Treinamento
ISO/IEC ® 27002:2013 Foundation

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 1

Boas Vindas

ISO/IEC ® 27002:2013 Foundation

Nível
Foundation

Prof. Adriano Martins

www.pmgacademy.com

Clique Aqui para Iniciar

Maior Aproveitamento

- ✓ Assistir no mínimo 2 vezes o Treinamento
- ✓ Realizar os Exercícios no final de cada módulo
- ✓ Breve leitura dos Termos no Glossário
- ✓ Executar todos os Simulados

! Dica para Questões e Simulados:
Corrigir as questões que estão erradas e **PRINCIPALMENTE** as **CORRETAS**

Programação

Módulo 1	▪ Introdução
Módulo 2	▪ Informação, Objetivos de Negócios e Requisitos de Qualidade
Módulo 3	▪ Riscos e Ameaças
Módulo 4	▪ Ativos de Negócio e Incidentes de Segurança da Informação
Módulo 5	▪ Medidas Físicas
Módulo 6	▪ Medidas Técnicas (Segurança de TI)
Módulo 7	▪ Medidas Organizacionais
Módulo 8	▪ Legislação e Regulamentos
Módulo 9	▪ Simulados

Sobre o EXIN

www.exin-exams.com

Esquema de Qualificação ISO/IEC 27002:2013

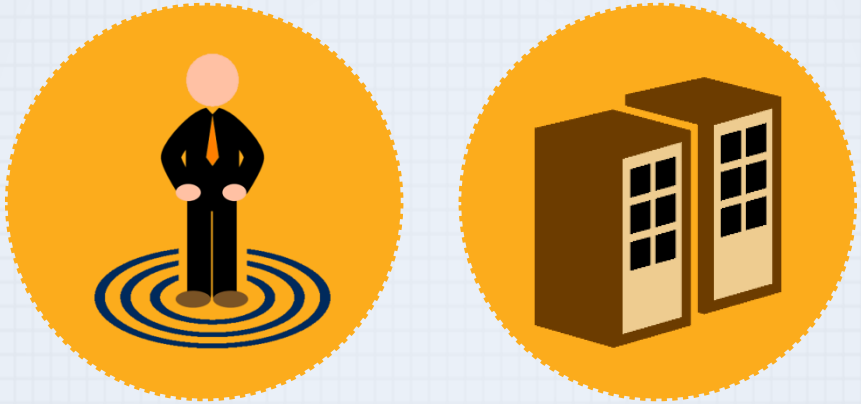
Propósito do Curso

Globalização

TI: Ativo valioso

Informação confiável

Público Alvo



Qualquer pessoa na organização que manuseia informações. É também aplicável a proprietários de pequenas empresas a quem alguns conceitos básicos de Segurança da Informação são necessários. Este módulo pode ser um excelente ponto de partida para novos profissionais de segurança da informação.

Pré-Requisitos

Detalhes do Exame

Pré requisitos:

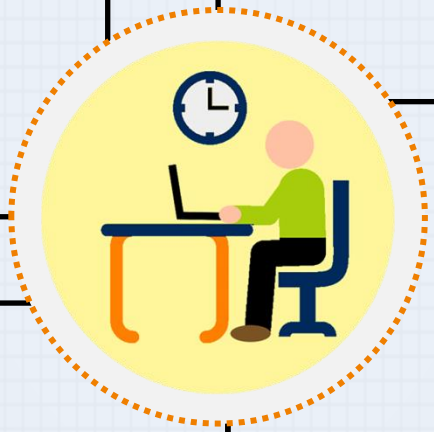
Nenhum

Tipo de exame:

Múltipla escolha em computador ou impresso em papel

Equipamentos eletrônicos permitidos:

não



Com consulta:

não

Tempo destinado ao exame:

60 minutos

Mínimo para aprovação:

65 % (26 de 40)

Número de questões:

40

Módulo 1

Formato do Exame

Conteúdo

10% - Segurança da Informação

- 2,5% - O conceito de Informação
- 2,5% - Valor da Informação
- 5% - Aspectos de Confiabilidade

30% - Ameaças e Riscos

- 15% - Ameaças e Riscos
- 15% - O Relacionamento entre Ameaças, Riscos e Confiabilidade da Informação

10% - Abordagem e Organização

- 2,5% - Política de Segurança e Segurança da Organização
- 2,5% - Componentes da Segurança da Organização
- 5% - Gerenciamento de Incidentes

40% - Medidas

- 10% - Importância das Medidas
- 10% - Medidas de Seguranças Físicas
- 10% - Medidas de Segurança Técnica
- 10% - Medidas Organizacionais

10% - Legislação e Regulamentações

Visão Geral

Medidas

- Físicas
- Técnicas
- Organizacionais

Introdução à Segurança da Informação

A segurança da informação é a disciplina que concentra na qualidade (confiabilidade)

Tríade

Disponibilidade, Confidencialidade e Integridade

Truque para execução da segurança da informação:

- Os requisitos de qualidade que uma organização pode ter para a informação;
- Os riscos para estes requisitos de qualidade;
- As medidas que são necessárias para minimizar esses riscos;
- Assegurar a continuidade da organização no caso de um desastre

Pronto para o próximo?

Clique acima em
“Sair da Atividade”

Treinamento de ITSM baseada na ISO/IEC ® 27002 Foundation

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 2

Informação, Objetivos de Negócio e Requisitos de Qualidade

O que veremos neste módulo?

- Forma, Valor e Fator do Sistema de Informação
- Tríade: Disponibilidade, Integridade e Confiabilidade
- Arquitetura e Análise da Informação
- Gestão da Informação

Introdução

S.I. diz respeito à Garantia de Proteção aos Dados

Dados ≠ Informações

"... Ação de informar ou informar-se. / Notícia recebida ou comunicada; informe. / Espécie de investigação a que se precede para verificar um fato ..."

Formas

Imagens de vídeo

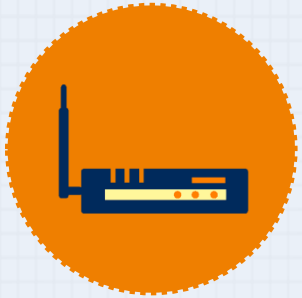
Textos de documentos

Palavras faladas

Sistema da Informação

Combinação de meios, procedimentos, regras e pessoas que asseguram o fornecimento de informações para um processo operacional

Estação de Trabalho



Cabos e wireless

Servidores

Armazenamento

Telefone

Exemplo

Telefone móvel é seguro?

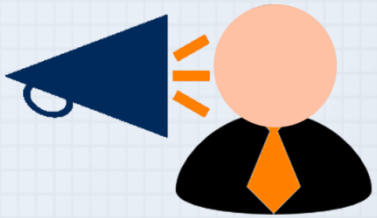
Valor da Informação

Sem significado → **Dados**

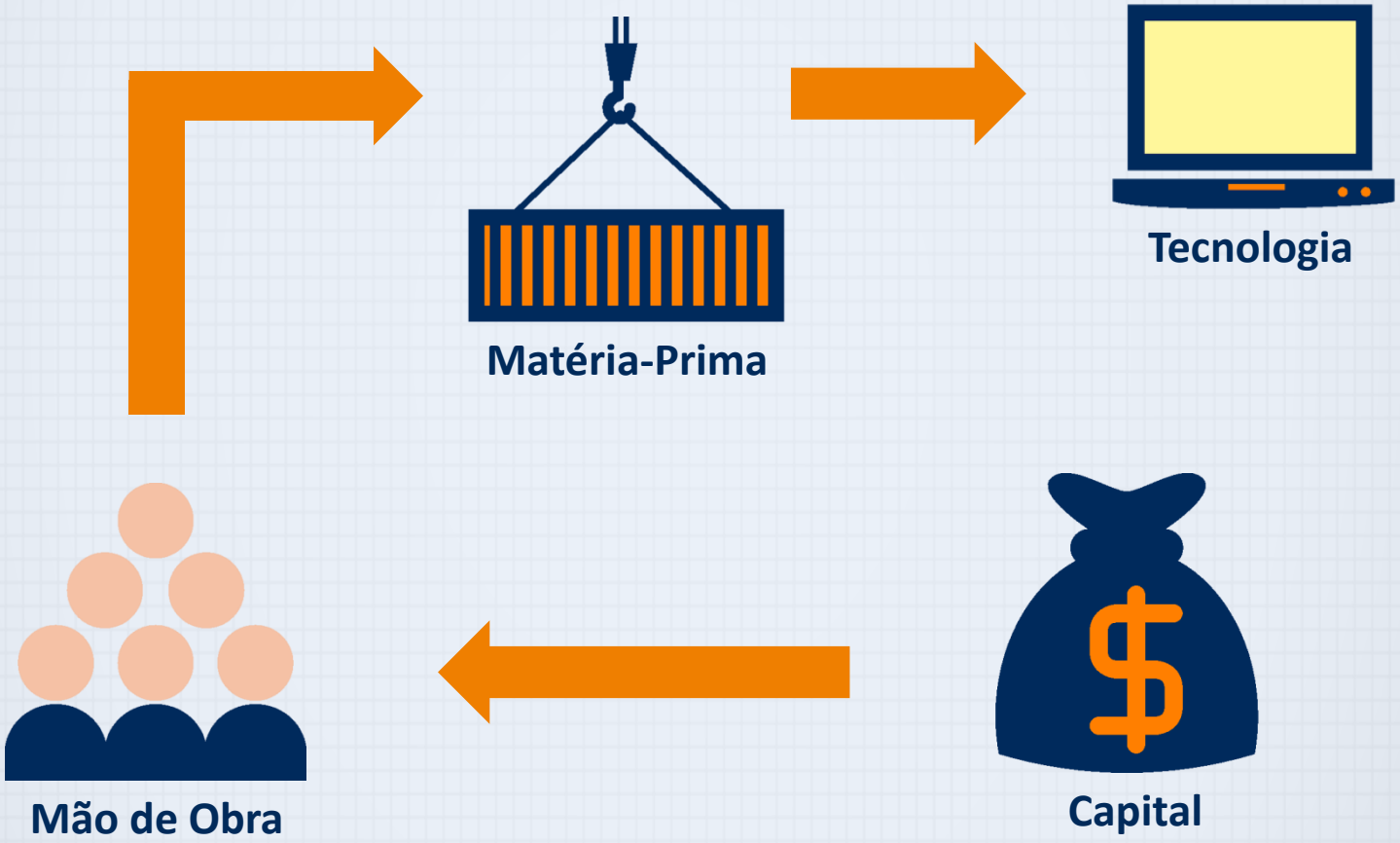
Com significado → **Informações**

Dados ou informações?

Quem define o valor é o destinatário



Informação como fator de produção

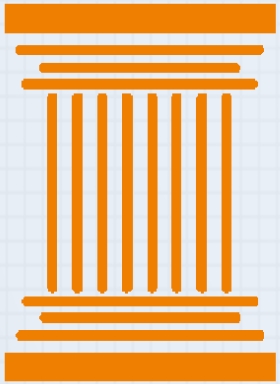


Disponibilidade, Integridade e Confiabilidade

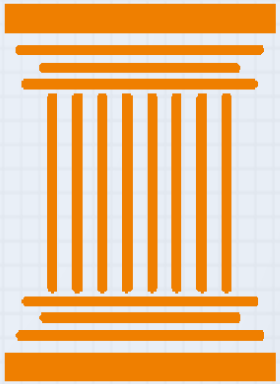
A recuperação da informação.

A indispensabilidade das informações dentro dos processos operacionais;

A importância da informação para os processos operacionais;



Pilares para uma análise de riscos, com base no CIA



Disponibilidade

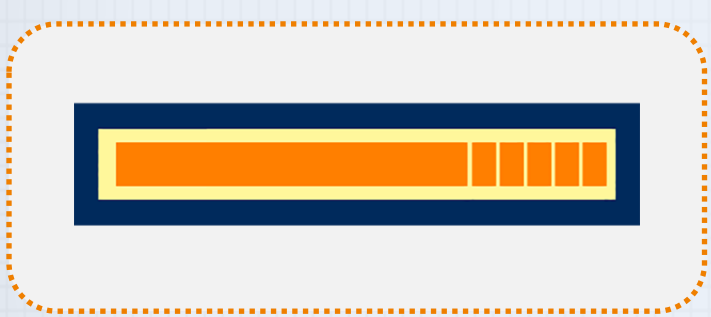
Pontualidade. Os sistemas de informação estão disponíveis quando necessários;

Continuidade. O pessoal pode continuar a trabalhar no caso de um fracasso ou indisponibilidade;

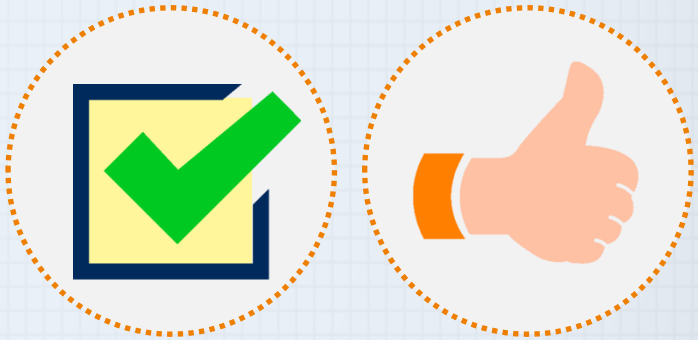
Robustez. Há capacidade suficiente para permitir que todos os funcionários trabalhem nos sistemas de informação.

Integridade

"...o grau em que a informação está atualizada e sem erros..."



Informação atualizada



Informação sem erros

Exemplo

Confidencialidade

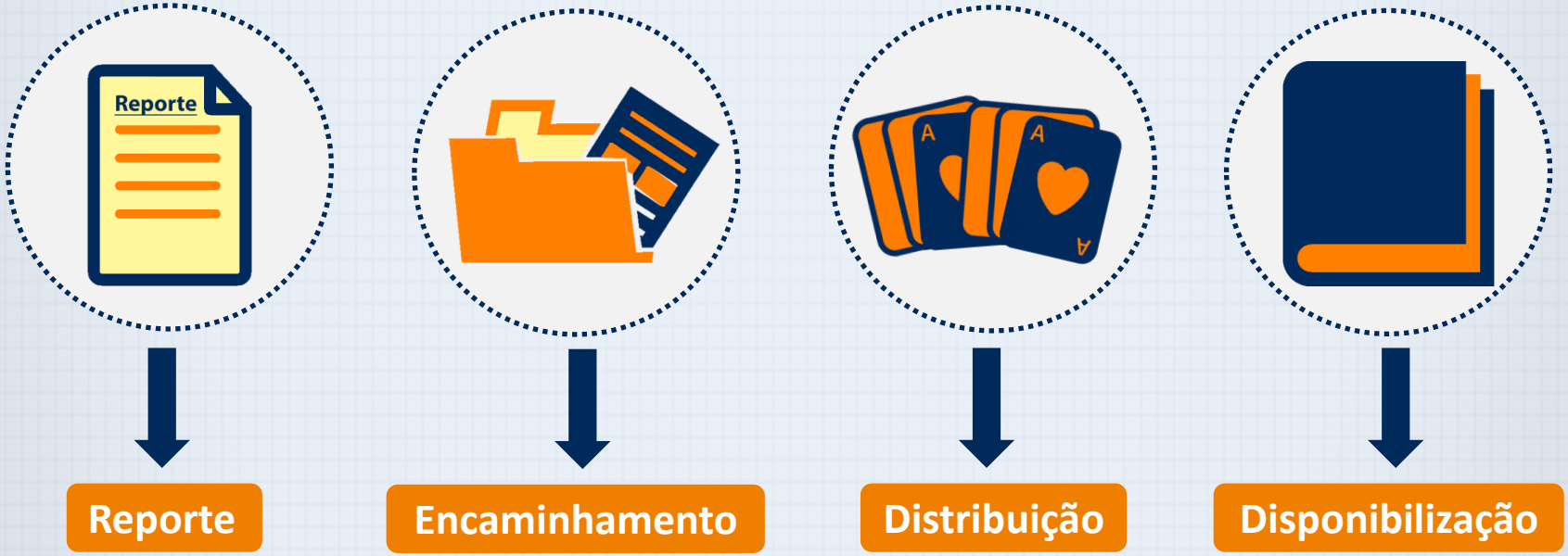
"...é o grau em que o acesso à informação é restrito a um grupo definido de pessoas autorizadas..."

Restrição de acesso

Privacidade

Arquitetura da Informação

"... processo que demonstra como será feita a prestação de informação ..."

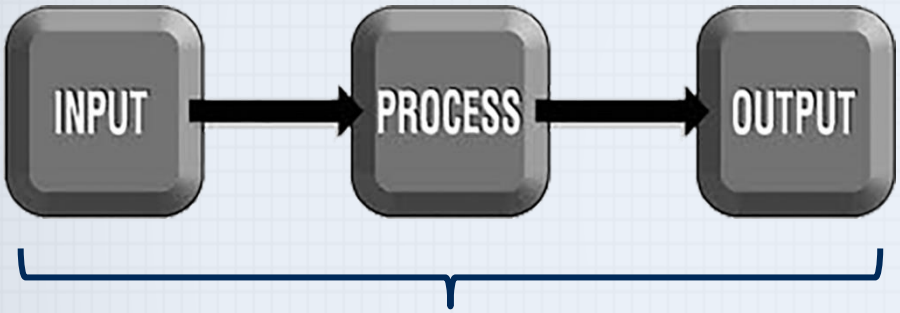


Exemplo

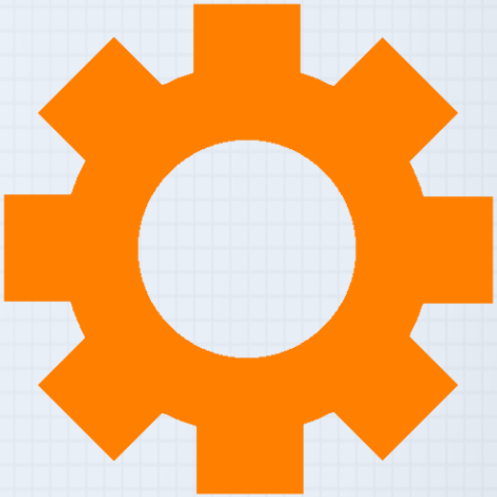
Conexão física para a Internet dá aos hackers potencial acesso aos sistemas do avião

Análise da Informação

Projetar um sistema baseado no seu Fluxo



Workflow



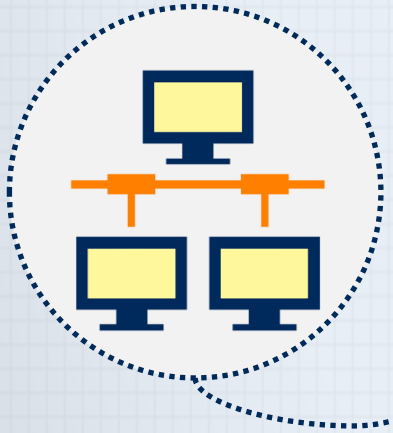
Em virtude do resultado da análise

Processos Operacionais e de Informações

Gestão da Informação e a Informática

Gestão da comunicação

Formula e dirige a política relativa à prestação de informação



Informática desenvolve

Informações

Resumo

- Gestão da Informação
- Forma da Informação
- Sistema da Informação
- Valor da Informação
- Disponibilidade
- Integridade
- Confidencialidade
- Arquitetura da Informação

Teste

Pronto para o próximo?

