devo priorizar as ações de segurança?
  - Devo aceitar esse risco?

- Ao se fazer uma análise de riscos é preciso, antes de qualquer coisa, conhecer muito bem o cenário da empresa e suas necessidades de segurança, além de seus problemas.
- Para se realizar uma análise de riscos pode-se usar algumas técnicas:
  - **Análise quantitativa**
  - **Análise qualitativa**
  - Análise preliminar de perigos
  - Análise preliminar de riscos
  - Estudo de operabilidade de riscos
  - Análise de modos de falha e efeitos
  - Análise de consequências e vulnerabilidade
  - Brainstorming
  - Diagrama de causa e efeito de Ishikawa

Análise Quantitativa

- Faz-se um levantamentos dos riscos e de todos os itens do cenário e valores são atribuídos
- Esses valores são reais e com base no negócio da empresa
- Esse valores são em termos do custo de substituição e também perda de produtividade
- Aqui temos a matriz GUT por exemplo.

Análise Qualitativa

- Faz-se um levantamentos dos riscos e de todos os itens do cenário e analisa as características de cada um deles, fazendo uma classificação.
- Usa critérios para estimar os impactos provocados pela exploração das vulnerabilidades dos ativos.
- É uma técnica bastante usada pois permite uma melhor quantificação dos impactos.
- Aqui podem ser analisados também os pontos positivos que se tem, ao contrário de outras técnicas.
- Aqui temos a análise SWOT por exemplo.

Matriz GUT

Matriz GUT

- Uma das ferramentas mais usadas para análise de riscos.
- Também conhecida como matriz de priorização.
- É uma ferramenta quantitativa.
- Objetivo: facilitar a identificação dos problemas mais críticos.

- **Gravidade:** Impacto do problema na empresa : considerar os prejuízos e dificuldades causados; quão grave é esse problema.

- **Urgência:** Relação com o tempo disponível ou necessário para resolver o problema; quando devemos tomar uma atitude para minimizar os impactos.

MAIOR URGÊNCIA ➔ MENOR TEMPO

- **Tendência:** Potencial ou padrão de crescimento do problema; o que ocorrerá com a situação e os impactos se nada for feito.

- Cada item levantado deve receber uma pontuação de 1 a 5 para cada um dos aspectos da matriz GUT.

- Deve ser realizado o cálculo para obter o produto (resultado da multiplicação) dos 3 aspectos:

RISCO = G * U * T

- O resultado desse cálculo pode nos oferecer 3 representações:
  - **VERDE – 1 a 42**
  - **AMARELO – 43 a 83**
  - **VERMELHO – 84 a 125**
- Usamos cores para melhor visualização dos impactos.

- Com o resultado do cálculo podemos ordenar o que é prioritário, sendo o que tem valor maior mais importante.

- Com os valores obtidos, recomenda-se que sejam organizados do maior para o menor, e os problemas que tiverem a maior prioridade serão os que devem ser tratados em um primeiro momento, justamente por serem os que têm maior Gravidade, Urgência e Tendência.

GRAVIDADE	URGÊNCIA	TENDÊNCIA
1 = SEM GRAVIDADE	1 = NÃO TEM PRESSA	1 = NÃO VAI PIORAR
2 = POUCO GRAVE	2 = PODE ESPERAR UM POUCO	2 = VAI PIORAR EM LONGO PRAZO
3 = GRAVE	3 = O MAIS CEDO POSSÍVEL	3 = VAI PIORAR EM MÉDIO PRAZO
4 = MUITO GRAVE	4 = COM ALGUMA URGÊNCIA	4 = VAI PIORAR EM POUCO TEMPO
5 = EXTREMAMENTE GRAVE	5 = AÇÃO IMEDIATA	5 = VAI PIORAR RAPIDAMENTE

Problemas Potenciais O que precisa ser melhorado?	Gravidade	Urgência	Tendência	Prioridade
Problema 1	5	5	5	125
Problema 2	5	5	5	125
Problema 3	5	4	5	100
Problema 4	5	4	5	100
Problema 5	5	5	2	50
Problema 6	5	5	2	50
Problema 7	5	5	2	50
Problema 8	3	5	1	15
Problema 8	3	5	1	15
Problema 10	3	5	1	15

Exemplo de tabela preenchida

Problemas	Gravidade	Urgência	Tendência	TOTAL	Priorização
Atraso na entrega dos servidores	4	4	3	48	2
Parada no fornecimento do link de internet	3	2	1	6	4
Ataque de vírus na rede	5	5	5	125	1
Falta de nobreak no Data Center	5	2	3	30	3

- É de extrema importância que as pessoas envolvidas na criação da matriz entendam os problemas em detalhes, para que a matriz não seja feita subjetivamente.

