Anexo I - Supremo Tribunal Federal
Praça dos Três Poderes, S/N
Brasília - DF - Brasil
CEP: 70.175.901

CONSELHO NACIONAL DE JUSTIÇA

Política de Segurança da Informação

Segurança da Informação

Apresentação das diretrizes da Gestão de Segurança da Informação no ambiente do Judiciário

Brasília – DF
Outubro de 2010

Preâmbulo

Esta política apresenta as diretrizes gerais para implantação da gestão de segurança da informação visando à proteção dos ativos de informação do Poder Judiciário.

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

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

Este documento disserta sobre o propósito, diretrizes, funções e responsabilidades, violações e sanções, revisões e atualizações, contatos e referencias.

Definições / Glossário

Para melhor compreender os termos utilizados nesta Política de Segurança da Informação é importante disseminar os seguintes conceitos:

Agentes do Judiciário: são todas as autoridades, membros, servidores, prestadores de serviço e colaboradores que geram, processam e descartam informações no âmbito do Judiciário Brasileiro.

Análise de riscos: uso sistemático da informação para identificar as fontes e estimar o risco. [ABNT ISO/IEC Guia 73:2005]

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

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

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

Avaliação de risco: 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]

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]

Segurança: estar livre de perigos e incertezas.

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

Valoração do risco: processo de comparar o risco estimado contra critérios de risco estabelecidos para determinar a significância do risco. [ABNT ISO/IEC Guia 73:2005]

Introdução

Toda informação que é criada, armazenada, processada e descartada por qualquer Agentes no Judiciário 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 a Política de Segurança da Informação do Poder Judiciário para ser adotada em todos os ambientes e processos deste.

Toda informação deve ser protegida conforme as regras definidas nesta Política. A adoção de procedimentos que garantam a segurança da informação deve ser prioridade constante no Judiciário, de forma que se possa reduzir falhas e danos que possam comprometer a imagem da Justiça ou trazer prejuízos a outrem.

De modo geral, esta política resume os princípios da Segurança da Informação que o Judiciário reconhece como sendo importantes e que devem estar presentes no cotidiano de suas atividades.

A Política de Segurança também demonstra o comprometimento do Judiciário com a Segurança da Informação, com o apoio de todos os servidores, colaboradores, prestadores de serviço, e todos aqueles que estão diretamente 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 e ambientes do Poder Judiciário, refletindo a visão do mesmo 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 do Judiciário Brasileiro, definindo funções e responsabilidades.

A Política de Segurança da Informação deve viabilizar e preservar a confidencialidade, a integridade e a disponibilidade das informações em todos os níveis de atividades desenvolvidas. Faz parte também do seu escopo proporcionar a segurança física e lógica

das informações, reduzir riscos, alcançar as conformidades legais, minimizar problemas causados por indisponibilidades dos serviços e proteger a imagem da Justiça Brasileira.

Estrutura Normativa da Segurança da Informação do Judiciário

A estrutura normativa da Segurança da Informação do Juiciário é composta documentos com três níveis hierárquicos relacionados a seguir:

- Política de Segurança da Informação (Política): constituída neste documento, define a estrutura, estabelece as diretrizes e define as responsabilidades referentes à segurança da informação. A Política é unificada para todo o Judiciário.
- Normas de Segurança da Informação (Normas): estabelecem obrigações e definem procedimentos a serem seguidos de acordo com as diretrizes da Política. As normas são
- Procedimentos de Segurança da Informação (Procedimentos): definem as regras operacionais conforme o disposto nas Normas e na Política de Segurança, permitindo sua utilização nas atividades do CNJ.

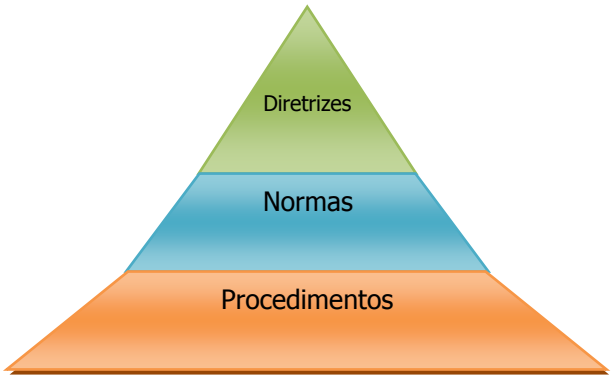

Figura 1 – Estrutura Normativa da Segurança da Informação do CNJ

A Política de Segurança da Informação, representada por este documento é unificada para todo o Judiciário. As normas e os procedimentos são elaborados por cada órgão do Poder Judiciário de forma a atender suas especificidades próprias, sempre de acordo com as diretrizes aqui definidas.