Clique acima em
“Sair da Atividade”

Treinamento ISO 27002 Foundation

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 3

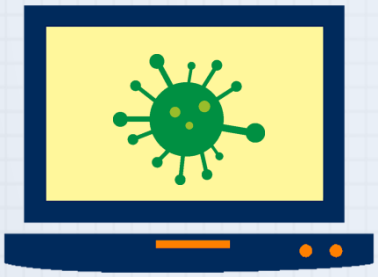
Ameaças e Riscos

O que veremos neste módulo?

- Análise de Riscos
- Medidas de Redução de Riscos
- Tipos de Ameaças
- Tipos de Danos

Introdução

Ameaça de roubo. Risco subjetivo ou objetivo?



Mapeamento das ameaças

Senha de acesso?

Na prática

Um empregado que não trabalha no RH mas pode obter acesso às informações deste departamento.

Um incêndio que pode iniciar em sua empresa.

Alguém que se apresenta como um empregado e tenta obter informações interna da empresa.

Sua empresa é atingido por uma falha de energia

Um hacker consegue acessar a rede da empresa.

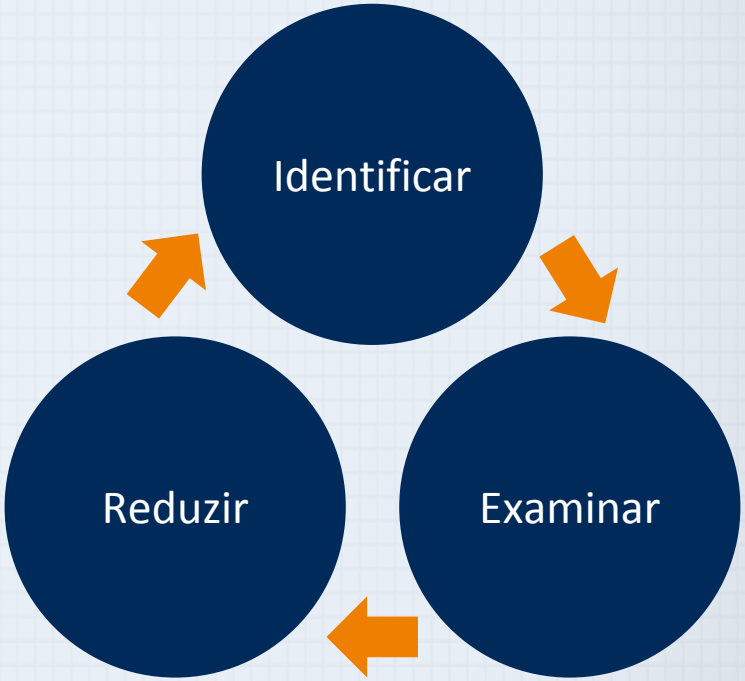
Gerenciamento de Riscos

Gerenciamento de Riscos:

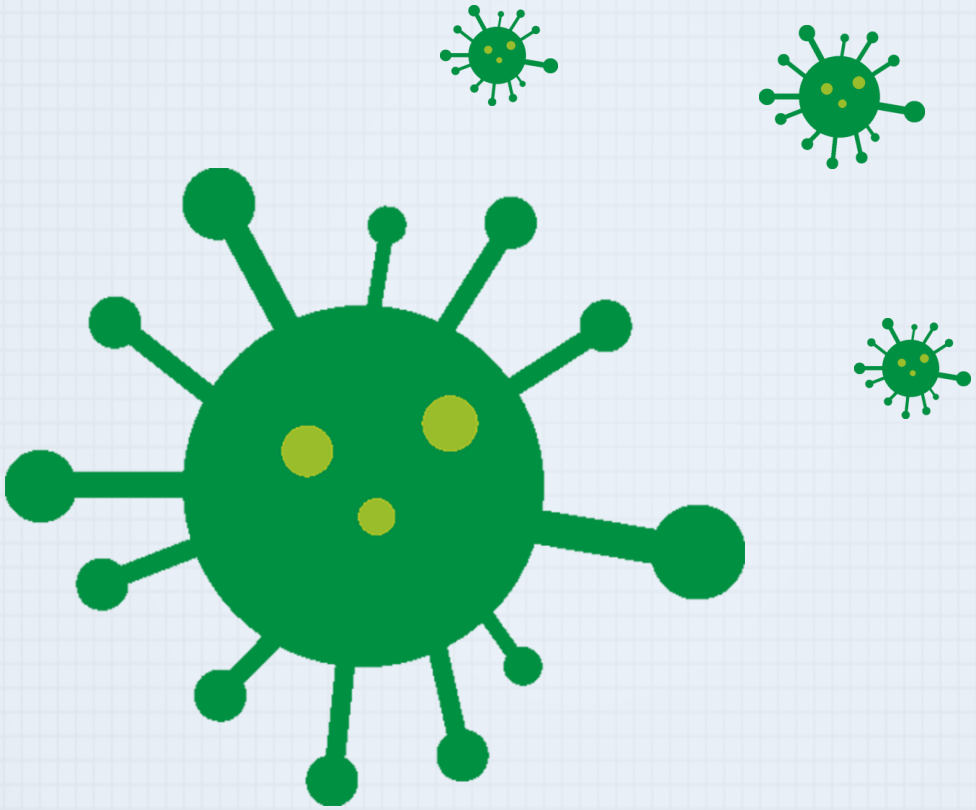
Ameaça manifestada: torna-se um **INCIDENTE**

Ameaça concretizada: Surge um **RISCO**, então... Medidas de segurança são tomadas

CICLO CONTÍNUO



Exemplo



Análise de Riscos

Serve para:

- Como ferramenta para Gestão de Riscos
- Determinar se as ameaças são relevantes
- Identificar riscos associados
- Garantir que as medidas de segurança sejam implantadas
- Evita gastos desnecessários em medidas de segurança
- Ajuda a conhecer os conceitos de segurança
- Avaliar corretamente os riscos

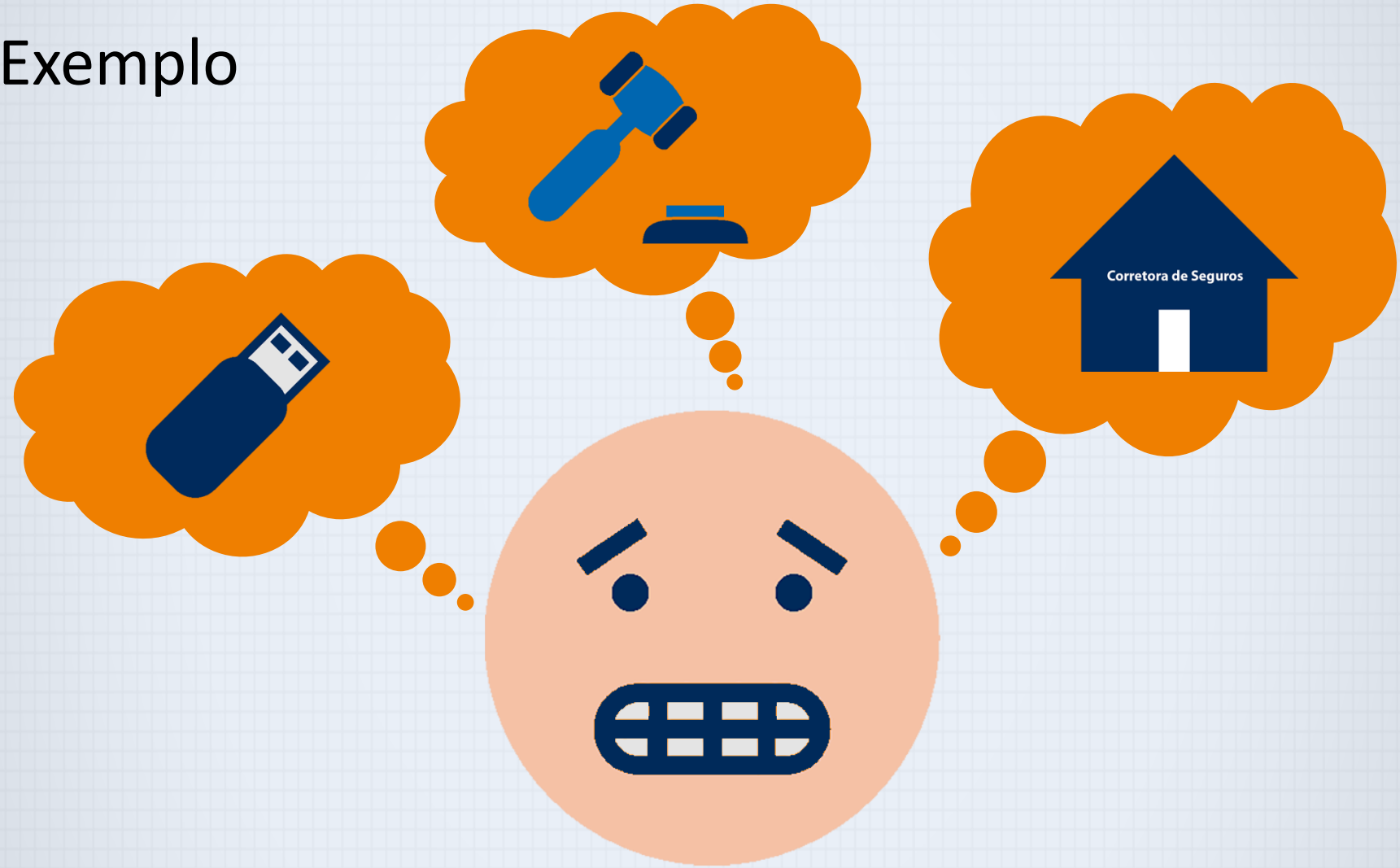
Objetivos

- Identificar os bens e os seus valores
- Determinar as vulnerabilidades e ameaças
- Determinar quais as ameaças se tornarão um risco
- Determinar um equilíbrio entre os custos

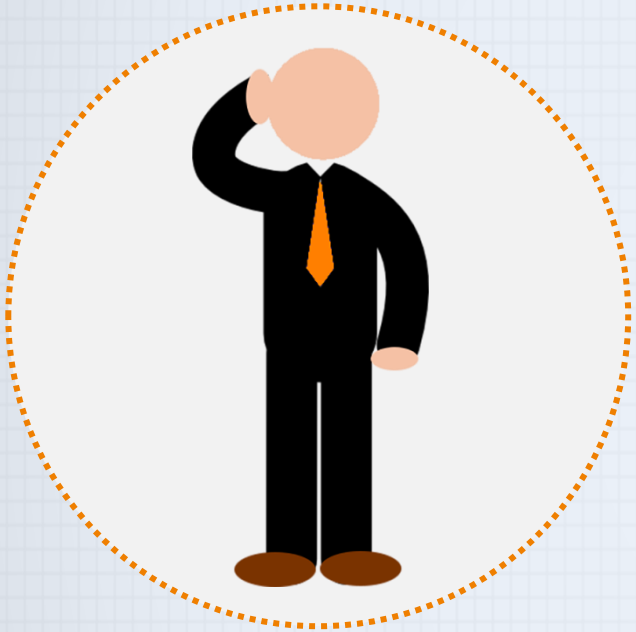
Tipo de Análise de Riscos: Quantitativo

- Baseado no impacto
- Baseado na perda financeira
- Baseado na probabilidade da ameaça tornar-se um incidente

Exemplo



Tipo de Análise de Riscos: Qualitativo



- Baseado nos cenários
- Baseado nas situações
- Baseado nos sentimentos

Medidas de Redução de Riscos

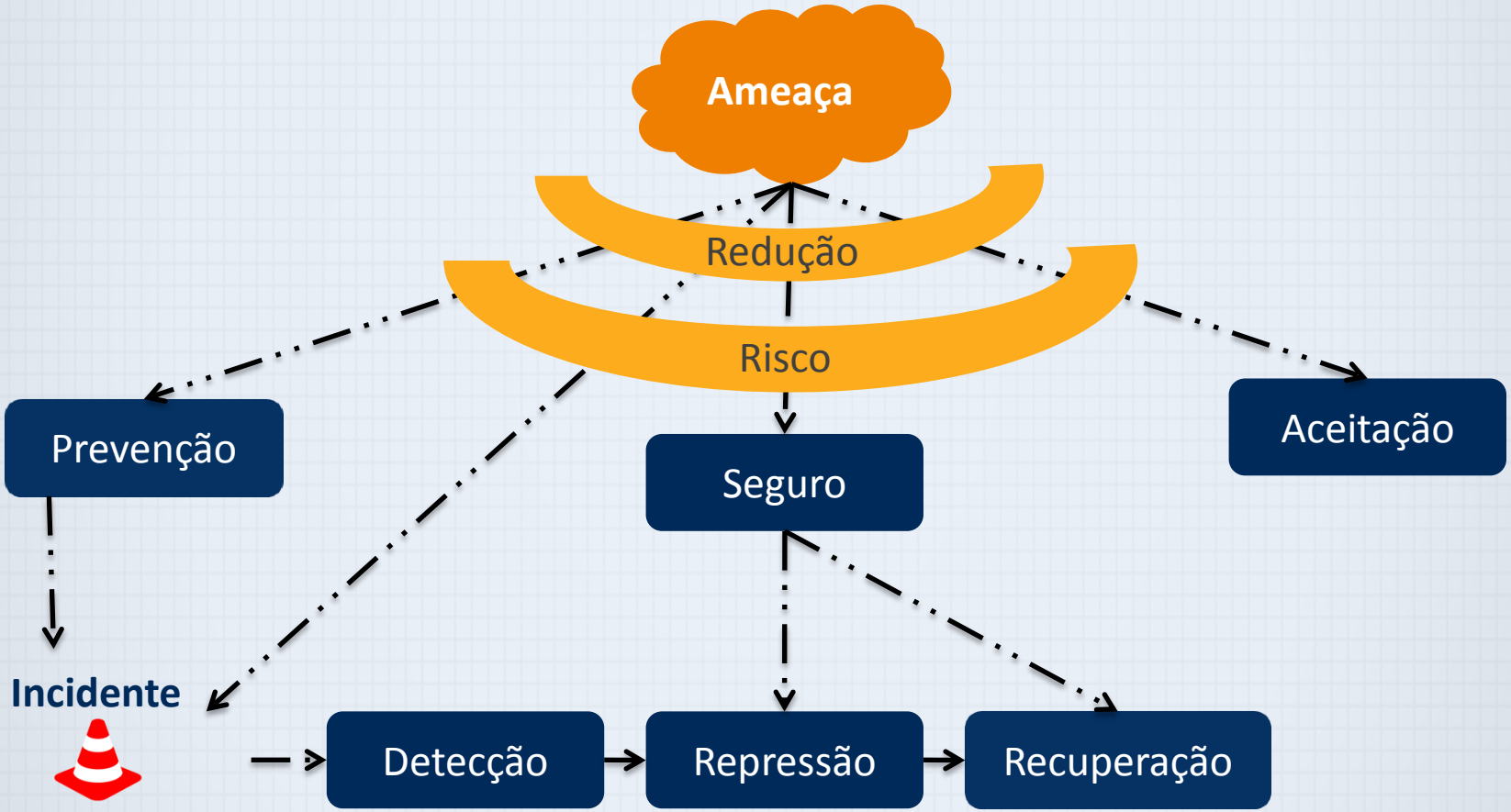
Objetivo:

- Reduzir a chance do evento ocorrer
- Minimizar as consequências

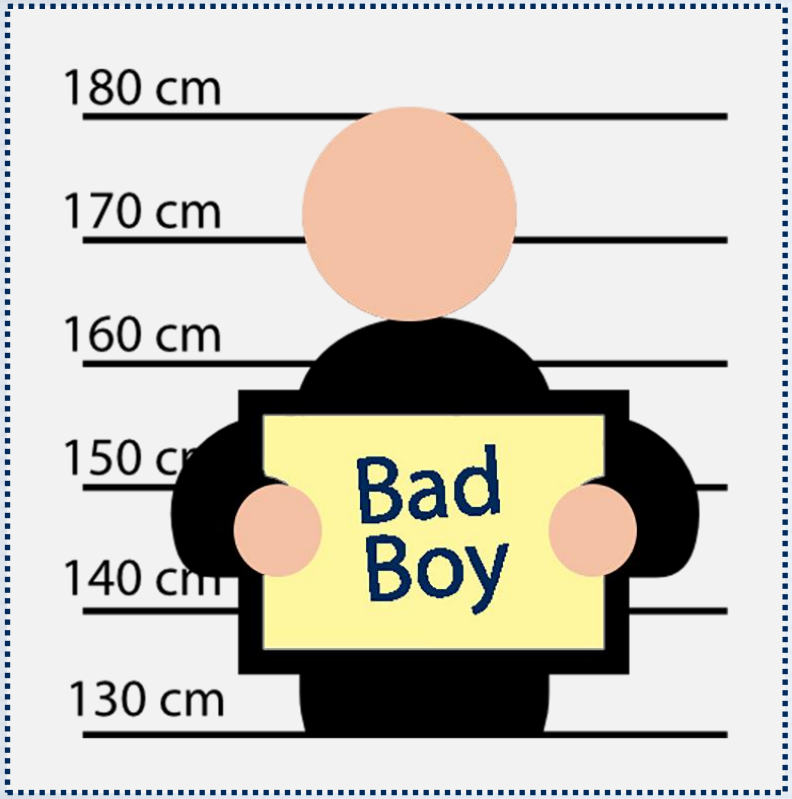
Através

Prevenção	Detecção	Repressão
Correção	Seguros	Aceitação

Tipos de Medidas de Segurança



Tipos de Ameaças



Humanas

Não-Humanas

Ameaça Humana

Ameaça Externa: Hacker

Funcionários Internos

Engenharia Social

Ameaça Não-Humana

Relâmpagos

Incêndios

Inundações

Tempestades

Catástrofes

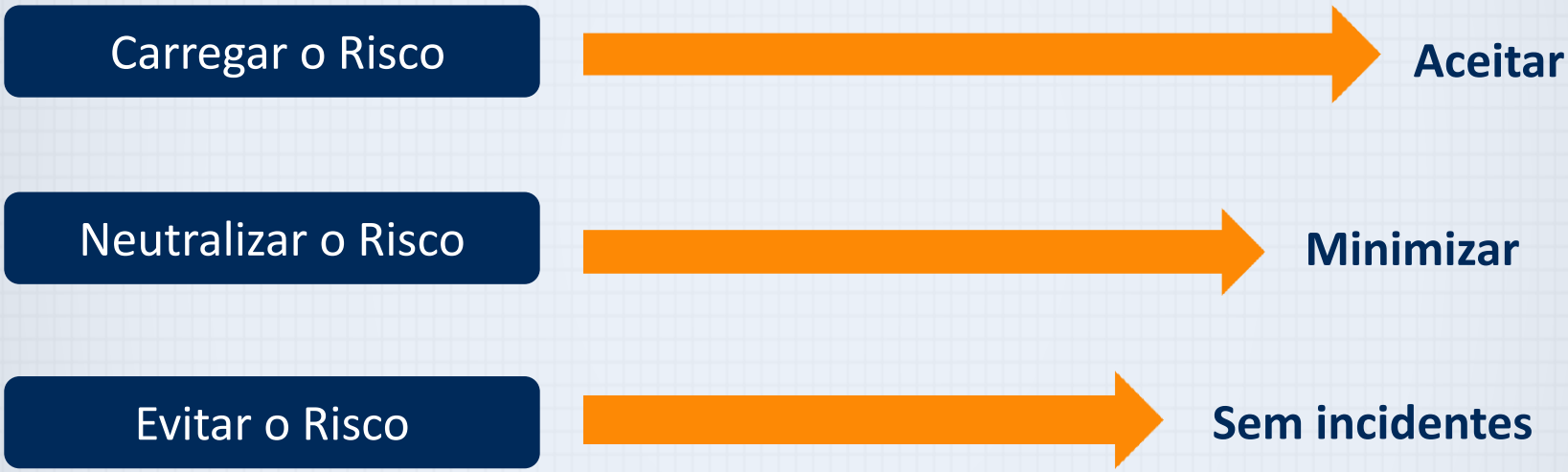
Exemplo

Tipos de Danos

- Danos diretos
- Danos indiretos
- ALE – Annual Loss Expectancy
- SLE – Single Loss Expectancy

Exemplo

Tipos de Estratégia de Risco



Diretrizes para implementar medidas de segurança

Exemplo

Resumo

- Diretrizes para implementação
- Gerenciamento de Riscos
- Análise de Riscos Quantitativo
- Análise de Riscos Qualitativo
- Medidas de Redução
- Tipo de Ameaça
- Tipo de Dano
- Tipo de Estratégia

Teste

Pronto para o próximo?