- O ideal é que uma equipe faça a matriz, para haver discussão e evitar problemas.

- Com a matriz GUT podemos definir o que deve ser feito primeiro... Temos que lembrar que nem todos os problemas podem ser resolvidos de uma vez, ao mesmo tempo.

Exemplo de aplicação em um “estudo de caso”

- Meu automóvel, que atinge este mês a cerca dos 200.000 quilômetros rodados, tem-me deixado cada vez mais apreensivo. O para lama dianteiro está amassado e começa a apresentar alguma ferrugem. De minha parte, não tomei nenhuma atitude, embora o conserto não seja caro.
- As pastilhas de freio estão gastas e, como se sabe, nessas condições o freio pode representar um sério risco. Um descuido maior e, além de danificar o disco de freio, posso sofrer um acidente, tornando as coisas muito mais sérias.
- Olho para os pneus. Meu Deus, que milagre! Após rodarem pelo menos 90.000 quilômetros, estão quase um espelho de tão lisos.

- No interior do carro, o estofamento do meu banco, embora não custe caro, precisa ser recosturado. Cada vez que me sento, lá se vão mais alguns pontos de costura.

- Além da lâmpada do teto estar queimada, sinto uma vibração no velocímetro, causada pelo cabo que, em breve, deve romper-se.

- As lâmpadas de freio também não estão funcionando. Não tenho ideia clara se isto é importante, pois afinal nunca me dei conta se elas funcionavam ou não.

- Tenho sentido muita dificuldade de engatar algumas marchas com o carro frio e, isto, decididamente, não é normal.

- Para insatisfação total do meu bolso, o carburador está entupido, o que faz com que o consumo tenha aumentado assustadoramente, pois tenho de manter o motor em rotação elevada.

- Com pouco dinheiro de sobra, preciso tomar muito cuidado para só gastar naquilo que for muito importante. Acho que um GUT pode ajudar-me bastante na solução deste difícil problema!

GRAVIDADE	URGÊNCIA	TENDÊNCIA
1 = SEM GRAVIDADE	1 = NÃO TEM PRESSA	1 = NÃO VAI PIORAR
2 = POUCO GRAVE	2 = PODE ESPERAR UM POUCO	2 = VAI PIORAR EM LONGO PRAZO
3 = GRAVE	3 = O MAIS CEDO POSSÍVEL	3 = VAI PIORAR EM MÉDIO PRAZO
4 = MUITO GRAVE	4 = COM ALGUMA URGÊNCIA	4 = VAI PIORAR EM POUCO TEMPO
5 = EXTREMAMENTE GRAVE	5 = AÇÃO IMEDIATA	5 = VAI PIORAR RAPIDAMENTE

Problema	G	U	T	I	P
Para lama dianteiro amassado e apresentando alguma ferrugem	1	2	2	4	4
Pastilhas de freio estão gastas	5	5	5	125	1
Pneus carecas	5	5	5	125	1
Estofamento precisa ser costurado	1	1	3	3	5
Lâmpada do teto queimada	3	3	2	18	3
Vibração/cabo velocímetro	3	4	4	48	2
Lâmpadas de freio não estão funcionando	5	5	5	125	1
Dificuldade em engatar marchas	4	3	4	48	2
Carburador entupido	5	5	5	125	1

Exemplo de aplicação em um processo

GRAVIDADE	URGÊNCIA	TENDÊNCIA
1 = SEM GRAVIDADE	1 = NÃO TEM PRESSA	1 = NÃO VAI PIORAR
2 = POUCO GRAVE	2 = PODE ESPERAR UM POUCO	2 = VAI PIORAR EM LONGO PRAZO
3 = GRAVE	3 = O MAIS CEDO POSSÍVEL	3 = VAI PIORAR EM MÉDIO PRAZO
4 = MUITO GRAVE	4 = COM ALGUMA URGÊNCIA	4 = VAI PIORAR EM POUCO TEMPO
5 = EXTREMAMENTE GRAVE	5 = AÇÃO IMEDIATA	5 = VAI PIORAR RAPIDAMENTE