Diretrizes

As Diretrizes da Política de Segurança da Informação constituem a base para a Gestão de Segurança da Informação no Judiciário e orientam a elaboração das Normas e dos Procedimentos. Estabelecem-se as seguintes diretrizes a serem seguidas por todos os órgãos do Judiciário:

- Estabelecimento de um Fórum Nacional de Gestão de Segurança da Informação, composto principalmente pelos responsáveis pela Área de Segurança da Informação de cada órgão do Judiciário. O Fórum tem como principal missão a unificação das ações e estratégias relativas à segurança da informação no âmbito do Judiciário.

- Estabelecimento em cada órgão do Poder Judiciário de um Comitê Gestor de Segurança da Informação multidisciplinar – CGSI – que será responsável pela aprovação das Normas de Segurança da Informação, dele fazendo parte representantes das principais áreas do órgão que tratam com ativos de informação. O Comitê também dará o suporte às ações estratégicas para a a gestão da Política de Segurança da Informação.

- Definição de Normas e Procedimentos de Segurança da Informação a serem aprovadas pelo CGSI.

- Implantação de um Sistema de Gestão de Segurança da Informação – SGSI – que permita:

    - Implantação de processo para classificação e gestão da classificação das informações. O processo 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.

    - Implantação de um processo de gestão de riscos operacional em Segurança da Informação com o objetivo de minimizar os riscos associados à informação, apresentando as medidas de segurança necessárias.

    - Implantação de um processo de continuidade do negócio visando reduzir para um nível aceitável a interrupção causada por desastres ou falhas nos recursos que suportam os processos críticos de informação do órgão.

    - Definição processo de validação das evidências de cumprimento da política de segurança da informação.

    - Implantação do processo para 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 a sistemas de informação sejam comunicadas e permitindo a tomada de ação corretiva em tempo hábil.

- Implantação de processo para validação dos aspectos referentes à segurança da informação de forma a evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança.

Funções e Responsabilidades

Esta Política regulamenta as atividades de segurança da informação do Poder Judiciário e deve ser obedecida por todos os Agentes do Judiciário, sendo responsabilidade de cada um o seu cumprimento. Para tanto, as principais funções e responsabilidades são:

Direção Geral

Cabe à Direção Geral de cada órgão:

- Aprovar e Publicar a Política de Segurança da Informação e suas revisões
- Tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas Normas encaminhados pelo Comitê Gestor de Segurança da Informação

Comitê Gestor de Segurança da Informação

Cabe ao Comitê Gestor de Segurança da Informação:

- Propor alterações nesta Política
- Aprovar a estrutura e os processos do Sistema de Gestão de Segurança da Informação
- Propor alterações e aprovar as Normas de Segurança da Informação
- Definir a classificação das informações pertencentes ou sob a guarda do CNJ, com base no inventário de informações apresentado pela Área de Gestão de Segurança da Informação e nos critérios de classificação constantes de Norma específica
- Analisar os casos de violação desta Política e das Normas de Segurança da Informação, encaminhando-os à Direção Geral, quando for o caso
- Propor medidas relacionadas à melhoria da segurança da informação do CNJ
- Propor o planejamento e a alocação de recursos no que tange à segurança da informação
- Determinar a elaboração de relatórios, levantamentos e análises que dêem suporte à gestão de segurança da informação e à tomada de decisão
- Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação
- Aprovar a relação de "proprietários" das informações do CNJ

Serão membros do Comitê Gestor de Segurança da Informação:

- Representantes do Comitê de Informática Junto à Presidência ou junto à Secretaria Geral, quando houver
- Diretoria/Secretaria de Tecnologia da Informação
- Diretoria/Secretaria de Gestão de Pessoas
- Representantes da Direção Geral
- Responsável pela Área de Segurança da Informação do órgão

O responsável pela Área de Segurança da Informação coordenará os trabalhos do Comitê e suas atribuições abrangerão a convocação das reuniões e a realização de outras atividades de suporte.

As reuniões do Comitê:

(a) Serão realizadas trimestralmente, podendo haver convocação extraordinária, sempre que necessário;
(b) Serão instaladas com a presença de, no mínimo, 2/3 (dois terços) dos membros do Comitê; e
(c) Serão registradas em ata.

As deliberações do Comitê serão pela maioria dos votos presentes.

Sempre que necessário outros profissionais do órgão e também convidados externos poderão participar das reuniões.

