

Segurança da Informação

(SI)



Carlos Henrique M. da Silva
carloshenrique.85@globo.com

OBJETIVOS

- Conceitos básicos que fundamentam os estudos sobre SI;
- Diferentes categorias de ativos existentes em uma empresa;
- Conceito de vulnerabilidades e ameaças dos ativos;
- Conceitos de integridade, confidencialidade e disponibilidade;
- Conceitos de análise de riscos (AR);
- Conceitos de política de segurança da informação (PSI);
- Conceito de análise de impacto ao negócio (BIA);
- Medidas de segurança;
- Normas de SI;
- Ferramentas;
- ETC.



SI – INTRODUÇÃO



A informação é algo que contém um significado e causa impacto em diferentes graus, tornando-a o elemento chave da extração e criação do conhecimento. O conhecimento só poderá ser formado quando o indivíduo for exposto à informação, deste modo é possível afirmar que poderá até haver informação sem conhecimento, mas não conhecimento sem informação.

SI – INTRODUÇÃO

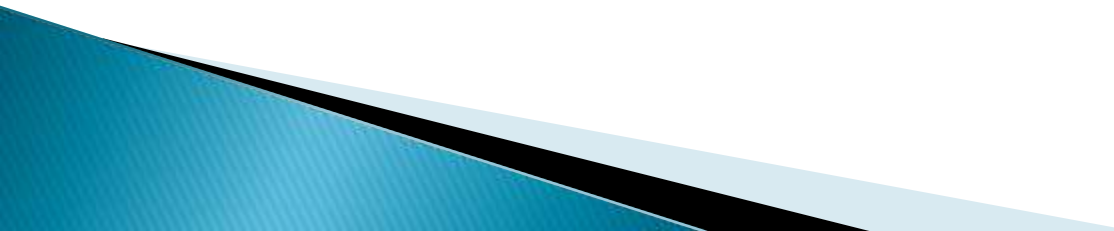
No mundo atual a posse e o uso do conhecimento passou a ser um fator estratégico decisivo para muitas empresas. Estamos vivendo a época batizada como "Era da Informação". Mas a informação é volátil, frágil. Hoje, ela pode desaparecer na velocidade de um pulso elétrico.

Atualmente, as informações constituem o objeto de maior valor para as empresas. Por esse e outros motivos a segurança da informação é um assunto tão importante para todos, pois afeta diretamente todos os negócios de uma empresa ou de um indivíduo.

Importância da Informação para o Negócio – A informação é um elemento essencial para a geração do conhecimento, para a tomada de decisões, e que representa efetivamente valor para o negócio.



SI – CONCEITOS

- **Ativo de Informação:** Qualquer elemento que tenha valor para uma organização.
 - **Valor do Ativo:** Quantificação de perda de determinado ativo quando esse tem sua **confidencialidade, integridade ou disponibilidade (Princípios Básicos da SI)** afetadas.
 - **Vulnerabilidade:** Falha no ambiente que ameace algum ativo.
 - **Ameaça:** Possibilidade de exploração de uma vulnerabilidade.
 - **Impacto:** Resultado da concretização de uma ameaça contra a vulnerabilidade de um ativo.
- 

SI – ATIVOS DE INFORMAÇÃO

- A segurança da informação tem como propósito proteger as **INFORMAÇÕES**, sem importar onde estejam situadas.
- Um sistema de segurança da informação tem por objetivo proteger e controlar os **ATIVOS DE INFORMAÇÃO**, garantindo os três princípios básicos da segurança da informação.



SI – ATIVOS DE INFORMAÇÃO

CLASSIFICAÇÃO DE ATIVOS

INFORMAÇÕES

EQUIPAMENTOS E SISTEMAS

PESSOAS

SOFTWARE
HARDWARE
ORGANIZAÇÃO

SI – ATIVOS DE INFORMAÇÃO

Ativos

Exemplo de Ativo:

Backup

Ativo

BACKUP

Vulnerabilidade

FITAS ANTIGAS



INDISPONIBILIDADE

Ameaças

PERDA DE INFORMAÇÃO

RETRABALHO

Após um longo período de uso as mídias utilizadas no Backup começam a se degradar diminuindo assim a capacidade de armazenar informação.

