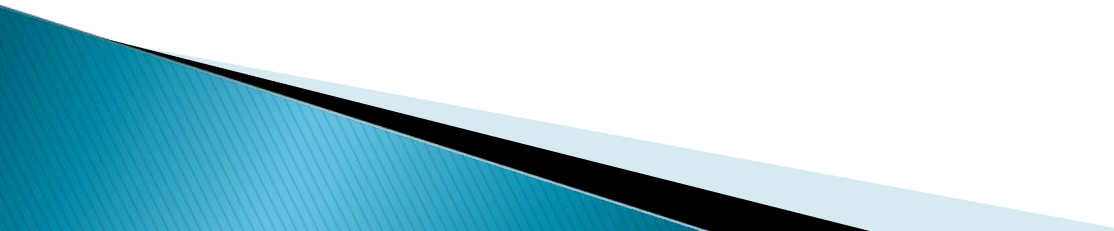


# Segurança da Informação (SI)



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

# Política de Segurança da Informação

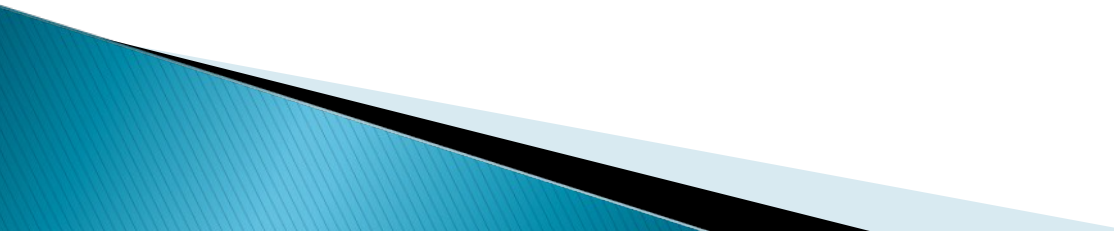
- ▶ A Política de Segurança da Informação é formada por um conjunto de Procedimentos, Normas, Diretrizes e Instruções que comanda as atuações de trabalho e define os critérios de segurança para que sejam adotados com o OBJETIVO de estabelecer, padronizar e normatizar a segurança e seus processos tanto no escopo humano como no tecnológico.
  - ▶ 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.
- 

# Política de Segurança da Informação

Muita gente confunde o que é uma norma e o que é uma diretriz, por isso vou citar um exemplo que contém as diferenças entre as duas:

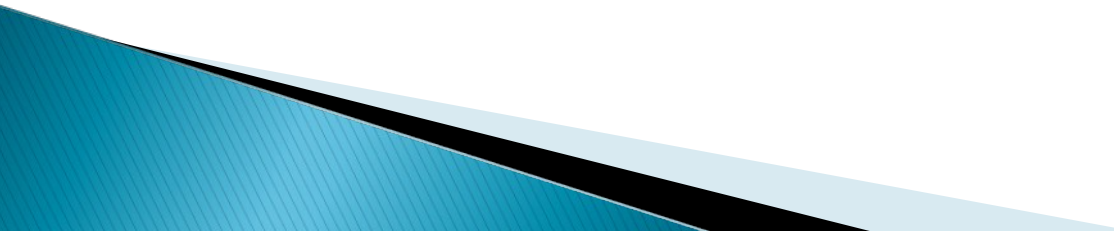
<b>DIRETRIZ</b> (abrangente)	<b>NORMA</b> (específica)
A diretriz é uma ordem. Exemplo: Todos os acessos a áreas críticas de informação deverão ser controlados e monitorados.	Um exemplo de como identificar uma norma é baseando-se no modelo dos <b>5W e 1H</b> . → COMO – <b>HOW</b> → O QUE – <b>WHAT</b> → QUEM – <b>WHO</b> → QUANDO – <b>WHEN</b> → OBJETIVO – <b>WHY</b> → ONDE – <b>WHERE</b>

