CONSELHO NACIONAL DE JUSTIÇA

Diretrizes Gerais

# Segurança da Informação

*Apresentação das Diretrizes para a Gestão de Segurança da Informação no âmbito do Judiciário*

**Brasília – DF**
**Abril de 2011**

## Preâmbulo

Este documento apresenta as diretrizes gerais para implantação da Gestão de Segurança da Informação (GSI) visando à proteção dos ativos de informação do Poder Judiciário.

Tais orientações devem ser devidamente compreendidas e adotadas em todos os níveis pelos órgãos do Judiciário Brasileiro.

Tem como objetivo a preservação dos aspectos de confidencialidade, integridade e disponibilidade das informações, bem como contribuir para que a missão do Judiciário seja cumprida.

## Definições / Glossário

Para melhor compreensão dos termos utilizados neste documento é importante disseminar os seguintes conceitos:

Agente do Judiciário: são todas as autoridades, membros, servidores, prestadores de serviço e colaboradores que manipulam informações no âmbito do poder judiciário

Ativo: Qualquer coisa que tenha valor para a organização. [ISO/IEC 13335-1:2004]

Ativos de Informação: são aqueles que geram, armazenam, processam, transmitem ou descartam informações.

Autenticidade: propriedade que permite a validação de identidade de usuários e sistemas.

Avaliação de riscos: processo global da análise de risco e da valoração do risco. [ABNT ISO/IEC Guia 73:2005]

CGSI: Comitê Gestor de Segurança da Informação.

Confidencialidade: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização. [ISO/IEC 13335-1:2004]

Disponibilidade: propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada. [ISO/IEC 13335-1:2004]

Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da Política de Segurança da Informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação. [ISO/IEC TR 18044:2004]

Gestão de riscos: atividades coordenadas para dirigir e controlar uma organização, no que se refere aos riscos. Normalmente inclui a avaliação do risco, o tratamento do risco, a aceitação do risco e a comunicação do risco.[ABNT ISO/IEC Guia 73:2005]

Incidente de segurança da informação: um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. [ISO/IEC TR 18044:2004]

Integridade: propriedade de proteção à precisão e perfeição da informação e de recursos. [ISO/IEC 13335-1:2004]

Proprietário da Informação: Agente do Judiciário que define quem tem acesso à informação e que tipo de privilégio de acesso.

Segurança da informação: preservação da disponibilidade, integridade, confidencialidade e autenticidade da informação; adicionalmente, outras propriedades, tais como responsabilidade, não repúdio e confiabilidade podem também estar envolvidas. [ABNT NBR ISO/IEC 17799:2005]

Tratamento de riscos: processo de seleção e implantação de medidas de controle para modificar um risco. [ABNT ISO/IEC Guia 73:2005]

## Introdução

Toda informação criada, armazenada, processada, transmitida e descartada por qualquer agente do Judiciário Brasileiro é considerada patrimônio valioso.

A informação pode ser gerada e manipulada de diversas formas: mensagens e arquivos eletrônicos, internet, meio impresso, verbal e outros.

Independentemente da forma, três aspectos da informação norteiam sua segurança:

- **Confidencialidade**: a informação só deve ser acessível a quem tem a devida autorização;
- **Integridade**: a informação deve manter-se inalterada desde sua geração ou alteração autorizada;
- **Disponibilidade**: a informação deve estar sempre disponível às pessoas autorizadas.

O presente documento constitui as Diretrizes Gerais para a Gestão da Segurança da Informação, para ser adotada em todos os ambientes e processos do Poder Judiciário.

Toda informação deve ser protegida conforme estabelecido nestas diretrizes. A adoção de procedimentos que garantam a segurança da informação deve ser prioridade constante no Poder Judiciário, de forma que se possa reduzir falhas e danos que possam comprometer a imagem da Justiça ou trazer prejuízos à sociedade brasileira.

As Diretrizes Gerais demonstram o comprometimento do Poder Judiciário com a Segurança da Informação, com o apoio de todas as autoridades, servidores, colaboradores, prestadores de serviço, e todos aqueles que estão direta ou indiretamente envolvidos na sua aplicação.

## Ojbetivos

Declarar formalmente o compromisso do Poder Judiciário com a Segurança da Informação.

Prover orientação e apresentar diretrizes sobre a Segurança da Informação para todos os órgãos do Poder Judiciário, refletindo a visão da Justiça diante da importância em proteger os seus ativos de informação. Além disso, também serve para nortear, através de suas diretrizes, as atividades de Segurança da Informação desenvolvidas no âmbito dos órgãos do Poder Judiciário.

## Diretrizes Gerais

As Diretrizes Gerais da Segurança da Informação constituem a base para a Gestão de Segurança da Informação e orientam a elaboração das Normas e dos Procedimentos. Estabelecem-se as seguintes diretrizes a serem seguidas por todos os órgãos do Poder Judiciário:

- Estabelecimento de um Fórum Nacional de Gestão de Segurança da Informação, composto principalmente pelos responsáveis pelo Comitê Gestor de Segurança

da Informação multidisciplinar (CGSI) de cada órgão. O Fórum tem como principal missão a unificação das ações e estratégias relativas à implantação dessas diretrizes.

