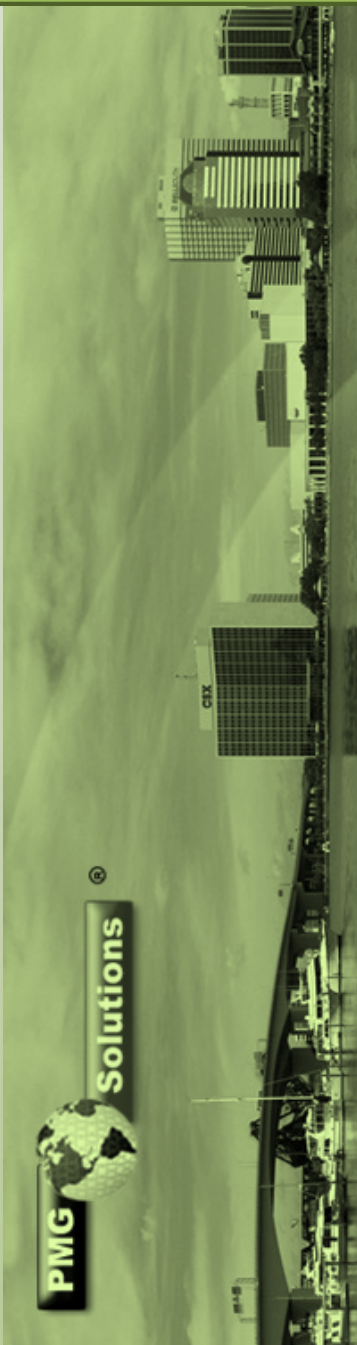


Versão Português  
(Brasil)



FUNDAMENTOS

# ISO/IEC 27002



*Da Teoria à Prática*



## Nota

ESTE DOCUMENTO CONTÉM INFORMAÇÕES PROPRIETÁRIAS, PROTEGIDAS POR COPYRIGHT. TODOS OS DIREITOS RESERVADOS. NENHUMA PARTE DESTE DOCUMENTO PODE SER FOTOCOPIADA, REPRODUZIDA OU TRADUZIDA PARA OUTRO IDIOMA SEM CONSENTIMENTO DA PMG SOLUTIONS CONSULTORIA E TREINAMENTO LTDA, BRASIL.

© Copyright 2010 - 2011, PMG Solutions

[www.pmg solutions.com.br](http://www.pmg solutions.com.br)

Código: T2011ISO27002

Versão 3.2.0



## Conteúdo

1.	INTRODUÇÃO .....	7
1.1.	Visão Geral.....	8
1.2.	Propósito do Curso .....	9
1.3.	Público Alvo .....	9
1.4.	Pré-Requisitos.....	10
1.5.	Detalhes do exame .....	10
1.6.	Introdução à Segurança da Informação .....	11
2.	INFORMAÇÃO, OBJETIVOS DE NEGÓCIOS E REQUISITOS DE QUALIDADE .....	13
2.1.	Introdução .....	16
2.2.	Formas .....	17
2.3.	Sistema da Informação.....	18
2.4.	Valor da Informação .....	21
2.5.	Informação como fator de produção .....	23
2.6.	Disponibilidade, Integridade e Confiabilidade .....	24
2.7.	Arquitetura da Informação.....	32
2.8.	Análise da Informação .....	34
2.9.	Gestão da Informação .....	37
3.	AMEAÇAS E RISCOS.....	<b>Erro! Indicador não definido.</b>
3.1.	Introdução .....	<b>Erro! Indicador não definido.</b>
3.2.	Na prática .....	<b>Erro! Indicador não definido.</b>
3.3.	Gerenciamento de Riscos.....	<b>Erro! Indicador não definido.</b>
3.4.	Análise de Riscos .....	<b>Erro! Indicador não definido.</b>
3.5.	Tipo de Análise de Riscos: Quantitativo .....	<b>Erro! Indicador não definido.</b>
3.6.	Tipo de Análise de Riscos: Qualitativo .....	<b>Erro! Indicador não definido.</b>
3.7.	Medidas de Redução de Riscos .....	<b>Erro! Indicador não definido.</b>
3.8.	Tipos de Medidas de Segurança.....	<b>Erro! Indicador não definido.</b>
3.9.	Tipos de Ameaças.....	<b>Erro! Indicador não definido.</b>
3.10.	Tipos de Danos .....	<b>Erro! Indicador não definido.</b>
3.11.	Tipos de Estratégia de Risco .....	<b>Erro! Indicador não definido.</b>
3.12.	Diretrizes para implementar medidas de segurança .....	<b>Erro! Indicador não definido.</b>
4.	ATIVOS DE NEGÓCIOS E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	<b>Erro! Indicador não definido.</b>
4.1.	Introdução .....	<b>Erro! Indicador não definido.</b>
4.2.	Quais são os ativos da empresa .....	<b>Erro! Indicador não definido.</b>
4.4.	Classificação .....	<b>Erro! Indicador não definido.</b>
4.5.	Gerenciamento de Incidentes de Segurança .....	<b>Erro! Indicador não definido.</b>
4.6.	Ciclo do Incidente .....	<b>Erro! Indicador não definido.</b>
4.7.	Papéis .....	<b>Erro! Indicador não definido.</b>
5.	MEDIDAS FÍSICAS .....	<b>Erro! Indicador não definido.</b>
5.1.	Introdução .....	<b>Erro! Indicador não definido.</b>
5.2.	Segurança Física .....	<b>Erro! Indicador não definido.</b>
5.3.	Equipamento .....	<b>Erro! Indicador não definido.</b>
5.4.	Cabeamento .....	<b>Erro! Indicador não definido.</b>

