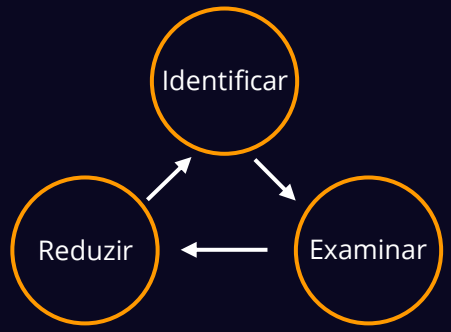
Prime

ISF – GERENCIAMENTO DE RISCOS

Gerenciamento de Riscos

É o processo de planejar, organizar, conduzir e controlar as atividades de uma organização visando minimizar os efeitos do risco sobre o capital e o lucro de uma organização.

Ciclo Contínuo:



A tarefa de monitorar esse processo é conduzida por um especialista em segurança da informação, tal como um Encarregado de Segurança da Informação (Information Security Officer – ISO) ou Chefe de Segurança da Informação (Chief Information Security Officer – CISO).

É todo processo de transformação de...

Quando uma ameaça surge, inicia o processo de análise de RISCO
Medidas de segurança devem ser tomadas.
Ex: Quando um novo vírus começa a circular e uma tempestade começa a se formar.

Quando uma ameaça se manifesta: torna-se um INCIDENTE
Ex: Hacker invadiu e houve uma falha de energia.

Objetivos e Propósito da **Análise de Riscos**

Objetivos

1. Identificar Ativos e seus Valores;
2. Determinar Vulnerabilidades e Ameaças;
3. Determinar o Risco das Ameaças se tornarem realidade e interromperem o Processo Operacional;
4. Estabelecer o equilíbrio entre os custos de um incidente e os custos de uma Medida de Segurança.

Tem o propósito de ser usado:

- ✓ Como ferramenta para Gerenciamento de Riscos;
- ✓ Como ferramenta para determinar quais ameaças são relevantes para os processos operacionais;
- ✓ Para identificar os riscos associados aos processos operacionais;
- ✓ Para garantir que as medidas de segurança sejam implantadas;
- ✓ Para evitar gastos desnecessários em medidas de segurança por falta de conhecimento de segurança;
- ✓ Para ajudar a conhecer os conceitos necessários de segurança;
- ✓ Para avaliar corretamente os riscos, incluindo os custo envolvidos em cada medida de segurança;
- ✓ Para ajudar no equilíbrio correto das medidas de segurança.

Análise de **Custo e Benefício**

- Parte do processo de Análise de Risco da Segurança da Informação

Questão:

- ✓ Um servidor custa $100,000.
- ✓ As Medidas da Segurança da Informação para esse servidor custam $150,000.
- ✓ Conclusão: as Medidas da Segurança da Informação são muito caras...
- ✓ Essa conclusão está Certa ou Errada?

Na Prática

- ? Com base na região onde você mora, cabe as casas ficarem com as portas e janelas trancadas?
- ? Existe ameaça de roubo ou arrombamento?
- ? A sua ou as casas da região são vulneráveis?
- ? Elas estão muito expostas ao risco? Elas chamam atenção?
- ? O risco é subjetivo ou objetivo?

Em um mapeamento das ameaças:

- Determine se há algo que possa ser feito para evitar a ameaça;
- Nem sempre os efeitos das medidas são claros:
  - ✓ Alarme na casa;
  - ✓ Seguro do patrimônio;
  - ✓ Senha trocada a cada 3 meses;
  - ✓ Backup diário.
- Infelizmente o benefício só é percebido quando temos problemas.

1. Identificamos o valor do ativo;
2. Identificamos o que é preciso proteger;
3. Analisamos as ameaças;
4. Analisamos as vulnerabilidades;
5. Avaliamos os riscos;
6. Aplicamos as medidas de proteção;
7. Monitoramos com os controles.

Ameaça

“A causa potencial de um incidente indesejado que pode resultar em danos a um sistema ou à organização.”

