Instituto Infnet

Segurança da Informação

FABIANO GISBERT

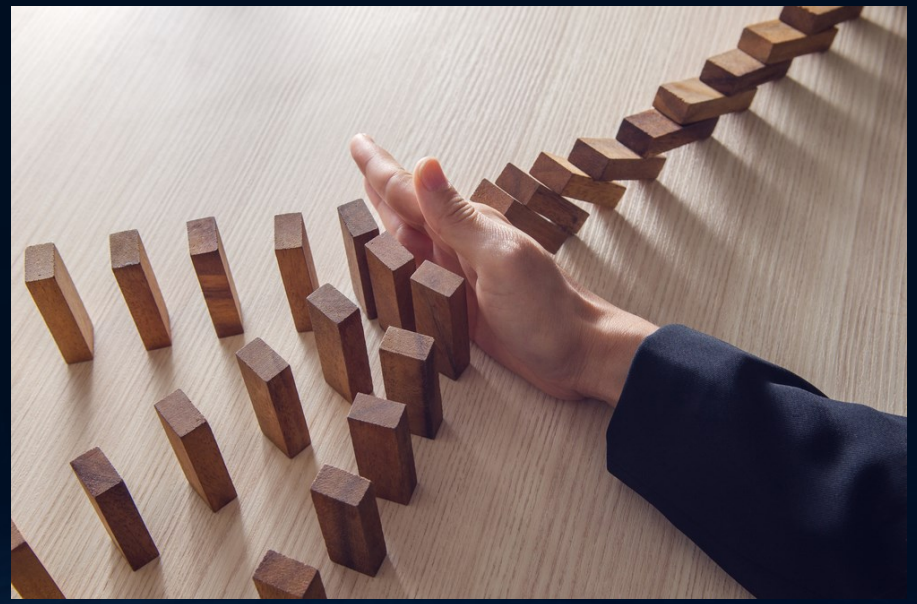
ETAPA 03

Gestão de Riscos

Instituto Infnet

Definição

Gestão de risco é o conjunto de atividades coordenadas que têm o objetivo de gerenciar e controlar uma organização em relação a potenciais ameaças, seja qual for a sua manifestação. Isso implica no planejamento e uso dos recursos humanos e materiais para minimizar os riscos ou, então, tratá-los.



Gestão de Riscos

Instituto Infnet

Risco à Segurança da Informação

Um risco é a iminência de um incidente de segurança quando uma ameaça explora uma vulnerabilidade em um ativo

Gestão de Riscos

Instituto Infnet

Vulnerabilidade

Pode ser visto como uma fraqueza, uma falha, ou falta de um elemento ou controle de um determinado ativo de uma empresa, que pode ser explorado por uma ou mais ameaças.

- Uma tecnologia que nunca recebeu configurações e correções para aumentar sua segurança;
- Um computador que não tiver um antivírus atualizado;
- Um sistema de autenticação que permite que o usuário tenha senhas fracas;
- Base de dados sem cópias de segurança, como backup ou replicação remota;
- Uma rede conectada à internet que não tem um equipamento de proteção, como um firewall

Gestão de Riscos

Instituto Infnet

Ameaça

Compreendida como um agente que tem o potencial de causar um incidente de segurança. Elas estão diretamente ligadas à vulnerabilidade, e quando são exploradas tornam-se um risco iminente ao ativo alvo

- Uma pessoa má intencionada que deseja obter informações privilegiadas é uma ameaça. Quando consegue obter um acesso não autorizado a uma base de dados através de uma vulnerabilidade explorada no sistema, essa pessoa torna-se um risco à confidencialidade da informação.
- Um software não licenciado que pode conter vírus ou algum código malicioso também pode ser considerado como uma ameaça.
- Um e-mail de fonte não conhecida, mas que contém um anexo que desperta algum interesse no destinatário.
- Um funcionário insatisfeito com as rotinas e diretrizes de trabalho e que detém conhecimentos que podem ferir a confidencialidade ou segurança da empresa é uma ameaça em potencial, que merece muita atenção.