5.5. Mídia de Armazenamento.....	<b>Erro! Indicador não definido.</b>
5.6. Anéis de Proteção.....	<b>Erro! Indicador não definido.</b>
5.7. Alarmes.....	<b>Erro! Indicador não definido.</b>
5.8. Proteção contra Incêndio .....	<b>Erro! Indicador não definido.</b>
5.9. Sinalização e Agente Extintores .....	<b>Erro! Indicador não definido.</b>
6. MEDIDAS TÉCNICAS (SEGURANÇA DE TI) .....	<b>Erro! Indicador não definido.</b>
6.1. Introdução .....	<b>Erro! Indicador não definido.</b>
6.2. Gerenciamento Lógico de Acesso .....	<b>Erro! Indicador não definido.</b>
6.3. Requisitos de Segurança para Sistemas de Informação .....	<b>Erro! Indicador não definido.</b>
6.4. Processamento Correto das Aplicações .....	<b>Erro! Indicador não definido.</b>
6.5. Criptografia.....	<b>Erro! Indicador não definido.</b>
6.6. A Política da Criptografia .....	<b>Erro! Indicador não definido.</b>
6.7. Tipo de Sistemas de Criptografia.....	<b>Erro! Indicador não definido.</b>
6.8. Segurança do Sistema de Arquivos .....	<b>Erro! Indicador não definido.</b>
6.9. Vazamento de Informações .....	<b>Erro! Indicador não definido.</b>
7. MEDIDAS ORGANIZACIONAIS .....	<b>Erro! Indicador não definido.</b>
7.1. Introdução .....	<b>Erro! Indicador não definido.</b>
7.2. Política de Segurança .....	<b>Erro! Indicador não definido.</b>
7.3. Pessoal.....	<b>Erro! Indicador não definido.</b>
7.4. Gerenciamento de Continuidade de Negócio.....	<b>Erro! Indicador não definido.</b>
7.5. Gerenciando a Comunicação e os Processos Operacionais .....	<b>Erro! Indicador não definido.</b>
8. LEGISLAÇÃO E REGULAMENTOS .....	<b>Erro! Indicador não definido.</b>
8.1. Introdução .....	<b>Erro! Indicador não definido.</b>
8.2. Observância dos regulamentos legais.....	<b>Erro! Indicador não definido.</b>
8.3. Conformidade.....	<b>Erro! Indicador não definido.</b>
8.4. Direitos de Propriedades Intelectuais (DPI) .....	<b>Erro! Indicador não definido.</b>
8.5. Proteção de Documentos Empresariais .....	<b>Erro! Indicador não definido.</b>
8.6. Confidencialidade .....	<b>Erro! Indicador não definido.</b>
8.7. Prevenção do uso indevido dos recursos de TI .....	<b>Erro! Indicador não definido.</b>
8.8. Política e Padrões de Segurança .....	<b>Erro! Indicador não definido.</b>
8.9. Medidas de Controle .....	<b>Erro! Indicador não definido.</b>

1.

# INTRODUÇÃO

## 1.1. Visão Geral

A palavra segurança tem por natureza um sentido negativo, afinal, só se aplica quando houver esta razão: quando houver um risco de que as coisas não estão como deveriam.

A segurança tem, portanto, tudo a ver com a proteção. Algo que tem sido feito para reduzir a chance de problemas ou minimizar as consequências. Um pneu sobressalente, pijamas das crianças à prova de fogo e políticas de seguros, são todas as formas de segurança. Um pneu sobressalente assegura que ficaremos menos preocupados com um pneu furado, a apólice de seguro cobre as consequências financeiras e os pijamas contra fogo reduzirá o risco de graves danos físicos a uma criança.

A informação tornou-se uma mercadoria valiosa na nossa sociedade e podemos ver isso mais claramente se percebermos que um processo de negócio não pode ser realizado sem informações. Afinal, o controle dos processos é sempre baseado nas informações dos gerentes. Muitas empresas não fazem mais nada, mas processam a informação, particularmente no caso do setor financeiro e do governo. O setor de serviços empresariais não faz mais do que coletar informações e, em seguida, apresentá-lo de outra forma.

Informações ainda desempenham um papel importante no nosso tempo livre, como músicas, livros e filmes em formato digital (MP3, CD, DVD), a Internet e todos os jogos fazem uso da informação digital. O explosivo crescimento de câmeras digitais, bem como telefones celulares, resultou em um número inestimável de fotos que são armazenadas em discos rígidos, tocadores portáteis, CDs, DVDs e pendrives. Assim, não é de se estranhar que nos últimos dez anos o tema da segurança da informação tornou-se interessante para as empresas e o governo.