Você já verificou a data de validade recomendada pelo fabricante de suas fitas de Backup?

SI – ATIVOS DE INFORMAÇÃO

1

Ativos

Exemplo de Ativo:

Software

Ativo

SOFTWARE

Vulnerabilidade

BUG



INDISPONIBILIDADE

Ameaças

PERDA DE INFORMAÇÃO

RETRABALHO

Este exemplo representa um software com uma vulnerabilidade muito comum que é um **Bug**. Este erro submete o ativo a diversas ameaças tais como: a Indisponibilidade, Perda de Informação, Retrabalho.

SI – ATIVOS DE INFORMAÇÃO

Exemplo de Ativo:
Hardware

Ativo

HARDWARE

Vulnerabilidade

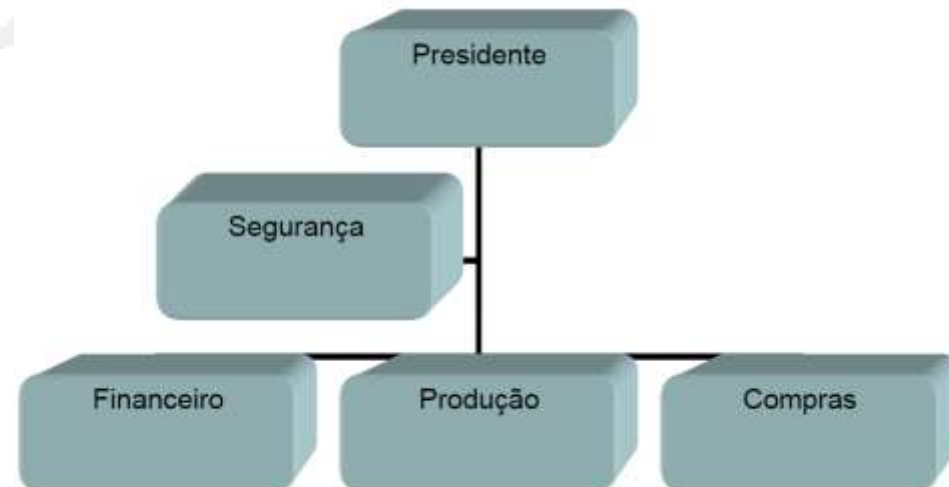
MÁ CONFIGURAÇÃO

Ameaças

INDISPONIBILIDADE

PERDA DE INFORMAÇÃO

RETRABALHO



SI – ATIVOS DE INFORMAÇÃO

Ativos

Exemplo de Ativo:

Humano

Ativo

HUMANO

Vulnerabilidade

DESATUALIZAÇÃO



FRAUDES

Ameaças

PERDA DE INFORMAÇÃO

RETRABALHO

A **desatualização tecnológica** é uma das vulnerabilidades com maior número de ocorrências dentro das organizações..

SI – PRINCÍPIOS BÁSICOS

- Existem três* princípios básicos da segurança da informação, são eles:

- Disponibilidade
- Confidencialidade
- Integridade



- * Existem autores que destacam mais de três, são eles: Autenticidade, Não repúdio, Legalidade, Privacidade e Auditoria

SI – DISPONIBILIDADE

- A informação está acessível à pessoas autorizadas sempre que necessário.

QUEBRA DE DISPONIBILIDADE

- Sistemas fora do ar
- Ataques de Negação de Serviço
- Perdas de Documentos
- Perda de Acesso à informação



SI – CONFIDENCIALIDADE

Somente Pessoas explicitamente autorizadas podem ter acesso à informação.