Gestão de Riscos

Instituto Infnet

Ativo

Um ativo é qualquer item (tangível ou não) que faz parte de uma infraestrutura de redes de computadores ou do ambiente onde será implantada a segurança da Informação

- Cabeamento estruturado
- Link de Internet
- Sistema Operacional
- Servidores
- Papéis confidenciais
- Pen Drive ou HD externo
- Aplicação
- Quadro de avisos

Gestão de Riscos

Instituto Infnet

Objetivo

Basicamente espera-se as seguintes ações num plano de gestão de riscos:

- conhecer os riscos associados à organização;
- estabelecer um conjunto equilibrado de requisitos de segurança em
- conformidade com os riscos identificados;
- transformar os requisitos de segurança em procedimentos a serem adotados em
- toda a organização;
- estabelecer laços de confiança na correção e efetividade dos mecanismos de
- segurança adotados;
- garantir que os riscos residuais mantenham-se em níveis toleráveis;
- integrar os esforços de todas as áreas da organização na busca por uma visão
- combinada sobre a confiança no sistema.

Gestão de Riscos

Instituto Infnet

Gestão de Riscos

Análise de Riscos

A análise de riscos é responsável, em um primeiro momento, pela identificação de bens, infraestrutura existente, ameaças, vulnerabilidades e controles, enfocando tanto questões tecnológicas como organizacionais.

Analisar essas informações, avaliar o impacto de determinadas ameaças e qualificar os riscos, de acordo com seu grau de impacto.

Por fim, propor soluções para a redução dos riscos levantados, alterações nas políticas de segurança e necessidades de treinamento de pessoal encerram essa etapa.

Gestão de Riscos

Instituto Infnet

Tratamento de Riscos

Tratar riscos significa concluir o processo de análise, implementando a solução que apresenta a melhor relação custo/benefício dos mecanismos a serem utilizados e priorizar as ações necessárias, para o tratamento adequado do risco.

Nesta etapa, deve-se efetivamente implementar soluções que reduzam os riscos apontados na fase anterior, determinando prazos, responsabilidades, configurações, etc.

Gestão de Riscos

Gerência e Manutenção dos Riscos

o objetivo principal é garantir a continuidade do processo. Monitorar a eficiência dos mecanismos empregados e a possível inserção de novos riscos, controlar mudanças na infraestrutura e de pessoal e disparar um novo ciclo no processo de gerência de riscos são funções importantes dessa fase.

Análise de Riscos

Objetivo

O principal objetivo da análise de riscos, etapa fundamental para que estratégias adequadas sejam traçadas e para que os mecanismos corretos sejam selecionados e implementados, é levar em consideração tanto questões organizacionais quanto tecnológicas para avaliar corretamente quais são esses bens, os riscos atrelados a eles e a melhor forma de protegê-los.