Este curso tratará do tema de segurança da informação de uma maneira simples e clara. Os módulos foram organizados de modo em que as pessoas que não são técnicas ou especialistas compreendam, inclusive, as medidas técnicas.

Há uma conexão entre risco e segurança: se não houvesse nenhum risco, não haveria necessidade de criação de qualquer segurança, e isso, custa tempo e dinheiro, e assim, se pode evitá-los, nós o faremos.

O tipo e o número de medidas que são tomadas dependem do risco. Após a introdução geral e uma explicação do valor da informação, o curso examinará as ameaças e os riscos. Examinando quais são os riscos e as maiores consequências que não são aceitáveis é objetivo de uma análise de risco. No campo da segurança da informação é preciso determinar as medidas que têm que ser tomadas em relação a estes riscos e ameaças. A análise também determina os argumentos para lidar com esses riscos.

Antes de discutir as medidas, o módulo 2 analisa como lidar com a segurança da informação em um organização. Temas como gestão, organização e requisitos de

qualidade são tratados. O módulo 3 examinará as ameaças e a análise de risco. Do módulo 4, em seguida, nos atentaremos aos incidentes de segurança da informação e as fraquezas. Os três módulos seguintes serão tratados sobre as medidas.

Este treinamento divide as medidas em três grupos:

- Medidas físicas, tais como bloqueios e cercas, mas também os armários e balcões de recepção;
- Medidas técnicas, como backups, software de códigos e funções de antivírus;
- Medidas Organizacionais como a segregação de funções, os acordos de confidencialidade e autorizações segundo o que é permitido para acessar.

O treinamento é, então, concluído com uma discussão sobre as regulamentações aplicáveis e da legislação. Há certas leis que impõem obrigações estatutárias para realizar medidas de segurança, por exemplo, a legislação de proteção de dados, que estabelece requisitos para a proteção da privacidade pessoal.

## 1.2. Propósito do Curso

Segurança da Informação tem se tornado cada vez mais importante.

A globalização da economia conduz a um crescente intercâmbio de informações entre as organizações (seus funcionários, clientes e fornecedores) e uma utilização crescente de redes, tais como a rede interna da empresa, a conexão com as redes de outras empresas e da Internet. Além disso, as atividades de muitas companhias se baseiam em TI e a informação tornou-se um ativo valioso. Proteção da informação é crucial para a continuidade e o bom funcionamento da organização: a informação deve ser confiável. No módulo de Fundamentos da Segurança da Informação baseados na norma ISO/IEC 27002 (ISFS), os conceitos básicos de segurança da informação e sua coerência serão tratados.

## 1.3. Público Alvo

Qualquer pessoa na organização que manuseia informações.

Este curso é destinado a todos em uma organização que deseja ter uma compreensão básica e, esses conhecimentos são importantes para todo o pessoal em uma empresa ou governo, já que todos trabalham com informação. Os gerentes funcionais precisam ter esta compreensão já questão responsável pela segurança das informações em seu departamento. Esse conhecimento é fundamental também para todas as pessoas das áreas de negócios, incluindo os trabalhadores por conta própria sem empregados, pois são responsáveis por proteger suas próprias informações. E, claro, este conhecimento constitui uma boa base para aqueles que consideram uma carreira como um especialista

em segurança da informação, seja como um profissional de TI ou um gerente de processo.

É também aplicável a proprietários de pequenas empresas, pois contém alguns conceitos básicos de Segurança da Informação que são extremamente necessários. Este curso pode ser um excelente ponto de partida para novos profissionais de segurança da informação.

#### 1.4. Pré-Requisitos

Não existem pré-requisitos para este curso e para exame de certificação do ISO/IEC 27002

#### 1.5. Detalhes do exame

- Tipo de exame: Múltipla escolha em computador ou impresso em papel
- Tempo destinado ao exame: 60 minutos
- Número de questões: 40
- Mínimo para aprovação: 65 % (26 de 40)
- Com consulta: não
- Equipamentos eletrônicos Permitidos: Não

#### 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 Segurança Físicas
  - 10% - Medidas de Segurança Técnica
  - 10% - Medidas Organizacionais
- 10% - Legislação e Regulamentações

## 1.6. Introdução à Segurança da Informação

Este treinamento dá uma visão geral da segurança da informação.

A segurança da informação é a disciplina que concentra na qualidade (confiabilidade) da prestação de informações e no gerenciamento da continuidade das operações. Qualidade neste contexto entende-se como a disponibilidade, confidencialidade e integridade da informação. Este curso ensinará o que estes requisitos de qualidade implicam como eles podem ser determinados e o que é necessário para garanti-los em uma organização. Esta área engloba o trabalho de especialista em segurança da informação. As pessoas que desempenham um papel aqui são discutidas em mais detalhes nos módulos pertinentes. Cada módulo irá explicar os assuntos específicos por meio de casos a partir de práticas diárias. Esses casos serão tão genéricos quanto possível e não específicos para um determinado tipo de organização.

Depois deste curso você terá uma compreensão geral dos assuntos que englobam a segurança da informação e saberá por que esse tema é tão relevante.