- Se algo resultar em dano, chamaremos de ameaça;
- Se o que temos é vulnerável, falho ou deficitário, abriremos brecha para o ataque;
- Aquele que aproveita a vulnerabilidade, é conhecido como agente ameaçador;

Um agente ameaçador pode ser:

- ✓ Um ladrão roubando seu patrimônio;
- ✓ Um invasor acessando a rede através de uma porta do firewall;
- ✓ Alguém acessando indevidamente os dados de terceiros;
- ✓ Um funcionário violando uma política de segurança;
- ✓ Ameaça de terrorismo e guerra a uma nação;
- ✓ Um tornado destruindo uma instalação;
- ✓ Um funcionário cometendo um erro não intencional expondo informações confidenciais.

As ameaças diferem em cada país dependendo do nível de desenvolvimento e do uso da internet.

No processo de Segurança da Informação:

- Ameaças (efeitos indesejáveis) são mapeadas na medida do possível;
- Verifica-se se algo pode ser feito para evitar essas ameaças;
- Determina-se quais medidas de segurança devem ser tomadas para evitar essas ameaças.

Ameaças **Humanas**

Tipos:

Ameaça intencional:

- Existem ameaças com os próprios funcionários:
  - ✓ Destroem informações após demissão;
  - ✓ Se vingam da empresa, vendendo ativos para a concorrência por não terem recebido um aumento.

A engenharia social:

- Faz uso de pessoas;
- Induzindo-as ao fornecimento voluntário de informações sensíveis;
- O engenheiro social se aproveita das fraquezas das pessoas para realizar seus objetivos;
- Encontram oportunidades no corredor da empresa, ao ligar para o Service Desk, no ônibus, etc.

Ameaça não-intencional:

- Acidentalmente pressionar a tecla "delete“;
- Inserir um pen drive com um vírus em uma máquina e espalhar o vírus por toda a rede.

Ameaças **Não-Humanas**

- Há também as ameaças não-humanas com influências externas, tais como:
  - ✓ Relâmpagos;
  - ✓ Incêndios;
  - ✓ Inundações;
  - ✓ Tempestades.
- Grande parte dos danos causados depende da localização do equipamento (por estarem vulneráveis):
  - ✓ Data Center localizado em local suscetível à vazamentos ou goteiras;
  - ✓ Localizado no subterrâneo, em uma área onde há água ou passível de inundação;
  - ✓ Salas que não têm janelas ou existem entradas e saídas de ar.
- Todas essas preocupações têm uma influência sobre os riscos que a organização irá enfrentar.
- Podemos subdividir as ameaças humanas e não-humanas em interrupções:
  - ✓ Na infraestrutura básica como equipamentos de informática, softwares ou banco de dados;
  - ✓ No ambiente físico, como edifícios, documentos físicos, instalações elétricas, abastecimento de água, aquecimento, ventilação e refrigeração.

Vulnerabilidade

Vulnerabilidade: Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

- ✓ Uma vulnerabilidade é uma fraqueza;
- ✓ É a ausência ou a fraqueza de uma proteção que pode ser explorada.

Exemplo:

- ✓ Uma porta ou janela que não tranca direito;
- ✓ Um servidor de desenvolvimento rodando sem atualização;
- ✓ Aplicações ou sistemas operacionais desatualizados;
- ✓ Acesso irrestrito para um modem;
- ✓ Uma porta aberta no firewall;
- ✓ Uma segurança física fraca que permita a qualquer pessoa entrar no Datacenter;
- ✓ Controle de senha fraco que permite o fácil acesso à sistemas e ambientes.

DOWNLOAD

Exposição

- Exposição é ficar exposto às perdas;
- Um agente ameaçador aproveita essa exposição;
- Uma vulnerabilidade expõe uma organização a possíveis ameaças;

Exemplo:

- ✓ Portas abertas no firewall;
- ✓ Protocolos habilitados sem necessidade, facilitando um Sniffer capturar o tráfego em tempo real;
- ✓ Se a gestão de senhas for fraca e as regras não forem aplicadas, a empresa fica exposta;
- ✓ Se uma empresa não tem seu cabeamento inspecionado e não estabelece medidas proativas de prevenção contra incêndios.