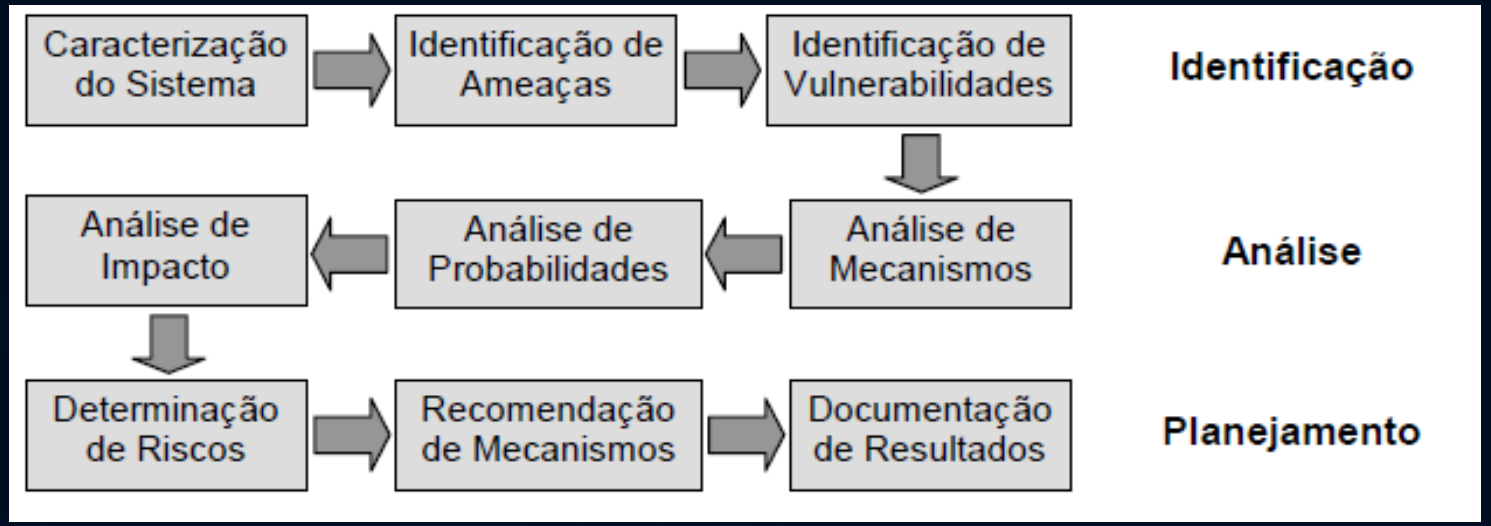
Análise de Riscos

Fases

O modelo utilizado pela NIST , divide a análise de riscos em três fases:

- Identificação;
- Análise;
- Planejamento.

Cada uma dessas fases pode, ainda, ser subdividida em vários passos, auxiliando na sistematização e execução da análise.



Análise de Riscos

Instituto Infnet

Identificação

O primeiro passo da análise de risco visa caracterizar o sistema e, com isso, definir o escopo do trabalho. O objetivo principal é levantar tanto informações técnicas quanto organizacionais, definindo as fronteiras e funções dos diferentes sistemas, a infraestrutura tecnológica já existente e os principais bens da organização.

Exemplo de dados levantados nessa etapa:

- requisitos funcionais do sistema;
- usuários do sistema;
- políticas de segurança existentes, sejam elas formais ou informais;
- mecanismos de segurança já implementados;
- topologia de rede atual;
- fluxo de informação no sistema;
- controles técnicos (mecanismos), de gerência (regras)

Análise de Riscos

Instituto Infnet

Identificação

O próximo passo é a identificação das ameaças ao sistema. Espera-se que nesta etapa seja gerada uma lista com as ameaças aos principais bens da organização, útil na definição dos riscos e no levantamento das vulnerabilidades existentes.

Vulnerabilidade	Agente	Ameaça
Contas de antigos funcionários não foram removidas do sistema	Antigos funcionários	Usar os serviços de acesso discado da empresa para obter dados internos
Firewall da empresa permite telnet externo e existe uma conta guest no servidor XYZ	Usuários não autorizados (e.g. hackers, antigos funcionários, concorrentes)	Conectar, via telnet, no servidor XYZ e navegar no sitema de arquivos através da conta guest
Vendedor identificou problemas de segurança em seu sistema; entretanto, novas correções (patches) não foram aplicados ao sistema	Usuários não autorizados (e.g. hackers, antigos funcionários, concorrentes)	Obter acesso não autorizado a arquivos críticos do sistema, através das vulnerabilidades conhecidas

Análise de Riscos

Instituto Infnet

Identificação

O passo seguinte é analisar os mecanismos e controles de segurança já implementados ou planejados pela organização como firewalls, IDSs, VPN's e verificadores de integridade, para minimizar os riscos de uma infraestrutura, seja através da prevenção, detecção ou reação a possíveis incidentes, e devem ser analisados para a determinação de sua real eficácia no sistema em questão.

