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.

Decreto nº 3.505/2000 da Presidência da República

Acórdão de nº 2471/2008 do Tribunal de Contas da União

Resolução nº 90/ 2009 do Conselho Nacional de Justiça

Diretrizes para Gestão de Segurança da Informação no âmbito do Poder Judiciário – CNJ Julho/2012

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.

Conjunto de Diretrizes

- **Estabelecimento de um Comitê Gestor de Segurança da Informação multidisciplinar (CGSI)**
- **Estabelecimento de um Fórum Nacional de Gestão de Segurança da Informação**
- **Estabelecimento de um Modelo de Gestão**
  - **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)**
  - **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**
  - **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:
    - Tratamento da Informação
    - Tratamento de Incidentes
    - Tratamento de Códigos Maliciosos
    - Controle de Acesso (lógico e físico) aos Sistemas de Informação
    - Utilização de Recursos de Tecnologia da Informação e da Comunicação (Internet, Redes Sociais, Correio Eletrônico, outros)
    - 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**
- **Implantação de uma equipe de resposta a incidentes de Segurança da Informação**

Tabela 1.0 – Conjunto de Diretrizes

Nº	Diretriz	Objetivo/Resposabilidade	Participantes	Abrangência
1	Estabelecimento de um Comitê Gestor de Segurança da Informação multidisciplinar (CGSI)	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. 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.	Representantes das principais áreas do órgão que tratam com ativos críticos para o negócio.	(Não especificado/detalhado)
2	Estabelecimento de um Fórum Nacional de Gestão de Segurança da Informação	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.	Composto, preferencialmente, pelos responsáveis do Comitê Gestor de Segurança da Informação de cada órgão do Poder Judiciário	(Não especificado/detalhado)
3	Estabelecimento de um Modelo de Gestão	Criação e a manutenção de um Sistema de Gestão de Segurança da Informação (SGSI) apoiado por uma Política de Segurança, Normas e Procedimentos.	(Não especificado/detalhado)	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;
4	Implantação de um Sistema de Gestão de Segurança da Informação (SGSI)	(Não especificado/detalhado)	(Não especificado/detalhado)	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.
5	Criação de uma Estrutura Normativa da Segurança da Informação	(Não especificado/detalhado)	(Não especificado/detalhado)	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.
6	Estabelecimento de um programa de capacitação e conscientização	Capacitar e conscientizar todos os envolvidos, inclusive usuários, em relação à adoção de comportamento seguro na utilização das informações	(Não especificado/detalhado)	Órgão do Poder Judiciário
7	Implantação de uma equipe de resposta a incidentes de Segurança da Informação	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	(Não especificado/detalhado)	Órgão do Poder Judiciário