GESTÃO DE SEGURANÇA DA INFORMAÇÃO

INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

Olá!

Ao final desta aula, você será capaz de:

1 - Conhecer as necessidades de segurança do ambiente corporativo;

2 - Identificar o valor da informação e conhecer o conceito de ativo;

3 - Conceitos básicos de segurança.

Nesta aula vamos compreender o ambiente corporativo e as motivações para a utilização de segurança da informação.

Para começarmos o nosso estudo vamos fazer a leitura de algumas notícias importantes. Para isso, clique no link abaixo:

http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/doc01_aula01_GSI.pdf

Após a leitura das notícias anteriores podemos concluir que o advento da internet e a globalização transformaram completamente o mundo que vivemos.

Estas transformações afetaram em cheio as organizações onde trabalhamos, quebrando diversos paradigmas e promovendo uma profunda reavaliação das prioridades daqueles que estão no comando das empresas. E esse será o objeto de estudo dessa disciplina.

O ambiente corporativo e a necessidade de segurança

O crescimento explosivo da internet e das tecnologias e aplicações a ela relacionadas está revolucionando o modo de operação das empresas, o modo como as pessoas trabalham e a forma como a tecnologia da informação apoia as operações das empresas e as atividades de trabalho dos usuários finais. Há três razões fundamentais para todas as aplicações de tecnologia da informação nas empresas. Elas são encontradas nos três papéis vitais que os sistemas de informação podem desempenhar para uma empresa.

Saiba mais

O papel estratégico dos sistemas de informação nas empresas cresce a cada dia e envolve a utilização de tecnologia da informação para desenvolver produtos, serviços e capacidades que confiram a esta empresa vantagens estratégicas sobre as forças competitivas que ela enfrenta no mercado mundial.

O valor da informação

Para compreendermos melhor o valor da informação no contexto atual vamos em primeiro lugar compreender o conceito de dado:

Dado

O **dado** é qualquer elemento identificado em sua forma bruta e que por si só não conduz a uma compreensão de determinado fato ou situação.

Informação

A **informação** é o dado trabalhado, que permite ao executivo tomar decisões. É a matéria-prima para o processo administrativo da tomada de decisão.

O **propósito da informação** é o de habilitar a empresa a alcançar seus objetivos pelo uso eficiente dos recursos disponíveis (pessoas, materiais, equipamentos, tecnologia, dinheiro e informação).

Para decidir sobre qualquer coisa, precisamos de informações, preferencialmente claras e oportunas. A informação é vital para o processo de tomada de decisão de qualquer corporação. Porém não basta produzir a informação no prazo previsto. É necessário disponibilizá-la para quem tem a real necessidade de conhecê-la. Além disso, é fundamental proteger o conhecimento gerado, quando este contiver aspectos estratégicos para a Organização que o gerou.

Em meio a tantas mudanças tecnológicas, sociológicas e comportamentais surgem também muitos desafios de negócios e gerenciais no desenvolvimento e implementação de novos usos da tecnologia da informação em uma empresa. Um destes desafios a ser considerado é a responsabilidade **ética** (é o ramo da filosofia que busca estudar e indicar o melhor modo de viver no cotidiano e na sociedade. Fonte: http://pt.wikipedia.org/wiki/96C3%89tica) referente ao uso da tecnologia da informação.

Vejamos a seguir alguns questionamentos sobre esse assunto!

Quais usos da tecnologia da informação poderiam ser considerados impróprios, irresponsáveis ou prejudiciais a outros indivíduos ou à sociedade?

Qual é o uso adequado da Internet e dos recursos de TI de uma organização? O que é preciso para ser um usuário final responsável de tecnologia da informação?

Como a empresa pode se proteger do crime com o uso de computadores e de outros riscos da tecnologia da informação?

