TI.exames Com êxito

EDUCAÇÃO E TREINAMENTO
PARA ALAVANCAR A SUA CARREIRA

Fundamentos da Segurança da Informação com base na ISO/IEC 27002

Curso e-learning completo

Preparatório para o exame EXIN ISO 27002 Foundation

Módulo 2

Informação, objetivos do negócio e requisitos de qualidade

Este módulo cobre:

1. Valor da informação
2. Ativos
3. Tipos de informação
4. Aspectos da informação: disponibilidade, integridade e confidencialidade
5. Análise da informação e gestão da informação
6. Exercícios

Slide 2

O que é informação? Qual o valor da informação?

"Informação é um ativo que, como qualquer outro ativo importante para os negócios, tem valor para a organização e consequentemente necessita ser adequadamente protegida."

NBR ISO/IEC 27002:2005

O valor da informação é determinado pelo valor que o usuário dá a ela. É o usuário que reconhece se é apenas um dado, ou se é informação. Enquanto certos usuários podem considerar um dado em particular desinteressante, outros usuários podem extrair informação com valor do mesmo dado.

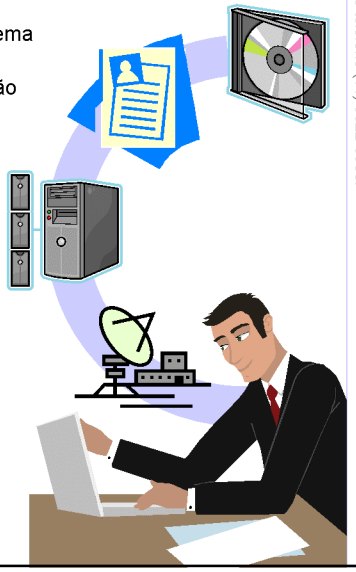
Os fatores padrão de produção de uma empresa normalmente são capital, mão-de-obra e matéria primas. Mas o negócio não pode existir sem informação. Alguns negócios têm informação como produto, como é o caso de consultorias, escritórios de contabilidade, etc. Em TI é comum considerar informação como um fator de produção.

Slide 3

Ativos

O que são ativos? (em relação à ISO/IEC 27001)

- Devem ser aqueles relevantes ao escopo do Sistema de Gestão de Segurança da Informação
- Um ativo da informação é algo a que a organização atribui valor, por exemplo:
  - → Informação eletrônica
  - → Documentos em papel
  - → Softwares
  - → Hardwares
  - → Instalações
  - → Pessoas
  - → Imagem e reputação da organização
  - → Serviços

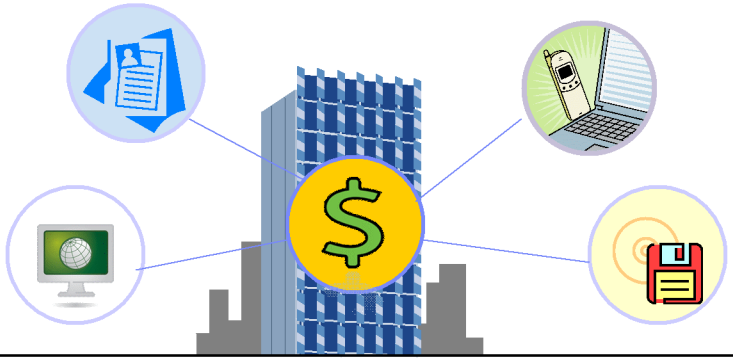


Slide 4

Ativos

Portanto:

- Para a ISO 27002, os ativos não incluirão necessariamente tudo que normalmente uma organização considera que tem valor.
- Uma organização deve determinar quais ativos podem materialmente afetar a entrega de um produto ou serviço pela sua ausência ou deterioração, ou causar dano à organização através de perda de disponibilidade, integridade ou confidencialidade.
- Deve-se definir qual é o valor de um ativo no caso de um incidente.



Slide 5

Tipos de informação

Alguns dados podem ser processados pela tecnologia da informação, quando são processados e adquirem significado.

A informação pode existir sob várias formas:


Impressa ou escrita em papel


Armazenada eletronicamente


Transmitida pelo correio ou por meios eletrônicos


Mostrada em vídeos


Verbal

A forma da informação vai impor restrições às medidas necessárias para sua proteção.

