Aula 1

Segurança em Sistemas de Informação

Prof. Douglas Eduardo Basso

1

Conversa Inicial

2

Conversa Inicial

- Vamos estudar alguns conceitos relacionados à segurança da informação, ao ciclo de vida dos dados, à classificação da informação e às premissas de segurança. Posteriormente serão apresentadas algumas normas e ISOs que estão intimamente relacionadas com a segurança da informação. O objetivo é mostrar os principais conceitos de segurança que servirão como base para o desenvolvimento da disciplina

3

História e conceitos

4

Introdução

- Para Galvão, a era da informação se desenvolve no momento em que é estabelecida uma plataforma por meio da qual se torna possível a todos os indivíduos com acesso a ela, independentemente de onde estejam, trocar experiências, compartilhar forma diferentes de fazer as coisas, comprar, vender e criar coletivamente

5

- Na era moderna, os ciclos de produção e consumo presentes em nossa economia estão cada vez mais velozes. A inovação tem sido muito presente e está vinculada ao sucesso, à qualidade dos produtos criados, ao consumismo acelerado e ao ritmo cada vez mais rápido. Todo esse cenário torna as informações um ativo muito valioso

6

Informação

- A informação é um grande ativo que, como qualquer outro componente valioso e importante de uma empresa, é essencial para os negócios de uma organização. De antemão requer e necessita de proteção adequada

7

Ciclo de vida

- Temos que observar e ter atenção ao tempo de vida que essa informação necessita ter. Em relação às fases do ciclo de vida das informações, podemos elencar as seguintes:

8

- Manuseio - quando a informação é criada, coletada, gerada ou alterada
- Armazenamento - quando a informação é consolidada, gravada ou retida
- Transporte - quando a informação é transferida, comunicada, transportada
- Descarte - quando a informação perde seu valor e é inutilizada ou descartada

9

Sistemas de informação

- Os sistemas de informação podem ser bases de dados, arquivos gravados em um disco, documentos físicos armazenados em armários, equipamentos de comunicação, impressoras, computadores portáteis, servidores, redes, equipamentos de comunicação, telefones, entre outros

10

Gestão da informação

- A tarefa de organizar todas informações de uma empresa, criar, coletar, controlar, planejar, utilizar, difundir e descartar suas informações de maneira eficaz e eficiente é da gestão da informação

11

Introdução à segurança da informação

12

Segurança da informação

- A segurança da informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa; isto é, aplica-se tanto às informações corporativas como às pessoas

13

Atributos da segurança e proteção de dados

- Segundo alguns padrões internacionais, existem alguns pilares que acabam criando toda a base em relação à segurança podemos destacar os seguintes: confidencialidade, integridade, disponibilidade, autenticidade, irretrabilidade e legalidade

14

Classificação da informação

- O grau de sigilo é uma classificação concedida a cada tipo de informação e baseada em critérios como nível de importância e de sigilo, pessoas com permissão de acesso, entre outros. É comum a maioria das empresas privadas utilizem como classificação os seguintes graus: confidencial, privada, sigilosa e pública

15

Ameaças à segurança

- As ameaças à segurança da informação são relacionadas diretamente à perda de uma de suas três características principais (tríade da gestão de segurança da informação):
  - Perda da confidencialidade
  - Perda da integridade
  - Perda de disponibilidade

16

Aspectos legais

- Em termos jurídicos, a segurança da informação no Brasil é o resultado da relação entre a ciência do direito e a ciência da computação, sempre empregando novas tecnologias. Trata-se do conjunto de normas, aplicações, conhecimentos e relações jurídicas, oriundas do universo digital

17

ISO 15408

18

ISO 15408

- A norma ISO/IEC 15408 é uma modelagem bem flexível com um grupo de métodos para a análise e a avaliação de aspectos relacionados a segurança de produtos e sistemas de tecnologia da informação, tais como: *hardware*, *software* e *firmware*

19

Componentes funcionais de segurança

- Os requisitos funcionais de segurança são apresentados em classes, grupos e componentes. As classes expressas são as seguintes:
  - Auditoria de segurança
  - Proteção das funcionalidades de segurança
  - Utilização dos recursos
  - Acesso aos alvos de avaliação

20

- Canais e caminhos confiáveis
- Proteção de dados de usuário
- Identificação e autenticação
- Gerenciamento de segurança
- Privacidade
- Comunicação
- Suporte à criptografia

21

Componentes de garantia de segurança

- Os componentes de garantia de segurança formam um caminho-padrão a ser seguido para mostrar os requisitos de segurança para os alvos de avaliação

22

Família ISO 27000

23

Família ISO 27000

- A família ISO/IEC 27000 apresenta uma série de normas relacionadas à segurança de ativos de informações das empresas. Com a utilização dessas normas, as organizações tornam todo seu ambiente computacional mais seguro

24

ISO 27001

- A ISO 27001, como mencionado anteriormente, é um guia que apresenta requisitos em relação a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, com o intuito de garantir a segurança da informação nas organizações que trabalham com dados sensíveis

25

Controles

- Os controles de segurança são salvaguardas ou contramedidas técnicas ou administrativas que evitam, neutralizam ou minimizam perdas ou indisponibilidades devido a ameaças agindo sobre a sua correspondente vulnerabilidade, o risco à segurança