Risco

- Efeito da incerteza sobre os objetivos;
- Combinação da probabilidade de um evento e sua consequência:
  - ✓ Um efeito é um desvio do que é esperado;
  - ✓ Pode ser positivo e/ou negativo.
- Os objetivos podem ter diferentes aspectos, como:
  - ✓ Financeiro;
  - ✓ Saúde e segurança;
  - ✓ Segurança da informação;
  - ✓ Metas ambientais.
- Podem ser aplicados em diferentes níveis:
  - ✓ Estratégico;
  - ✓ Em toda a organização;
  - ✓ Projeto;
  - ✓ Produto;
  - ✓ Processo.

Outros Termos em **Relação aos Riscos**

Risco residual

- Risco que permanece após o tratamento do risco;
- O risco residual pode conter riscos não identificados;
- Também pode ser conhecido como “risco retido”.

Aceitação do risco

- A decisão de aceitar um risco.

Tratamento de riscos

- É o processo de seleção e implementação de medidas para modificar os riscos;
- O tratamento de riscos pode envolver:
  - ✓ Evitar o risco ao optar por não começar ou continuar com a atividade que dá origem ao risco;
  - ✓ Potencializar o risco a fim de perseguir uma oportunidade;
  - ✓ Remover a fonte de risco;
  - ✓ Alterar a probabilidade;
  - ✓ Alterar as consequências;
  - ✓ Dividir o risco com um terceiro ou terceiros (incluindo contratos e financiamento do risco);
  - ✓ Manter o risco através de uma escolha consciente;

- Lidam com consequências negativas referenciados como “mitigação de riscos”, “eliminação de riscos”, “prevenção de riscos” e “redução de riscos”;
- O tratamento de riscos pode criar novos riscos ou modificar riscos existentes.

Relação entre **Ameaça e Risco**

Exemplos de Riscos

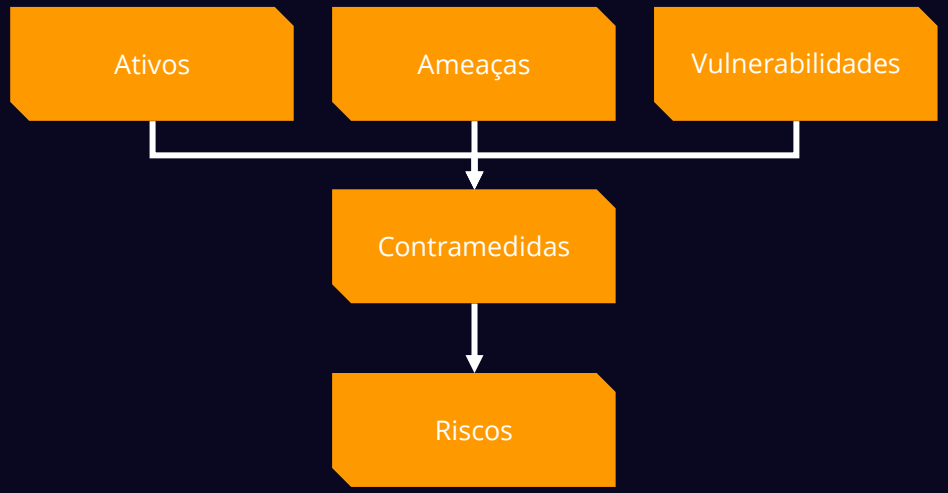
- Firewall com portas abertas;
- Usuários sem treinamento nos processos e procedimentos;
- Ataque ao site;
- Engenharia social com os funcionários da TI;
- Vulnerabilidade no SO do servidor;
- Um incêndio ou enchente;
- Um funcionário que não trabalha no RH obtendo acesso a informações sensíveis ou privadas;
- Sua empresa é atingida por uma falha de energia;
- Um hacker consegue obter acesso à rede wireless de TI da empresa;
- Vazamento de informação confidencial de uma equipe de call center;
- Manter a porta do Datacenter aberta;
- Falta de atualização de software aplicativos;
- Equipamento emprestado para um parente de funcionário.