Processo: Cadastro de Clientes

Ativos	Vunerabilidade	Ameaça	Controle	G	U	T	Impacto
Computador	Energia elétrica	Queda de Energia	No-Break	3	5	5	75
	Travamento	Vírus	Anti- Virus	5	4	4	80
	Quebra	Mau uso	Equipamento Reserva	3	2	1	6
Servidor	Roubo de dados	Hackers	Firewall	3	5	4	60
	Energia elétrica	Queda de Energia	Gerador	3	3	4	36
	Arquivo Corrompido	HD com defeito	Backup	2	5	3	30
Link de Internet	Queda de conexão	Cabeamento	Fail Over	4	5	3	60
	Lentidão	Operadora	Suporte On Site	5	4	5	100
	Sobrecarga	Alta demanda	QoS	3	3	4	36

Análise SWOT

Análise SWOT

- Ferramenta de análise de riscos qualitativa.
- Avalia o cenário como um todo, de acordo com os seguintes aspectos:
  - **Strenghts (pontos fortes)**
  - **Weakness (pontos fracos)**
  - **Opportunities (oportunidades)**
  - **Threats (ameaças)**
- Também é trabalhada em forma de matriz.

- Strenghts (pontos fortes): o que o cenário tem de bom e que não precisa ser melhorado
- Weakness (pontos fracos): o que o cenário tem, mas não está bom, precisa ser melhorado
- Opportunities (oportunidades): oportunidades de crescimento e melhoria que o cenário apresenta
- Threats (ameaças): itens críticos do cenário

Pontos fortes	**Pontos fracos**
Oportunidades	**Ameaças**

Ajuda	*Atrapalha*
Forças	Fraquezas
Oportunidades	Ameaças

- **Exemplo**
  - Analisando o data center da empresa XPTO, temos os seguintes aspectos:

1. Sem controle de acesso
2. Cabeamento estruturado
3. Racks com espaço disponível
4. Servidores antigos
5. Nobreaks não testados
6. Sem rotina de backup
7. Sistema de detecção de incêndio
8. Espaço físico ocioso
9. Contrato de suporte para os servidores
10. Link de internet doméstico

Pontos fortes
2 – 7 – 9

Pontos fracos
4 – 5 – 10

Oportunidades
3 – 8

Ameaças
1 – 6

Plano de gerenciamento de risco

Plano de gerenciamento de risco

- Após a análise de risco devemos criar um plano de gerenciamento de risco usando os dados coletados, podemos “calcular o risco”.

- Crie uma estratégia que aprimore a infraestrutura de TI para mitigar as vulnerabilidades mais importantes para obter aprovação da gerência.

- Defina o processo de mitigação (medidas de segurança). Podemos incrementar a segurança da infraestrutura de TI mas não podemos eliminar todos os riscos. Quando um desastre ocorre, resolvemos o ocorrido, investigamos o que o causou e, tentamos prevenir que aconteça novamente ou que ao menos as consequências sejam menos severas.

Como “calcular o risco”

- Existem diversas formas de calcular o risco, tudo dependerá dos índices a serem utilizados. Um exemplo de fórmula que poderia ser utilizada seria fazer a seguinte equação matemática:
  - Risco = ((T.A X T.V X T.I)/M)
    - R = Risco
    - T.A = Total das Ameaças
    - T.V = Total das Vulnerabilidades
    - T.I = Total dos Impactos
    - M = Medidas de Proteção
  - Nesta fórmula ainda poderia ser acrescentada a variável P, onde P é a probabilidade de ocorrer o evento (vezes por ano)
    - Ficaria então: ((T.A X T.V X T.I)/M)*P

Medidas de Segurança

- Podem ser estabelecidas em função do parâmetro de tempo e necessidade, podendo ser de 4 tipos e sendo geralmente conhecidas como medidas PDCR.
  - **Preventivas:** ação de tentar evitar que o problema ocorra. Exemplo: antivírus.
  - **Detectivas:** ação de detectar um determinado problema. Exemplo: monitoramento ativo do antivírus.
  - **Corretivas:** ação de corrigir algo que as outras duas ações não conseguiram evitar. Exemplo: limpeza de um arquivo contamidado.
  - **Restauradoras:** recuperar algo perdido. Exemplo: restore de um arquivo danificado.

Outros itens importantes

- Revisão constante dos Riscos/Ameaças/Vulnerabilidade.

- Análise de custo/benefício.
  - É necessário trocar o equipamento.
  - É necessário reparar o equipamento.
  - É necessário recriar o ambiente.
  - É necessário recriar a informação (este é o mais complexo e o mais caro).

Possíveis erros na análise de risco

- Um escopo muito abrangente.
- Período de tempo da análise ou muito longo ou muito pequeno.
- Falta de comprometimento da alta administração.
- Basear-se exclusivamente na tecnologia.
- Basear-se exclusivamente nas pessoas.
- Falta de verbas para mitigação.
- Equipe diminuta.
- Não conhecimento total do negócio da empresa.