Análise de Riscos

Instituto Infnet

Probabilidade do Risco

De posse das informações já coletadas, o objetivo agora é determinar qual a probabilidade de que uma potencial vulnerabilidade seja explorada, sempre levando em conta o par ameaça/vulnerabilidade e os mecanismos já existentes.

Pela dificuldade de uma análise completamente quantitativa, o quadro abaixo exemplifica uma classificação qualitativa bem simples que poderia ser usada:

Probabilidade	Definição
Alto	O agente da ameaça é altamente motivado e suficientemente capaz e os mecanismos para prevenir a exploração das vulnerabilidades existentes são ineficazes
Médio	O agente da ameaça é motivado e capaz, mas os mecanismos existentes podem impedir a exploração das vulnerabilidades do sistema
Baixo	O agente da ameaça não é motivado e suficientemente capaz, ou os mecanismos para prevenir a exploração das vulnerabilidades são eficazes

Análise de Riscos

Instituto Infnet

Impacto do Risco

Complementando a fase de análise, é necessário que seja feito um estudo sobre o impacto que cada par ameaça/vulnerabilidade pode causar nos bens do sistema, um dos principais passos na análise de riscos.

Os critérios usados para a análise de impacto estarão sempre baseados nos pilares da segurança: confidencialidade, integridade, autenticidade e disponibilidade.

Impacto	Definição
Alto	A exploração da vulnerabilidade pode: (1) resultar em altas perdas financeiras; (2) violar significantemente bens intangíveis; (3) resultar em perdas humanas ou em sérios danos;
Médio	A exploração da vulnerabilidade pode: (1) resultar em perdas financeiras; (2) violar bens intangíveis; (3) resultar em sérios danos;
Baixo	A exploração da vulnerabilidade pode: (1) resultar na perda de algum bem convencional; (2) afetar bens intangíveis;

Análise de Riscos

Instituto Infnet

Matriz de Riscos

A Matriz dos riscos, por sua vez, é a conjunção de todos os passos já realizados, representando o centro de toda a análise de riscos. O termo **risco** representa a probabilidade de que uma ameaça se manifeste, através da exploração de uma vulnerabilidade, aliado ao impacto causado por esse incidente

Análise de Riscos

Instituto Infnet

Matriz de Riscos

A interpretação dos níveis de risco obtidos em cada par ameaça/vulnerabilidade deve ser feita com base na necessidade de adoção de medidas corretivas. Em casos onde o nível obtido foi alto, é fundamental que sejam tomadas medidas imediatas, sem as quais não é recomendável que o sistema continuem operando. Quando a avaliação apontar para um nível de risco médio, ações e planos corretivos são necessários em um período de tempo razoável, durante o qual o sistema pode continuar em operação. Já os níveis de risco baixos, medidas corretivas podem ser adotadas ou pode-se optar por aceitar esses riscos.

Probabilidade de Ameaça	Impacto		
	Baixo (10)	**Médio** (50)	**Alto** (100)
Alto (1,0)	**Baixo** 10 x 1,0 = 10	**Médio** 50 x 1,0 = 50	**Alto** 100 x 1,0 = 100
Médio (0,5)	**Baixo** 10 x 0,5 = 5	**Médio** 50 x 0,5 = 25	**Médio** 100 x 0,5 = 50
Baixo (0,1)	**Baixo** 10 x 0,1 = 1	**Baixo** 50 x 0,1 = 5	**Baixo** 100 x 0,1 = 10

Tratamento dos Riscos

Instituto Infnet

Objetivo

Representa o planejamento das medidas a serem tomadas, na forma de recomendações de mecanismos, e a documentação dos resultados obtidos ao final de todos os passos. O objetivo maior é reduzir os riscos avaliados a níveis aceitáveis, propondo mecanismos e práticas de segurança. Isso servirá de entrada para a etapa de seleção e implementação de mecanismos, quando planos mais detalhados serão traçados.