# LEGISLAÇÃO E REGULAMENTAÇÃO

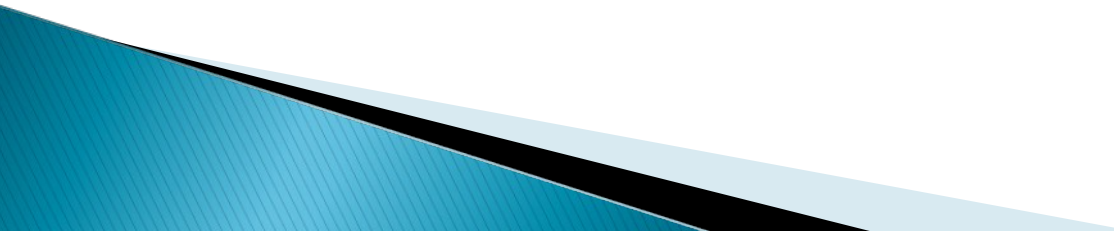
- ▶ É muito importante lembrar que a PSI não é um documento independente com regras de conduta desconexas de tudo o que já existe. NÃO, a política é na verdade a continuidade de regras, normas e leis já existentes. De fato é a especificação e detalhamento maior desses atos legais.
  - ▶ Se a empresa possuir algum regimento ou regulamento interno, este deve ser não apenas respeitado mas como também referenciado na PSI, o mesmo deve acontecer com as normas e as leis.
  - ▶ Por exemplo, as punições previstas para o não-cumprimento da PSI devem respeitar as leis trabalhistas, como a CLT.
- 

# NORMAS PARA PSI

Algumas normas definem aspectos que devem ser levados em consideração ao elaborar uma PSI. Entre essas normas estão a **BS 7799** (elaborada pela British Standards Institution) e a **NBR ISO/IEC 17799** (a versão brasileira desta primeira). A ISO começou a publicar a série de normas **27000**, em substituição à ISO 17799 (e por conseguinte à BS 7799), das quais a primeira, **ISO 27001**, foi publicada em 2005.



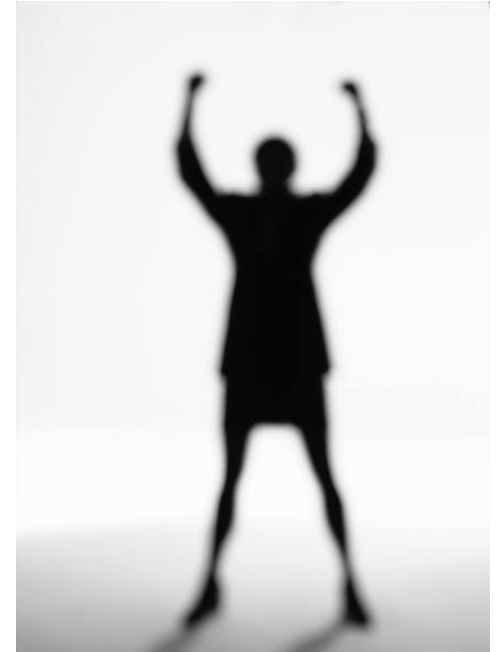
# ANÁLISE DE RISCOS

- ▶ A política deve estar baseada na análise de risco e ter como objetivo a padronização de ambientes e processos de forma a diminuir os riscos. Sua criação está diretamente ligada à concretização dessa análise pois, através do levantamento das vulnerabilidades, pode-se elaborar a documentação de segurança, com o objetivo de minimizar os riscos de que as ameaças se transformarem em incidentes.
- 



# ÁREAS DE NORMALIZAÇÃO DA PSI

- ▶ PROCESSUAL
- TECNOLÓGICA
- HUMANA



# ÁREAS DE NORMALIZAÇÃO DA PSI

## PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

- ▶ Formalizar os processos de segurança que serão implementados na empresa. Exemplos destes processos são: a classificação da informação, o processo de análise de riscos e as responsabilidades e alçadas de decisão neste e processos de exceção às normas de segurança, afinal, estas não de haver.

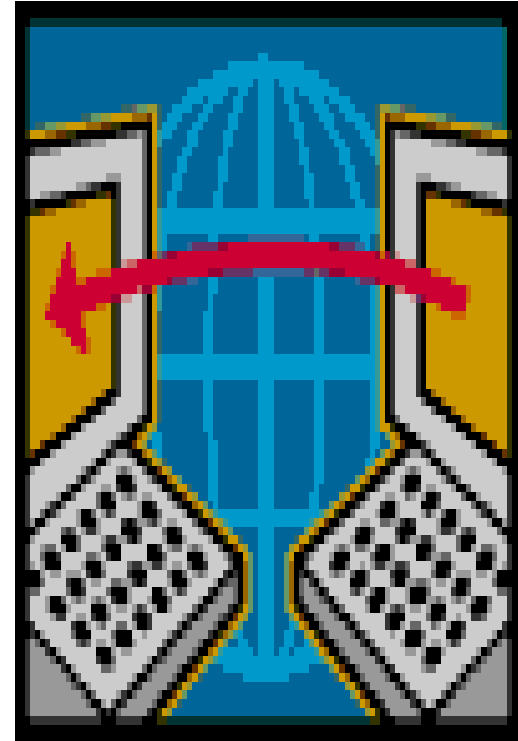




# ÁREAS DE NORMALIZAÇÃO DA PSI

## TECNOLÓGICA

- Alguns consideram que a segurança das informações é apenas um problema tecnológico. Mas o importante é definir os aspectos mais relevantes e críticos do bom funcionamento de servidores, estações de trabalho, acesso à Internet, etc. Para isso, o apoio da administração é fundamental, pois sem ela o programa de segurança ficaria sem investimentos para a aquisição dos recursos necessários. No entanto, não se deve deixar de lado as questões relacionadas à boa conduta e à ética profissional dos usuários.