Clique acima em
“Sair da Atividade”

Treinamento ISO 27002 Foundation

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 4

Ativos de Negócios e Incidentes de Segurança da Informação

O que veremos neste módulo?

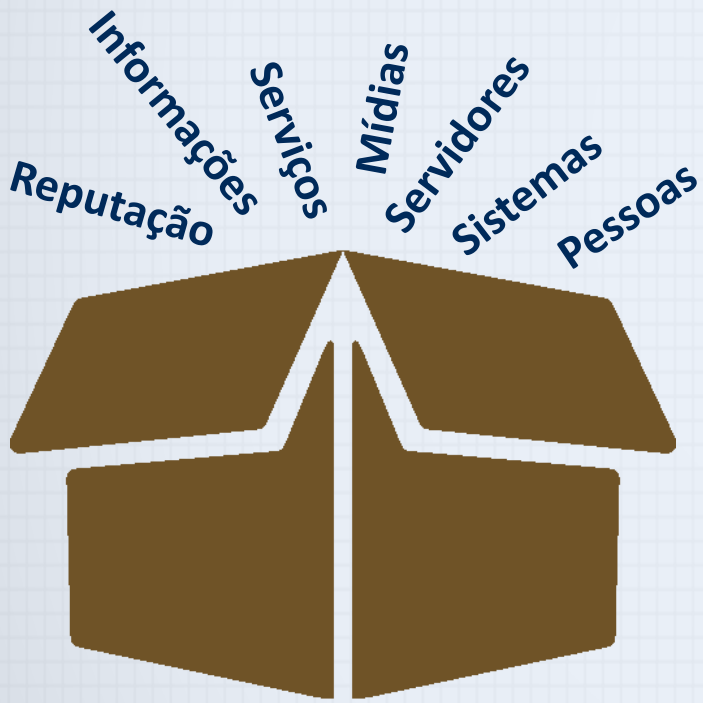
- Ativos de Negócios
- Classificação dos Ativos
- Gerenciamento de Incidente
- Ciclo de Incidentes
- Papéis

Introdução

Processo de Segurança da Informação é Contínuo

Deve ser apoiada pela Alta Administração

Quais são os ativos da empresa



As informações que são gravadas sobre os bens da empresa são:

- O tipo de ativo de negócio;
- Proprietário do processo;
- Localização do ativo;
- O Formato do ativo;
- A Classificação;
- Valor do ativo para o negócio.

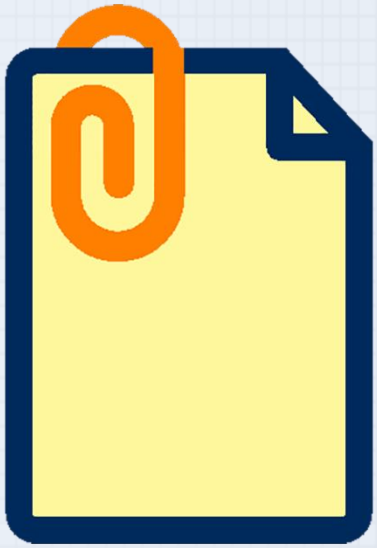
Gerenciamento de Ativos de Negócios

Acordos

- Como lidar com os ativos
- Como as mudanças acontecem
- Quem inicia as mudanças e como são testadas

COBIT® GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY

Acordos de como lidar com os ativos da empresa



Quanto mais complexo o ativo,
mais importante uma instrução de uso

O uso dos ativos de negócio

Regras de utilização

Termos

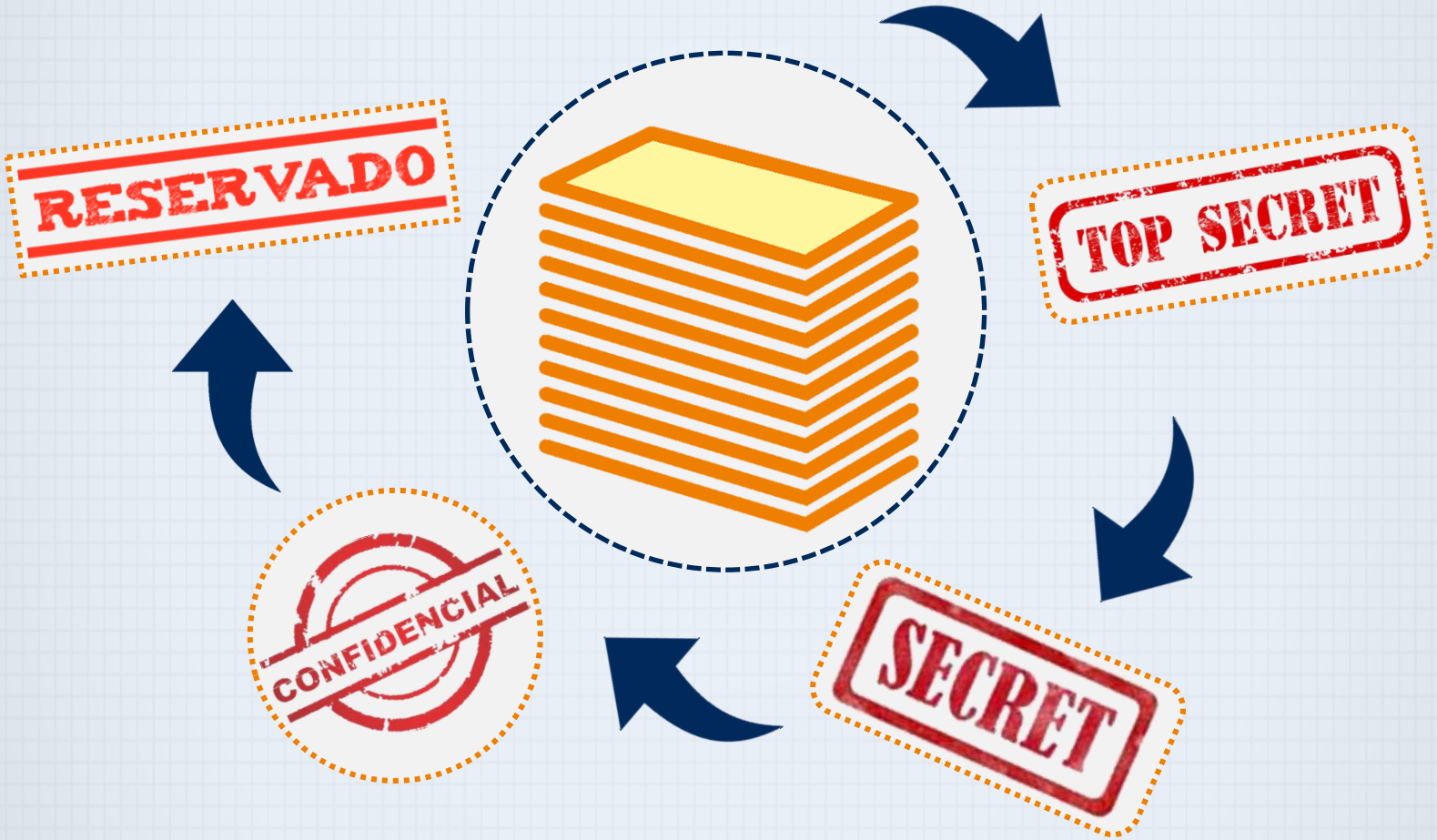
Designar
(forma especial de categorização)

Proprietário
(responsável por um ativo
de negócio)

Classificação
(níveis de sensibilidade)

Graduar
(classificar a informação apropriadamente)

Classificação



Gerenciamento de Incidentes de Segurança

Reporte dos Incidentes de Segurança

Os relatórios devem ser usados como:

- Uma forma de aprender
- Reporte de incidentes

Os relatórios devem ser usados como:

- Data e hora
- Nome da pessoa que reporta o incidente
- Localização (onde foi o incidente?)
- Qual é o problema?
- Qual é o efeito que o incidente causou?
- Como foi descoberto?

Exemplo

Incidentes de segurança

Um procedimento contém instruções do que fazer diante de um incidente

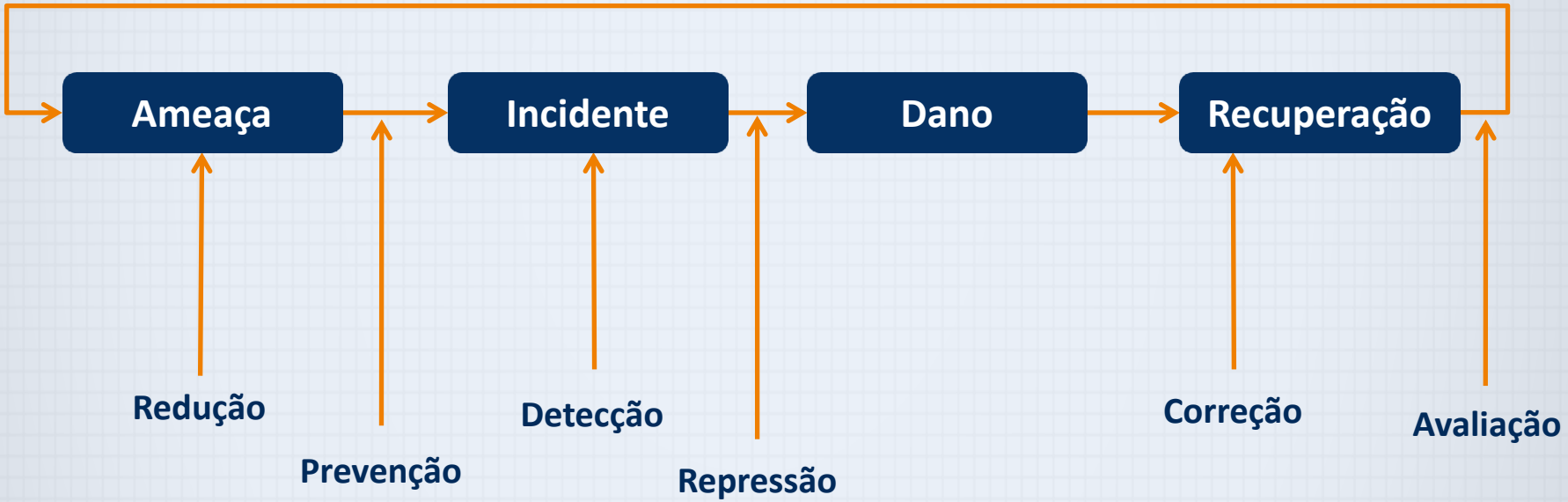
Reportando Fraquezas de Segurança

Reportar fraquezas e deficiências, mais cedo possível

Registro de Ruptura

É importante que as informações pertinentes sejam coletadas e armazenadas

Medidas no ciclo de vida do Incidente



Papéis

Resumo

- Ativos de Negócios
- Classificação dos Ativos
- Gerenciamento de Incidentes
- Ciclo de Vida dos Incidentes
- Papéis

Teste

Pronto para o próximo?

Clique acima em
“Sair da Atividade”

Treinamento ISO 27002 Foundation

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 5

Medidas Físicas

O que veremos neste módulo?

- Segurança Física
- Anéis de Proteção
- Alarmes
- Proteção contra incêndio

Introdução

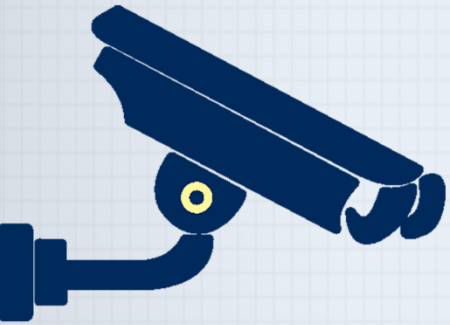
Empresa Privada:

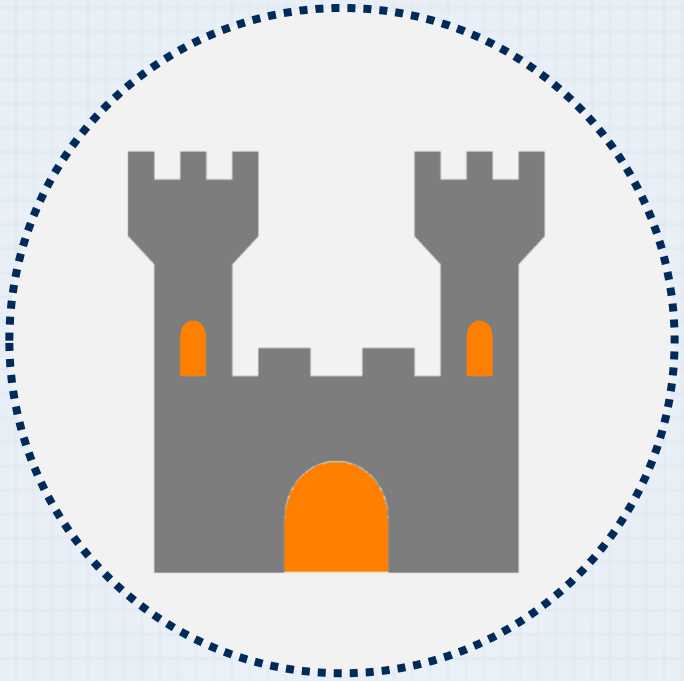
Acesso mais restritivo

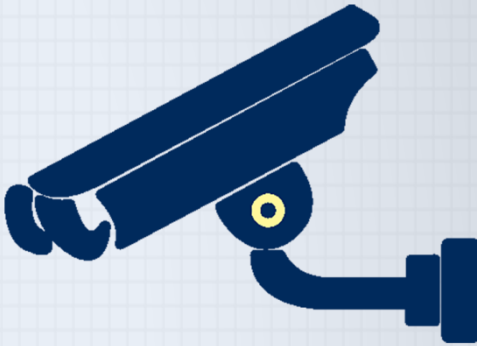
Empresa Pública:

Acesso mais liberado

Segurança Física







Segurança física faz parte da segurança da informação, porque todos os ativos da empresa devem ser fisicamente protegidos

Equipamento

Cabeamento

- Cuidado com as interferências
- Proteção contra chiados e ruídos
- Fonte dupla de energia

Mídia de Armazenamento

Mídias Convencionais

Muitas impressoras podem armazenar informações em seu próprio disco rígido.