QUEBRA DE CONFIDENCIALIDADE

- Conversas no elevador, restaurantes, etc. sobre assuntos confidenciais de trabalho, disponibilizando assim a informação para todos à sua volta.
- Engenharia Social



SI – INTEGRIDADE

A informação acessada é completa, sem alterações ou distorções, e portanto, confiável. Mesmo estando errada.

QUEBRA DE INTEGRIDADE

- Falsificação de documentos
- Alteração de registro no BD



SI – VULNERABILIDADES

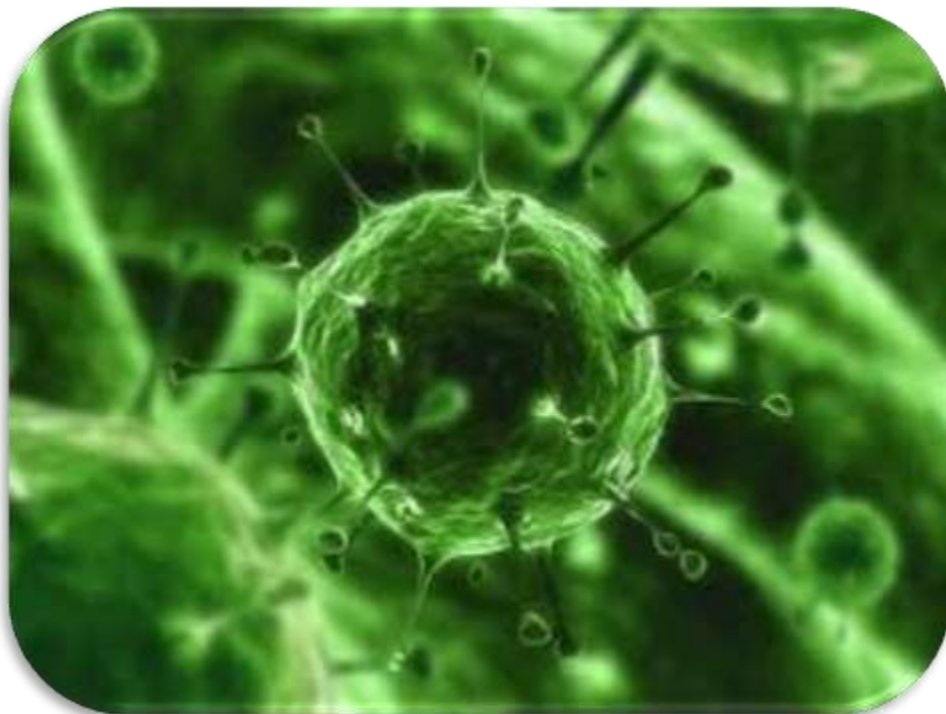
São fraquezas inerentes aos ativos de informação que podem ser exploradas por ameaças ocasionando um incidente de segurança da informação. É possível que um ativo de informação possua uma vulnerabilidade que, de fato, nunca será efetivamente explorada por uma ameaça.



SISTEMA IMUNOLÓGICO FRACO

SI – AMEAÇAS

São agentes externos ao ativo de informação que, exploram as vulnerabilidades pra gerar a quebra de um ou mais dos três princípios básicos da segurança da informação (confidencialidade, integridade e disponibilidade), ou seja, um incidente de segurança da informação.



VÍRUS

SI – INCIDENTES

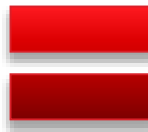
Um incidente de segurança da informação é a ocorrência de um evento que possa interromper os processos do negócio de um ou mais dos três princípios básicos de segurança da informação (confidencialidade, integridade e disponibilidade).



INCIDENTE



VULNERABILIDADE



AMEAÇA



INCIDENTE

SI – PROBABILIDADE

Probabilidade é a chance que um incidente de segurança da informação tem de acontecer, considerando o grau das vulnerabilidades presentes nos ativos de informação e o grau das ameaças que possam explorar essas vulnerabilidades. Mas esses graus são relativos, ou seja, mesmo as mais baixas vulnerabilidades poderão representar probabilidades consideráveis, se o grau da ameaça for muito grande.



