CONSELHO NACIONAL DE JUSTIÇA

Diretrizes

# Segurança da Informação

# Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário

**Brasília – DF**
Junho de 2012

## Preâmbulo

Este documento apresenta as Diretrizes para a implantação da Gestão de Segurança da Informação (GSI) no Poder Judiciário, visando à proteção, principalmente, dos ativos críticos de negócio.

Tais orientações devem ser devidamente compreendidas como linhas mestras de conduta 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.

Estas diretrizes reforçam, no âmbito do Judiciário, a aplicação dos dispositivos estabelecidos no Decreto nº 3.505/2000 da Presidência da República, no Acórdão de nº 2471/2008 do Tribunal de Contas da União e na Resolução nº 90/2009 do Conselho Nacional de Justiça.

## 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 geram e manipulam informações no âmbito do Poder Judiciário.

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

Ativo Crítico: aquele que gera, armazena, processa, transmite e descarta informações de valor e criticidade altos para o negócio.

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]

Comitê Gestor de Segurança da Informação (CGSI): grupo de pessoas com a responsabilidade de promover a implementação das ações de Segurança da Informação.

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

Diretriz: descrição que orienta o que deve ser feito e como, para se alcançarem objetivos estabelecidos nas políticas. [ISO/IEC 27002:2005]

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]

Política de Segurança da Informação: documento que declara o comprometimento da direção e estabelece o enfoque da organização para gerenciar a Segurança da Informação (...) Convém que um documento da política de segurança da informação seja aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes. [ISO/IEC 27002:2005]

Salva-guarda de Processo Crítico: ações vitais para o órgão que devem ser conduzidas adequadamente, a fim de evitar falhas que possam gerar, entre outros, prejuízos, comprometimento de imagem e, até, a inviabilização do negócio.

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

Regras Operacionais: conjunto de instruções que orientam os usuários sobre a utilização de algum recurso de tecnologia da informação e comunicação.

Recurso de Tecnologia da Informação e Comunicação: equipamentos servidores de rede, estações de trabalho, equipamentos de conectividade, todo e qualquer *hardware* e *software* que compõem soluções e aplicações de TI.

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]

Usuário: pessoa que utiliza sistemas e/ou demais recursos de tecnologia da informação e comunicação do órgão.

## Introdução

Toda informação gerada, 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, entre 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 a serem adotadas pelo Poder Judiciário em todos os ambientes.

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 a reduzir falhas e danos que possam comprometer a imagem da Justiça ou trazer prejuízos à sociedade brasileira.

O Poder Judiciário, por meio de suas autoridades, membro, servidores, prestadores de serviço e todos aqueles que estão direta ou indiretamente envolvidos, se comprometem com a aplicação destas diretrizes.

## Objetivos

- 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 desse Poder diante da importância em proteger, principalmente, os seus ativos críticos. Além disso, também serve para nortear, por meio de suas diretrizes, as atividades de Segurança da Informação desenvolvidas no âmbito dos órgãos do Poder Judiciário.

## Diretrizes

As Diretrizes 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 Comitê Gestor de Segurança da Informação multidisciplinar (CGSI), em cada órgão do Poder Judiciário, que será responsável por promover a cultura de Segurança da Informação, bem como pela elaboração da Política e aprovação das Normas e de Procedimentos de Segurança da Informação, dele fazendo parte representantes das principais áreas do órgão que tratam com ativos críticos para o negócio. O CGSI deve, ainda:
    - Apoiar as ações estratégicas para a implantação dos processos mínimos especificados para o Modelo de Gestão;
    - Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação, avaliando, inclusive, a possibilidade de criação de área específica para Gestão da Segurança da Informação;
    - Propor alterações na Política de Segurança da Informação;
    - Propor normas relativas à Segurança da Informação.
- Estabelecimento de um Fórum Nacional de Gestão de Segurança da Informação, composto, preferencialmente, pelos responsáveis do Comitê Gestor de Segurança da Informação de cada órgão do Poder Judiciário. O Fórum tem como principal missão a unificação das estratégias e ações relativas à implantação destas diretrizes no Judiciário, bem como o relacionamento com agrupamentos similares dos Poderes Executivo e Legislativo, com o objetivo de compartilhar conhecimentos e propor ações conjuntas.
- Estabelecimento de um Modelo de Gestão que permita a criação e a manutenção de um Sistema de Gestão de Segurança da Informação (SGSI) apoiado por uma Política de Segurança, Normas e Procedimentos. O Modelo de Gestão deve contemplar, no mínimo, os seguintes processos:
    - Planejamento Estratégico da Segurança da Informação;
    - Gestão da Política de Segurança, das Normas e dos Procedimentos;
    - Classificação da Informação;
    - Controle de Acesso;
    - Gestão de Riscos;
    - Gestão da Continuidade do Negócio;
    - Gestão de Resposta a Incidentes;
    - Gestão de Mudanças;
    - Divulgação e Conscientização;
    - Auditoria e Conformidade;
- Implantação de um Sistema de Gestão de Segurança da Informação (SGSI), a partir dos processos do Modelo de Gestão, 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 por meio de análise sistemática e periódica;

- Gestão de acesso (lógico e físico) 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 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, principalmente, 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, principalmente, dos ativos críticos de Tecnologia da Informação e da Comunicação;

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

- Criação de uma Estrutura Normativa da Segurança da Informação que contemple, no mínimo:

    - Política de Segurança (Política). Deve contemplar a estrutura, diretrizes e responsabilidades referentes à Segurança da Informação;

    - Normas de Segurança da Informação (Normas). Devem contemplar obrigações a serem seguidas de acordo com as diretrizes estabelecidas na Política de Segurança. As normas devem abranger, no mínimo, o Tratamento da Informação, o Tratamento de Incidentes, o Tratamento de Códigos Maliciosos, o Controle de Acesso (lógico e físico) aos Sistemas de Informação, a Utilização de Recursos de Tecnologia da Informação e da Comunicação (Internet, Redes Sociais, Correio Eletrônico, outros), e a Política de Geração e Restauração de Cópias de Segurança;

    - Procedimentos de Segurança da Informação (Procedimentos). Devem contemplar regras operacionais de acordo com o disposto nas Diretrizes e Normas de Segurança estabelecidas, permitindo sua utilização nas atividades do órgão.

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

- Implantação de uma equipe de resposta a incidentes de Segurança da Informação para avaliar fragilidades e eventos de segurança associados, principalmente, aos ativos críticos de TIC, de forma que esses eventos possam ser comunicados para tomada de ação corretiva em tempo hábil.

## Vigência

Estas Diretrizes entram em vigor da data de sua publicação.

## Acompanhamento

Caberá à Comissão de Tecnologia da Informação, Comunicação e Infraestrutura do Conselho Nacional de Justiça, com o apoio do Comitê Nacional de Gestão de Tecnologia da Informação e Comunicação do Poder Judiciário, acompanhar a implementação dessas diretrizes, estabelecendo, caso a caso, prazos para implementação, que não deverão ser superiores a dois anos a contar da aprovação deste documento.

## Referências

Norma ABNT ISO/IEC 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 2012.

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 2012.

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 2012.

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 2012.

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 2012.

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 2012.

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 2012.

_____. 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 2012.

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 2012.

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 2012.