E quanto a informação? Qual delas é valiosa na sua organização?

- ✓ Empregados (conhecimento e experiência);
- ✓ Produto ou serviço vendido;
- ✓ Dados pessoais de fornecedores, clientes e empregados;
- ✓ Processos internos;
- ✓ Manuais/procedimentos;
- ✓ Informações financeiras etc.

Ameaças, Riscos e Análise de Risco

- Você tem:
  - ✓ Um patrimônio valioso?
  - ✓ Uma vizinhança perigosa?
  - ✓ Uma casa com portas que não trancam direito?
- **Então você corre o risco de ser roubado!**



Quando uma Ameaça se materializa, surge um Risco para a organização.
Tanto a extensão do risco, quanto o gerenciamento de sua avaliação determinam se Medidas devem ser tomadas a fim de minimizar o Risco e o que ele pode se tornar.

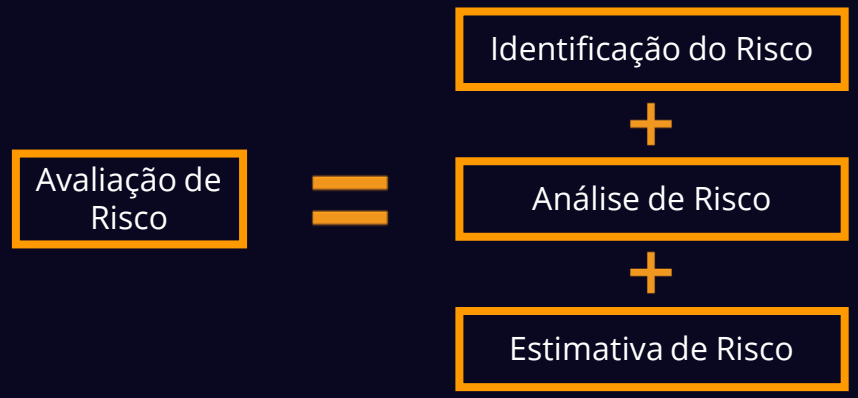
Sabendo disso, o que você vai fazer?

- ✓ Arrumar a fechadura da porta?
- ✓ Colocar um alarme?
- ✓ Fazer seguro?
- ✓ Aceitar o risco?

Contramedida ou Salvaguarda

- Uma contramedida, ou simplesmente medida de segurança, é posta em prática para mitigar o risco em potencial;
- Controle pode ser usado também como sinônimo para contramedida ou salvaguarda;
- Podendo ser:
  - ✓ Uma configuração de software;
  - ✓ Um dispositivo de hardware;
  - ✓ Um procedimento que elimine a vulnerabilidade;
  - ✓ Procedimento que reduza a probabilidade de um agente ameaçador ser capaz de explorar a vulnerabilidade.
- Exemplos de contramedidas incluem:
  - ✓ A gestão de senhas fortes;
  - ✓ Um guarda de segurança;
  - ✓ Mecanismos de controle de acesso em sistemas operacionais;
  - ✓ Implementação de senhas do basic input/output system (BIOS);
  - ✓ Treinamento de conscientização sobre segurança;
- Software antivírus atualizado.

Matemática da **Avaliação de Riscos**



- ✓ Uma das primeiras atividades da identificação dos controles de SI;

- Avaliação de Risco deve incluir:
  - ✓ Uma abordagem sistemática para estimar a magnitude dos Riscos (Análise de Risco);
  - ✓ Processo de comparar os riscos estimados em relação aos critérios de risco para determinar a significância dos Riscos (Estimativa de Risco).

Avaliação de Riscos

Identificação do risco

- É o processo de encontrar, reconhecer e descrever riscos;
- Envolve a identificação das suas fontes, eventos, causas e suas potenciais consequências;
- Pode envolver também os dados históricos, análise teórica, opiniões, pareceres fundamentados e de especialistas, e necessidades das partes interessadas.

Análise de riscos

- Um processo para compreender a natureza do risco;
- Tem a finalidade de determinar o nível de risco;
- Proporciona a base para a estimativa do risco;
- Base para as decisões sobre o tratamento do Risco;
- A análise de riscos inclui a estimativa do risco.