- Estabelecimento de um Modelo de Gestão que permita a criação e a manutenção de um Sistema de Gestão de Segurança da Informação apoiado por uma Política de Segurança, normas e melhores práticas. O Modelo de Gestão deve contemplar, no mínimo, os seguintes processos:
    - Planejamento Estratégico da Segurança da Informação;
    - Gestão de Riscos;
    - Gestão da Política de Segurança, das Normas e dos Procedimentos;
    - Classificação da Informação;
    - Gestão da Continuidade do Negócio;
    - Gestão da Resposta a Incidentes;
    - Auditoria;
    - Divulgação e Conscientização;
    - Gestão da conformidade com normas legais.
- Estabelecimento em cada órgão do Poder Judiciário de um Comitê Gestor de Segurança da Informação multidisciplinar (CGSI) que será responsável pela elaboração da Política de Segurança da Informação e da aprovação das Normas e de Procedimentos de Segurança da Informação, dele fazendo parte representantes das principais áreas do órgão que tratam com ativos de informação. O CGSI também dará suporte às ações estratégicas para a implantação dos processos mínimos especificados para o Modelo de Gestão.
- Criação de uma Estrutura Normativa da Segurança da Informação que contemple, no mínimo:
    - Política de Segurança. Deve definir a estrutura, estabelecer as diretrizes e definir as responsabilidades referentes à Segurança da Informação;
    - Normas de Segurança da Informação (Normas). Devem estabelecer obrigações a serem seguidas de acordo com as diretrizes da Política de Segurança. As Normas de Segurança devem contemplar, no mínimo, o controle de acesso aos sistemas de informação, a utilização de recursos de Tecnologia da Informação e Comunicações (TIC), o acesso à internet e às redes sociais, a utilização de correio eletrônico (e-mail) e a política de cópias de segurança (backup);
    - Procedimentos de Segurança da Informação (Procedimentos). Devem definir as regras operacionais conforme o disposto nas Diretrizes, Normas e na Política de Segurança, permitindo sua utilização nas atividades do órgão.
- Implantação, a partir dos processos do Modelo de Gestão, de um Sistema de Gestão de Segurança da Informação (SGSI) que permita:

- Classificação e gestão da classificação das informações. O SGSI deve ser capaz de inventariar e classificar as informações de acordo com sua confidencialidade e associá-las a um Proprietário da Informação.

- Avaliação contínua dos riscos de segurança da informação através de análise sistemática e periódica;

- Gestão de acesso a sistemas de informação de forma que o acesso seja controlado e esteja de acordo com as Normas e os Procedimentos definidos;

- Gestão de riscos operacional em Segurança da Informação com o objetivo de minimizar os riscos associados à informação, apresentando as medidas de segurança necessárias;

- Continuidade do negócio, visando reduzir para um nível aceitável a interrupção causada por desastres ou falhas nos ativos que suportam os processos críticos de informação do órgão;

- Validação das evidências de cumprimento da Política de Segurança da Informação;

- Inventário e gestão dos ativos de Tecnologia da Informação;

- Definição e utilização de Termos de Responsabilidade para acesso às informações classificadas.

- Estabelecimento de um programa de capacitação e conscientização de todos os usuários em relação à adoção de comportamento seguro na utilização das informações;

- Implantação de uma equipe de resposta a incidentes de Segurança da Informação de forma que as fragilidades e eventos de segurança associados aos ativos de informação sejam comunicados e permitindo a tomada de ação corretiva em tempo hábil.

## Referências


Norma ABNT ISO/IEC 17799 27002:2005 e ABNT ISO/IEC 27001:2006 e/ou normas que as sucederem;

Gabinete de Segurança Institucional da Presidência da República – GSI. Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf>. Acesso em: 17 de abril de 2010.

Presidência da República – Casa Civil - Decreto Nº 3.505, de 13 de junho de 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 17 de abril de 2010.

SANS Institute, Technical Writing for IT Security Policies in Five Easy Steps, 2001. Disponível em: <http://www.sans.org/reading_room/whitepapers/policyissues/technical-writing-security-policies-easy-steps_492>. Acesso em: 14 de abril de 2010.

SANS Institute, Information Security Policy - A Development Guide for Large and Small Companies, 2007. Disponível em: < http://www.sans.org/reading_room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies_1331 >. Acesso em: 15 de abril de 2010.

SANS Institute, Security Policy Roadmap – Process for Creating Security Policies, 2010. Disponível em: <http://www.sans.org/reading_room/whitepapers/policyissues/ security-policy-roadmap-process-creating-security-policies_494>. Acesso em: 15 de abril de 2010.

Cultura de Segurança da Informação

IT Governance Institute – ITGI. An Introduction to the Business Modelo f Information security. 2009b. Disponível em: <http://www.isaca.org>, na seção de downloads. Acesso em: 16 de abril de 2010.

National Institute of Standards and Technology - NIST, Information Technology Training Requirements: A Role- and Performance-Based Model, NIST 800-16,1998. Disponível em: < http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf >. Acesso em: 17 de abril de 2010.

_____. NIST, Buinding an Information Technology Security Awareness and Training Program, NIST 800-50, 2003. Disponível em: <http://csrc.nist.gov/publications/ nistpubs/800-50/NIST-SP800-50.pdf >. Acesso em: 17 de abril de 2010.

Organização para Cooperação e Desenvolvimento Econômico - OCDE, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002. Disponível em: <http://www.oecd.org/document/42/0,3343, en_2649_34255_15582250_1_1_1_1,00.html>. Acesso em: 17 de abril de 2010.

SANS Institute, Technical Writing for IT Security Policies in Five Easy Steps, 2001. Disponível em: <http://www.sans.org/reading_room/whitepapers/policyissues/technical-writing-security-policies-easy-steps_492>. Acesso em: 14 de abril de 2010.