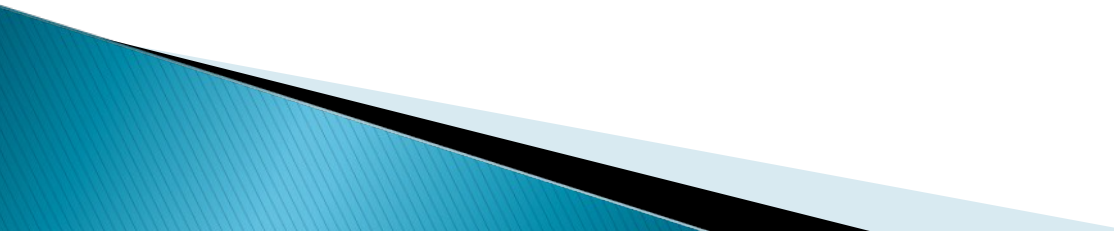
# ÁREAS DE NORMALIZAÇÃO DA PSI

## HUMANA

- ▶ Outros vêem a segurança como um problema unicamente humano. É importante **definir primeiro a conduta considerada adequada para o tratamento das informações** e dos recursos utilizados. Assim, sem o apoio da administração, o programa de segurança não consegue dirigir as ações necessárias para modificar a cultura da segurança atual. O resultado é um programa de segurança sem o nível de **cultura** desejado e a falta de um monitoramento mais apropriado ao orientar funcionários, fornecedores, clientes e parceiros. No entanto, **não se deve deixar de lado as questões tecnológicas e sua sofisticação**, uma vez que também são fatores determinantes para a implementação de soluções de segurança adequadas e eficientes.



# ELABORAÇÃO DA PSI

- ▶ Para elaborar uma política de segurança da informação, é importante levar em consideração as exigências básicas e as etapas necessárias para a sua produção.
    - A) Exigências da política
    - B) Etapas de produção
- 

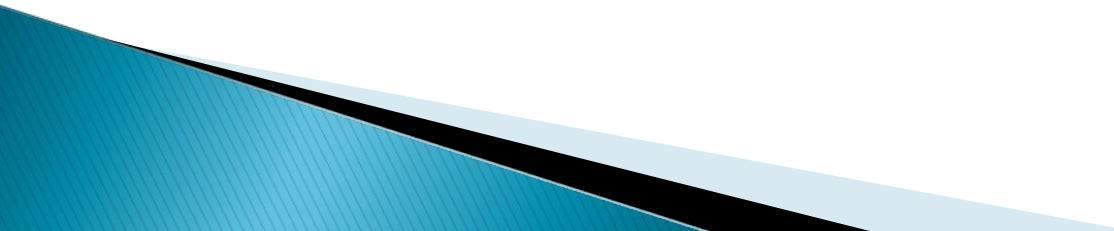
# ELABORAÇÃO DA PSI

## EXIGÊNCIAS DA PSI

- ▶ A política é elaborada tomando-se como base a, legislação existente, cláusulas contratuais, a cultura da empresa e o conhecimento especializado de segurança dos profissionais envolvidos na sua aplicação e comprometimento. É importante considerar que para a elaboração de uma política de segurança institucional é preciso:
  - **Criar o Comitê de Segurança responsável por diversas definições que constarão na política;**
  - **Elaborar o documento final.**
  - **Oficializar o uso da política.**

# ELABORAÇÃO DA PSI

## INTEGRAR O COMITÊ DE SEGURANÇA

- ▶ Formar uma equipe multidisciplinar que represente grande parte dos aspectos culturais, técnicos e administrativos da empresa e que se reúna periodicamente dentro de um cronograma pré-estabelecido.
  - ▶ Esse comitê é formado por um grupo de pessoas responsáveis por atividades referentes à criação e aprovação de requisitos e demandas de segurança na empresa.
  - ▶ Nas reuniões, são definidos os critérios de segurança adotados em cada área e o esforço comum necessário para que a segurança alcance tais critérios.
- 



# ELABORAÇÃO DA PSI


## PARTES QUE INTEGRAM O DOCUMENTO FINAL

Devem aparecer as preocupações da administração no que se refere à segurança para que todas as normas, procedimentos e instruções possam vir a serem definidos. Deve também conter:

- A definição da própria política e seus objetivos;
- Uma declaração da administração que apoie os princípios estabelecidos e uma explicação das exigências de conformidade com relação a:
  - Legislação e cláusulas contratuais;
  - Educação e formação em segurança da informação;
  - Prevenção contra ameaças (vírus, hackers, incêndios, intempéries, etc.)