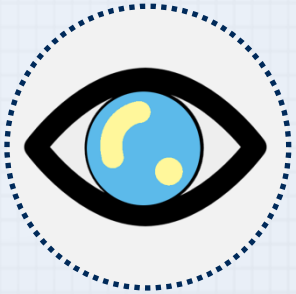
Anel Externo

Construções

Vidros Blindados

Portões Resistentes

Impressão Digital

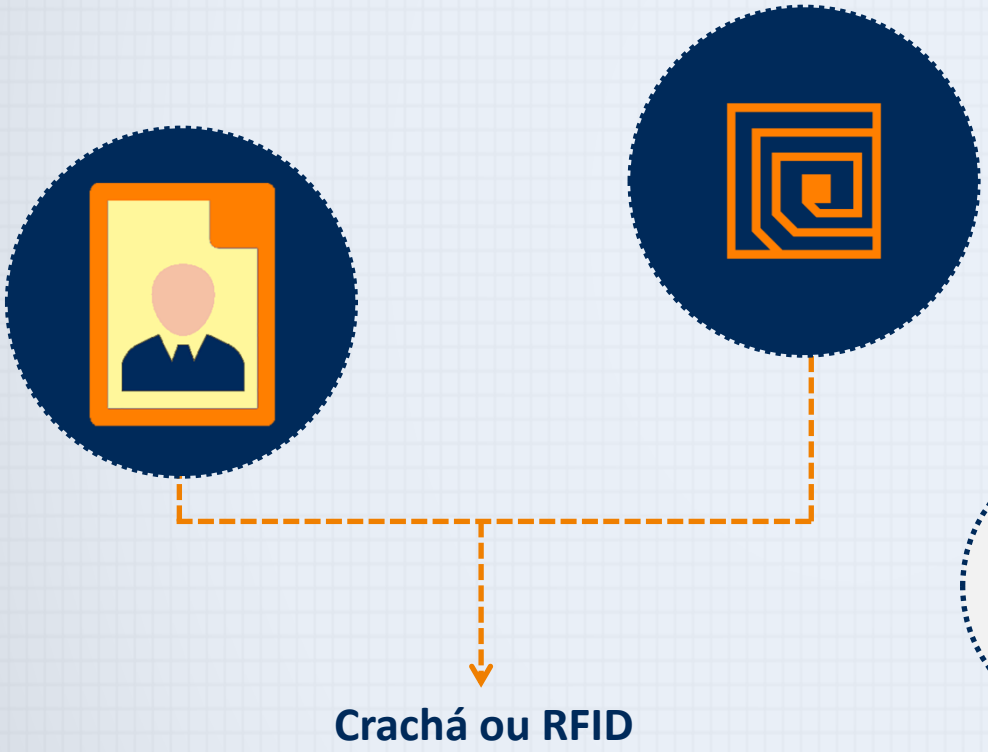


Biometria da IRIS

Reconhecimento das mãos

Gestão de Acesso

Gerenciamento eletrônico de acesso



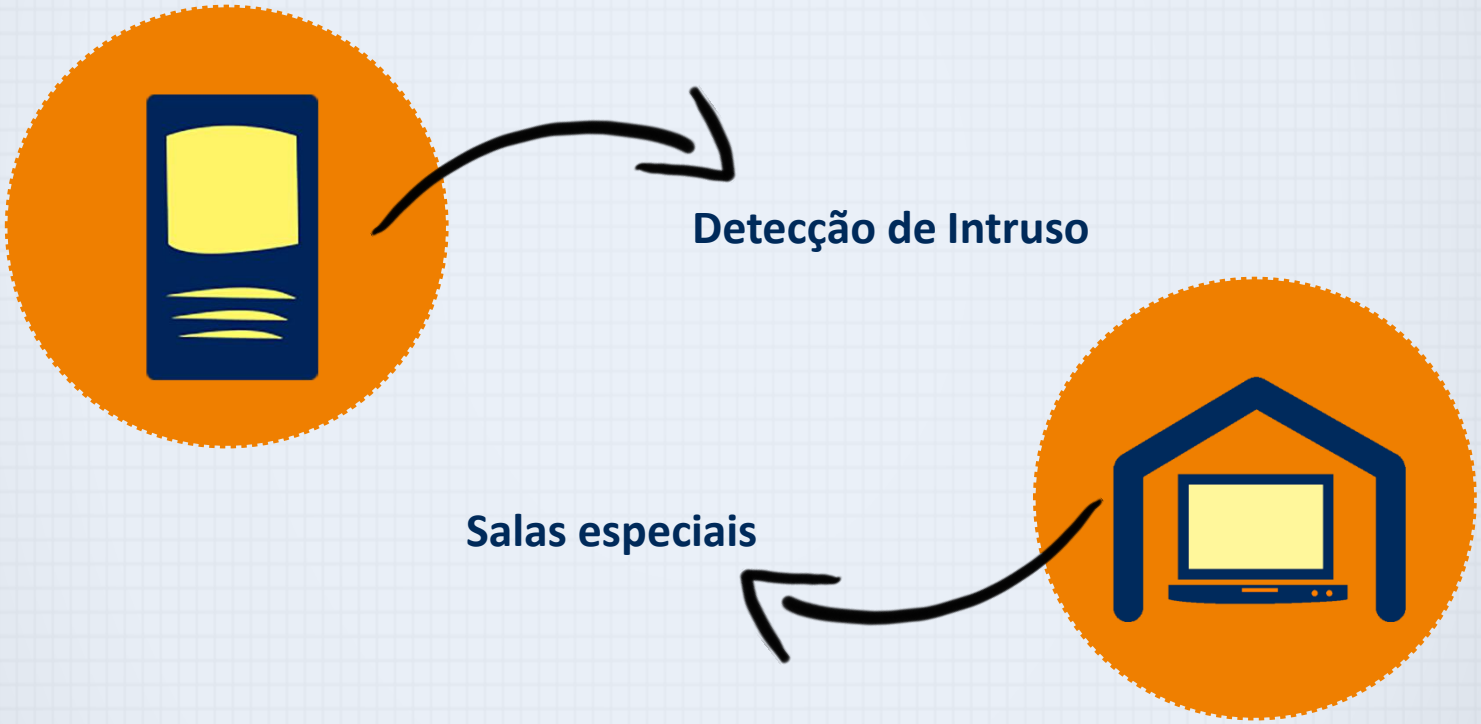
Medidas adicionais

Exemplo

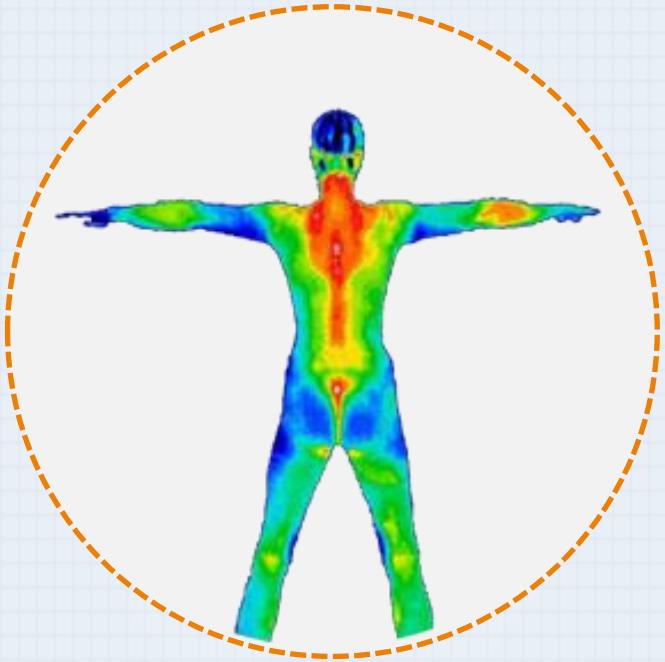
Em mais da metade das maternidades em Ohio, nos EUA, ambos, a mãe e a criança, colocam uma etiqueta RFID em forma de pulseira ou tornozeleira, desta forma, as mães esperam que seus filhos não sejam perdidos, raptados ou dados aos pais errados.

Espaço de Trabalho

Proteção dos espaços de trabalho



Detecção de Intruso



O método mais comum e mais utilizado para detecção passiva de intrusos são os de infravermelho, onde movimentos aparentes são detectados quando há um objeto com uma temperatura

Sala Especial – Parte I

Entrega e retirada segura

Sala de armazenamento de materiais sensíveis

Sala de servidores

Sistema de refrigeração

Sala Especial – Parte II

Baterias e UPS

Desumidificador

Extintores de incêndio

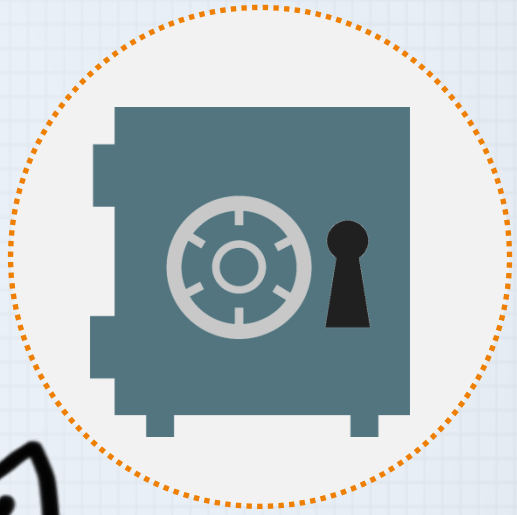
Exemplo

1

2

Objeto

O objeto refere-se a parte mais sensível que tem que ser protegida, ou seja, o anel interno.

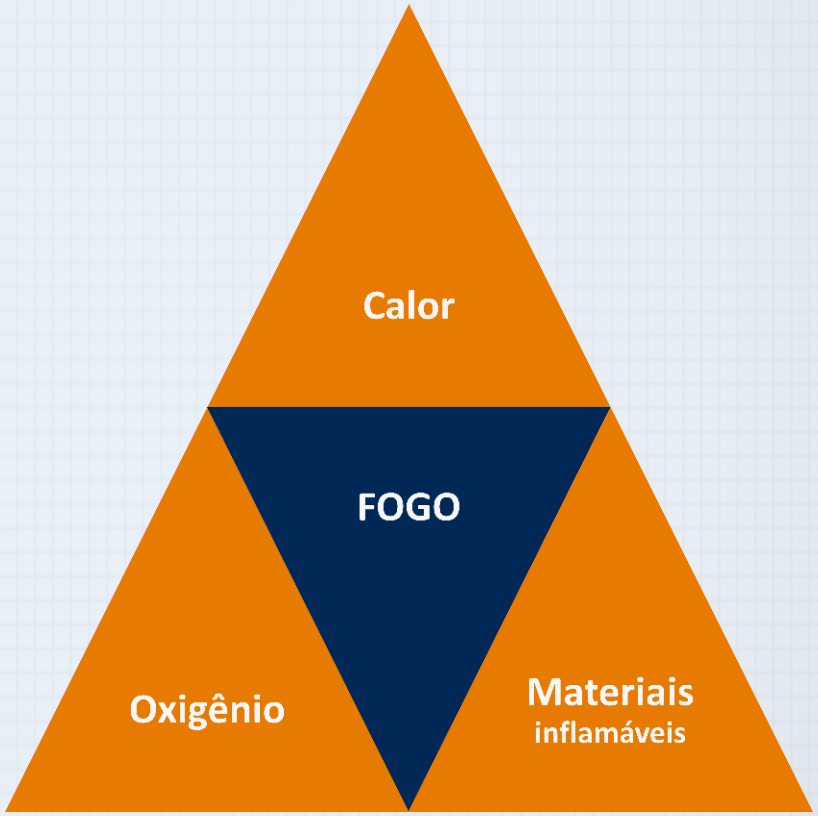


Armários à prova de fogo → Cofres

Alarmes

- Detecção Infravermelho Passivo
- Câmeras
- Detecção de vibração
- Sensores de quebra de vidro
- Contatos magnéticos

Proteção contra Incêndio



Sinalização e Agentes Extintores

Os vários agentes extintores de fogo são:

- Gases inertes
- Espuma
- Pó
- Água
- Areia

Resumo

- Agentes extintores
- Anel Externo
- Construções
- Espaço de Trabalho
- Objeto
- Alarmes
- Proteção contra incêndio
- Sinalização

Teste

Pronto para o próximo?

Clique acima em
“Sair da Atividade”

Treinamento de ITSM baseada na ISO/IEC ® 27002 Foundation

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 6

Medidas Técnicas (Segurança de TI)

O que veremos neste módulo?

- Gerenciamento de Acesso Lógico
- Requisitos de Segurança para SI
- Criptografia
- Política de Criptografia
- Tipos de Sistemas de Criptografia
- Segurança de Arquivos de Sistemas
- Vazamento de Informação

Introdução

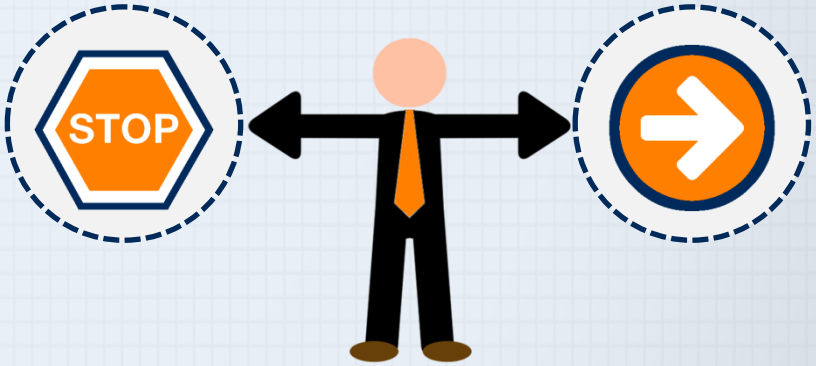
Proteção dos dados

As informações devem ser confiáveis

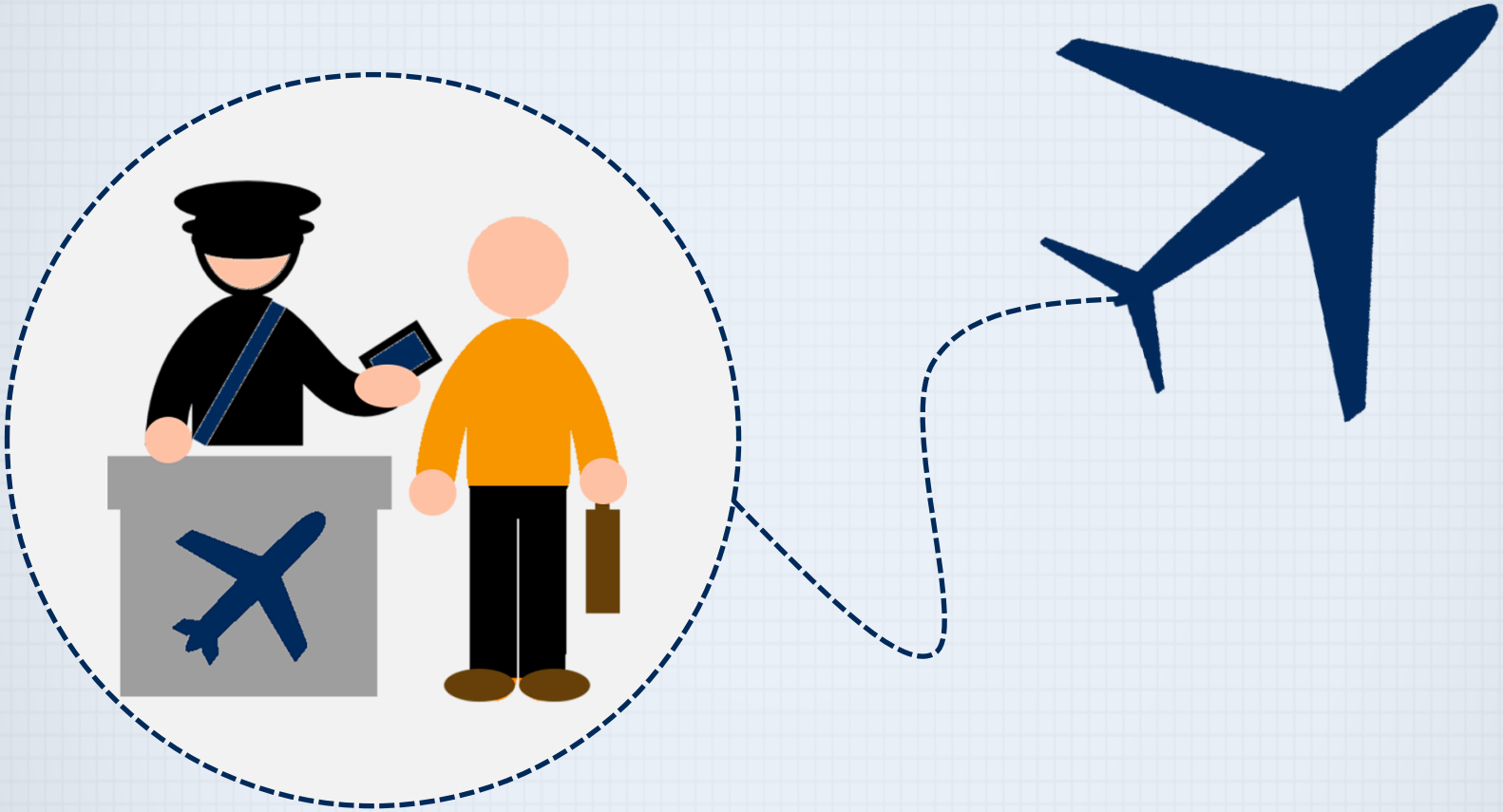
Gerenciamento Lógico de Acesso

Controle de Acesso Discricionário (DAC). Com o Controle de Acesso Discricionário, a decisão de conceder o acesso à informação encontra-se com o próprio usuário.

Controle de Acesso Obrigatório (MAC). O controle de acesso obrigatório é definido e organizado centralmente para que as pessoas tenham acesso aos sistemas de informação.



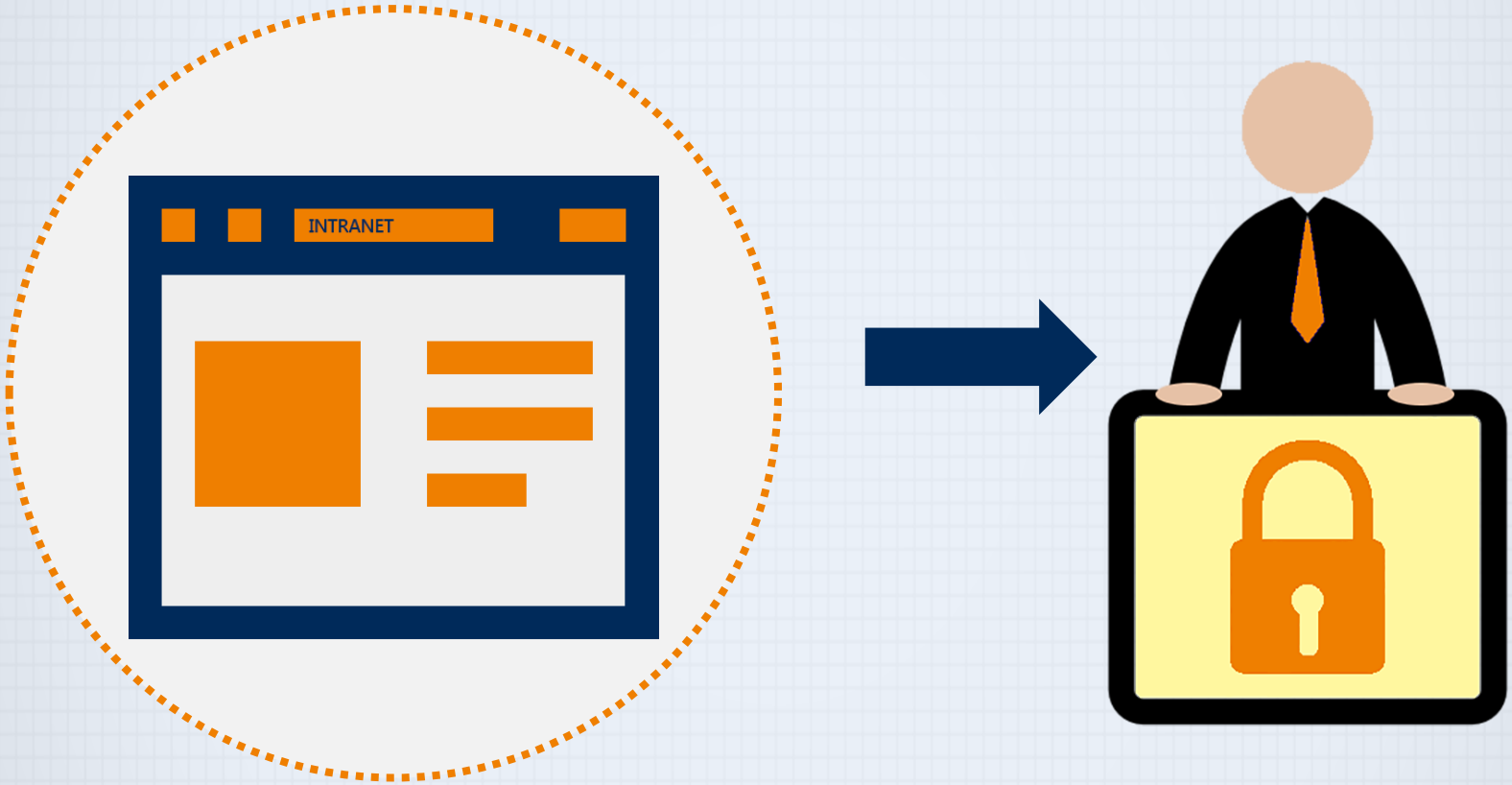
Exemplo



Requisitos de Segurança para SI

- Os requisitos de segurança precisam ser acordados e documentados na fase de Planejamento do Projeto.
- Deve fazer parte de um “Business Case”
- Implementar medidas de segurança na fase de concepção do projeto fica geralmente mais barato
- Mantenha um contrato com o fornecedor, indicando as exigências de segurança