Estimativa do risco

- Atribuição de valores à probabilidade e consequências de um risco (quantitativa ou qualitativa);
- Atribuição de valores ao impacto que um risco pode ter e a probabilidade de sua ocorrência.

Avaliação de **Riscos na Prática**

Riscos identificados

- Foi identificado na avaliação de risco uma ameaça de ataque de pishing nos e-mails dos executivos.
- Foi identificado que uma nova lei exige a troca de dados bancários entre instituições financeiras.
- Foi estabelecido na diretriz na empresa que não é mais permitido manter documentos na impressora.

Riscos analisados e estimados:

- O pishing tem um grande impacto, mas baixa probabilidade, pois os executivos são cautelosos.
- A nova lei não é bem entendida pela empresa, e de impacto corporativo e estratégico.
- A nova diretriz foi criada devido cópias indevidas no passado, porém, com chances médias de ocorrer novamente.

Importante fator no avaliação destes riscos identificados:

- Teremos que pensar nos controles, como firewall, políticas, controle de acesso, antivírus etc.
- Será que o custo das medidas de controles são mais caros que os ativos que se quer proteger?
- Uma boa avaliação vai ajudar:
  - ✓ A responder essa questão;
  - ✓ Priorizar as ações;
  - ✓ Implementar os controles adequados para proteção.

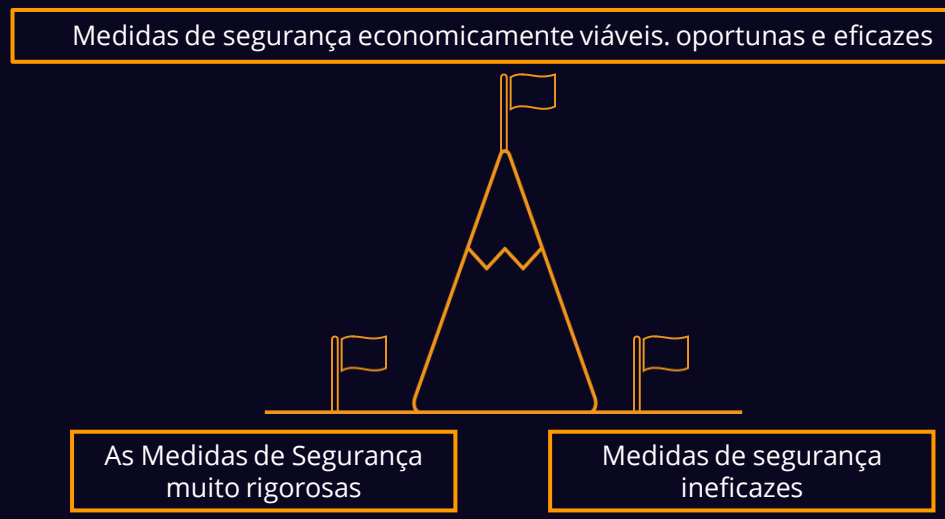
Processo de **Avaliação de Riscos**

- É uma das primeiras etapas do projeto para identificar os controles;
- Ela identifica, quantifica e prioriza os riscos segundo critérios de aceitação do risco;
- Esse processo pode ter que ser realizado inúmeras vezes para cobrir diferentes partes da organização ou sistemas de informação;
- Deve incluir a análise do risco e estimativa do risco;
- Devem ser analisadas periodicamente para tratar de mudanças nos requisitos de segurança e nas situações de risco, por exemplo, em ativos, ameaças, vulnerabilidades, impactos, etc.;
- Devem ser realizadas de maneira metódica, capaz de produzir resultados comparáveis e reproduzíveis;
- Deve ter um escopo claramente definido, para ser eficaz;
- Deve incluir as relações com as avaliações de risco de outras áreas, se for o caso.