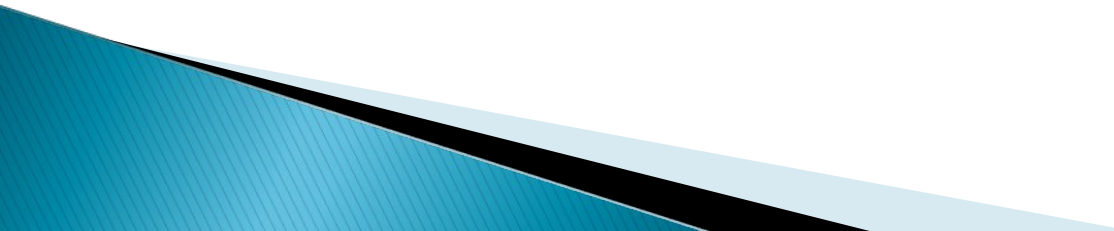
# ELABORAÇÃO DA PSI

## PARTES QUE INTEGRAM O DOCUMENTO FINAL

- ▶ Deve conter também a atribuição das responsabilidades das pessoas envolvidas, ficando claro os papéis de cada um na gestão e execução dos processos no que diz respeito a segurança;
  - ▶ Não esquecer que toda documentação já existente sobre como realizar as tarefas deve ser analisada com relação aos princípios de segurança das informações, para aproveitar ao máximo as práticas atuais, avaliando e agregando segurança a essas tarefas.
- 

# ELABORAÇÃO DA PSI

## OFICIALIZAR A POLÍTICA

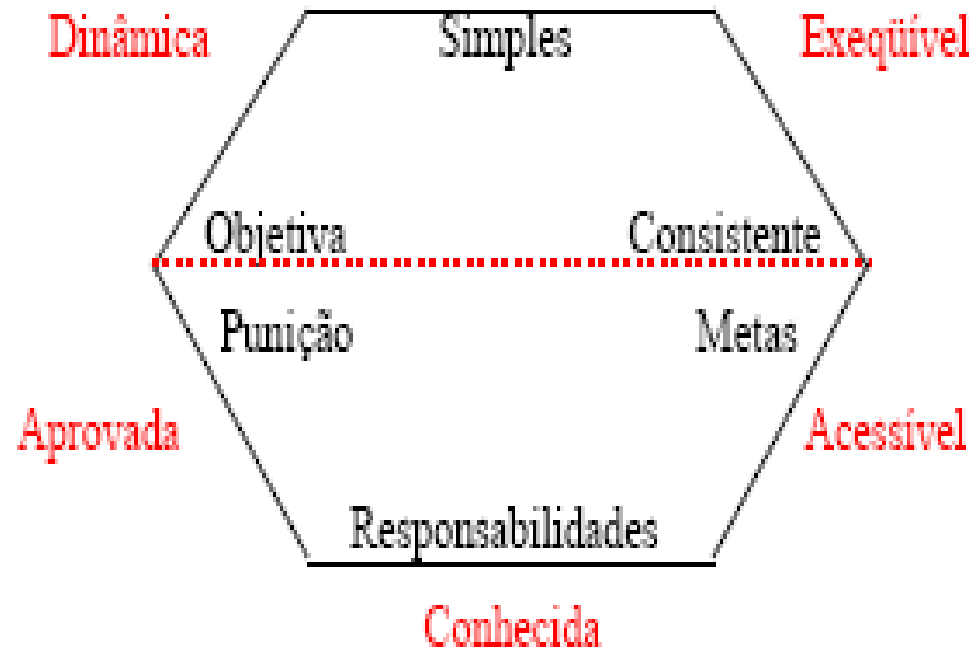
- ▶ A oficialização de uma política tem como base a sua aprovação por parte da administração da empresa.
  - ▶ Deve ser publicada e comunicada de maneira adequada para todos os funcionários, parceiros, prestadores de serviços e clientes.
  - ▶ Uma vez que as políticas são guias para orientar a ação das pessoas que interagem com os processos da empresa, apresentamos a seguir exemplos que ilustram como essas ações podem comprometer a eficácia da política de segurança.
- 