"Não importa a forma que a informação toma, ou os meios pelos quais ela é compartilhada ou armazenada. Ela deve sempre ser apropriadamente protegida."

NBR ISO/IEC 27002:2005

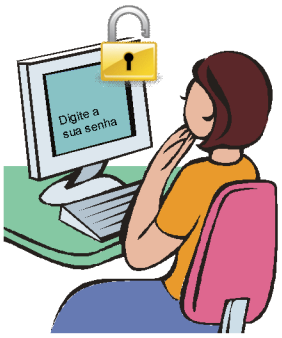
Slide 6

Tipos de informação a serem protegidas

Internas - informações que você não gostaria que a concorrência soubesse, etc.

De clientes e fornecedores - informações que eles não gostariam que você divulgasse, etc.

De parceiros - informações que necessitam ser compartilhadas com outros parceiros comerciais, etc.



Slide 7

Estado da informação

A Informação pode ser:

- Criada
- Transmitida
- Processada
- Usada
- Armazenada
- Corrompida
- Perdida
- Destruída

Slide 8

Outros conceitos importantes

Sistemas de informação

- Transferir e processar informações ocorre por meio de um sistema de informação, o que não é necessariamente um sistema de TI. Por exemplo: cabines telefônicas, celulares e impressoras.
- Um sistema de informação é uma combinação de meios, procedimentos, regras e pessoas que forneçam informação para um processo operacional.
- Este sistema pode ser melhorado por um sistema de TI que inclui:
  - → Estação de trabalho
  - → Transmissão de dados por rede, cabos ou wireless
  - → Servidores, incluindo os equipamentos, sistema operacional e software
  - → Armazenamento de dados, por exemplo discos, e-mails e base de dados
  - → Telefones com suas centrais e antenas

Arquitetura da informação

- Segurança da informação está muito relacionada com arquitetura da informação, que é o processo focado em preparar o fornecimento da informação dentro da organização. A segurança da informação visa garantir que as informações fornecidas por este processo tenham integridade, confidencialidade e disponibilidade.

Slide 9

Outros conceitos importantes

Processos operacionais e a informação

- No ambiente de negócio há uma forte relação entre processos operacionais e informação. Existem 3 tipos básicos de processos: primários – diretamente relacionados com a realização do produto ou serviço) – , processos-guias (de gestão) – que tratam planejamento e estratégias, por exemplo – e processos de suporte – como compras, vendas e RH. O valor da informação vai depender da importância que ela terá para estes processos.

Análise da informação

- Significa elaborar um desenho de como a informação flui dentro da organização. Por exemplo, podemos analisar por onde caminha a informação no processo de reserva de um hotel, quando esta reserva é feita por meio de um website.

Gestão da informação

- A gestão da informação formula e direciona a política relativa ao fornecimento de informação em uma organização. Dentro deste sistema um gestor da informação pode usar a arquitetura da informação ou realizar analise da informação. È mais do que processamento automático da informação, pode ser por exemplo comunicação externa à organização, com a mídia, com as partes interessadas, etc.

Informática

- O termo informática relaciona-se à ciência lógica usada para trazer estrutura à informação e ao sistema. A palavra é também utilizada para o desenvolvimento de programas.

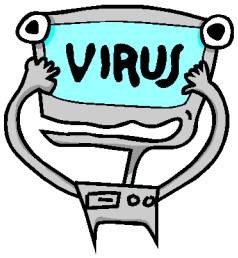
Slide 10

O que é segurança da informação?

A ISO/IEC 27002:2005 define:

Segurança da Informação - é a proteção da informação contra diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio.

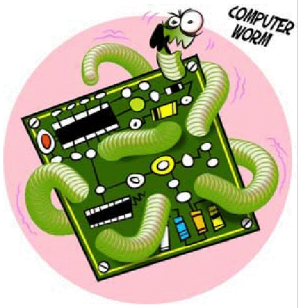
Exemplo:
Os vírus não são apenas um tipo de **malware**. Outros tipos incluem os **spywares** e alguns tipos de **adwares**. Os spywares vasculham o que o usuário faz em seu computador. Isso pode incluir a captura de logins e senhas. Já os adwares são softwares aplicativos que exibem propagandas aos usuários quando usam um aplicativo maior como o navegador. Alguns adwares contêm códigos que fornecem aos anunciantes um acesso extenso às informações particulares.