Cada um de nós em nossa vida diária está envolvido com a segurança da informação, muitas vezes sob a forma de medidas, que são por vezes aplicadas conosco e às vezes implementados por nós mesmos. Considere, por exemplo, o uso de uma senha no computador. Muitas vezes essas medidas tornam-se um incômodo, pois tomam o nosso tempo e mal sabemos o que estão protegendo.

O truque para execução da segurança da informação é equilibrar uma série de aspectos:

- 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.

O objetivo principal deste curso é a educação e é por isso que cada módulo tem diversos exemplos de casos reais e os eventos recentes que ilustram a vulnerabilidade das informações. Não é nossa intenção assustá-lo com estes eventos, mas sim torná-lo consciente. Devido ao seu caráter geral, este curso serve também para a formação de uma conscientização interna na empresa. Neste curso temos a tendência de falar sobre as grandes organizações, mas os assuntos abordados são também aplicáveis aos ambientes domésticos, bem como pequenas organizações e empresas que não tenha nenhum departamento de segurança que, em tais situações, as funções de segurança são realizadas por uma única pessoa.



# 2.

**INFORMAÇÃO, OBJETIVOS  
DE NEGÓCIOS 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



Garantia de  
Proteção aos Dados



Dados  
≠  
Informações



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



## Informação, Objetivos de Negócios e Requisitos de Qualidade



### 2.1. Introdução

Segurança da Informação diz respeito à garantia da proteção de dados. Lembrando que dados por si só, são apenas códigos, sem significado algum, já a informação, é uma coleção de dados devidamente tratados que representam algum significado lógico.

Exemplo: Zona Norte, Inglês fluente, R\$ 5 mil, Consultor. Esses dados isolados, não representam nada, mas como são dados de um currículo, tornam-se informações essenciais para uma tomada de decisão, como por exemplo, na contratação de um profissional.

Apesar da palavra “informação” representar diversos conceitos dentro da área de TI, nós alinharemos a definição segundo o dicionário Aurélio: “Ação de informar ou informar-se. / Notícia recebida ou comunicada; informe. / Espécie de investigação a que se procede para verificar um fato”.

De qualquer forma, segurança da informação envolve a definição, implementação, manutenção e avaliação de um sistema coerente de medidas que garantam a integridade, disponibilidade e confidencialidade de informações, sejam elas manuais ou informatizadas.

# Formas



- Imagens de vídeo
- Textos de documentos
- Palavras faladas



## Informação, Objetivos de Negócios e Requisitos de Qualidade



### 2.2. Formas

Como dito antes, para se obter um significado, os dados podem ser processados através da tecnologia da informação para tornar-se uma informação. E se utilizamos a tecnologia para esse processo de transformação, de dados para informação, significa que essas informações podem tomar-se de diversas formas.

Quando se trata da Segurança da Informação, as informações que nos deparamos em nosso dia-a-dia podem ser manifestadas de diversas formas, sejam através das imagens de um vídeo, de textos em um documento, das palavras faladas ou ouvidas de um Podcast, por exemplo.

No entanto, a segurança da informação deve ser tomada independente da sua forma, ou seja, devem-se tomar medidas de proteção ou impor restrições de acessos que sejam necessárias para proteger essas informações.

# 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



**Informação, Objetivos de Negócios e Requisitos de Qualidade**



## 2.3. Sistema da Informação

A transformação de dados em informações, incluindo a sua transferência e processamento é realizado pelos Sistemas de Informações. Esses sistemas podem ser um arquivo em um sistema, uma imagem dentro do diretório, um telefone celular e impressora.

No contexto da Segurança da Informação, um sistema de informação é toda a combinação de meios, procedimentos, regras e pessoas que asseguram o fornecimento de informações para um processo operacional.

Um dos maiores desafios da TI é a dependência que as áreas de negócios têm com a tecnologia, o quão seus negócios utilizam da TI para alavancar seus resultados, conseqüentemente, criando outro grande desafio para a TI, garantir o bom funcionamento desses sistemas através das ações da Segurança da Informação.

Como já foi dito, um sistema de TI consiste em meios tecnológicos que estão relacionados uns aos outros de alguma forma. Esses meios incluem:

- Estação de trabalho contendo sistemas operacionais e outros softwares instalados;
- Transporte de dados via rede, cabo ou via wireless;

- Servidores Centrais de aplicações ou outros sistemas e/ou softwares;
- Armazenamento de dados, por exemplo, espaço em disco, caixas postais de e-mail e bando de dados;
- Telefones, PABX e antenas.

## Exemplo



### Informação, Objetivos de Negócios e Requisitos de Qualidade



#### 2.3.1. Exemplo

A seguir, um exemplo de um risco de segurança em um sistema da informação:

Usuários de smartphones com o sistema operacional Symbian S60 estão sendo advertidos sobre os vírus Beselo. Este Worm pode se espalhar via MMS e Bluetooth. O Worm está disfarçado como o arquivo Sex.mp3, love.jpg ou beauty.rm. Como resultado, os usuários acreditam que é um arquivo multimídia e assim instalam o Worm. Após a instalação, o Worm se espalha cada vez mais. Ele também se copia no cartão de memória do telefone.