26

Tratamento de riscos

- Toda a organização deve definir algumas convenções e critérios para determinar os riscos que podem ser aceitos ou não. Ao ser avaliado, o risco precisa ser classificado. Alguns controles são desejáveis dentro desse cenário:
  - Aplicação de controles adequados para redução de riscos
  - Entendimento em relação aos riscos, política clara de aceitação de riscos

27

- Evitar as ocorrências de riscos, identificar e mitigar as causas
- Aplicar controles apropriados e fazer transferências de riscos a outras partes como fornecedores, parceiros e seguradoras
- Desenvolver e atender requisitos identificados em avalições de risco

28

- Reduzir os riscos a níveis aceitáveis
- Atender requisitos e restrições relacionadas à legislação nacionais e internacionais
- Criar um equilíbrio na relação de riscos e o tratamento para a redução, tendo em vista sempre as exigências e limitações da organização, o investimento e a operação de controles que podem causar falhas de segurança

29

Contramedidas

- Durante a análise de riscos, é levantada uma série de ameaças relacionadas com sua respectiva importância. Ao avaliarmos as ameaças, é necessária a criação de contramedidas que possam minimizar as ameaças. Para Baars, existem seis categorias diferentes:
  - Contramedidas preventivas visam a evitar acidentes
  - Contramedidas de redução visam a diminuir a probabilidade de uma ameaça ocorrer

30

- Contramedidas de detecção visam a detectar incidentes
- Contramedidas repressivas visam a limitar um incidente
- Contramedidas corretivas visam a recuperar os danos causados por um incidente
- A aceitação de riscos também é uma possibilidade. Alguns investimentos em contramedidas podem ser caros e de difícil de justificativa

31

Tipos de ameaça

- Em se tratando dos tipos de ameaças, identificar, classificar e enumerar são atividades frequentes dos profissionais de segurança da informação. As listas de ameaças podem ser classificadas como humanas e não humanas

32

Estratégias de riscos

- Existem algumas estratégias comuns para combater os riscos. Podemos elencar algumas, tais como:
  - Prevenção de riscos
  - Redução de riscos
  - Tolerância aos riscos

33

34

ISO 31000

- Essa norma trata desse processo sistemático e lógico com todas as suas especialidades. Mesmo que todas as organizações gerenciem os riscos de alguma maneira, essa norma traz um número de princípios que precisam ser atendidos para tornar a gestão de riscos mais eficaz

35

Princípios

- A gestão de riscos deve atender alguns princípios, entre os quais podemos destacar:
  - A gestão de riscos cria e protege valor
  - A gestão de riscos é parte integrante de todos os processos organizacionais
  - A gestão de riscos é parte da tomada de decisões

36

- A gestão de riscos aborda explicitamente a incerteza
- A gestão de riscos é sistemática, estruturada e oportuna
- A gestão de riscos baseia-se nas melhores informações disponíveis
- A gestão de riscos é feita sob medida

37

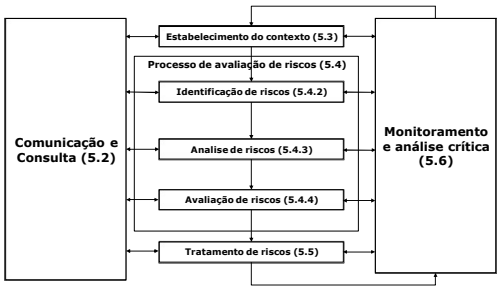
- A gestão de riscos considera fatores humanos e culturais
- A gestão de riscos é transparente e inclusiva
- A gestão de riscos é dinâmica, iterativa e capaz de reagir a mudanças
- A gestão de riscos facilita a melhoria contínua da organização

38

Estrutura

- Para atingir os objetivos da gestão de riscos, é preciso uma boa estrutura e gestão para o fornecimento de fundamentos e os arranjos necessários para que essa gestão seja incorporada à organização, em todas as suas áreas e níveis

39



40

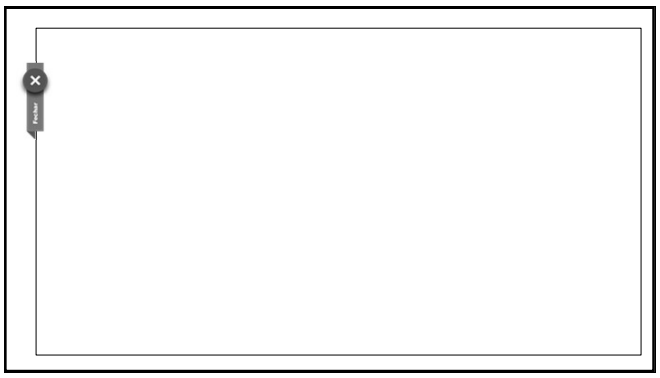
Monitoramento e registros de gestão de riscos

- O monitoramento e análise da gestão de riscos requer uma vigilância regular. As responsabilidades desse monitoramento devem estar bem definidas, a fim de garantir controles eficientes ao longo da operação da empresa

41

- Desenvolver a cultura dentro da organização de aprendizado contínuo
- As vantagens na reutilização de informações para fins de gestão
- Os valores e tempos envolvidos na criação e manutenção de registros
- A obrigação em relação a registros legais, regulatórios e operacionais
- Os guias de acesso, a facilidade de recuperação e meios de armazenamento
- O tempo e período de retenção
- A sensibilidade e importância das informações

42



43