

# SEGURANÇA DA INFORMAÇÃO APLICADA A NEGÓCIOS



	Norma	Organização responsável
Normas para práticas e controles internos de TI	<b>ITIL®</b>	<b>OGC</b> <small>Official Information Management Capability</small>
	<b>COBIT</b> <small>Control Objectives for Information and Related Technology</small>	<b>IT Governance Institute</b>
	<b>BS15000</b> <b>ISO 20000</b>	<b>BSI</b>   <b>ISO</b> International Organization for Standardization
Normas de segurança de TI	<b>BS 7799</b>	<b>BSI</b>
	<b>ISO/IEC FDIS 17799:2005(E)</b>	<b>ISO</b> International Organization for Standardization
	<b>ABNT NBR ISO/IEC 17799:2005</b>	<b>ABNT</b> ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS



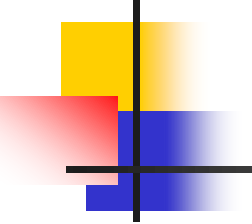
Carlos Henrique M. da Silva  
[carloshenrique.85@globocom.com](mailto:carloshenrique.85@globocom.com)



# Conceitos de Segurança da Informação

---

- **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.



# Informação e sua Importância para o Negócio da Organização

---

- A informação é um elemento essencial para a geração do conhecimento, para a tomada de decisões, e que representa efetivamente valor para o negócio dentro de cada um de seus processos.
- O custo para proteger esse Ativo cresce cada vez mais. Segurança movimentará US\$ 244 mi em 2011 no Brasil. Segundo a consultoria Frost & Sullivan, mercado local de SI deve crescer 17% este ano e atingir faturamento de US\$ 460 milhões em 2016.
- Entendemos que a informação representa valor para o negócio, conforme foi citado acima, então, podemos afirmar que a informação é um bem, um ativo da organização, por isso, deve ser preservado e protegido da mesma forma que os demais ativos da organização.



# Segurança da 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.

# Princípios básicos da Segurança da Informação

- 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

# 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





# 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



# 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







# Política de Segurança da Informação (PSI)

---

- A Política de Segurança da Informação é formada por um conjunto de normas e procedimentos que de algum modo regulam o comportamento dos funcionários.
- Deve indicar como as coisas devem acontecer na organização no que se refere à segurança da informação.
- Objetivo Principal: Estabelecer um padrão de comportamento que seja conhecido por todos na organização e que sirva como base para decisões da alta administração em assuntos relacionados com a segurança da informação.

