

 MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES AGÊNCIA ESPACIAL BRASILEIRA	Nº da Norma Complementar à POSIC/AEB	Revisão	Emissão	Folha
	05/GTPOSIC/AEB	-	-	01/03
<b>Auditoria e Conformidade</b>				

## ORIGEM

**Grupo de Trabalho da Política de Segurança da Informação e Comunicações - AEB**

## REFERÊNCIA NORMATIVA

- Decreto nº 3.505, de 13 de junho de 2000.
- Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008 e respectivas Normas Complementares publicadas no D.O.U pelo DSIC/GSIPR.
- ABNT NBR ISO/IEC 27001:2006.
- ABNT NBR ISO/IEC 27002:2005.
- Livro de Avaliação de Conformidade, 5ª Edição, maio de 2007 do Instituto Nacional de Metrologia, Qualidade e Tecnologia – Inmetro.  
Padrões de Interoperabilidade do Governo Eletrônico (e-PING).
- Padrões de Auditoria – TCU
- Política de Segurança da Informação e Comunicações - ICMBio

## CAMPO DE APLICAÇÃO

Esta Norma se aplica no âmbito da Agência Espacial Brasileira

## SUMÁRIO

- 1 Objetivo
- 2 Conceitos e Definições
- 3 Considerações Iniciais
- 4 Princípios e Diretrizes
- 5 Vigência

## APROVAÇÃO

**JOSÉ RAIMUNDO BRAGA COELHO**  
Presidente

## 1 OBJETIVO

Estabelecer diretrizes para avaliação de conformidade e auditoria nos aspectos relativos à Segurança da Informação e Comunicação no âmbito da Agência Espacial Brasileira - AEB.

## 2 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

**Recursos Computacionais:** são os equipamentos, as instalações e bancos de dados direta ou indiretamente administrados, mantidos ou operados por todos os setores da AEB, tais como:

- Computadores e terminais de qualquer espécie;
- Impressoras;
- Redes;
- Equipamentos afins;
- Banco de dados ou documentos residentes em disco, fita ou outros meios de armazenamento de informação;

## 3 CONSIDERAÇÕES INICIAS

- I. A AEB está inserida em um contexto de regulamentos derivados de leis, contratos e acordos que deve respeitar e observar, para que não seja alvo de ações e também para que possa proteger-se contra terceiros. As políticas e procedimentos adotados devem refletir esses requisitos, atuando na prevenção de tais eventos;
- II. Devem ser levantados os aspectos legais de segurança aos quais as atividades da AEB estão submetidas de forma a evitar ações penais decorrentes da não observância de tais aspectos por desconhecimento ou omissão;
- III. Ameaças e riscos devem ser reavaliados periodicamente para garantir que a AEB esteja efetivamente protegida. Tanto no surgimento de novas ameaças ou na extinção de outras, as políticas são atualizadas para refletir a realidade presente;
- IV. A avaliação de conformidade em SIC deve ser contínua e aplicada visando contribuir com a Gestão de Segurança da Informação;
- V. As não-conformidades relativas ao descumprimento da legislação, normas e procedimentos serão consideradas riscos de segurança da informação e comunicações e devem ser tratadas;

## 4 PRINCÍPIOS E DIRETRIZES

- I. O uso dos recursos de tecnologia da informação e comunicações disponibilizados pela AEB é passível de monitoramento e auditoria e devem ser implementados e mantidos, sempre que possível, mecanismos que permitam a sua rastreabilidade;
- II. A entrada e a saída de ativos de informação da AEB serão registradas e autorizadas por autoridade competente mediante procedimento formal;
- III. A área de tecnologia da informação manterá registros e procedimentos, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos, à rede interna e à internet, sempre que possível.

## **5 VIGÊNCIA**

Esta Norma Complementar entra em vigor na data de sua publicação.