A F-Secure (provedor de segurança móvel e computador) aconselha os utilizadores a ignorar o pedido para instalação com o seguinte comunicado. "Não há nenhuma razão para uma foto solicitar a sua própria instalação."

Como vimos, há a necessidade de quebrarmos alguns paradigmas sobre sistema de informação, principalmente àqueles que acreditam que um telefone móvel não possa ser considerado um risco para a TI.

# Valor da Informação



Dados ou informações?

k a j e  
f b l v y  
c d h g m  
w x z



## Informação, Objetivos de Negócios e Requisitos de Qualidade



### 2.4. Valor da Informação

O valor é atribuído à informação segundo os seus interesses.

Para deixar mais claro esta afirmação, vamos encadear as idéias, lembrando algo que já vimos.

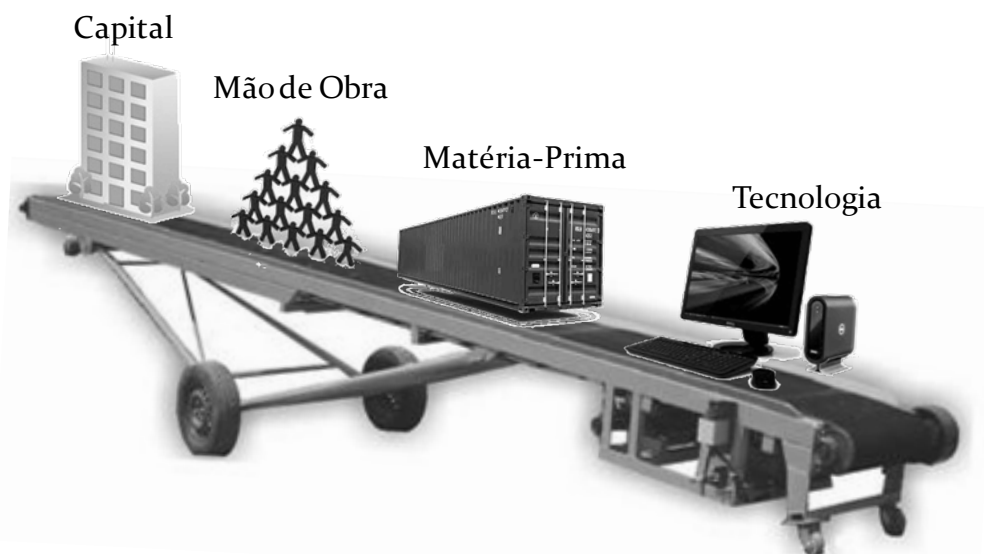
- Informação que não tem significado algum é chamado de dados;
- Informações que fazem sentido são constituídas de dados com algum significado;

Se algo é meramente um dado ou uma informação, é determinado, principalmente, pelo destinatário, ou seja, por aquele que lê, ouve ou utiliza. Enquanto algumas pessoas podem considerar um determinado conjunto de dados pouco interessante, outros podem ser capazes de extrair informações valiosas a partir destes dados. O valor da informação é, portanto, determinado pelo valor que o receptor lhe atribui.

Vamos imaginar um leigo em assunto econômicos e financeiros visualizando um painel de negociações de papéis da Bovespa em um Home Broker, com mensagens passando na tela, com visualizações de gráficos apontando para cima e outros para baixo, códigos jamais vistos, cores piscando na tela, números, indicadores, etc. Ou ainda, imaginar um painel de uma aeronave com diversos indicadores, avisos sonoros e luzes. Para quem

não conhece ou não se interessa pelo assunto, esses dados não representam nenhum valor para o receptor.

# Informação como fator de produção



## Informação, Objetivos de Negócios e Requisitos de Qualidade



### 2.5. Informação como fator de produção

Os fatores padrão da produção de uma empresa ou organização são: capital, a mão de obra e matéria-prima. A tecnologia da informação é também um grande fator de produção, já que existe uma grande dependência da TI ao negócio.

As empresas não podem existir sem a informação. Uma indústria que perde as informações do seu estoque geralmente terá muita dificuldade de continuar suas operações sem perder algum cliente, ou cair no descrédito no mercado. Algumas empresas, como um escritório de contabilidade, ainda tem informações como o seu único produto.

Consideremos também o mercado financeiro onde a informação é o principal “produto”, além da importância da disponibilidade do canal de comunicação, para obter essas informações.

# Disponibilidade, Integridade e Confiabilidade

- A importância da informação para os processos operacionais;
- A indispensabilidade das informações dentro dos processos operacionais;
- A recuperação da informação.



## Informação, Objetivos de Negócios e Requisitos de Qualidade



### 2.6. Disponibilidade, Integridade e Confiabilidade

Ao proteger o valor da informação, nós olhamos para três fatores, que são os requisitos de qualidade que a informação tem que satisfazer. A informação deve ser confiável, ou seja, ele deve ter as seguintes propriedades, conforme o chamado “CIA”:

- Confidencialidade (confidentiality)
- Integridade (integrity)
- Disponibilidade (availability)

Ao invés do termo de confidencialidade, algumas empresas podem utilizar o termo, exclusividade.