Exemplo



Processamento Correto das Aplicações

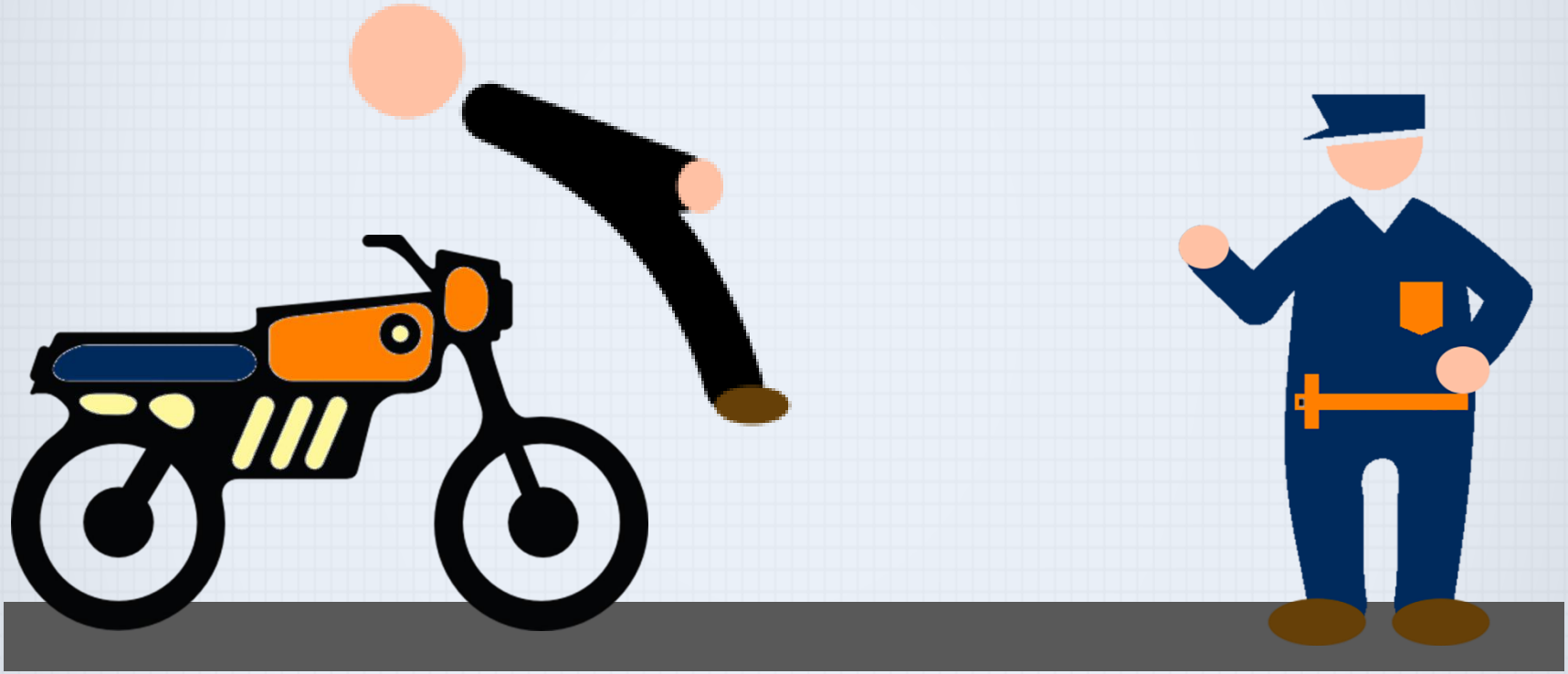
Sem perdas

Sem erros

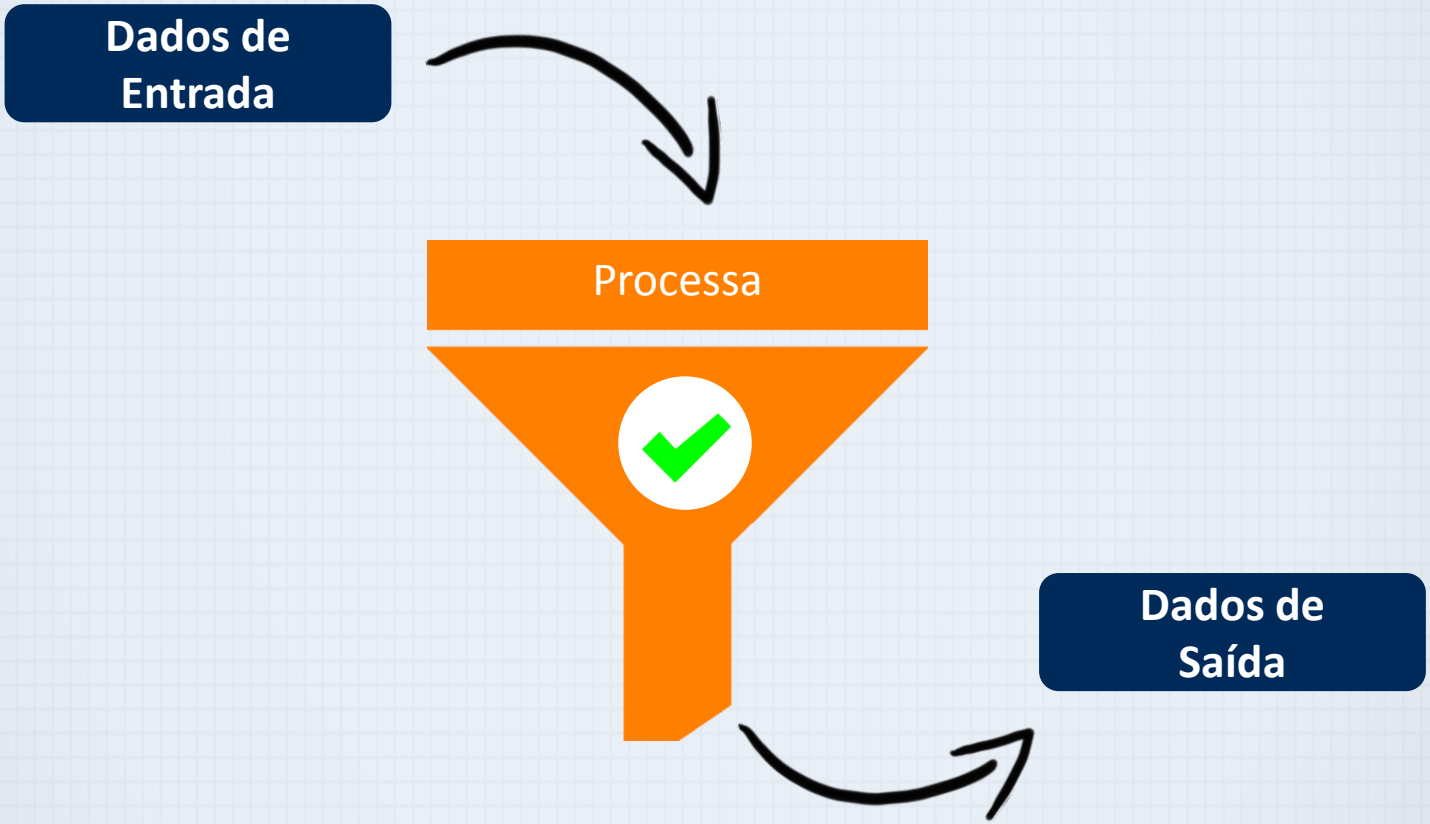
Seguras

Gerenciamento da validação dos dados que são inseridos no sistema, o processamento interno e a saída de dados ou informações

Exemplo



Validação dos dados de Entrada e Saída

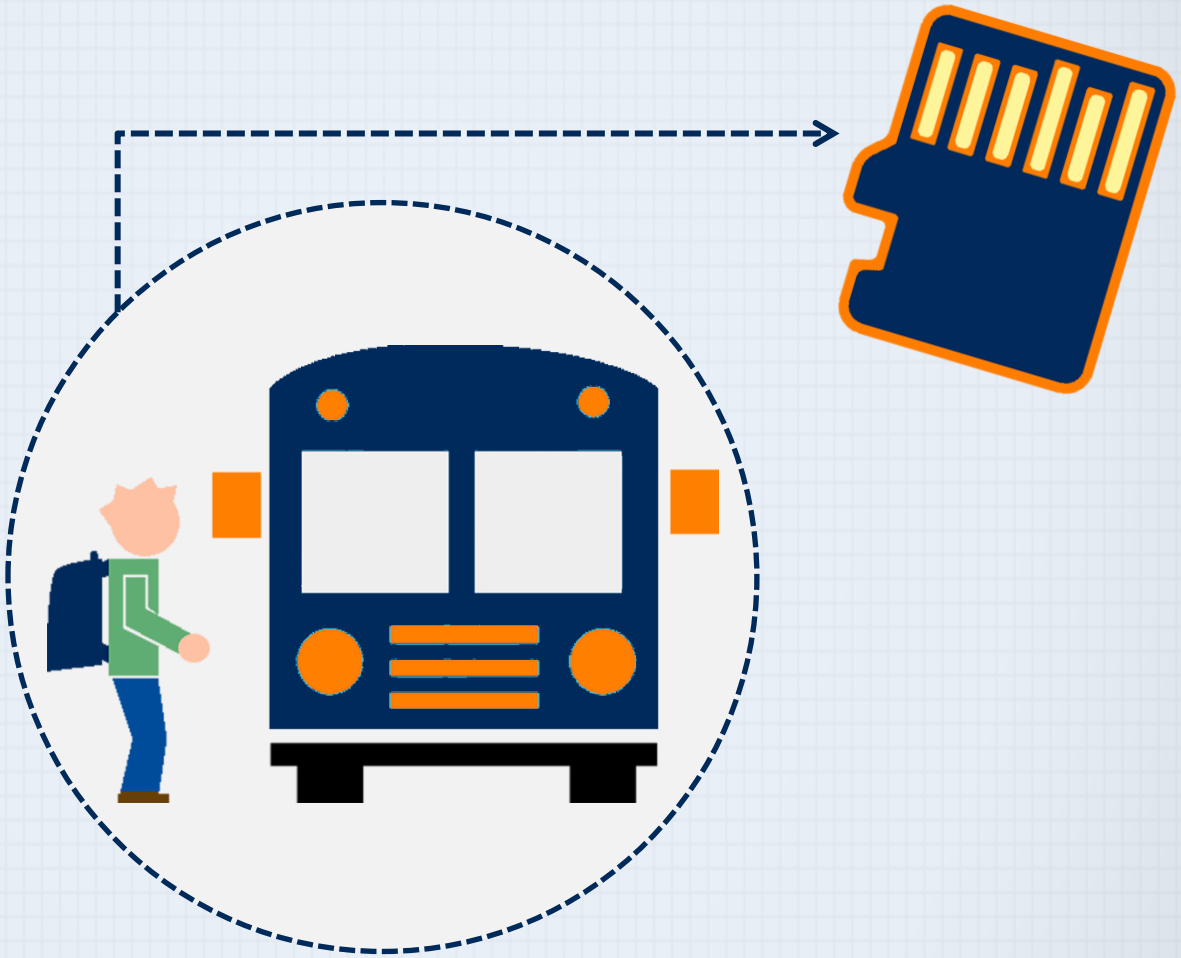


Criptografia

Análise Criptográfica serve para:

- Desenvolver Algoritmos
- Quebrar Algoritmos de Inimigos

Exemplo



A Política da Criptografia

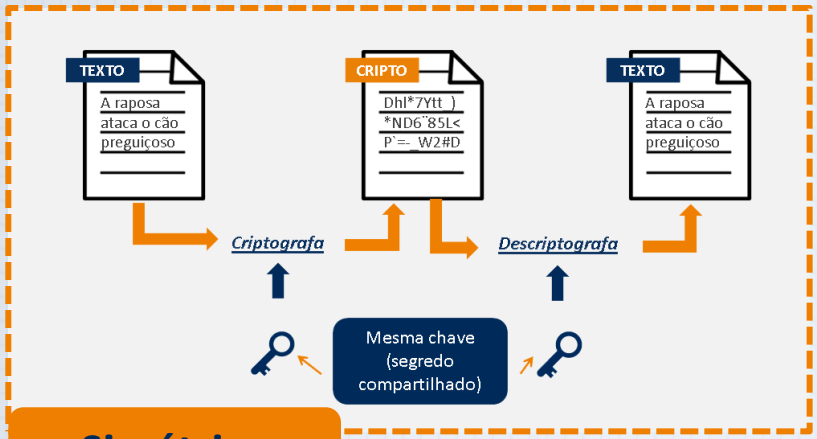
Deve conter:

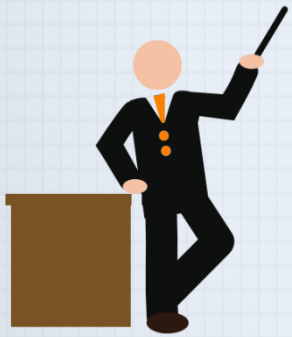
- Para que a organização usa a criptografia
- Que tipo de criptografia é utilizada
- Quais aplicações usam criptografia
- Controle e gestão de chaves
- Backup
- Controle

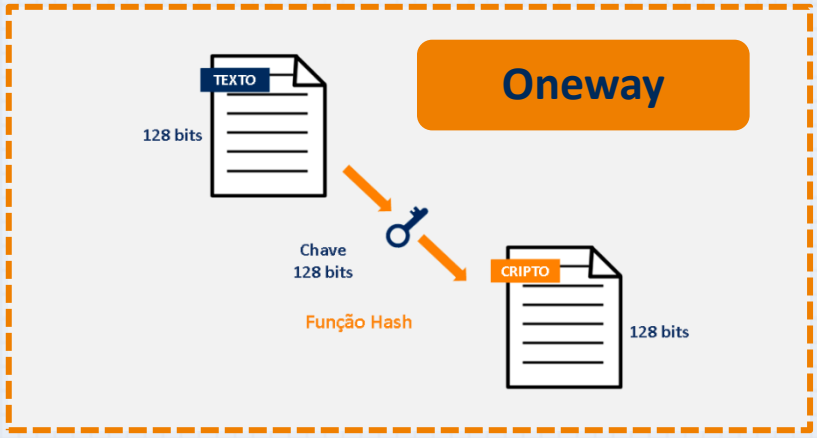
Gestão das Chaves

- São protegidas
- Quais pares foram emitidos?
- Para quem?
- Quando?
- Qual a validade?

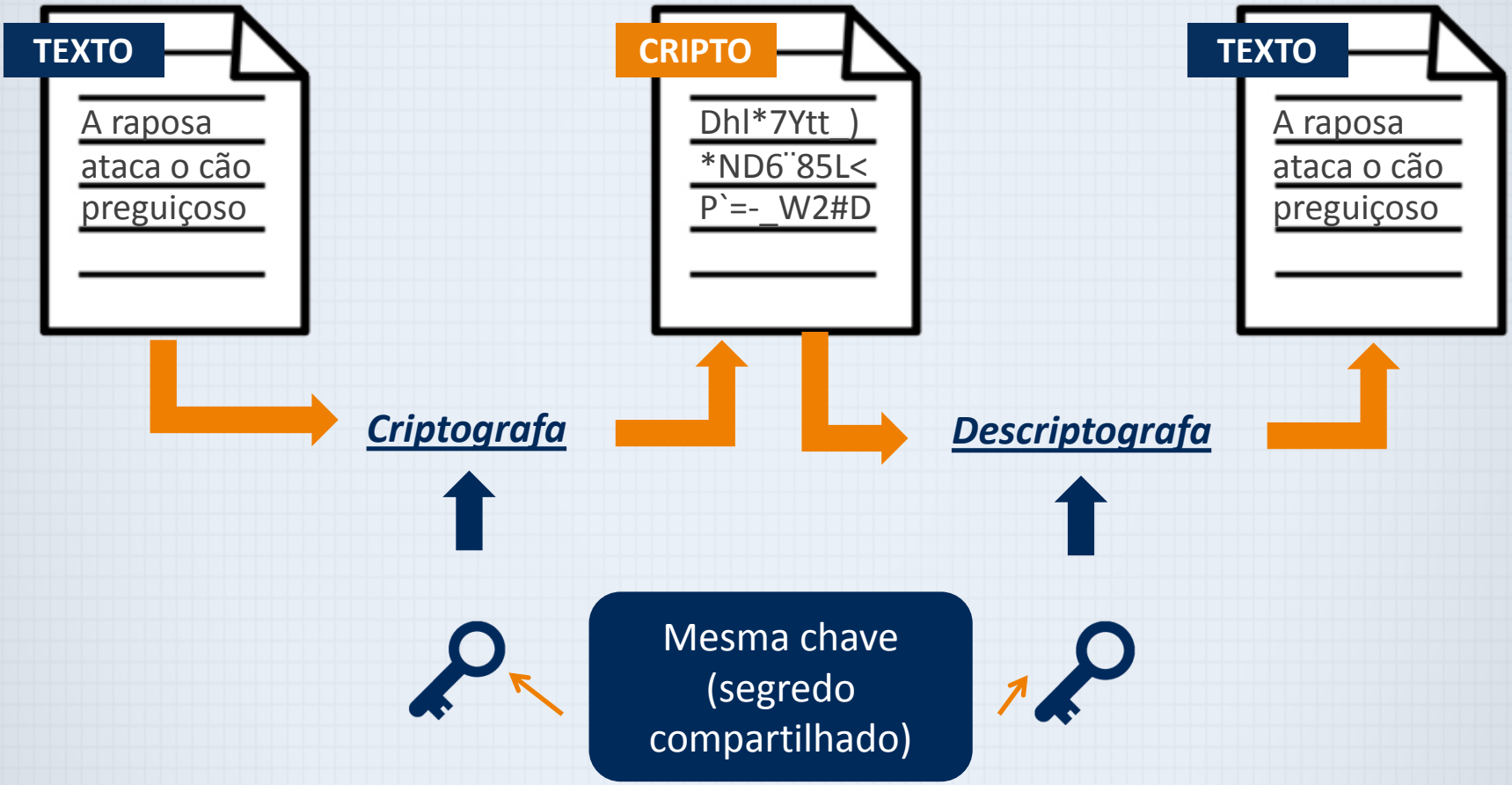
Tipo de Sistemas de Criptografia



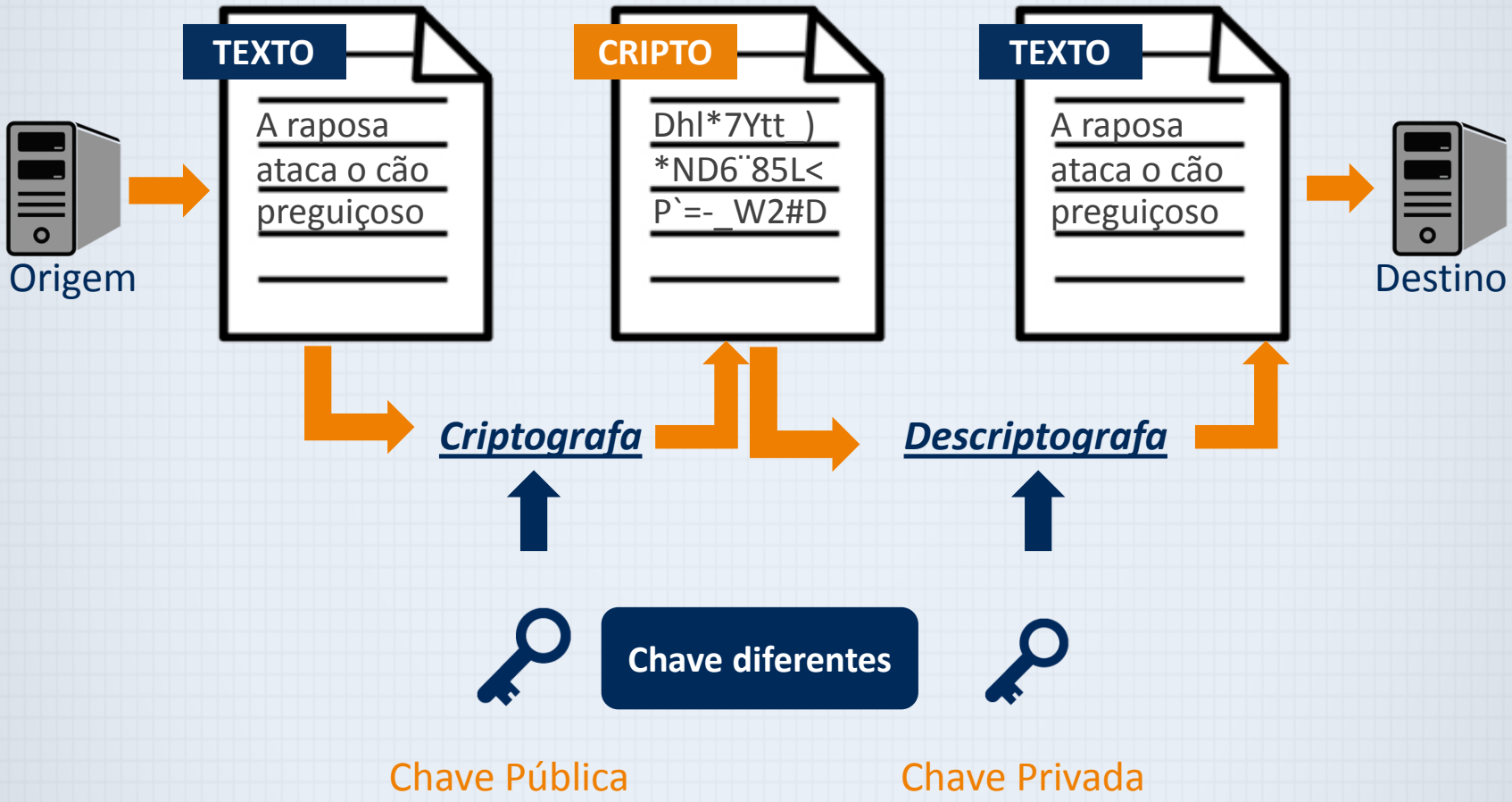




Simétrica


TEXTO
A raposa ataca o cão preguiçoso
Criptografa
CRIPTO
Dhl*7Ytt_)
*ND6¨85L<
P`=-_W2#D
Descriptografa
TEXTO
A raposa ataca o cão preguiçoso
Mesma chave (segredo compartilhado)