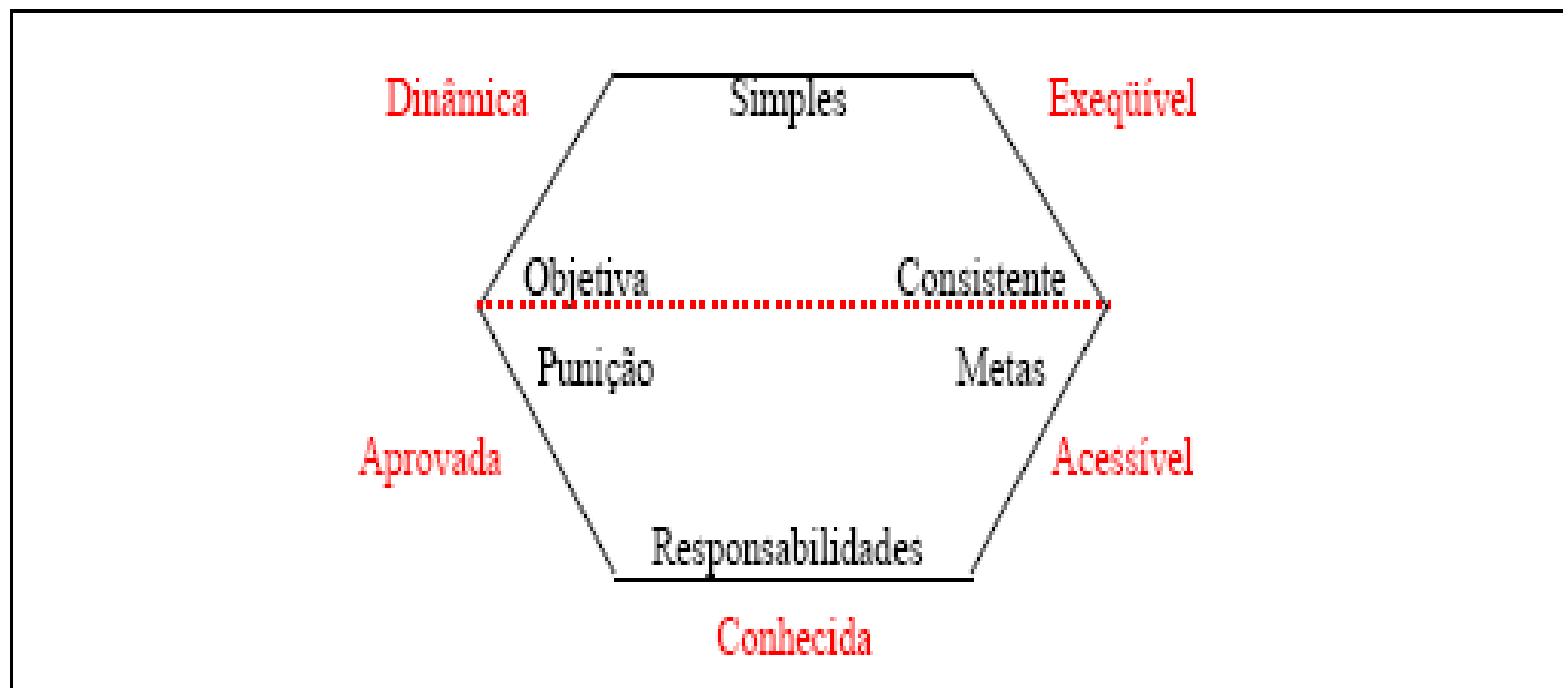


# Estrutura da Política de Segurança da Informação (PSI)

---

- 1. Definições gerais;**
  - a. Carta do diretor;**
  - b. Conceitos de SI.**
- 2. Objetivos e metas;**
- 3. Responsabilidades pela PSI;**
- 4. Registro de incidentes;**
- 5. Diretrizes;**
- 6. Normas;**
- 7. Revisão da PSI;**
- 8. Questões Legais e de Regulamentação;**
- 9. Pensando na Auditoria;**
- 10. Composição da Política\*;**
- 11. Características Inerentes da Política\*;**
- 12. Características de Uso da Política\*.**

# Composição, Características Inerentes e de Uso da Política de Segurança da Informação (PSI)



Fatores Externos



Fatores Internos



# Análise de Impacto ao Negócio (BIA)

---

- A Análise de Impactos nos Negócios é feita buscando identificar os processos críticos que apóiam o negócio da organização, e qual impacto para o negócio caso as ameaças mapeadas venham a se concretizar.

## **Calculo do Impacto**

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

Relevância do Processo: Quão importante é o processo ao negócio da organização.

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



# Análise de Risco (RA)

---

- 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.
- A relevância de cada um dos processos de negócio na empresa é um ponto-chave que deve ser considerado durante a realização da análise de riscos.



# Análise de Risco (RA)

---

## **Como Calcular o Risco de um Incidente acontecer com um Ativo?**

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

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

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



# Análise de Risco (RA)

---

## 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.

# Normas

	Norma	Organização responsável
Normas para práticas e controles internos de TI	<b>ITIL</b> ®	<b>OGC</b> <small>Office of Government Commerce</small>
	<b>COBIT</b> <small>GOVERNANCE, CONTROL, and AUDIT for INFORMATION and RELATED TECHNOLOGY</small>	<b>IT</b> <small>GOVERNANCE INSTITUTE®</small>
	BS15000	<b>BSi</b>
	ISO 20000	<b>ISO</b> International Organization for Standardization
Normas de segurança de TI	BS 7799	<b>BSi</b>
	ISO/IEC FDIS 17799:2005(E)	<b>ISO</b> International Organization for Standardization
	ABNT NBR ISO/IEC 17799:2005	<b>ABNT</b> ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS





# Normas

---

- **ITIL:** Melhores práticas para prover a qualidade de serviços de TI
- **COBIT:** Práticas que auxiliam a gestão e controle de iniciativas de TI
- **BS 15000:** Foi a 1ª norma formal para gestão de serviços de TI. Fornece especificações claras para implementação de um processo de gestão de TI.
- **ISO 20000:** Substituiu a BS 15000 em 5/12/2005.
- **ISO 17799:2005:** Código de práticas com orientações para gestão de SI.
- **“Família” ISO 27000:** Incluem normas sobre requisitos de sistemas de gestão de SI, gestão de riscos, métricas e medidas, e diretrizes para implementação.



# Normas

NORMA	PONTO FORTE	PONTO FRACO
ITIL	Processos de operação	Segurança e desenvolvimento de sistemas
COBIT	- Controles - Métricas - Processos	São linhas gerais que não indicam “como” fazer
ISO 17799	Controle de segurança	É um guia genérico sem material específico

- As normas podem ser aplicadas de forma conjunta na busca pela excelência nos serviços de TI.

# 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.





**Carlos Henrique M. da Silva**  
**[carloshenrique.85@globo.com](mailto:carloshenrique.85@globo.com)**

---

**OBRIGADO!**

- 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)

