

# Política de Segurança da Informação e Comunicações (POSIC)



O SEGREDO É A ATITUDE

A *idade*

**DICA** Disponibilidade

*Significa estar acessível e utilizável quando demandado*

**I**ntegridade

*Propriedade de salvaguarda da exatidão de informações*

**C**onfidencialidade

*Garantia da proteção contra revelação não autorizada*

**A**utenticidade

*Certeza absoluta de que a informação provém de fontes anunciadas e que não foi alvo de mutações ao longo da transmissão*

## O que é Política de Segurança da Informação?

### Definição ABNT NBR ISO/IEC 27002

Prover uma orientação e apoio da direção para Segurança da Informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

## Por que é importante?

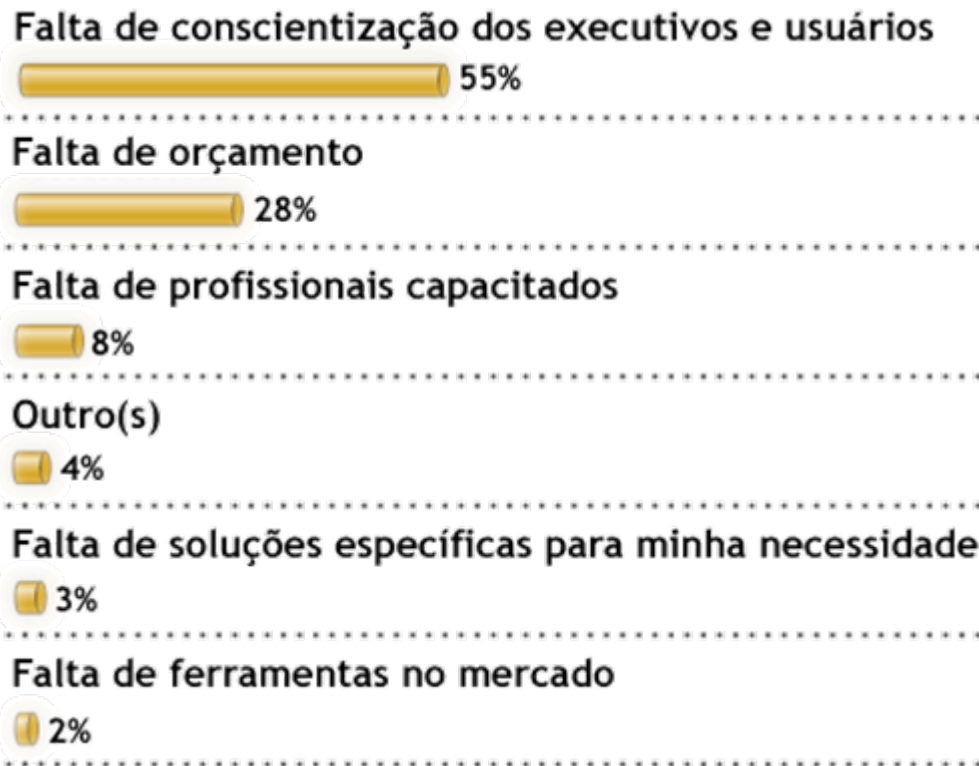
- Serve como **linha-mestra** das atividades relacionadas à Segurança da Informação e Comunicações.
- Demonstra o **comprometimento** da alta direção com a Segurança da Informação.
- Busca garantir a implementação de controles de segurança apropriados. Ela é usada para auxiliar na seleção de produtos e no desenvolvimento de processos e documentos.

## O que está contemplado pela POSIC do Ministério da Saúde?

- Ativos de maior relevância de acordo com a estratégia da política nacional de informação e informática em saúde.