Análise de Risco

A Avaliação de Riscos precisa da Análise de Risco, então a análise é:

- ✓ O processo que define e analisa os perigos;
- ✓ Que ajuda a adquirir uma visão/compreensão dos riscos que a organização está enfrentando e que precisa se proteger;
- ✓ Fornece a base para a avaliação de risco e para as decisões para lidar com o risco;
- ✓ Não esquecer que essa análise de risco vai incluir a estimativas de risco.
- ✓ Relatório de análise de riscos pode ser usado para alinhar os objetivos da tecnologia com os do negócio;
- ✓ Análise de riscos pode ser quantitativo ou qualitativo;
- ✓ Serve para trazer o seguinte equilíbrio:



Nota: os riscos possuem “donos” que também devem estar envolvidos na análise e avaliação de riscos.

Tipos de **Análises de Riscos**

Exemplos de casos:

- ✓ Uma corretora de seguros e os detalhes das apólices dos assegurados tornam-se públicos.
- ✓ Dados pessoais de testemunhas em um processo penal são divulgados.
- ✓ Um funcionário perdeu um pendrive e o seu conteúdo cai nas mãos da imprensa que automaticamente é feito a publicação do assunto.

Que tipo de análise poderíamos fazer com estes 3 exemplos?

- ✓ Qual o impacto?
- ✓ Qual a chance de acontecer?
- ✓ Qual a consequência?

Análise Quantitativa de Risco:

- ✓ Objetivo de calcular um Valor do Risco com base no nível do prejuízo financeiro e na probabilidade de que uma Ameaça possa se tornar um Incidente de Segurança da Informação;

Análise Qualitativa de Risco:

- ✓ Baseia-se em cenários e situações e as chances de uma Ameaça se tornar realidade são analisadas com base em intuições.

Tipo de Análise de Riscos: **Quantitativo**

- ✓ **Baseados no impacto;**
- ✓ **Baseado na perda financeira;**
- ✓ **Baseado na probabilidade da ameaça tornar-se um incidente.**

- Neste tipo de análise, consideremos o valor de cada elemento compostos pelo custo:
  - ✓ Das medidas de segurança;
  - ✓ Bem como os ativos, como edifícios, hardware, software, informações e impacto dos negócios.
- É fornecida uma imagem clara do risco financeiro total;
- As medidas adequadas podem então ser determinadas;
- Uma parte importante disso é determinar quais riscos residuais são aceitáveis;
- Os custos das medidas não devem exceder o valor do objeto protegido e do risco;
- Uma análise de riscos puramente quantitativa é praticamente impossível;
- Uma análise quantitativa de risco tenta atribuir valores a todos os aspectos, mas isso nem sempre é possível;

- Pode ser atribuído um valor a um servidor com defeito: por exemplo, o valor de compra e depreciação, o valor do software, salários etc. Agora tente dar um valor ao dano causado a uma empresa;
- Pode ser possível determinar em algumas ocasiões, mas nem sempre.

Tipo de Análise de Riscos: **Qualitativo**

✓ Baseado nos cenários;
✓ Baseado nas situações;
✓ Baseado nos sentimentos.

- Números e valores monetários não são atribuídos a componentes e perdas;
- Pode ser definido, por exemplo, como baixo, médio e alto, ou, provável, certo, possível, raro e improvável, etc.;
- Utilizam bom senso, melhores práticas, intuição e experiência;
- Exemplos de técnicas qualitativas são Delphi, brainstorming, esboços sequenciais (storyboarding), grupos de discussão, pesquisas, questionários, listas de verificação, reuniões entre duas pessoas e entrevistas;
- A equipe de análise de riscos considera a cultura da empresa e os indivíduos envolvidos na análise;
- É reunido pessoal com experiência e conhecimento das ameaças sob avaliação;
- A este grupo é apresentado um cenário que descreve as ameaças e as potenciais perdas, e cada membro então responde com sua intuição e experiência sobre a probabilidade da ameaça e a extensão do dano que pode resultar.

- As análises quantitativa e qualitativa do risco têm, cada uma, suas vantagens e desvantagens.
- A administração, em consulta com especialistas, determina qual método deve ser aplicado em cada situação particular.

OBRIGADO

ISF – GERENCIAMENTO
DE RISCOS