# ESTRUTURA DA 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\*.


\* ILUSTRADOS NO PRÓXIMO SLIDE

# COMPOSIÇÃO, CARACTERÍSTICAS INERENTES E DE USO DA PSI

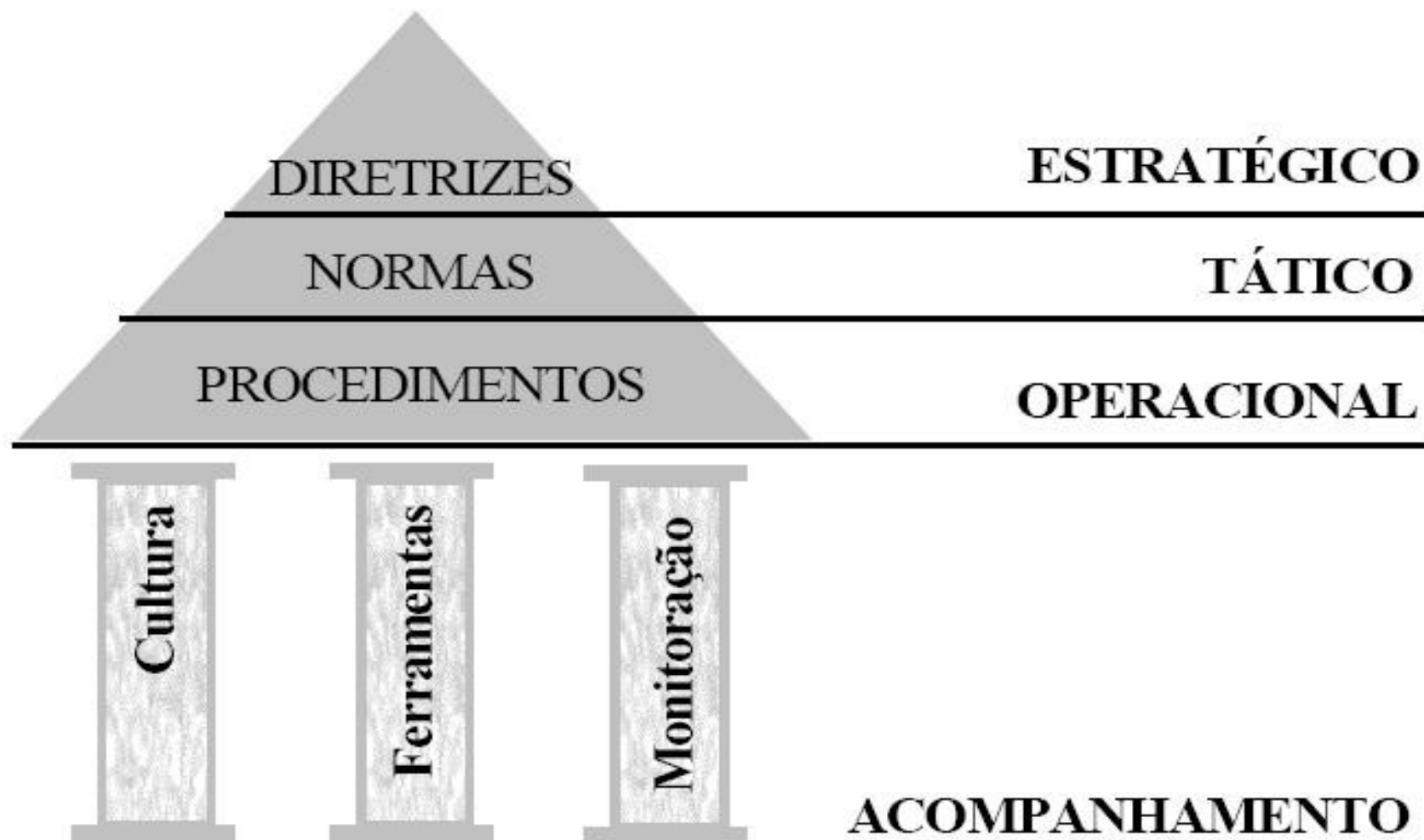




# DOCUMENTOS DA PSI


- ▶ Caso já exista um padrão de estruturação de documentos para as políticas dentro da empresa, ele pode ser adotado. No entanto, sugerimos a seguir um modelo de estrutura de política que pode ser desenvolvido dentro da sua organização. Apesar de mudanças de nomenclatura de empresa para empresa, é muito freqüente encontrar esta divisão em três níveis. Nesse modelo, vemos que uma política de segurança está formada por três grandes seções:
    - **Diretrizes;**
    - **Normas;**
    - **Procedimentos e as Instruções de Trabalho.**
- 