Os conselhos que são dados para o tratamento das ameaças em uma análise de risco são baseados em três pilares. O ponto de partida é a influência que os requisitos do CIA têm sobre o valor da informação:

- A importância da informação para os processos operacionais;
- A indispensabilidade das informações dentro dos processos operacionais;
- A recuperação da informação.

# 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. Não há capacidade suficiente para permitir que todos os funcionários trabalhem nos sistemas de informação.



## Informação, Objetivos de Negócios e Requisitos de Qualidade



### 2.6.1. Disponibilidade

Disponibilidade é o grau em que a informação está disponível para o usuário e para o sistema de informação que está em operação no momento que a organização requer.

As características de disponibilidade são:

- Pontualidade. Os sistemas de informação estão disponíveis quando necessários;
- Continuidade. O pessoal pode continuar a trabalhar no caso de um fracasso ou indisponibilidade;
- Robustez. Não há capacidade suficiente para permitir que todos os funcionários trabalhem nos sistemas de informação.

E agora, alguns exemplos de medidas de disponibilidade:

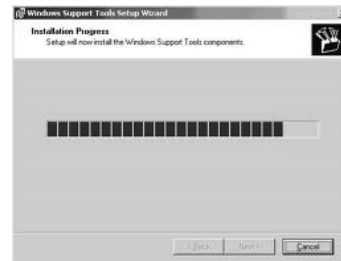
- A gestão e armazenamento de dados diminuem a chance de perda de informações. Os dados são, por exemplo, armazenados em um disco de rede, ao invés do disco rígido do computador;
- Os procedimentos de backup são criados. Os requisitos legais quanto ao tempo de armazenamento devem ser estabelecidos. A localização do backup é separada

fisicamente do negócio, a fim de garantir a disponibilidade em casos de emergência;

- Procedimentos de emergência são criados para assegurar que as atividades recomecem assim que possível, após uma ruptura em grande escala.

# Integridade

Informação atualizada



Informação sem erros



**Informação, Objetivos de Negócios  
e Requisitos de Qualidade**



## 2.6.2. Integridade

Integridade é o grau em que a informação está atualizada e sem erros. As características da integridade são as correções e a integridade das informações.

E agora, alguns exemplos de medidas de integridade:

- Alterações nos sistemas e dados são autorizadas. Por exemplo, um membro da equipe entra com um novo preço para um artigo no site, e outra verifica a regularidade do preço antes de ser publicado.
- Ações dos usuários são gravadas, que servirá como registros de uma mudança na informação.
- Ações em sistemas críticos, por exemplo, na instalação de um novo software, não pode ser realizada por apenas um pessoa. Ao segregar funções, cargos e as autoridades, pelo menos, duas pessoas serão necessárias para realizar uma mudança que tem consequências importantes.
- A integridade dos dados pode ser assegurada através de técnicas de criptografia, que protegerá as informações contra acesso não autorizado ou alteração. A política e a gestão para a criptografia pode ser definida em um documento distinto.

- Criar mecanismos que obriguem as pessoas a usarem termos corretos. Por exemplo, um terceirizado é sempre chamado de “terceirizado”, “prestador de serviços” é um termo diferente e não se pode inserir em um banco de dados cadastrais.

# Exemplo



## 2.6.3. Exemplo

Segundo a empresa de segurança Finjan, os criminosos estão usando computadores e servidores de *crimeware* da Argentina e da Malásia para vender logins de hospitais e de outros profissionais de saúde. Os especialistas em segurança, regularmente encontram todos os tipos de informações interessantes de servidores invadidos. Nesta ocasião, os dados dos hospitais e dos prestadores de serviços de saúde, informações de negócios de uma companhia aérea, dados dos impostos e números de seguro social, foram obtidos através do roubo de identidade.

Usando os dados dos pacientes roubados, os criminosos são capazes de adquirir medicamentos e tratamentos que podem em seguida, vendê-los. Para as vítimas, isso pode ter consequências para a sua cobertura de seguro e nos registros médicos, que podem resultar em tratamentos prejudiciais e incorreta, diz Finjan.

Nos servidores *crimeware*, a empresa encontrou logins Citrix de um hospital americano e de outras instituições médicas.

\* *Crimeware* é um termo genérico que caracteriza todo tipo de tentativa de roubo de fundos

# Confidencialidade

Restrição de acesso



Privacidade



## Informação, Objetivos de Negócios e Requisitos de Qualidade



### 2.6.4. Confidencialidade

A confidencialidade é o grau em que o acesso à informação é restrito a um grupo definido de pessoas autorizadas. Isso também inclui medidas para proteger a privacidade.

E agora, alguns exemplos de medidas de confidencialidade:

- Acesso à informação é concedido com base na necessidade. Não é necessário, por exemplo, para um colaborador da área financeira visualizar os relatórios das discussões com o cliente.
- Medidas para garantir que as informações não caiam em mãos erradas. Garantir, por exemplo, que documentos confidenciais não sejam mantidos sobre a mesa enquanto não estão presentes (política de mesa limpa).
- Gerenciamento de acesso lógico para garantir que as pessoas não autorizadas ou os processos não tenham acesso aos sistemas, bases de dados e programas. Um usuário, por exemplo, não tem o direito de alterar as configurações de uma estação de trabalho.
- A segregação de funções é criada entre os desenvolvedores de sistemas e os usuários da organização. Um desenvolvedor de sistema não pode, por exemplo, fazer qualquer alteração de salários.