Slide 11

Storm Worm

- Foi no fim de 2006 que os especialistas em segurança de computadores identificaram pela primeira vez o worm. O público começou a chamar o vírus de Storm Worm porque uma das mensagens de e-mail tinha como assunto: "230 mortos em temporal na Europa". Porém, as empresas de antivírus deram a ele outros nome: a Symantec o chama de Peacomm e a McAfee de Nuwar.
- O Storm Worm é um cavalo de Tróia. O seu payload é outro programa, embora nem sempre o mesmo. Algumas versões desse vírus transformam os computadores em zumbis ou robôs. E quando são infectados, tornam-se vulneráveis ao controle remoto da pessoa responsável pelo ataque. Alguns hackers utilizam o Storm Worm para criarem um correio de botnet e usá-lo para enviar spam.



- Muitas versões do Storm Worm enganam a vítima para que ela baixe o aplicativo através de links falsos para notícias ou vídeos. O responsável pelos ataques geralmente muda o assunto da mensagem para refletir acontecimentos atuais. Por exemplo, um pouco antes das Olimpíadas de Pequim 2008, uma nova versão do worm apareceu em e-mails com assuntos como: "outra catástrofe arrasa a China" ou "o terremoto mais letal da China". O e-mail dizia conter links para vídeos e notícias relacionadas ao assunto, mas na verdade clicar no link fazia ativar o download do worm para o computador da vítima.

Slide 12

Exemplos de ameaças à informação

- Funcionários descontentes ou desmotivados
- Baixa conscientização nos assuntos de segurança
- Crescimento do processamento distribuído e das relações entre profissionais e empresas
- Aumento da complexidade e eficácia das ferramentas de hacking e dos vírus
- E-mail
- Inexistência de planos de recuperação a desastres
- Desastres (naturais ou não, como incêndio, inundação, terremoto, terrorismo)
- Falta de políticas e procedimentos implementados

Slide 13

Exemplos de impactos

- Perda de clientes e contratos
- Danos à imagem
- Perda de produtividade
- Aumento no custo do trabalho para conter, reparar e recuperar
- Aumento de seguros
- Penalidades e multas

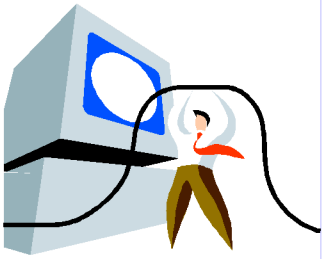
Slide 14

Que aspectos da informação devemos avaliar?

Aspectos da informação:

- **Confidencialidade:** assegurar que a informação é acessível somente às pessoas autorizadas.
- **Integridade:** proteger a exatidão e a completeza (ou completude) da informação e dos métodos de processamento.
- **Disponibilidade:** assegurar que os usuários autorizados tenham acesso à informação e ativos associados, quando necessário.

Em inglês usa-se a sigla CIA como mnemônico:
Confidentiality
Integrity
Availability

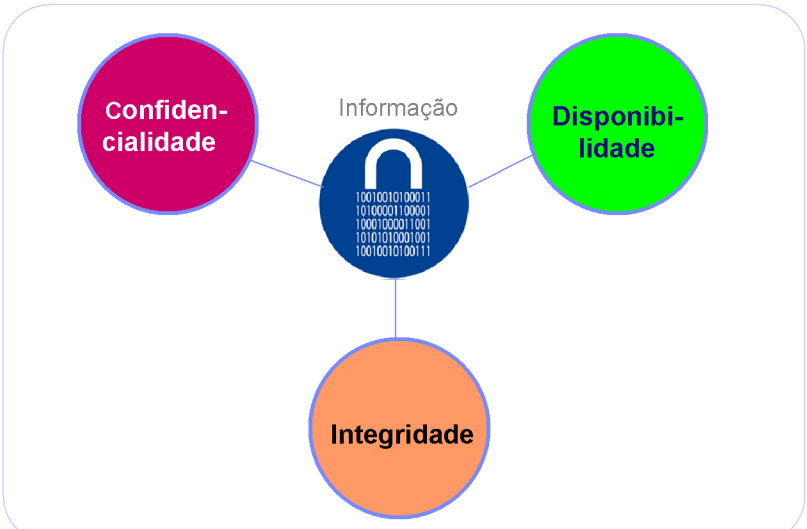


O ponto de partida é verificar a influência que os requisitos da CIA tem sobre o valor da informação:

- A importância da informação para processos operacionais
- Quanto a informação é indispensável nestes processos
- A recuperabilidade da informação

Slide 15

Equilíbrio entre os aspectos



Slide 16

Disponibilidade

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

São características de disponibilidade

- **Pontualidade:** o sistema de informação está disponível quando necessário.
- **Continuidade:** a organização pode continuar trabalhando no caso de falha.
- **Robustez:** existe capacidade suficiente, o que permite que toda organização trabalhe no sistema.

Exemplos de medidas de disponibilidade

- **Gestão e armazenamento de dados**, por exemplo: dados armazenados em um disco de rede e não em um HD de um PC.
- **Procedimentos de back up**, com armazenamento em local físico diferente.
- **Procedimentos de emergência** para garantir que as atividades recomecem tão cedo quanto possível no caso de um acidente.

Slide 17

Integridade

Integridade é o grau em que a informação é atualizada sem erros. As características da integridade são ela ser correta e completa.

Um acontecimento real:

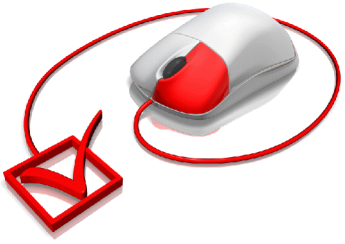
- De acordo com a empresa de seguros Finjan, criminosos usam servidores da Argentina e da Malásia para identificar e vender logins de hospitais e de outros provedores de serviços de saúde.
- Usando dados roubados de um paciente os criminosos são capazes de adquirir remédios e tratamentos que podem vender.

- Para as vítimas isso pode trazer consequências na sua cobertura de seguro de saúde ou assistência médica, e nos seus registros médicos.
- Segundo a Finjan, foram pegos em uso logins de hospitais e de instituições médicas americanas.

Slide 18

Integridade

Exemplos de medidas de integridade



- Mudanças autorizadas de dados. Por exemplo: alteração de um preço conforme definido pela administração.
- Uso correto dos termos. Por exemplo: uma empresa que presta serviços de suporte em informática define que os clientes serão sempre chamados de usuários e a palavra cliente não irá, então, ser usada nem constar no banco de dados.
- As ações de usuários são registradas e portanto pode-se determinar quem alterou determinada informação.
- Ações importantes como a implantação de um novo software não podem ser realizadas por apenas uma pessoa. Por caminhos separados no mínimo duas pessoas devem trabalhar na mudança.
- Uso de criptografia para impedir acesso à informação e assegurar sua proteção.

Slide 19

Confidencialidade

Confidencialidade é o grau no qual o acesso à informação é restrito para determinados grupos de pessoas autorizados a ter este acesso. Confidencialidade também inclui medidas de proteção a privacidade.

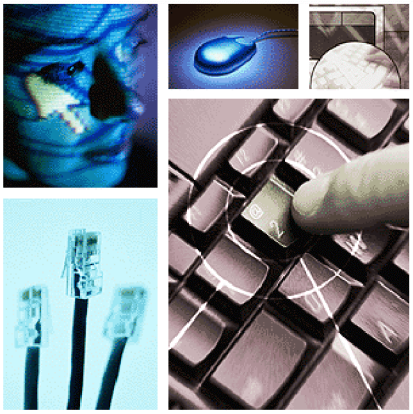
Exemplos de medidas de confidencialidade

- Acesso à informação garantido somente onde necessário.
- Empregados tomam medidas para garantir que a informação não é encontrada por aqueles que dela não necessitam.
- Gestão de acesso lógico garante que pessoas ou processos não autorizados não tenham acesso a sistemas automatizados, bases de dados ou programas.
- Uma separação é criada entre o sistema de desenvolvimento da organização, os processos da organização e os usuários. Um desenvolvedor, por exemplo, não pode alterar salários.
- Uma separação rígida é criada entre os ambientes de desenvolvimento, teste, aceitação e produção.
- Nos processos onde dados são utilizados, medidas são tomadas para garantir a privacidade das pessoas e terceiros.