# DOCUMENTOS DA PSI




# DOCUMENTOS DA PSI

## DIRETRIZES (ESTRATÉGICO)

- ▶ **Conjunto de regras gerais de nível estratégico** em que são expressados os valores de segurança da organização que a empresa entende como sendo importantes. É endossado pelo líder empresarial da organização e tem como base sua **visão e missão** para abarcar toda a filosofia de segurança das informações.
  - ▶ As diretrizes **correspondem às preocupações da empresa sobre a segurança das informações**, ao estabelecer seus objetivos, meios e responsabilidades.
  - ▶ As diretrizes estratégicas, no contexto da segurança, correspondem a todos os **valores que devem ser seguidos** para que o principal patrimônio da empresa, que são as informações, tenha o nível de segurança exigido.
- 

# DOCUMENTOS DA PSI

## NORMAS (TÁTICO)


- ▶ Conjunto de **regras gerais da segurança das informações** que devem ser usadas por todos os segmentos envolvidos nos processos de negócio da instituição e que normalmente são elaboradas com foco em assuntos mais específicos como controle de acesso, uso da Internet, uso do correio eletrônico, acesso físico, etc.
  - ▶ As normas, por estarem em um **nível tático, podem ser específicas para o público a que se destinam**. Normalmente esta divisão ocorre para:
    - Normas de segurança para técnicos;
    - Normas de segurança para usuários.
- 

# DOCUMENTOS DA PSI

## NORMAS DE SEGURANÇA PARA TÉCNICOS

- ▶ Regras gerais de segurança da informação dirigidas para os que cuidam de ambientes informatizados (administradores de rede, analistas, etc.), elaboradas de forma genérica cobrindo coisas como periodicidade para troca de senhas, backups, acesso físico e outros.

## NORMAS DE SEGURANÇA PARA USUÁRIOS

- ▶ Regras gerais de segurança das informações com o propósito de regular a utilização dos recursos, elaborada de forma genérica cobrindo coisas como cuidados com senhas, procedimentos para autorizar um acesso que os usuários solicitam, cuidados no uso do e-mail, entre outros.
- 



# DOCUMENTOS DA PSI

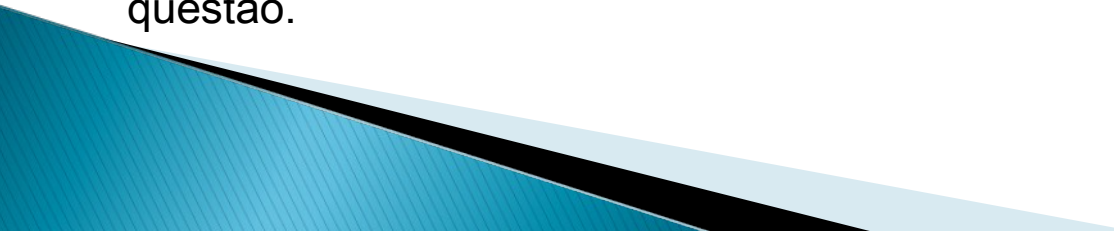
## PROCEDIMENTOS E INSTRUÇÕES DE TRABALHO (OPERACIONAL)

### ► PROCEDIMENTOS

Conjunto de orientações para realizar atividades operacionais relacionadas a segurança. Estas atividades operacionais envolvem procedimentos passo a passo que são detalhados, permitindo que sua execução seja padronizada, garantindo a observação de aspectos de segurança.