Face a tantas mudanças tecnológicas, sociológicas e comportamentais, o profissional de TI deve levar em consideração os aspectos éticos sobre os danos potenciais ou riscos no uso da TI nas corporações:

	• Ampliar o conhecimento do mercado;

Aplicações de ti	• Aumentar a capacidade de resposta; • Aperfeiçoar as comunicações; • Melhorar a seleção de estratégias.
Danos potenciais	Qual a probabilidade de clientes, funcionários, parceiros empresariais ou concorrentes serem afetados por: • Invasões de privacidade • Informações imprecisas • Conluio • Exclusão de facilidades essenciais
Riscos potenciais	Qual a probabilidade de ocorrência de ações legais, boicotes dos consumidores, paralisações no trabalho e outras ameaças?
Respostas possíveis	Os riscos e custos podem ser atenuados por: • Auto-regulação • Defesa • Educação • Código de ética • Incentivos • Certificação

Estas são algumas das perguntas e considerações que delineiam as dimensões éticas dos sistemas de informação que iremos estudas nas próximas páginas.

Agora que você já compreendeu as necessidades dos ambientes corporativos, vamos entender o conceito de segurança.

O que é segurança?

...É estar livre de perigos e incertezas;

...É um estado ou condição que se aplica a tudo aquilo que tem valor para a organização que é chamado de ativo;

Existem diversos tipos de ativos (Segundo a norma 150/IEC 13335-1:2004, um ativo é qualquer coisa que tenha valor para a organização) em uma organização. Estes ativos podem ser organizados e classificados através de diversas propriedades. Esta classificação permite a organização dos ativos em grupos com características semelhantes no que diz respeito às necessidades, estratégias e ferramentas de proteção.

Dessa forma, os ativos podem ser classificados como:

Tangível (aquilo que pode ser tocado): Informações impressas ou digitais , Sistemas, Móveis, pessoas etc.

Intangível: Marca de um produto, Imagem de uma empresa, Confiabilidade de um banco etc.

Podemos classificar as proteções de acordo com a sua ação e o momento na qual ela ocorre. De acordo com a finalidade elas podem ser:

Preventivas: Evita que acidentes ocorram

Desencorajamento: Desencoraja a prática de ações

Monitoramento: Monitora o estado e o funcionamento

Detecção: Detecta a ocorrência de incidentes

Limitação: Diminui danos causados

Reação: Reage a determinados incidentes

Correção: Repara falhas existentes

Recuperação: Repara danos causados por incidentes

A partir deste ponto já conseguimos diferenciar segurança e segurança da informação:

Segurança da Informação

Visa à proteção de ativos de uma empresa que contém informações.

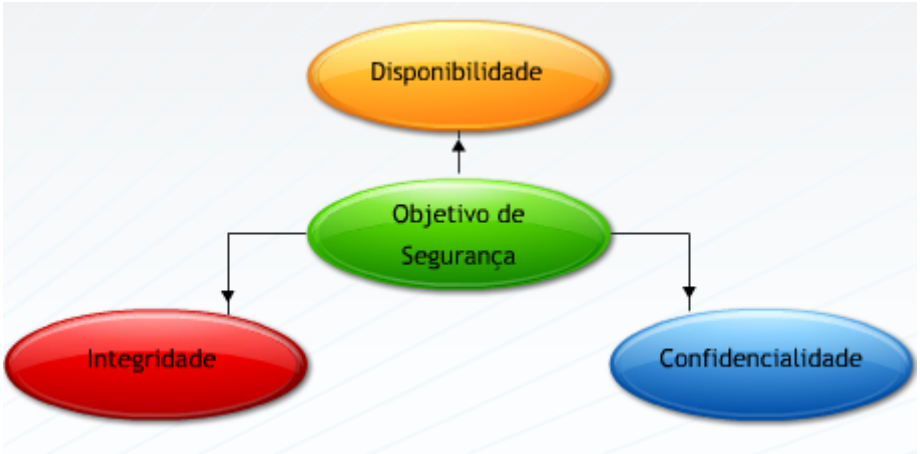
Ativos de Informação

São aqueles que produzem, processam, transmitem ou armazenam informações.

A seguir, vamos estudar os princípios fundamentais da Segurança da informação.