- Segregações entre ambientes de desenvolvimento, teste, homologação e ambiente de produção.
- No processamento e utilização dos dados, as medidas são tomadas para garantir a privacidade das pessoas e terceiros. O departamento de Recursos Humanos tem, por exemplo, sua rede própria, que não é acessível a outros departamentos.
- O uso de computadores por usuários finais é cercado com medidas para que a confidencialidade das informações seja garantida. Um exemplo é uma senha que dá acesso ao computador e à rede.

# Arquitetura da Informação



## Informação, Objetivos de Negócios e Requisitos de Qualidade



### 2.7. Arquitetura da Informação

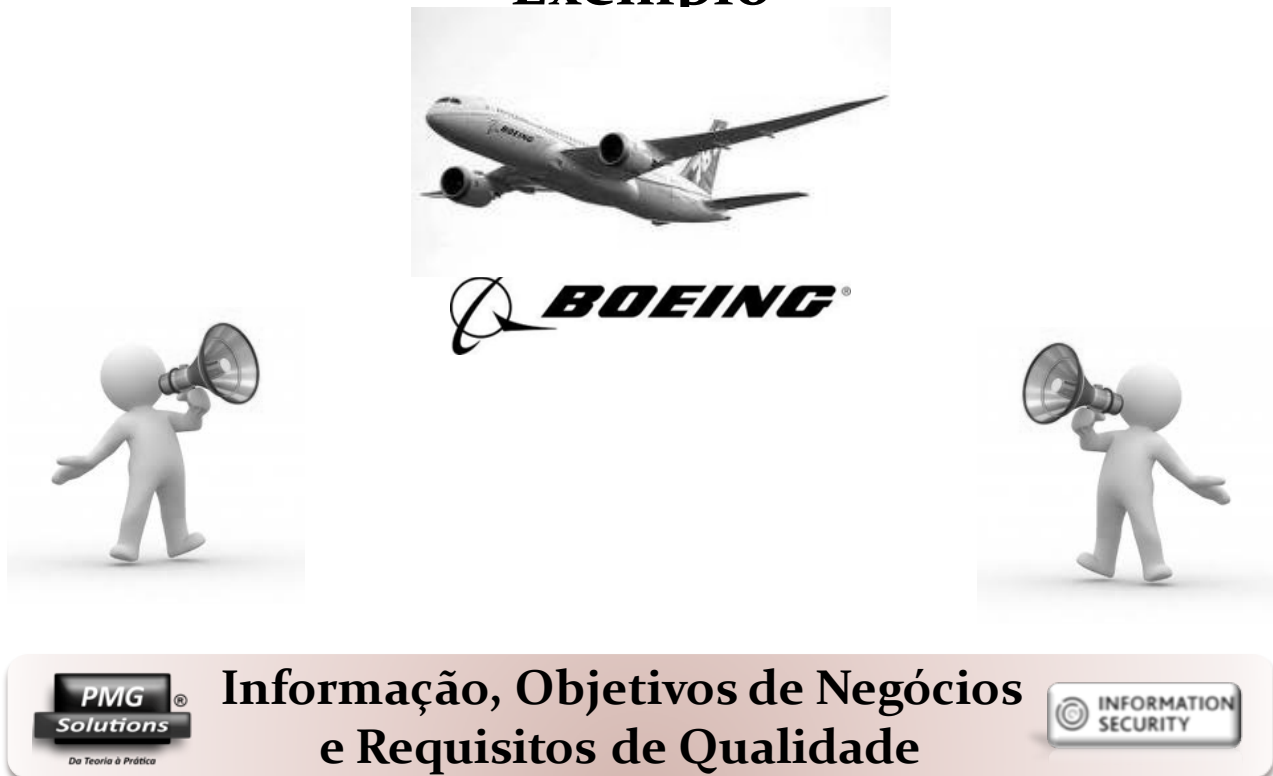
A segurança da informação está intimamente relacionada com a arquitetura da informação. A arquitetura da informação é o processo que foca na organização de como será feita a prestação de informação dentro de uma empresa.

Essa prestação pode ser entendida também como o reporte, encaminhamento, distribuição, disponibilização das informações da companhia.

Como brevemente descrito, certas exigências são definidas para o fornecimento de informações. A segurança da informação pode ajudar a garantir que os requisitos são realizados na arquitetura de informação. A Arquitetura da Informação é focada principalmente na realização da necessidade da informação da organização e da forma que esta pode ser organizada.

Já a Segurança da Informação poderá apoiar este processo, garantindo a integridade, disponibilidade e confidencialidade das informações.

## Exemplo



### 2.7.1. Exemplo

Agora, um exemplo de problemas do tratamento da arquitetura da informação.

O Novo Boeing 787 Dreamliner pode ter um sério problema de segurança. Segundo a American Federal Aviation Administration (FAA), teoricamente é possível os passageiros do avião fazerem logon no sistema de controle do avião. Parece que há uma conexão física entre a rede de computadores que fornece aos passageiros, acesso à internet e a navegação do avião, comunicação e sistemas de controle.