Tratamento dos Riscos

Níveis de Tratamento

1.Mitigá-lo - através da aplicação de controles específicos;

2. Transferi-lo - através de atividades como um seguro;

3. Aceitá-lo - simplesmente tomando o conhecimento mas sem adoção de medidas de controle;

4. Evitá-lo - executando outra atividade, tomando outro caminho, não utilizando o item.

Tratamento dos Riscos

Níveis de Tratamento

1.Mitigá-lo - através da aplicação de controles específicos;

2. Transferi-lo - através de atividades como um seguro;

3. Aceitá-lo - simplesmente tomando o conhecimento mas sem adoção de medidas de controle;

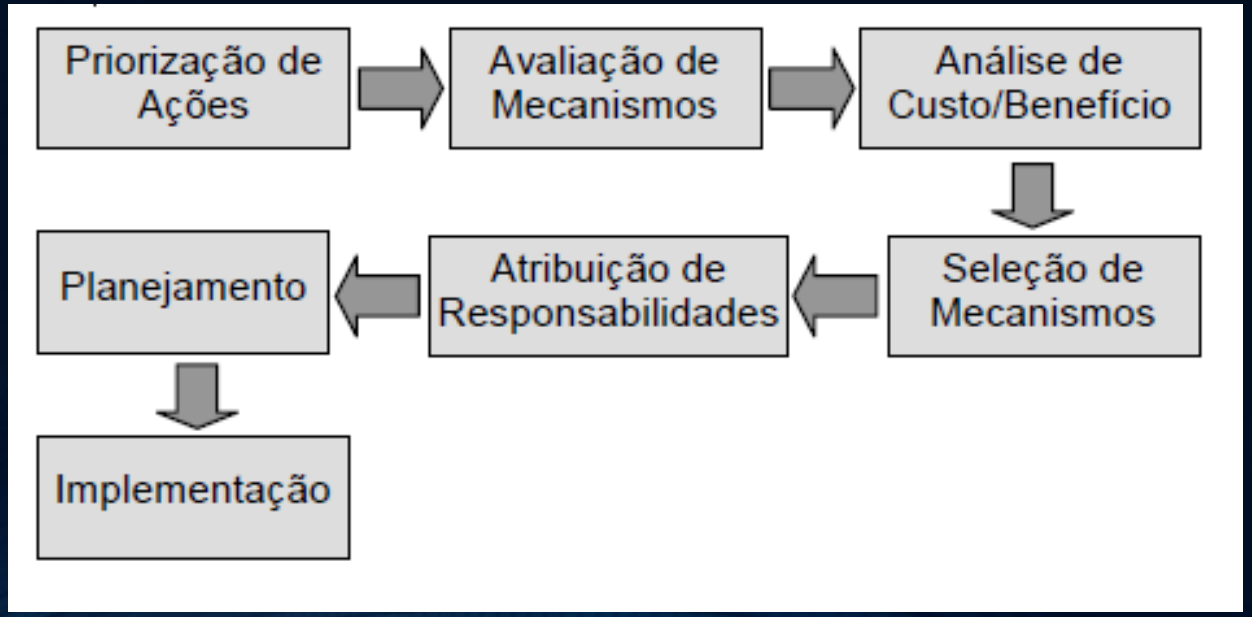
4. Evitá-lo - executando outra atividade, tomando outro caminho, não utilizando o item.

Tratamento dos Riscos

Instituto Infnet

Fases do Tratamento

A exemplo da etapa de análise, o processo de minimização de riscos possui alguns passos característicos, descritos pelo NIST:

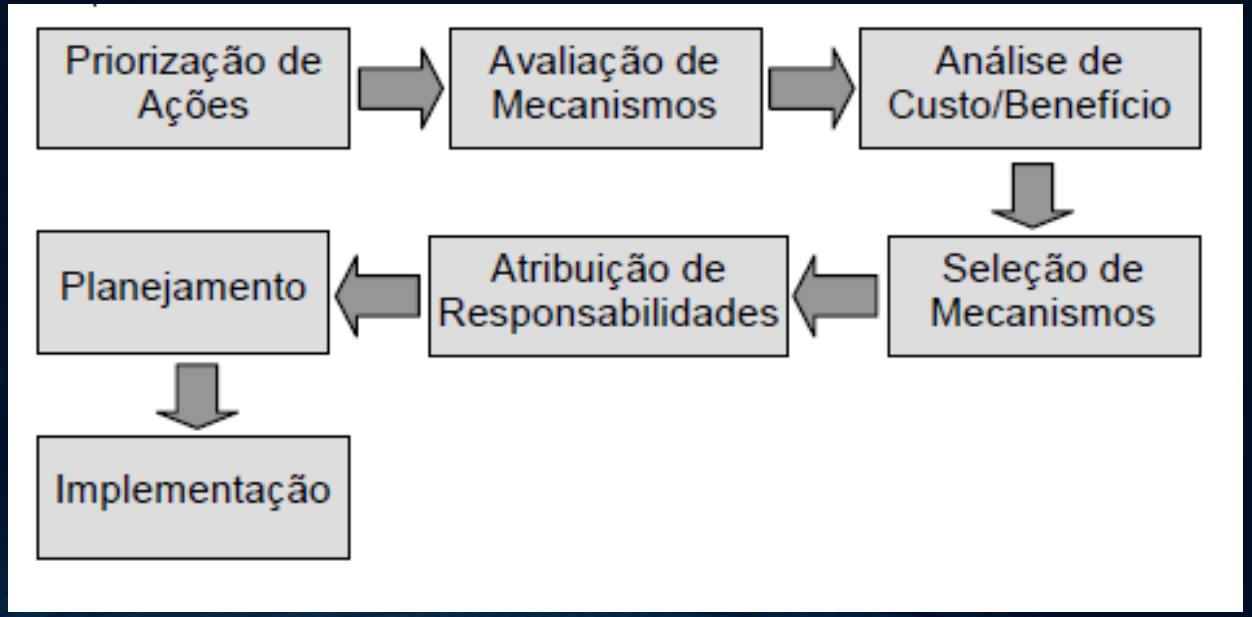


Tratamento dos Riscos

Instituto Infnet

Fases do Tratamento

A exemplo da etapa de análise, o processo de minimização de riscos possui alguns passos característicos, descritos pelo NIST:



Tratamento dos Riscos

Instituto Infnet

Fases do Tratamento

Priorização: as ações são classificadas por ordem de importância, para que as medidas mais urgentes sejam tomadas com certa prioridade

Avaliação dos Mecanismos: reavaliar os mecanismos sugeridos na análise de riscos, tendo em vista questões como aplicabilidade, compatibilidade, aceitação pelos usuários e facilidade de manutenção, entre outros critérios

Análise Custo/Benefício: refina a seleção dos mecanismos e adequando os gastos com as vantagens obtidas.

Seleção dos Mecanismos: determina os mecanismos e as práticas mais adequadas e vantajosas para a redução dos riscos da organização.

Tratamento dos Riscos

Instituto Infnet

Fases do Tratamento

Atribuição de Responsabilidades: a atribuição das responsabilidades de implementação deve ser expressa por uma lista dos responsáveis pela implementação de cada mecanismo indicado.

Planejamento: planejar o processo de implementação propriamente dito, priorizando as ações mais relevantes e determinando prazos de execução.

Implementação: execução dos planos traçados resulta na implementação de todos os mecanismos selecionados e, consequentemente, na redução dos riscos existentes.

Gerência e Manutenção dos Riscos

Objetivo

O objetivo principal desta etapa é garantir a continuidade do processo de gestão de segurança, monitorando a eficiência dos mecanismos empregados e a possível inserção de novos riscos, controlando mudanças de infraestrutura e de pessoal e, principalmente, disparando um novo ciclo no processo de gerência.

Além disso, planos de contingência e práticas tradicionais de manutenção são tarefas também importantes nesta etapa.

FIM DA ETAPA 03