### ► INSTRUÇÕES DE TRABALHO

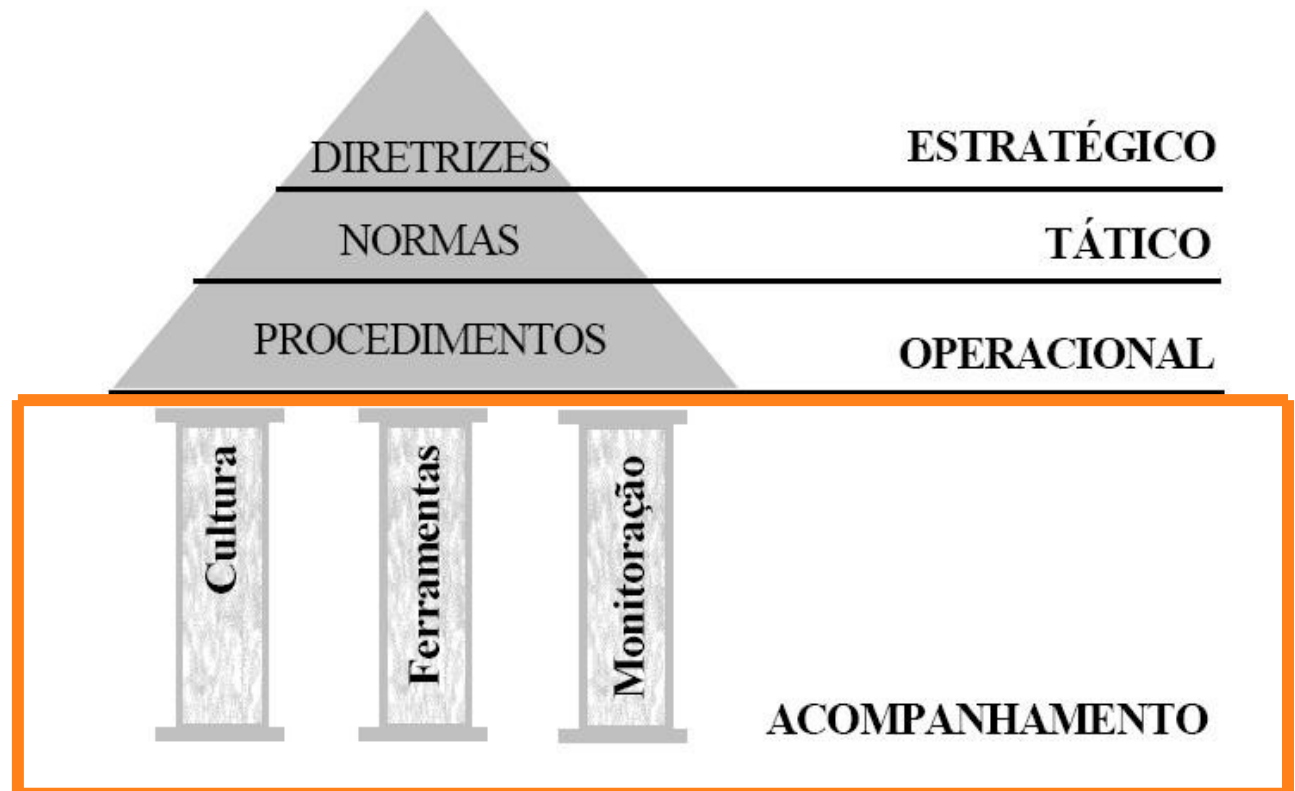
Conjunto de comandos operacionais a serem executados no momento da realização de um procedimento de segurança estabelecido por uma norma para os usuários em questão.



# ACOMPANHAMENTO DA POLÍTICA

- ▶ Para que seja efetiva, a política de segurança precisa contar com os seguintes elementos como base de sustentação:

- Cultura
- Ferramentas
- Monitoramento



# ACOMPANHAMENTO DA POLÍTICA

## CULTURA

- ▶ O treinamento de pessoas deve ser constante, de forma que toda a empresa esteja atualizada em relação aos conceitos e normas de segurança, além de formar a consciência de segurança para torná-la um esforço comum entre todos os envolvidos.



Cultura

# ACOMPANHAMENTO DA POLÍTICA

## FERRAMENTAS

- ▶ Os recursos humanos, financeiros e as ferramentas devem estar de acordo com as necessidades de segurança. Parte da segurança pode ser automatizada ou mais bem controlada com ferramentas específicas, como dispositivos de controle de acesso, mecanismos antifraude, etc.



Ferramentas

# ACOMPANHAMENTO DA POLÍTICA

## MONITORAMENTO

- ▶ A implementação da política de segurança deve ser **constantemente monitorada**. É necessário efetuar um ciclo de manutenção para manter a política sempre atualizada e refletindo a realidade da empresa. Deve-se também **adaptar a segurança às novas tecnologias**, às mudanças administrativas e ao surgimento de novas ameaças.



MONITORAMENTO



# IMPLANTAÇÃO DA POLÍTICA

O sucesso da implantação de um sistema e uma política de segurança na empresa depende em grande parte do profundo conhecimento dos processos envolvidos nessa implantação.

Uma política se encontra bem implementada quando:

- Reflete os objetivos do negócio, isto é, está sempre de acordo com os requisitos necessários para alcançar as metas estabelecidas.
- Agrega segurança aos processos de negócio e garante um gerenciamento inteligente dos riscos.
- Está de acordo com a cultura organizacional e está sustentada pelo compromisso e pelo apoio da administração.
- Permite um bom entendimento das exigências de segurança e uma avaliação e gerenciamento dos riscos a que a organização está submetida.