“A probabilidade do pão cair com o lado da manteiga virado para baixo é proporcional ao valor do carpete.”

– Joseph Murphy –

SI – IMPACTO

Resultado da ação bem sucedida de uma ameaça ao explorar as vulnerabilidades de um ativo, atingindo assim um ou mais conceitos da segurança da informação. O impacto se denomina pelos danos/prejuízos causados por um incidente de segurança da informação ocorrido no negócio organização.

O tamanho ou grau de um impacto no negócio da organização depende do grau da relevância dos ativos de informação para os processos da organização, ou seja, quanto maior for a relevância do ativo para a organização, maior será o impacto de um incidente de segurança da informação caso ele venha acontecer.

É preciso definir um grau de impacto para cada incidente de segurança da informação que possa vir ocorrer. Este grau de impacto será de extrema importância para o cálculo do risco, que veremos mais à frente.



SI – INTRODUÇÃO

Negócio da Organização

Incidente de Segurança da Informação

Ameaças

Informação

Ativos de Informação

Vulnerabilidades

Confidencialidade

Integridade

Disponibilidade

Grau de Ameaça

Grau de Vulnerabilidade

Impacto

Probabilidade

Risco

SI – ANÁLISE DE IMPACTO AO NEGÓCIO (BIA)

É feita buscando identificar os processos críticos que apoiam o negócio da organização, e qual impacto para o negócio caso as ameaças mapeadas venham a se concretizar.

Calculo do Impacto


$$\text{Impacto} = \frac{(\text{Relevância do Processo} + \text{Relevância do Ativo})}{2}$$

Relevância do Processo: Importância do processo ao negócio.

Relevância do Ativo: Importância do ativo no processo de negócio.



SI – ANÁLISE DE RISCOS (AR)

- É realizada para identificar os riscos aos quais estão submetidos os ativos, ou seja, para saber qual é a probabilidade de que as ameaças se concretizem e o impacto que elas causarão ao negócio.
 - A análise de risco possibilita identificar o grau de proteção que os ativos de informação precisam, podendo assim, não só proporcionar o grau adequado de proteção a esse ativo, mas principalmente utilizar de forma inteligente os recursos da organização.
- 

SI – ANÁLISE DE RISCOS (AR)

Calculo de Risco de um Incidente a um Ativo?

$$\text{Risco} = \frac{(\text{Probabilidade} + \text{Impacto} + \text{Índice ocorrências anteriores})}{3}$$

Onde:

$$\text{Probabilidade} = \frac{(\text{Grau de Ameaça} + \text{Grau de Vulnerabilidade})}{2}$$

$$\text{Índice de Ocorrências} = (\text{Total de dias no ano}^* \text{ em que houve incidentes})$$

* Ano = 365 dias SEMPRE.

SI – ANÁLISE DE RISCOS (AR)

Exemplo de Análise de Risco

- Concluimos que, a partir do momento em que são conhecidos os **RISCOS**, é possível tomar decisões a respeito dos ativos mais críticos.

SI – CONCLUSÃO

- A Segurança da Informação é um processo que envolve todas as áreas de negócio de uma organização e deve ser entendida como mais uma disciplina orientada a atingir a missão estabelecida.

1

Medidas de Segurança

As medidas de Segurança tem como função reduzir ao máximo o impacto das ameaças sobre os ativos.

Sem Medidas De Segurança



Após

Com Medidas De Segurança



Jogo dos 10 erros



RESPOSTAS

OBRIGADO!

Carlos Henrique M. da Silva

carloshenrique.85@globo.com

- Formado em Análise de Sistemas
- Pós-Graduado em Auditoria em T.I.
- Gerente de TI da CLIOC – Coleção de *Leishmania* do Instituto Oswaldo Cruz – Fiocruz
- Certificado em Gestão de Segurança da Informação e Gerenciamento de T.I. pela Academia Latino-Americana (Microsoft TechNet / Módulo Security)