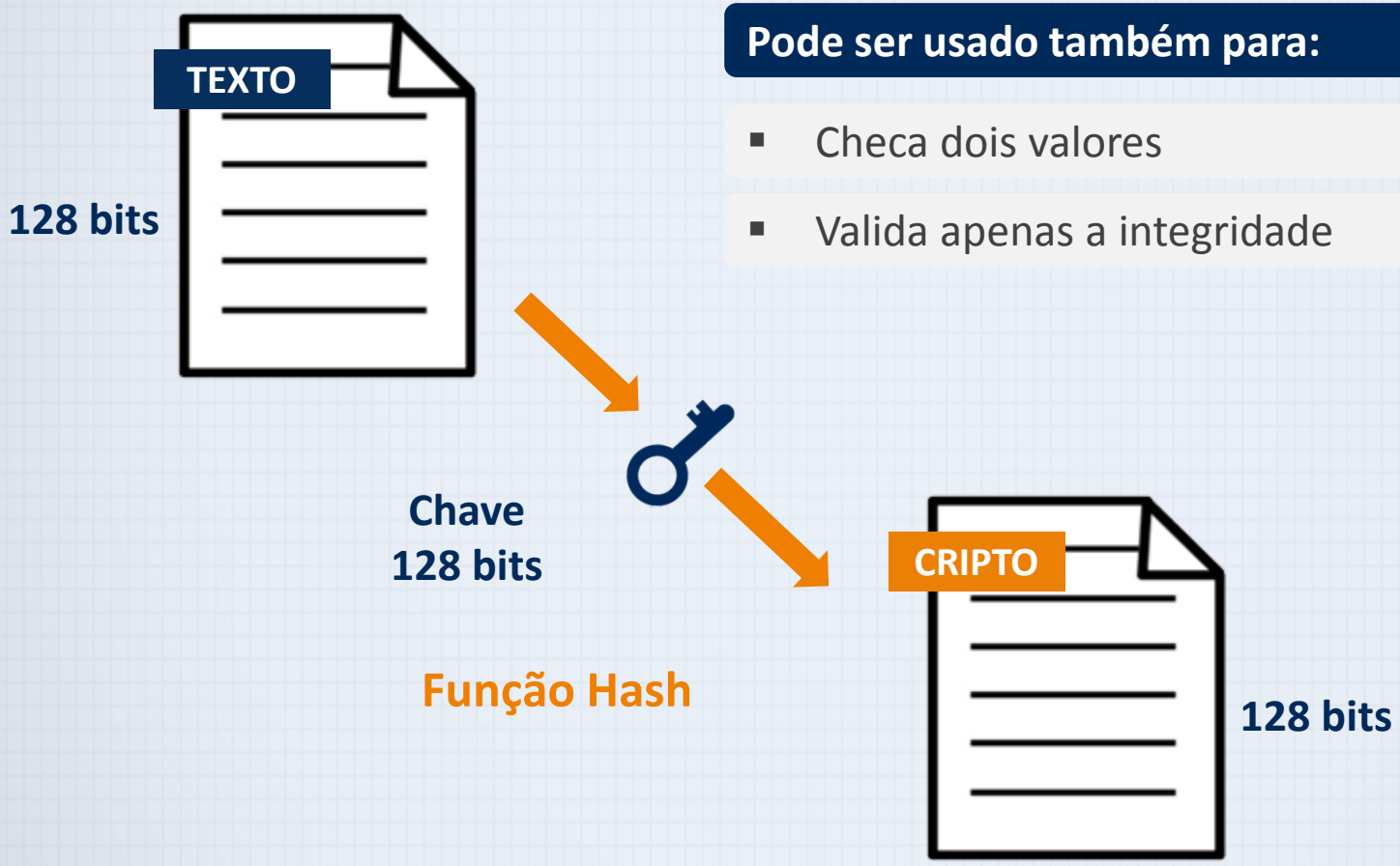
Assimétrica



Exemplo


Solicita um certificado
Recebe o certificado
Certification Authority
Contrato
Solicita acesso
Acesso concedido
Médico
Companhia de Seguro

Criptografia One-Way



Pode ser usado também para:

- Checa dois valores
- Valida apenas a integridade

Segurança do Sistema de Arquivos

- Gestão de Acesso aos Códigos-Fonte do Programa
- Segurança de Dados de Teste
- Segurança nos Processos de Desenvolvimento e Suporte

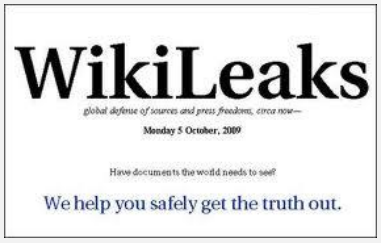
Vazamento de Informações

Para manutenção

Ou *back door*

Através de canais secretos de comunicação:

Exemplo atual:



Terceirização do Desenvolvimento de Sistemas

- Supervisionado pelo contratante

- Avalie a obtenção de direitos de propriedade

- Verifique questões de segurança, como os canais ocultos

Resumo

- Gerenciamento de Acesso Lógico
- Requisitos de Segurança
- Criptografia
- Chaves Públicas
- Simétricas
- Assimétricas
- Política de Criptografia
- Tipos de Sistemas de Criptografia
- Segurança de Arquivos
- Vazamento de Informação

Teste

Pronto para o próximo?

Clique acima em
“Sair da Atividade”

Treinamento ISO 27002 Foundation

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 7

Medidas Organizacionais

O que veremos neste módulo?

- Política de Segurança
- Pessoal
- Gerenciamento de Continuidade de Negócio
- Gerenciamento da Comunicação e Processos Operacionais

Introdução

Medidas Organizacionais

ISO/IEC 27001 e 27002

Desastres

Comunicação

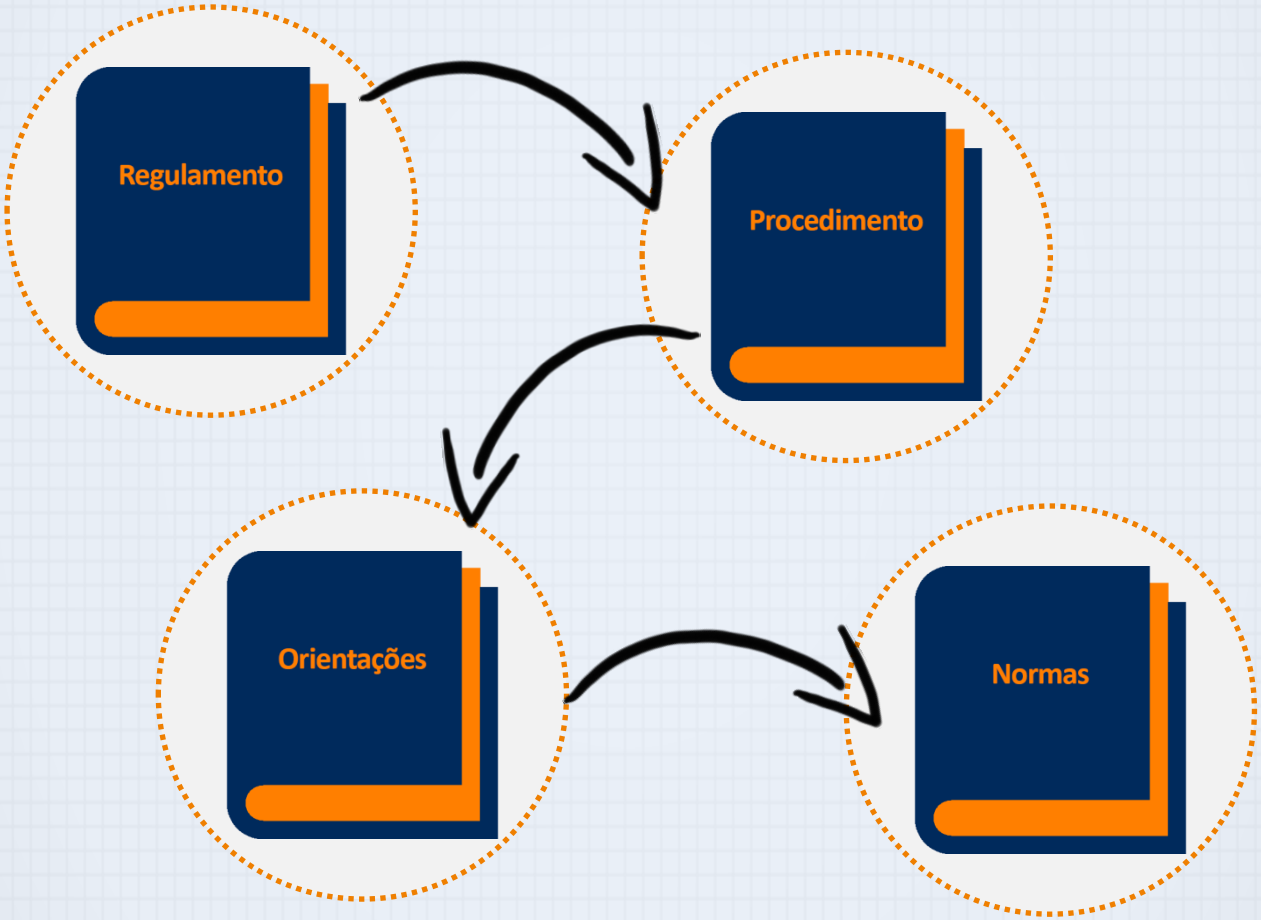
Política de Segurança da Informação

A Política de Segurança da Informação deve ser aprovada pelo conselho administrativo e publicada à todos os interessados e envolvidos.

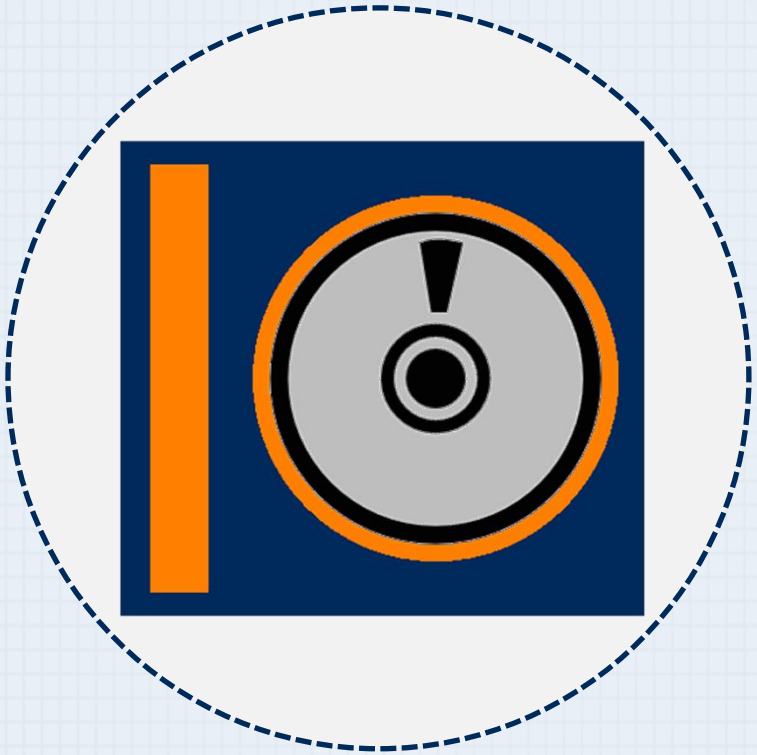
Pode ser incluída no processo de admissão de um funcionário.

Mantido na Intranet, por exemplo.

Hierarquia



Exemplo

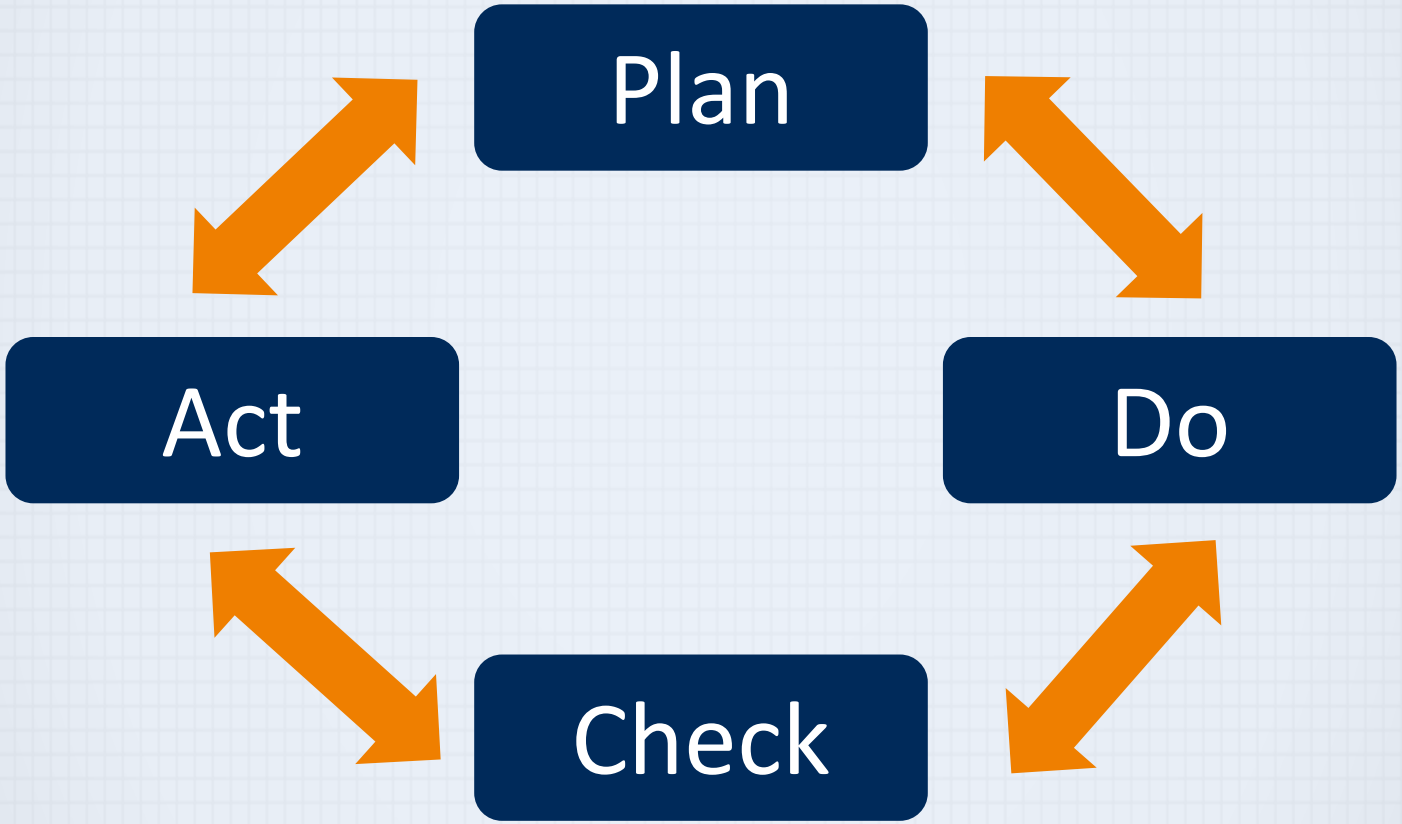


O Grupo Virgin Richard Branson, perdeu um **CD** contendo o nome de 3.000 clientes

Avaliando a Política de SI

- Ter uma Política é uma coisa, cumpri-la é outra.
- Uma Política contém: Procedimento, Política de Documento, Diretrizes, etc.
- Parte de um ISMS (Information Security Management System)

Modelo PDCA



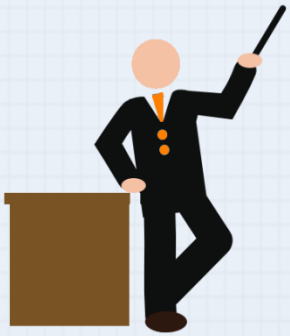
Os 18 domínios do ISO/IEC 27002:2013

- 0 - Introdução
- 1 – Escopo
- 2 -Referências Normativas
- 3 – Termos e Definições
- 4 – Estrutura da Norma
- 5 - Políticas de Segurança da Informação
- 6 – Segurança da Informação Organizacional
- 7 – Segurança de Recursos Humanos
- 8 – Gerenciamento de Ativos
- 9 – Controle de Acesso
- 10 - Criptografia
- 11 – Segurança Ambiental e Física
- 12 – Segurança Operacional
- 13 – Segurança da Comunicação
- 14 – Manutenção, Desenvolvimento e Aquisição de Sistemas
- 15 – Relacionamento com Fornecedores
- 16 – Gerenciamento de Incidentes de Segurança da Informação
- 17 – Aspectos de Segurança da Informação do Gerenciamento de Continuidade de Negócio
- 18 - Conformidade

Segurança dos Recursos Humanos

- Responsabilidades
- Contrato e Código de Conduta

Antes



Durante

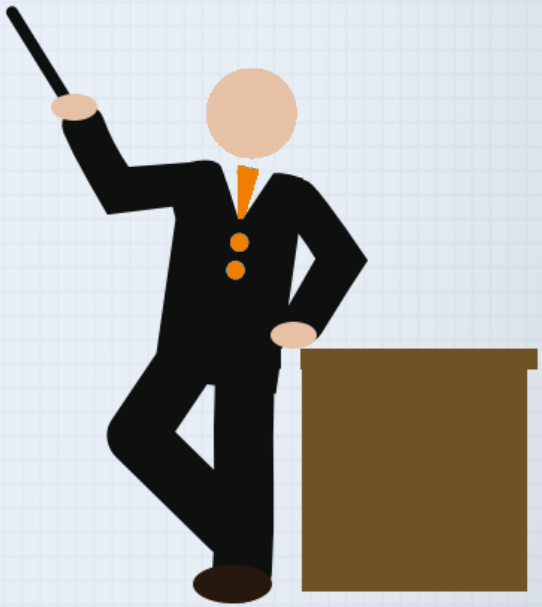
Depois

Acompanhamento da política de SI

A política de segurança da informação é avaliada periodicamente e, se necessário, modificada. Para qualquer alteração na política deve se ter a permissão do conselho administrativo da empresa.