Cada empresa, ao tratar segurança da informação e, independentemente de sua área de negócio e dos objetivos de segurança que deseje, normalmente irá utilizar um ou os três princípios fundamentais de segurança conhecido como a tríade CID ou, em inglês, AIC ou **CIA** (Availability, Integrity, Confidentiality).

O nível de segurança requerido para obter cada um destes três princípios difere de empresa para empresa, pois cada empresa possui uma combinação única de requisitos de negócio e de segurança. Entretanto, todas as ações ou medições de segurança realizados em cada organização irão envolver sempre um ou mais princípios.



Disponibilidade:

- Trata-se da possibilidade de acesso continuo, ininterrupto, constante e atemporal às informações;
- Esta propriedade indica que o acesso aos serviços oferecidos pelo sistema deveria ser sempre possível para um usuário, entidade, sistema ou processo autorizado e aprovado.

Integridade

- Trata-se da manutenção das informações tal e qual tenham sido geradas:
- Esta propriedade indica que os dados e informações não deveriam ser alterados ou destruidos de maneira não autorizada e aprovada.

Confidencialidade

- Trata-se da manutenção do segredo, do sigilo ou da privacidade das informações;
- Esta propriedade indica que os dados e informações não deveriam ser acessíveis a, ficar disponíveis para ou ser divulgados a usuários, entidades, sistemas ou processos não autorizados e aprovados.

Fatores que impactam na segurança de uma organização

- **Valor**

  Importância do ativo para a organização. Como já falamos pode ser avaliado por propriedades mensuráveis ou abstratas, ou seja, tangível ou intangível.

  Exemplo de valor intangível: Comprometimento da imagem de uma empresa por causa do vazamento de urna informação;

  Exemplo de valor tangível: valor financeiro, o lucro que ele provê ou custo de substitui-lo;

- **Ameaça**

  Evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas.

  Exemplo: um incêndio, uma enchente, a invasão de um computador ou um roubo.

- **Vulnerabilidade**

  A ausência de um mecanismo de proteção ou falhas em um mecanismo de proteção existente. São as vulnerabilidades que permitem que as ameaças se concretizem.

  O que irá determinar se uma invasão de computador pode ou não afetar os negócios de uma empresa é a ausência ou existência de mecanismos de prevenção, detecção e eliminação, além do correto funcionamento destes mecanismos.

- **Impacto**

  Tamanho do prejuízo, medido através de propriedades mensuráveis ou abstratas, que a concretização de uma determinada ameaça causará; Devemos Levar em consideração que diferentes ameaças possuem

impactos diferentes e que dependendo do ativo afetado, podemos ter também impactos diferentes para uma mesma ameaça.

Exemplo: O impacto de uma invasão a um servidor de banco de dados pode ser maior que o impacto da invasão da máquina da secretária da gerência de operações.

- **Risco**

  Medida que indica a probabilidade de uma determinada ameaça se concretizar, combinada com os impactos que ela trará. Quanto maior a probabilidade de uma determinada ameaça ocorrer e o impacto que ela trará, maior será o risco associado a este incidente.

Apresentamos a seguir a interação dos diversos componentes de segurança:

Podemos concluir que um Problema de segurança é:

A perda de qualquer aspecto de segurança importante para minha organização.

E podem ser de diferentes tipos:

Desastres naturais: Tempestades, inundações, incêndio etc.

Operação Incorreta: Erro do usuário ou administrador do sistema.

Ataque ao sistema: Visando algum lucro.

Saiba mais

Site com notícias sobre segurança www.seginfo.com.br

Site do centro de estudo, respostas e incidentes de segurança no Brasil: www.cert.br

O que vem na próxima aula

Na próxima aula, aprenderemos o seguinte tema: O ciclo de vida da informação

E, abordaremos os seguintes assuntos:

•Assunto 1: Por que proteger a informação.

•Assunto 2: Quando proteger a informação.

•Assunto 3: O ciclo de vida da informação.

CONCLUSÃO

Nesta aula, você:

- Compreendeu a necessidade de segurança nos ambientes corporativos.
- Conheceu o valor da informação e o conceito de ativo.
- Identificou os principais elementos de um sistema de segurança da informação.