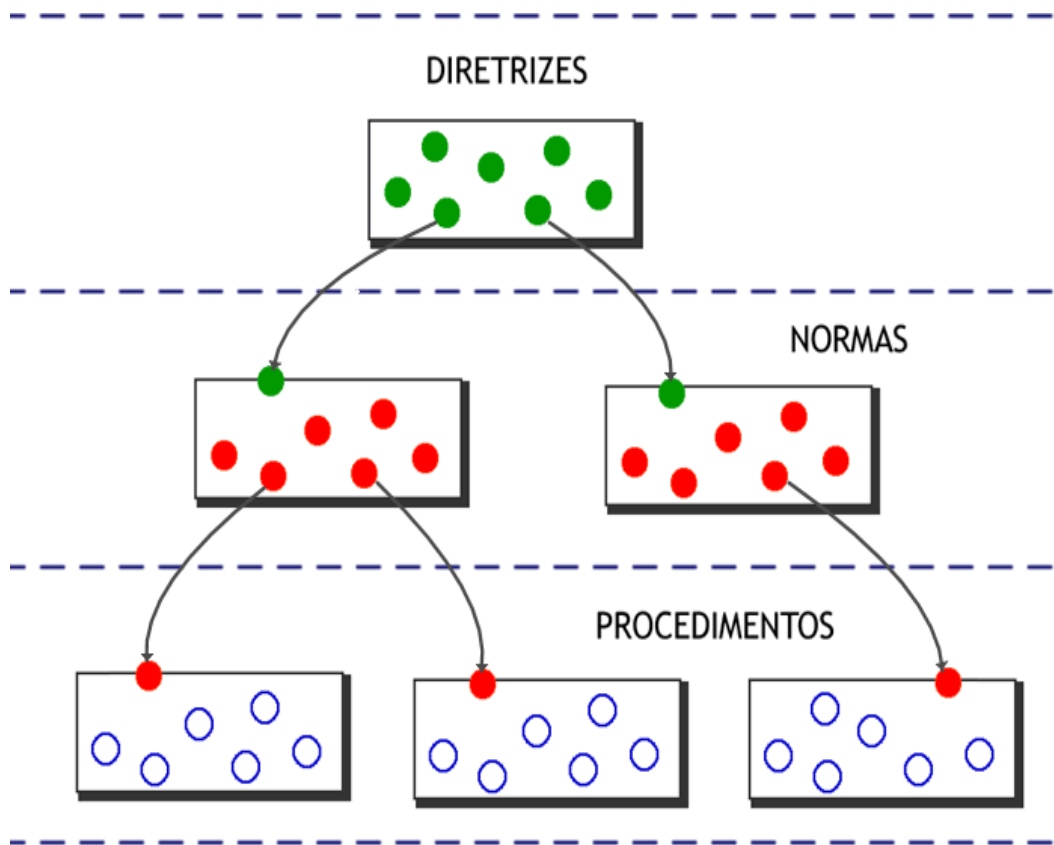
## Maiores obstáculos para implementação de uma Política de Segurança da Informação.



Fonte: PESQUISA NACIONAL DE SEGURANÇA DA INFORMAÇÃO 2006 - Módulo Security Solutions S/A

## Alinhamento estratégico

- Estruturação



34 Diretrizes

25 Normas

“N”  
Procedimentos

## Requisitos e Motivadores

- LEGAIS (até 2006)  
Decreto lei nº 3.505/2002  
Acórdão TCU 461/2004

- LEGAIS (após 2006)  
Instrução Normativa GSI/PR nº 01 de 2008  
Norma Complementar GSI/PR nº 03 de 2009