# IMPLANTAÇÃO DA POLÍTICA

A IMPLANTAÇÃO DA PSI DEPENDE DE:

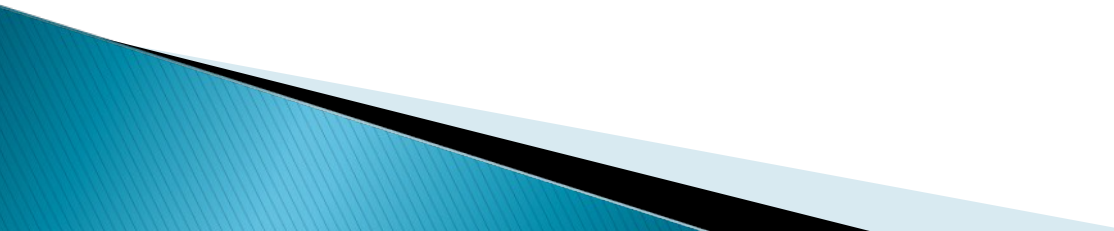
- ▶ Uma boa estratégia de divulgação entre os usuários.
- ▶ Campanhas, treinamentos, bate-papos de divulgação, sistemas de aprendizagem.
- ▶ Outros mecanismos adotados para fazer da segurança um elemento comum a todos.



# TEMAS DA POLÍTICA

Para elaborar uma política, é necessário **delimitar os temas que serão transformados em normas.**

A divisão dos temas de uma política depende das necessidades da organização, e sua delimitação é feita a partir de:

- Conhecimento do ambiente organizacional, humano e tecnológico;
  - Compilação das preocupações sobre segurança por parte dos usuários, administradores e executivos da empresa.
- 

# TEMAS DA POLÍTICA

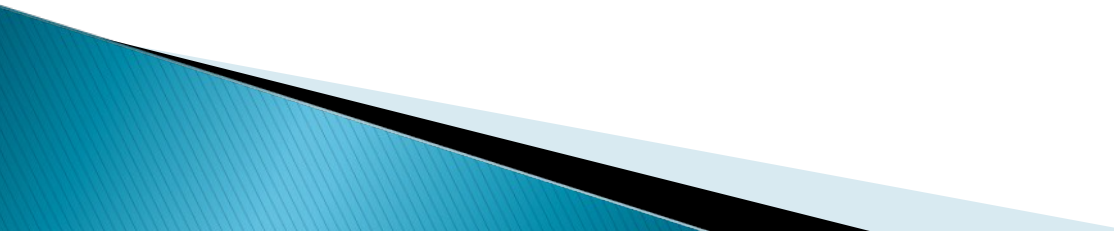
## ALGUNS EXEMPLOS DE TEMAS POSSÍVEIS SÃO:

- ▶ **Segurança física:** acesso físico, infra-estrutura do edifício, datacenter.
- ▶ **Segurança da rede corporativa:** configuração dos sistemas operacionais, acesso lógico e remoto, autenticação, Internet, gerenciamento de mudanças, desenvolvimento de aplicativos.
- ▶ **Segurança de usuários:** composição de senhas, segurança em estações de trabalho.
- ▶ **Segurança de dados:** criptografia, classificação, privilégios, cópias de segurança e recuperação, antivírus, plano de contingência.
- ▶ **Aspectos legais:** práticas pessoais, contratos e acordos comerciais, leis e regulamentações governamentais.

# USOS DA POLÍTICA


Uma vez elaborada, a política de segurança é importante para garantir que haja controles adequados após a sua implementação.

Ela deve cumprir com pelo menos dois propósitos:

- Ajudar na seleção de produtos e no desenvolvimento de processos.
  - Realizar uma documentação das preocupações da direção sobre segurança para garantir o negócio da empresa.
- 


# USOS DA POLÍTICA

Quando a política é utilizada de forma correta, podemos dizer que traz algumas vantagens como:

- Permite definir controles em sistemas.
  - Permite estabelecer os direitos de acesso com base nas funções de cada pessoa.
  - Permite a orientação dos usuários em relação à disciplina necessária para evitar violações de segurança.
  - Estabelece exigências que pretendem evitar que a organização seja prejudicada em casos de quebra de segurança.
  - Permite a realização de investigações de delitos nos computadores.
  - É o primeiro passo para transformar a segurança em um esforço comum.
- 

# CONCLUSÃO

COMO UMA POLÍTICA DE SEGURANÇA TEM UM IMPACTO NA FORMA DE TRABALHO DIÁRIO DAS PESSOAS, ELA DEVE SER:

- ▶ CLARA (escrita em boa forma e linguagem formal, porém acessível);
  - ▶ CONCISA (evitar informações desnecessárias ou redundantes);
  - ▶ DE ACORDO COM A REALIDADE PRÁTICA DA EMPRESA (para que possa ser reconhecida como um elemento institucional).
  - ▶ ATUALIZADA PERIODICAMENTE (Revisão da PSI).
- 



# 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)