Slide 20

Resumo

- Alcançamos a segurança da informação através da implementação de um conjunto adequado de controles, incluindo políticas, procedimentos, estrutura organizacional e funções de hardware e software.
- Cada empresa é única em suas exigências e requisitos de controle e para os níveis de confidencialidade, integridade e disponibilidade.
- Nem todos os controles e orientações incluídas na norma ISO/IEC 27002 podem ser aplicáveis. Da mesma forma, controles não inclusos na norma podem ser identificados como necessários.



Slide 21

Exercício

Considere uma empresa de consultoria na área de informática que deseja implantar o SGSI conforme a norma ISO 27001 na sua área de vendas, dentro do seguinte escopo:

Gerenciamento do sistema de segurança da informação para vendas de treinamento, consultoria e auditoria em segurança de informação na Rua Pau Brasil 111, São Paulo, SP, Brasil.

- 1) Identifique, do seu ponto de vista, os possíveis ativos da informação dentro deste processo. Considere: informações de entrada, informações de saída, equipamentos, registros, recursos humanos, comunicação, ferramentas de software, softwares e outros.
- 2) Valorize ao menos 3 destes ativos com base na perda da confidencialidade, disponibilidade e integridade. Considere cores para identificar o valor de cada ativo, sendo:
  - verde o menor valor
  - vermelho o maior valor
  - amarelo o valor intermediário

As respostas dependem de critérios pessoais, por isso é importante que os profissionais que estejam realizando a análise padronizem seus conceitos antes de finalizar o tratamento de riscos.

Slide 22

Resposta do exercício - item 1

Informações de entrada	Informações de saída	Equipamentos
Contrato Comercial/Técnico Critérios: Legislação, Regulamentações, Políticas	–Treinamento Manuais, Slides/Apresentações, Apostilas –Consultoria Metodologia,Padrões de relatório –Auditoria Checklist, Padrões de Relatório Critérios: Procedimentos, Clientes	– Modem – Firewall – Router – Hub – 1 Servidor – 2 Desktop – 2 Notebook Critérios: Procedimentos, Padrões
Registros	**Recursos Humanos**	**Comunicações**
–Análise Crítica de Projeto –Verificações de Projeto –Alterações de Projeto (Lições aprendidas) Critérios: Procedimentos	–5 pessoas –Contratados Critérios: Legislação, Procedimentos e Políticas	–1 fax –5 telefones –2 linhas telefônicas –Link da internet Critérios: Procedimentos
Outros	**Software**	**Ferramentas (Software)**
–Instalações (escritório) Critérios: Procedimentos	–IOS 12.2 –Windows 2000 –Windows XP Pro –Windows 2000 Pro Critérios: Padrões	–Retina –LanGuard Scanner –Anti-virus Critérios: Padrões

Slide 23

Resposta do exercício - item 2

Descrição	Disponibilidade	Integridade	Confidencialidade	Valor	Comentário
Contrato Comercial/Técnico					Acarreta dano, mas o processo pode ser executado
Manuais					Pequeno impacto ao processo
Slides/Apresentações					Sem impacto significativo
Apostilas					Pequeno impacto ao processo
Metodologia					Acarreta dano, mas o processo pode ser executado
Padrões de Consultoria					Sem impacto significativo
Checklist					Acarreta dano, mas o processo pode ser executado
Padrões de Relatório					Pequeno impacto ao processo
Alterações de Projeto					Acarreta dano, mas o processo pode ser executado
Consultor 1					Peça-chave do processo
Consultor 2					Peça-chave do processo
Administrador					Peça-chave do processo
Modem					Pode acarretar danos ao processo
Firewall					Pode acarretar danos ao processo
Router					Pode acarretar danos ao processo
Hub					Pode acarretar danos ao processo
Servidor					Peça-chave do processo
Desktop					Acarreta dano, mas o processo pode ser executado
Notebook					Acarreta dano, mas o processo pode ser executado
Windows 2000 Server					Peça-chave do processo

Slide 24