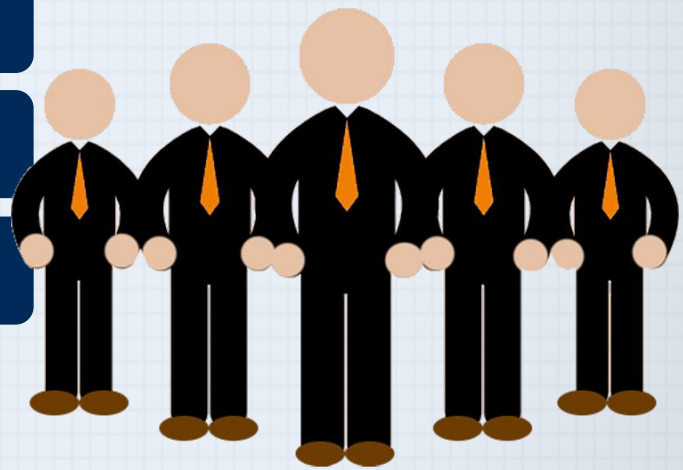
A Organização da Segurança da Informação

- Devem ser aceitos por todos
- Alta Direção devem dar exemplo
- Depende da natureza da empresa
- Definição de responsabilidades

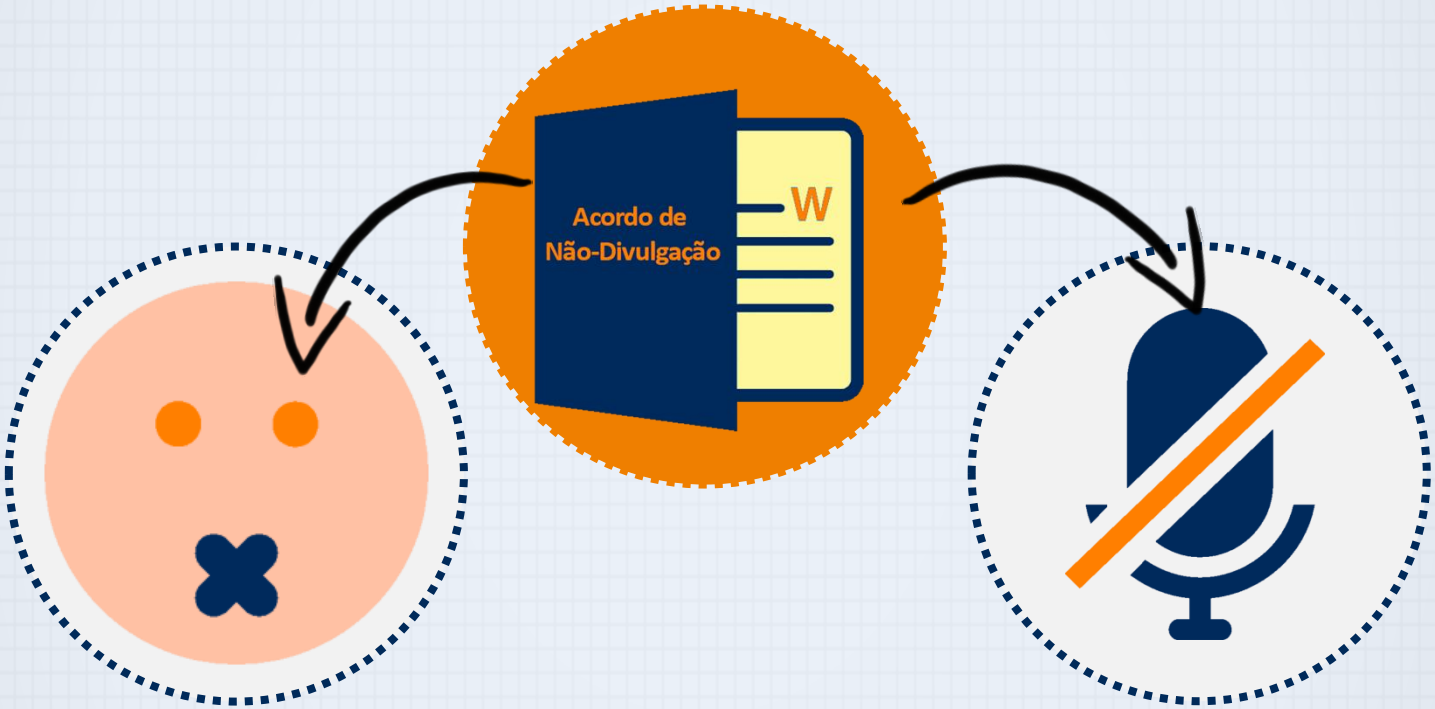


Pessoal

- Patrimônio da empresa
- Todos são responsáveis pela empresa
- Conhecimento do código de conduta
- Definição de responsabilidades
- Penalidade e sanções frente à um incidente
- Rigorosos procedimentos de desligamento



Acordo de Não-Divulgação



Trabalhos que exigem confidencialidade, exige-se um NDA assinado

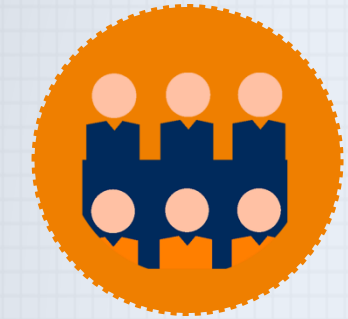
Contratantes

Os acordos escritos com o fornecedor, como uma agência de recrutamento, devem incluir sanções em caso de violações.

Arquivos Pessoais

Dados como acordos assinados, declarações, perfil do cargo, contrato de trabalho, NDA, etc.

Conscientização da Segurança



Sensibilização

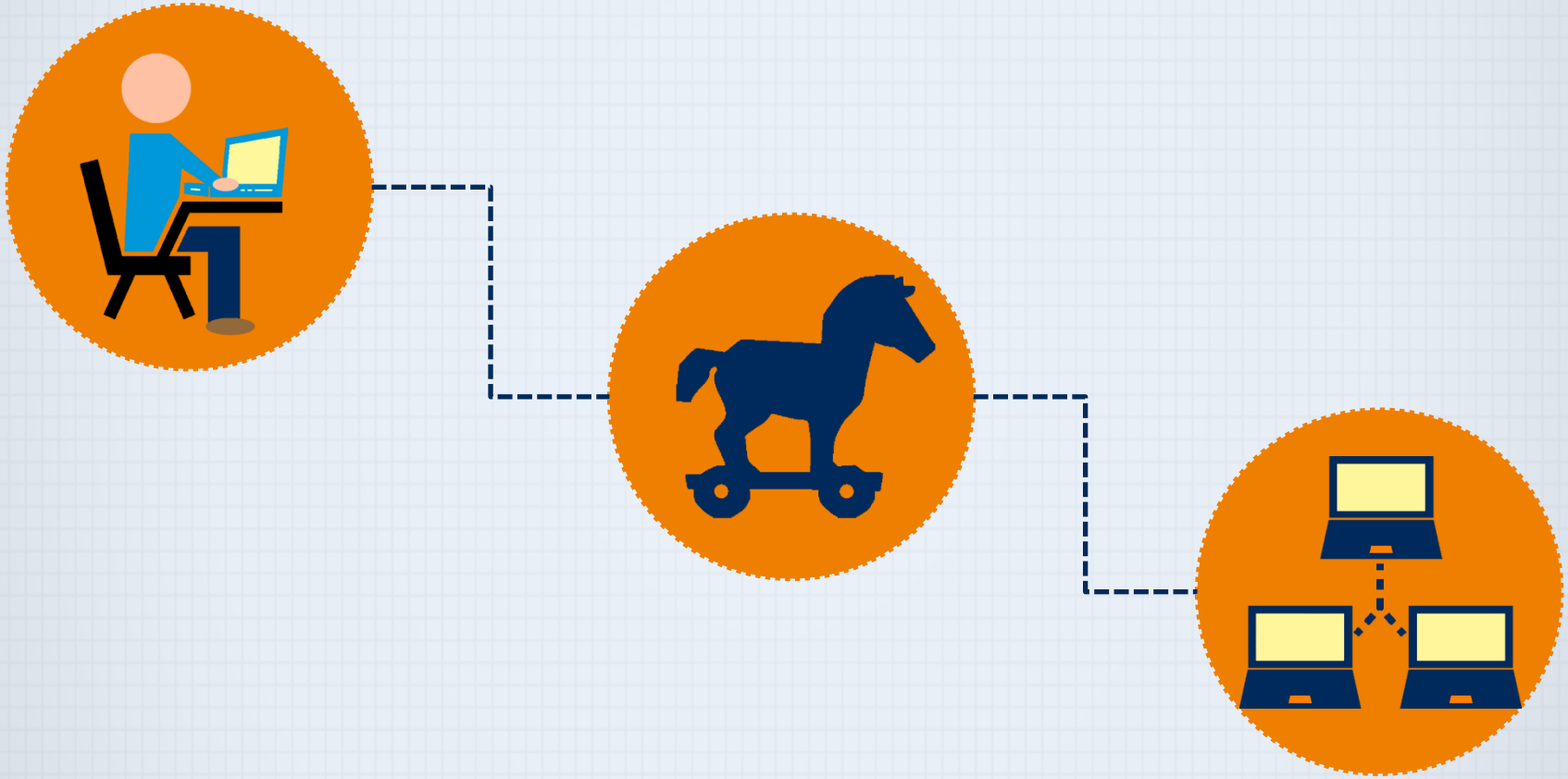
Cursos

Documentação

Conscientes

Proteção contra Engenharia Social

Exemplo



Acesso

- Uso obrigatório de um crachá
- Registro de entrada e saída
- Visitantes são monitorados desde a recepção

Gerenciamento de Continuidade de Negócio

BPC – Business Continuity Planning

DRP – Disaster Recovery Planning

Continuidade

Continuidade diz respeito à disponibilidade dos sistemas de informação no momento em que eles são necessários.

O que são Desastres?

- Placa de rede com defeito
- Uma inundação
- Falha em um sistema
- Falha de energia

Plano de evacuação

Alerta contra bomba

DRP

- DRP – Disaster Recovery Planning

DRP: Existe agora um desastre e tenho que voltar a trabalhar;

BCP: Nós tivemos um desastre e tenho que voltar à situação de como era antes do desastre.

Exemplo

Locais Alternativos

Local Alternativo

- Site Redundante: Para empresas que tem diversas localidades e um único Data Center
- Hot Site sob demanda: Site Móvel

Ações e Considerações

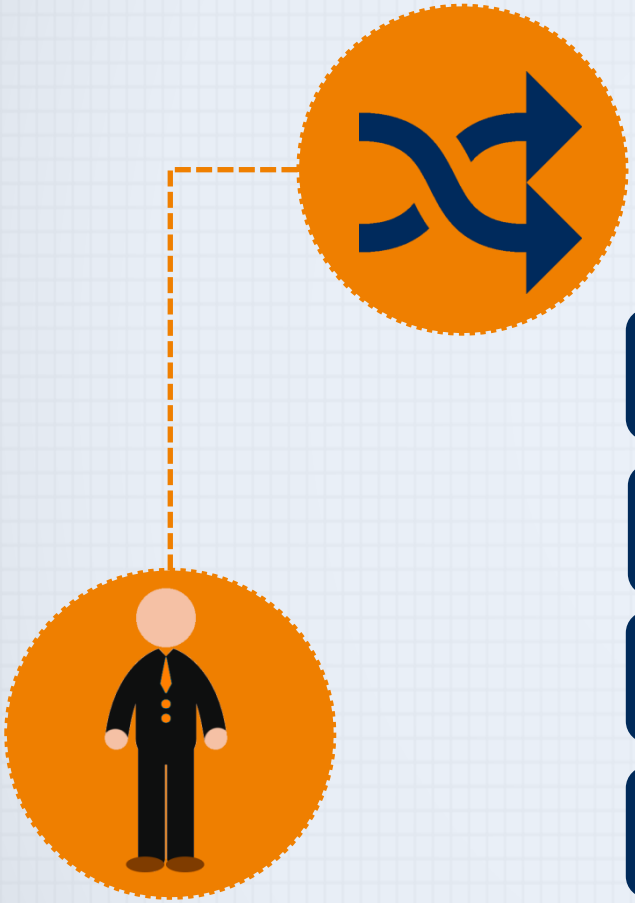
- Teste o BCP, já que as catástrofes não acontecem só com os outros
- Mudanças nos processo de negócios devem refletir no BCP
- Pessoas são ativos da empresa, consequentemente podem não estar mais disponíveis após um desastre

Gerenciando a Comunicação e os Processos Operacionais

A fim de manter uma gestão e um controle eficaz da TI, é importante documentar os procedimentos para o funcionamento dos equipamentos

Objetivo do processo é certificar que não haverá mal entendido quanto a maneira em que o equipamento tem que ser operado

Gestão de Mudanças



- Planejar antecipadamente
- Cada mudança tem uma consequência
- Definida como pequena, média e grande mudança
- Segregue as funções

Segregação de Funções

Tarefas e responsabilidades devem ser separadas para evitar que alterações não autorizadas sejam executadas e alterações não intencionais ou evitar o uso indevido de ativos da organização

Revisão deve ser realizada

Determine o acesso à informação

Tarefas são divididas

Segregue as funções

Desenvolvimento, Teste, Homologação e Produção

Ambientes para cada finalidade

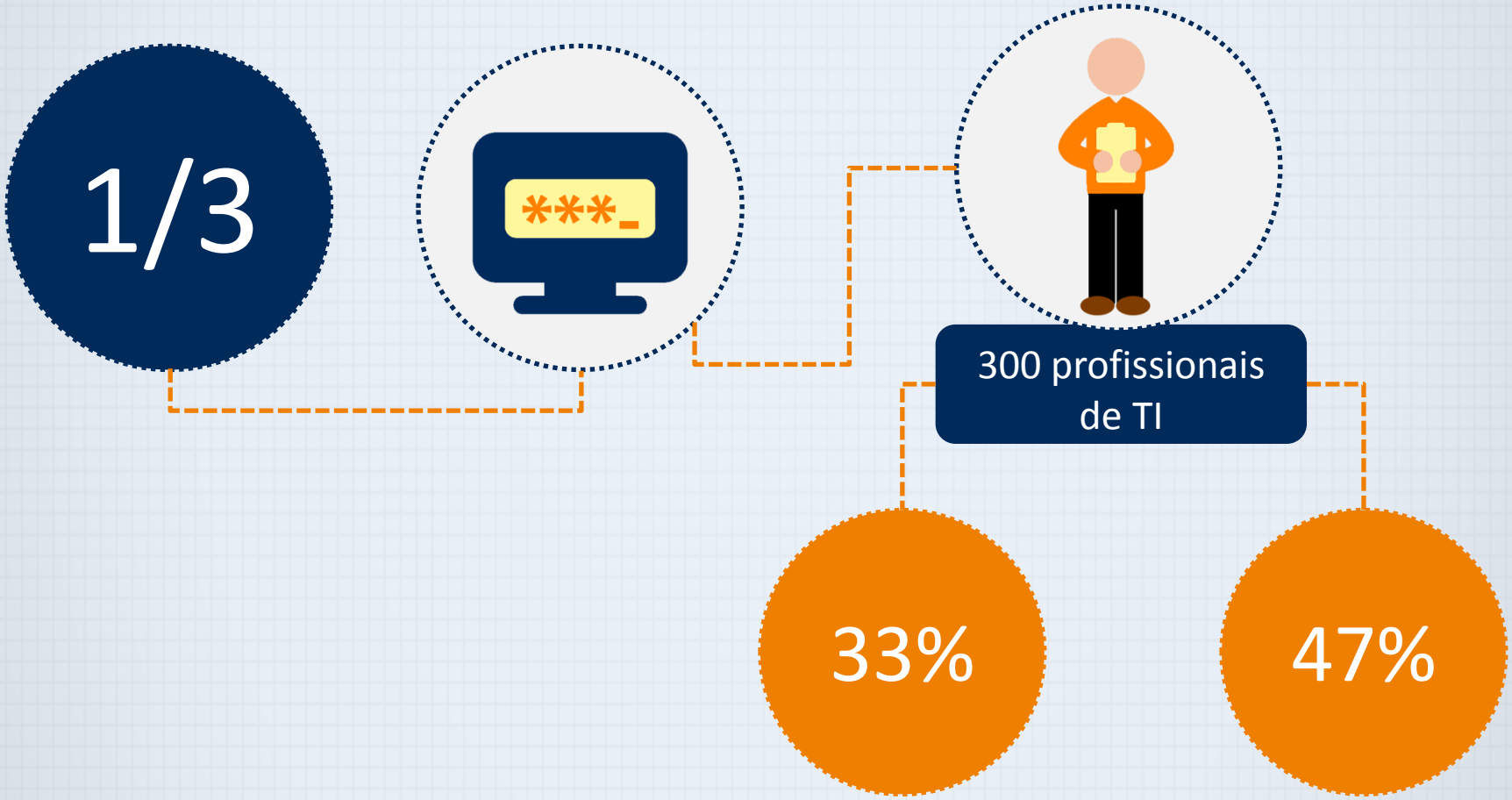
Exemplo

Gestão de Serviços de Terceiros

Nem todas as atividades importantes são feitas internamente

- Elaborar um bom contrato
- Estabeleça um SLA
- Valide através de uma auditoria

Exemplo



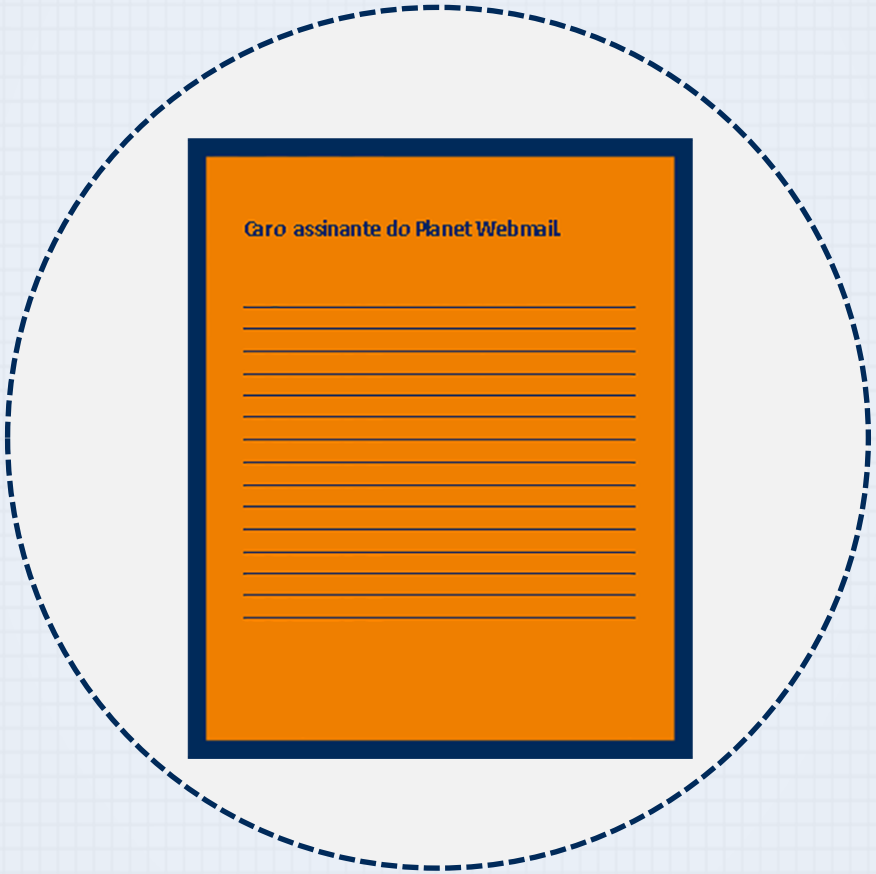
Proteção contra Phishing, Malware e Spam

Malware é uma combinação de palavras suspeitas e programas indesejáveis, tais como vírus, worms, trojans e spyware.