Proprietário da Informação

O Proprietário da Informação é o gerente da área do órgão responsável pela concessão de acesso à informação a ele relacionada ou sob sua guarda. A ele cabe:

- Elaborar matriz de cargos e funções e respectivos direitos de acesso para todas as informações sob sua guarda
- Autorizar acesso às informações sob sua guarda, observada a matriz definida no item anterior
- Analisar relatórios de acesso fornecidos pela área de segurança da informação corrigindo desvios porventura observados
- Participar das reuniões do Comitê quando convocado

Assessoria Jurídica

À Assessoria Jurídica do órgão cabe:

- Informar ao Comitê alterações legais ou regulatórias que impliquem responsabilidade ou ação que envolvam a gestão da segurança da informação
- Avaliar, sempre que solicitada, as Normas, os Procedimentos e os Termos de Sigilo referentes à gestão da segurança da informação
- Auxiliar o Comitê nas demais questões legais.

Área de Segurança da Informação

Cabe à área de Gestão de Segurança da Informação:

- Propor a estrutura e os processos do Sistema de Gestão de Segurança da Informação – SGSI – sendo que entre os processos devem estar previstos o planejamento, a execução e operação, o monitoramento, o controle e a auditoria da Segurança da Informação
- Nas reuniões do Comitê: convocar, coordenar os trabalhos, lavrar atas e prover apoio às reuniões
- Disponibilizar as informações de gestão de segurança da informação solicitadas pelo Comitê
- Divulgar amplamente a Política e as Normas de Segurança da Informação para todos os Agentes
- Propiciar orientação e treinamento sobre a Política de Segurança da Informação e suas Normas a todos os Agentes
- Propor ações relacionadas à melhoria da segurança da informação do órgão
- Definir procedimentos e realizar a gestão dos sistemas de controle de acesso do órgão, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários
- Identificar e Analisar os riscos relacionados à Segurança da Informação do órgão e apresentar relatórios periódicos sobre tais riscos ao CGSI, acompanhados de proposta de aperfeiçoamento do ambiente, quando for o caso
- Executar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações do órgão;
- Solicitar ou requisitar informações às demais áreas do órgão
- Realizar testes e averiguações em sistemas, equipamentos e outros recursos, com o intuito de verificar o cumprimento da Política e das Normas de Segurança da Informação
- Implantar mecanismo de registro e controle de não-conformidade a esta Política e às Normas de Segurança da Informação, comunicando ao CGSI as não-conformidades ocorridas.

Coordenadoria de Gestão de Pessoas

Cabe à área de Recursos Humanos:

- Obter a assinatura do Termo de Responsabilidade dos Agentes, arquivando-o nos respectivos prontuários
- Comunicar à Área de de Segurança da Informação, de imediato, todos os desligamentos, afastamentos e modificações no quadro funcional do CNJ.

Agentes do Judiciário

Cabe a todos os Agentes do Judiciário:

- Cumprir as diretrizes definidas nesta Política, além das Normas e dos Procedimentos aprovados pelo respectivo órgão de forma pró-ativa
- Compreender ameaças externas que podem comprometer a segurança das informações do órgão tais como: fraudes, grampos telefônicos e interceptação de mensagens, vírus de computador, etc.
- Assegurar que informações confidenciais do órgão estejam devidamente protegidas
- Evitar discutir assuntos confidenciais de trabalho em ambientes públicos
- Não divulgar ou compartilhar senhas de acesso, que serão sempre pessoais e intransferíveis
- Utilizar apenas softwares homologados pelo órgão
- Seguir rigorosamente as normas de uso de Internet e Correio Eletrônico do órgão
- Alertar a Área de Segurança da Informação sobre violações de Normas ou dessa Política
- Buscar orientação da área de segurança da informação em caso de dúvidas relacionadas à segurança da informação
- Proteger as informações contra acesso não autorizado pelo órgão
- Assegurar que os todos os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo órgão

Violações e Sanções

Os Agentes do Judiciário deverão conhecer e zelar pelo cumprimento da Política de Segurança da Informação. A desobediência às Normas que serão estabelecidas implicará nas sanções administrativas previstas em regulamentações internas, e legislação em vigor.

Revisões e Agenda de Atualizações

A Política de Segurança da Informação deverá ser analisada anualmente de forma crítica, visando a sua aderência e concordância aos objetivos do Poder Judiciário e legislação vigente, como forma de melhoria contínua.

Informações para contato

Definição do comite

Apresentar e-mail

hotsite

Criação de email

Referências

Norma ABNT ISO/IEC 1779927002:2005 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.