Esta conexão física é um grande problema de segurança, pois dá aos hackers acesso potencial aos sistemas mais importantes do avião. Segundo a FAA, a melhor solução é remover completamente este conexão física.

A Boeing afirmou que a empresa já tinha conhecimento do relatório da FAA e que já estão trabalhando em uma solução. Segundo a Boeing, no entanto, a rede dos passageiros e o sistema do avião não se conectam completamente, não sendo possível comprometer o controle do sistema. Especialistas de TI dizem que a utilização de um firewall de software apenas, não é o suficiente para proteger um sistema tão importante.

# Análise da Informação

Projetar um sistema baseado no seu Fluxo



Em virtude do resultado da análise



**Informação, Objetivos de Negócios  
e Requisitos de Qualidade**



## 2.8. Análise da Informação

A análise da informação fornece uma imagem clara de como uma organização lida com o fluxo ou *workflow* da informação dentro da empresa.

Por exemplo, um registro de hóspede de um hotel através do site. Esta informação é passada para o departamento da administração, que em seguida aloca um quarto. A recepção sabe que o cliente vai chegar hoje. O departamento de serviços domésticos sabe que a sala deve ser limpa para a chegada do hóspede. Em todas essas etapas, é importante que a informação seja confiável. Os resultados de uma análise da informação podem ser usados para projetar um sistema de informação.

# Processos Operacionais e de Informações



• Processo Primário



• Processo orientativo



• Processo de apoio



## Informação, Objetivos de Negócios e Requisitos de Qualidade



### 2.8.1. Processos Operacionais e de Informações

Em um ambiente de negócio, existe uma estreita ligação entre os processos operacionais e as informações. Um processo operacional é o processo que está no coração do negócio. Em um processo operacional, as pessoas trabalham em um produto ou serviço para um cliente. Um processo operacional tem as seguintes etapas:

- Entrada;
- Processo;
- Saída.

Existem vários tipos de processos operacionais:

- O processo primário. Por exemplo, o processo de fabricação de uma bicicleta em uma determinada indústria.
- Processo orientativo. Por exemplo, processo de planejamento estratégico da empresa.
- Processos de apoio. Por exemplo, processos de compra e venda ou processos de RH para contratação de recursos.

A informação tornou-se um fator de produção importante na realização dos processos operacionais. Um dos métodos para determinar o valor da informação é verificar o papel da informação no processo.

Cada processo operacional estabelece requisitos específicos para a prestação de informações. Há processos que são muito dependentes da disponibilidade de informações, por exemplo, o website da empresa, enquanto outros processos estão mais dependentes da correção absoluta das informações, como os preços dos produtos e assim por diante.

# Gestão da Informação e a Informática



Gestão da  
comunicação



Informática desenvolve



Informações



**Informação, Objetivos de Negócios  
e Requisitos de Qualidade**



## 2.9. Gestão da Informação

Gestão da informação formula e dirige a política relativa à prestação de informação de uma organização. Dentro deste sistema, um gerenciador de informações pode fazer uso da arquitetura e análise da informação.

A gestão da informação envolve muito mais do que o tratamento automatizado da informação realizado por uma organização. Em muitos casos, a comunicação externa e a comunicação com a mídia fazem parte da estratégia de gestão da informação.

### Informática

A expressão informática refere-se à ciência lógica usada para trazer a estrutura de informação e sistemas. É importante entender que a informática pode ser usada para desenvolver programas, sistemas e aplicações, com o objetivo de gerar informações através do fornecimento de dados.

# Resumo

Gestão da Informação

Forma da Informação

Arquitetura da Informação



Sistema da Informação

Confidencialidade

Valor da Informação

Integridade

Disponibilidade



## Informação, Objetivos de Negócios e Requisitos de Qualidade



Neste capítulo você aprendeu sobre as várias formas de sistemas de informação. Você também foi introduzido no trio: disponibilidade, confidencialidade e integridade. Finalmente, você viu como a segurança da informação é importante para os processos operacionais, arquitetura da informação e na gestão da informação.

# Teste



## Informação, Objetivos de Negócios e Requisitos de Qualidade



1. O que não é considerado um Sistema de Informação para o ISO/IEC 27002?
  - a. Fax
  - b. Servidores de Impressão
  - c. E-mail
  - d. Imagens de um vídeo
  
2. Qual destes é uma medida de Integridade?
  - a. Gerenciamento de acesso lógico
  - b. Criação de procedimento de emergência
  - c. Segregação de função
  - d. Técnicas de criptografia
  
3. Qual destes não é uma medida de Disponibilidade?
  - a. Procedimentos de backup
  - b. Utilização de senha de acesso
  - c. Armazenamento de dados
  - d. Criação de procedimento de emergência

4. Qual destes não é uma forma de prestação de contas na arquitetura da informação?
- a. Reporte
  - b. Encaminhamento
  - c. Armazenamento
  - d. Distribuição
5. Qual destes não é um tipo de processo operacional?
- Processo Primário
  - Processo Secundário
  - Processo Orientador
  - Processo de Apoio

**Gabarito**

1. d.	2. d.	3. b.	4. c.
5. b.			