Ciclo PDCA

Ciclo PDCA

- O Ciclo PDCA é uma metodologia de gestão de quatro passos para **implantar melhorias em processos ou produtos**.

- Devido seu modelo intuitivo e fácil de aplicar, ele traz reais ganhos para as organizações, pois aumenta as chances de **sucesso na execução das tarefas**.

- Pode ser usado na implementação da segurança da informação.

Ciclo PDCA


Planejar
• Ações
• Responsáveis
Fazer
• Cronograma
• Guardar informações
Checar
• Medir resultados
• Acompanha-mento
Corrigir
• Repetir o ciclo
© PLANARE

Ciclo PDCA

- O conceito do ciclo PDCA fica fácil de entender quando olhamos para o significado da sua sigla em inglês:

  - **P** (*plan*, planejar)
  - **D** (*do*, fazer)
  - **C** (*check*, acompanhar)
  - **A** (*act*, corrigir)

- O que o ciclo PDCA sugere é que qualquer atividade de gestão ou planejamento estratégico executada na empresa, seja conduzida seguindo essas quatro fases. Vamos entender melhor cada uma.

P (plan, planejar) - Fase de planejamento

- Ao iniciar qualquer melhoria em processos ou produtos, **planejar as ações deve ser a primeira fase do processo**. Esta é a primeira fase do ciclo PDCA, representada pela letra “P”.

- Na fase de planejamento, algumas questões precisam estar muito claras, tanto para os gestores quanto para suas equipes:

  - Quais os objetivos deste projeto?
  - Quem são os responsáveis por cada tarefa?
  - Como serão realizadas as tarefas?
  - Qual o prazo de início e término de cada tarefa?

D (do, fazer) - Fase de execução

- Só depois de estar claro quem são os responsáveis, o que eles precisam fazer e como, é que se deve dar início a fase de **execução das ações,** representada pela letra “D” no ciclo PDCA.

- Esta é a fase onde todas as tarefas são realizadas. Cada membro da equipe já deve ter sido comunicado sobre suas responsabilidades e prazos de entrega de cada atividade. Suas responsabilidades são a realização das tarefas, **cumprindo as datas de entrega e atendendo o padrão de qualidade esperado.**

C (check, acompanhar) - Acompanhamento

- Esta pode ser considerada a fase mais importante do ciclo PDCA, e o que faz este modelo ser tão eficiente.

- Após a execução das ações que foram planejadas, os gestores devem se **reunir continuamente com suas equipes** para a validação de tudo que foi executado.

- Nesta fase, deverá ser feito uma **comparação entre o planejado e o realizado**. Esta comparação deverá validar se os prazos estão sendo cumpridos, se a qualidade está dentro do esperado e se houve algum desvio sobre o planejamento.

C (check, acompanhar) - Acompanhamento

- Note que **não é necessário aguardar o fim da execução de cada tarefa** para realizar esta validação. A frequência das reuniões de acompanhamento pode variar de acordo com cada projeto. Em algumas situações, pequenas reuniões diárias são sugeridas, em outros casos podem ser semanais ou até mensais.

- Quanto mais frequente for realizado o acompanhamento, **mais rápido poderá ser detectado qualquer desvio** sobre a finalização do projeto, facilitando assim as tomadas de decisão da próxima fase do ciclo PDCA.

A (act, corrigir)
Correção dos desvios e revisão das ações

- Ao fazer o acompanhamento próximo das tarefas, é comum a identificação de desvios sobre o que foi planejado. Da mesma forma, é natural a detecção de necessidades de melhorias sobre algumas ações.

- A última fase do ciclo PDCA trata justamente de ajustes no percurso. Durante o acompanhamento, pode ser necessário **retornar ao planejamento e rever alguns prazos**, alterar algumas ações ou incluir novas tarefas.

A (act, corrigir)
Correção dos desvios e revisão das ações

- O termo “Ciclo” é utilizado justamente porque o PDCA sugere esta **revisão constante de todas as fases**.
- Em um projeto com data de término, o PDCA só é finalizado junto com o projeto.
- Na gestão de uma empresa ou de uma equipe, sua utilização é contínua, pois novas atividades surgem diariamente.


Action (Agir)
Plan (Planejar)
1 Identificação do Problema
2 Análise do Fenômeno
3 Análise do Processo
4 Plano de Ação
5 Execução
6 Verificação
7 Ação
8 Padronização
A
P
C
D
Check (Verificar)
Do (Executar)