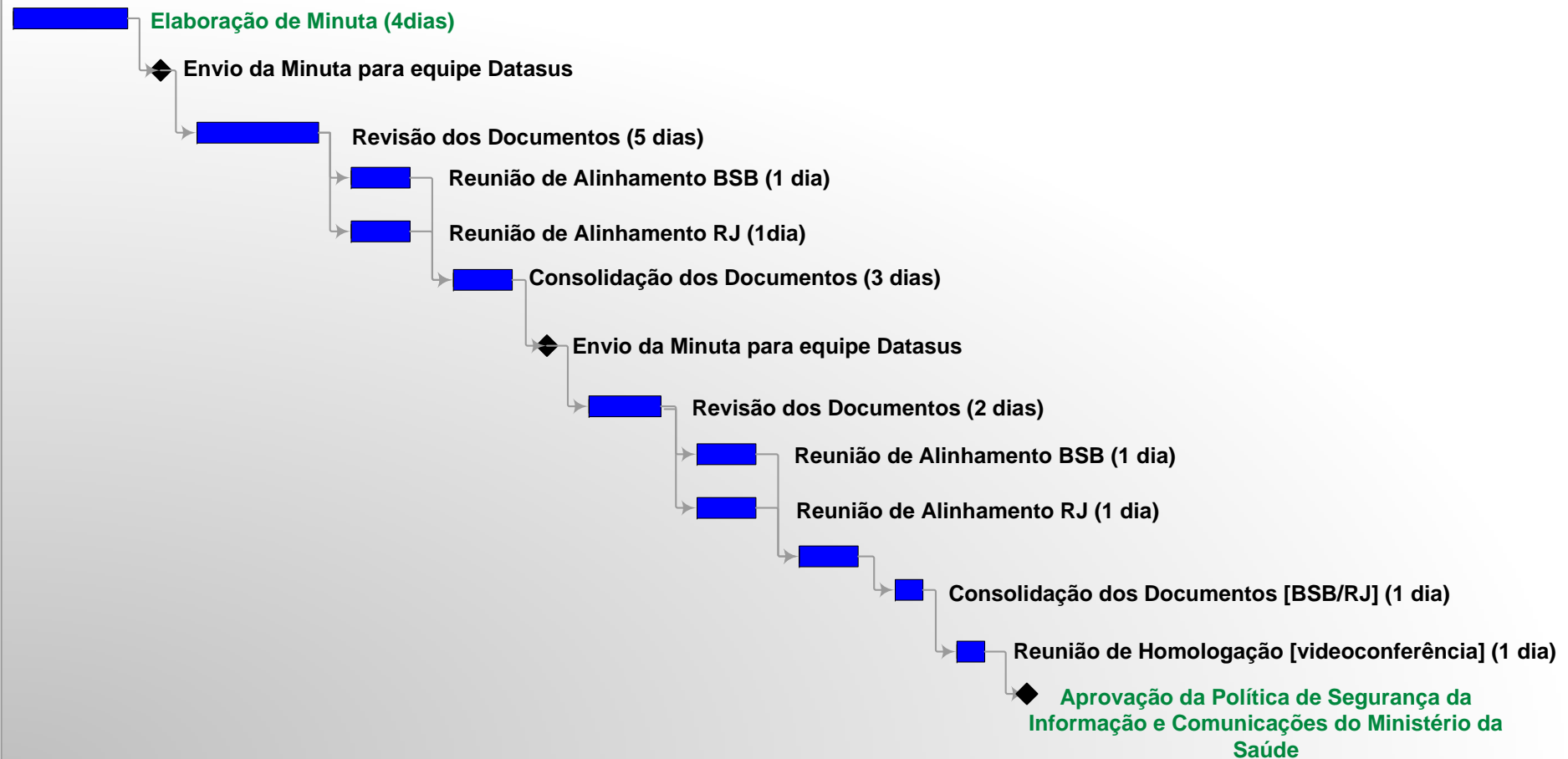
- ESPECÍFICOS  
Política Nacional de Informação e Informática em Saúde (PNIIS)



## Motivadores

<b>Decreto 3.505/ 2002</b>	<b>IN 01 GSI/ PR</b>	<b>Acórdão TCU 461/ 2004</b>
I - dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;	VII - aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações;	"...as inconformidades têm origem na inexistência de uma política de segurança formal, que deve abranger tanto a segurança física quanto a lógica. Resta então se recomendar ao Datasus que a política de segurança a ser implementada contemple a educação e o treinamento em segurança de informação."

## Plano de execução – Método de trabalho



## Marcos principais

- Desenvolvida entre junho e agosto de 2007 (Equipes Datasus RJ e BSB)
- Aprovada e publicada em 09 de julho de 2008 (portaria nº 207, publicada no D.O.U.)

## Princípios utilizados

- Não ser proibitiva
- Conceituada a partir de análises de riscos
- Segurança como facilitador no alcance de objetivos estratégicos do Ministério da Saúde
- Custo < Benefício
- Responsabilidade de todos, sem exceção
- Segurança aplicada aos processos, pessoas, ambientes e tecnologia.

## Princípios da PNIIS na POSIC

- PNIIS (diretriz)

7. Dotar a área de saúde de **instrumentos jurídicos, normativos e organizacionais** que a capacite a **assegurar a confidencialidade, a privacidade e a disponibilidade dos dados e das informações** individualmente identificadas em saúde, garantindo a sua autenticidade e integridade, através de certificação digital.

## POSIC Datasus

- Diretrizes:
  - Propriedade da Informação
  - Classificação da Informação
  - Permissão de acesso
  - Continuidade dos Negócios
  - Treinamento e Capacitação
  - Monitoramento

## Resultados Imediatos

- Aumento do investimento em Segurança da Informação e Comunicações no MS/Datasus
- Disponibilização de Recursos Humanos para a coordenação de atividades de SIC.
- Criação de comitês (operacional e gestor)
- Estabelecimento de um plano diretor de segurança da informação para o período 2008/2011
- Conscientização das equipes internas do Datasus

## Próximos Passos

- Estabelecer oficialmente uma coordenação de segurança da informação e comunicações no Datasus
- Divulgar a POSIC para todos os colaboradores
- Conscientizar e educar constantemente (campanha de divulgação da POSIC)



## Conscientização – campanha





# Segurança da Informação

O SEGREDO É A ATITUDE

# Política de Segurança da Informação e Comunicações (POSIC)



O SEGREDO É A ATITUDE