Spam é um nome coletivo para mensagens indesejadas

Phishing é uma forma de fraude na internet onde a vítima recebe um e-mail pedindo-lhe para verificar ou confirmar seus dados bancários

Exemplo



Exemplo

Exemplo

Exemplo

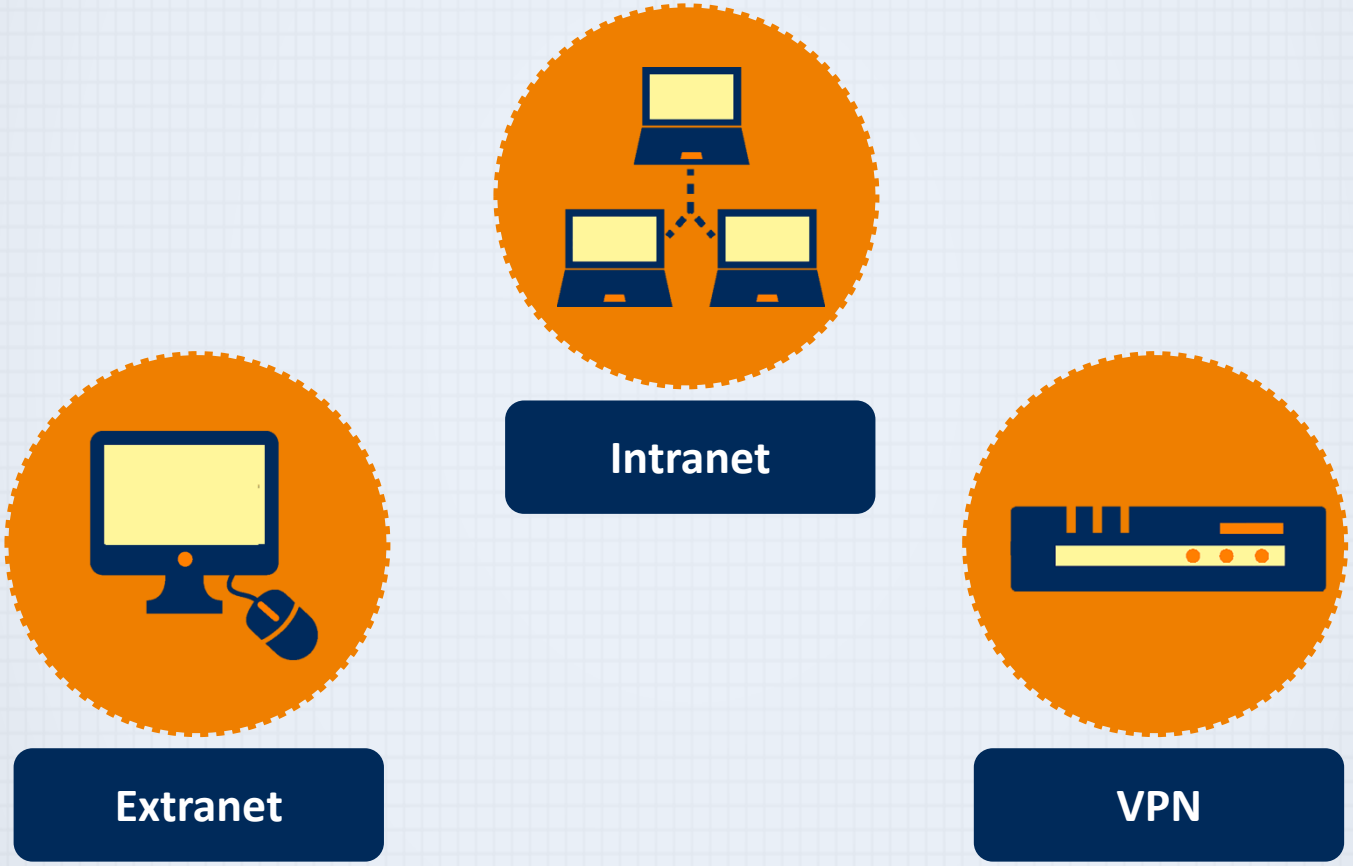
Internet Banking

Nederlandse Vereniging van Banken

Backup e Restore

- Estabeleça regularidade
- Teste
- Atendimento aos requisitos
- Armazene

Gerenciamento de Segurança de Rede



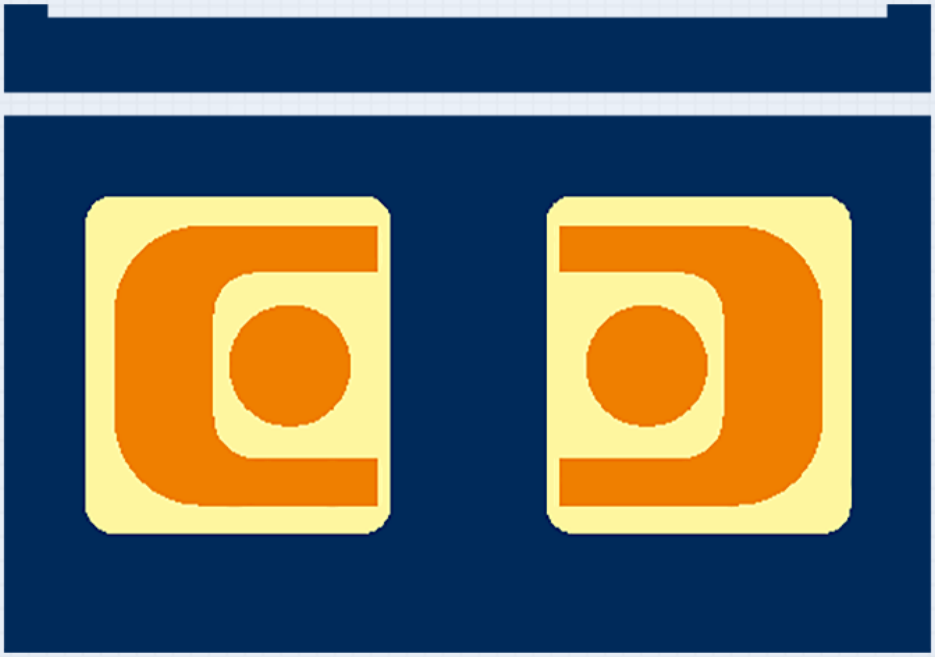
Exemplo

Exemplo

Manuseio de Mídia

- Publicação não autorizada
- Alteração
- Deleção ou destruição
- Interrupção das atividades empresariais

Exemplo



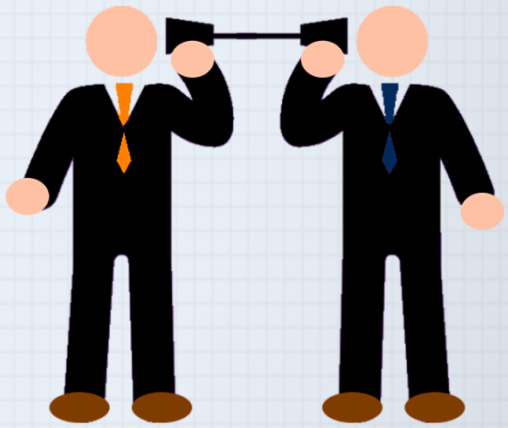
Equipamento Móvel

Eles são mais do que apenas um hardware, eles também contêm software e dados. Muitos incidentes ocorrem envolvendo equipamentos móveis.

Os procedimentos devem ser desenvolvidos para o armazenamento e manuseio de informações, a fim de protegê-lo contra a publicação não autorizada ou o uso indevido. O melhor método para isso é a classificação ou graduação

Troca de Informação

- Fazer acordos internos e externos
- Expectativas claramente documentadas
- Cuidados com as Mensagens Eletrônicas
- Cuidados com os Sistemas de Informações Empresariais



Exemplo

Serviços para e-commerce

- Proteção extra
- Confidencialidade e Integridade

Exemplo

Informações Publicamente Disponíveis

Corretas, íntegras e seguras

De empresas privadas e públicas

Resumo

- Política de Segurança
- Os domínios da ISO/IEC
- Pessoal e Segregação de Funções
- NDA
- Continuidade de Negócio (DRP e BCP)
- Gerenciamento de Mudanças
- Gerenciamento de Comunicação
- Vírus, Malware, Phishing, Rootkit, Botnets, Spyware, Logic Bomb, Hoax, Trojan e Worm
- Gerenciamento de Segurança

Teste

Pronto para o próximo?

Clique acima em
“Sair da Atividade”

Treinamento ISO 27002 Foundation

Área de Aprendizagem

www.pmgacademy.com

Official Course

Módulo 8

Legislação e Regulamentações

O que veremos neste módulo?

- Observância dos Regulamentos Legais
- Conformidade
- Direitos de Propriedade Intelectual
- Proteger documentos comerciais
- Confidencialidade
- Prevenção do uso indevido
- Política e Padrões de Segurança
- Medidas de Controle e Auditoria

Introdução

A legislação abrange as áreas de tributação, contabilidade, privacidade, financeiro e regulamentação para os bancos e empresas.

Observância dos regulamentos legais

Cada empresa, deve observar a legislação local, regulamentos e obrigações contratuais, principalmente, onde serão executadas as operações comerciais, ou seja, em outros paises.

Exigências legais podem variar bastante, particularmente na área da privacidade e, portanto, a maneira que se lidará com a informação, que pode ser privada e diferente.

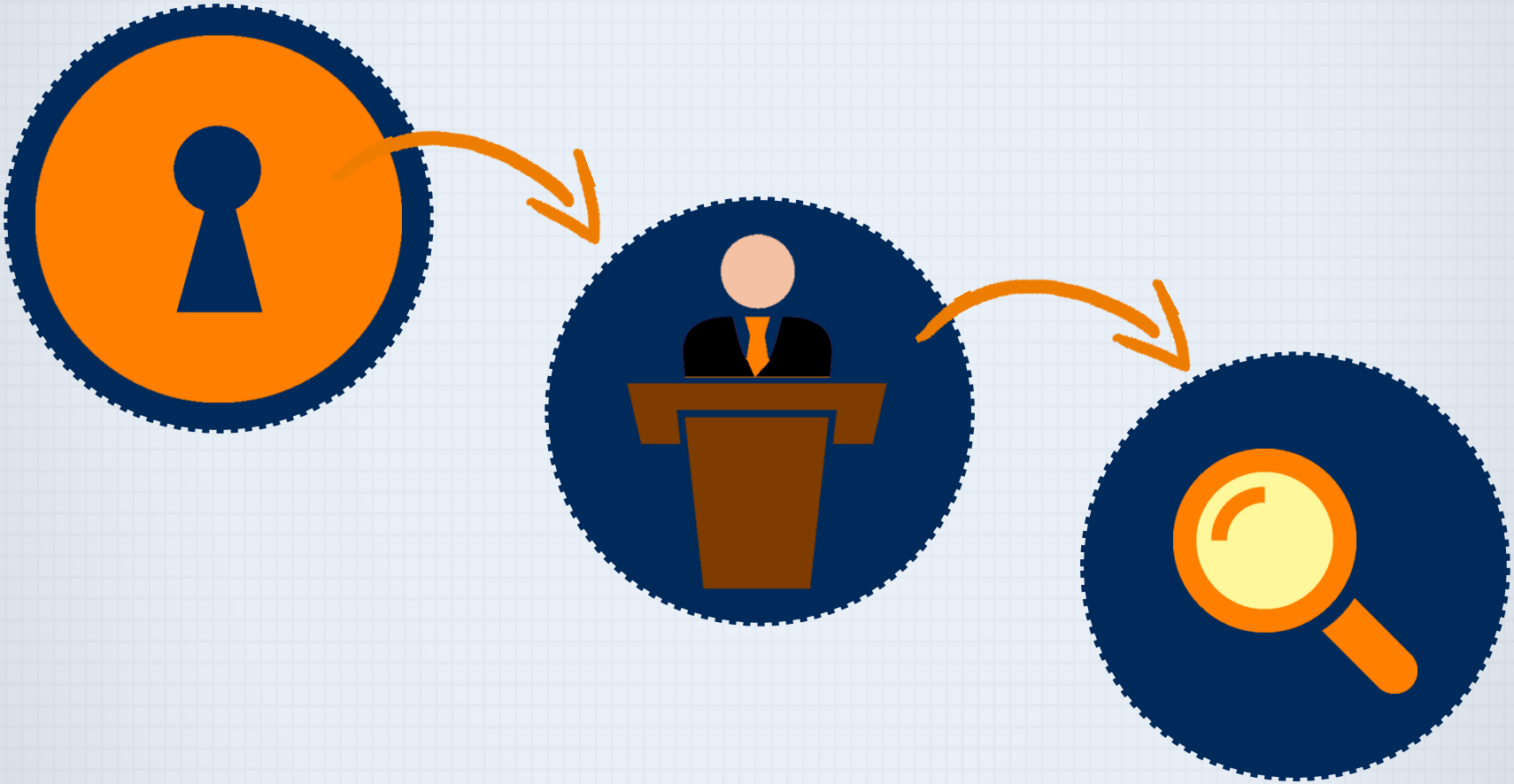
Conformidade

- Obrigatoriedade
- Rastreabilidade
- Tolerância
- Flexibilidade
- Dedicação

Padrão internacionalmente aceito

ISO/IEC 27002:2013

Exemplo



Medidas para a Conformidade

- Política Interna contendo as legislações e as regulamentações nacionais
- Procedimentos para aplicação prática
- Análise de Riscos para assegurar os níveis de segurança

Direitos de Propriedades Intelectuais

- Publicar uma Política
- Conscientização e inclusão do DPI à Política
- Incluir os direitos de Uso
- Comprar softwares de fornecedores idôneos
- Respeitar a forma de licenciamento de código aberto
- Identificar e manter registro dos ativos
- Mantenha as licenças de uso dos programas

Exemplo

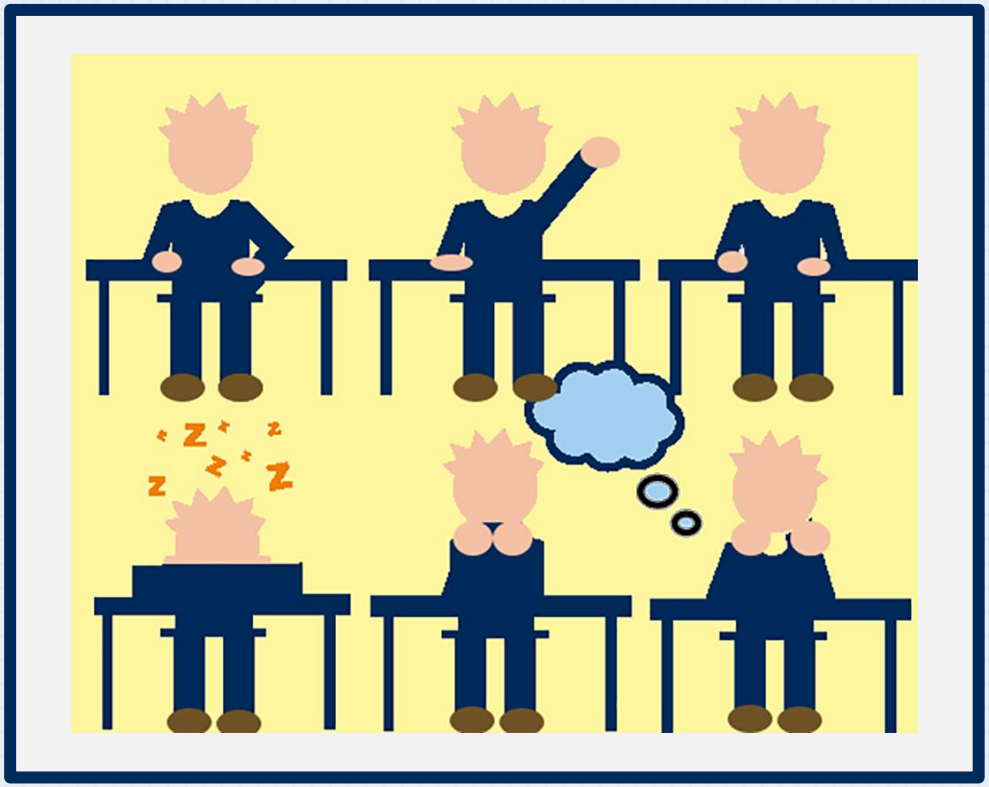
Proteção de Documentos Empresariais

- Documentos precisam ser protegidos contra perda, destruição e falsificação
- Os registros devem ser classificados de acordo com o tipo
- Prazo e meios de armazenamentos devem ser determinados
- Considere a perda de qualidade do armazenamento ao longo do tempo
- Estabeleça procedimentos para evitar a perda de informações

Confidencialidade

- Sob uma legislação
- Política de proteção
- Nomeação de um responsável
- Medidas técnicas de proteção

Exemplo



Prevenção do uso indevido dos recursos de TI

- Como os recursos são utilizados
- Monitore o uso
- Cumpra os regulamentos
- Código de conduta
- Veja a legislação do país

Exemplo

Política e Padrões de Segurança

Conselho Administrativo

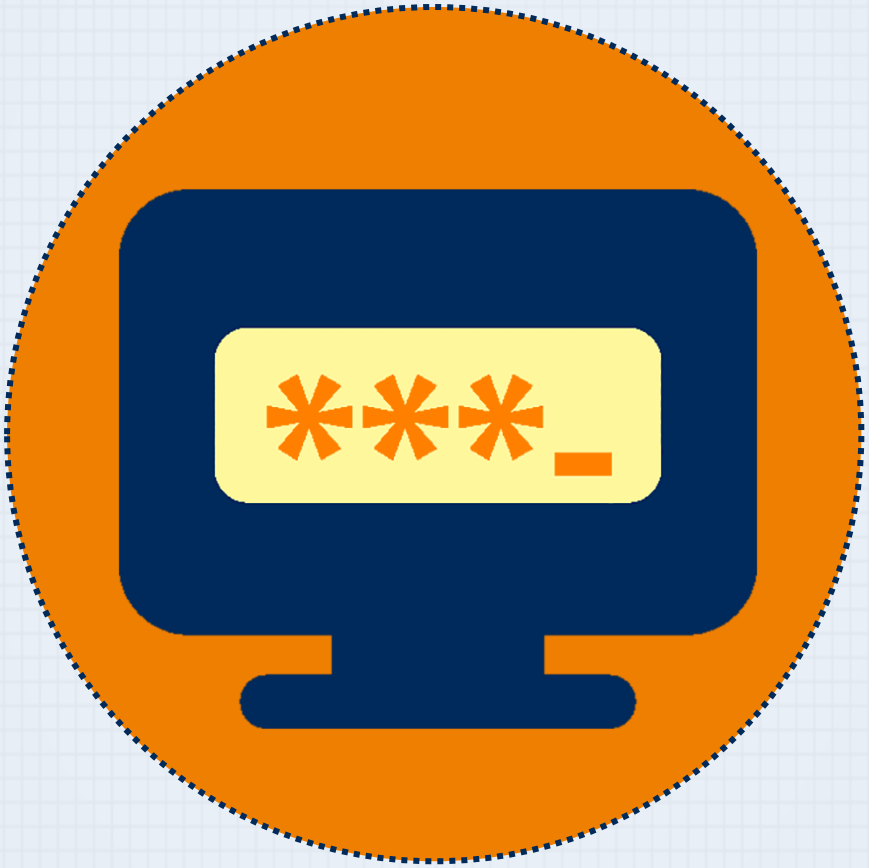
Gerentes Funcionais

Operacional

Medidas de Controle e Auditoria

- Está incluído na política?
- É observado na prática?
- Será que a medição esta sendo feita?

Exemplo



Auditoria de Sistema da Informação

- Envolve riscos
- Afeta a capacidade
- Cuidados com o exame de um item por duas pessoas destintas
- Emissão de notificação de auditoria

Proteção auxiliar utilizando os Sistemas de Informação

- Medidas de segurança são válidas também para os auditores

Não importa
como uma organização planejou a sua segurança, a segurança é tão forte quanto o elo mais fraco!

Resumo

- Observância dos Regulamentos Legais
- Conformidade
- Direitos de Propriedade Intelectual
- Proteger Documentos Comerciais
- Confidencialidade
- Prevenção do Uso Indevido
- Políticas e Padrões de Segurança
- Medidas de Controle
- Auditoria

Teste

Pronto para o próximo?

Clique acima em
“Sair da Atividade”