Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia Catarinense
Conselho Superior

RESOLUÇÃO Nº 044 – CONSUPER/2013

Dispõe sobre a aprovação da Política de Segurança da Informação do IF Catarinense.

O Presidente do Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia Catarinense – IF Catarinense, Professor Francisco José Montório Sobral, no uso de suas atribuições conferidas pelo Decreto de 24/01/2012, publicado no Diário Oficial da União no dia 24/01/2012, e considerando:

I - a responsabilidade da Alta Administração do IF Catarinense com a definição de uma política de segurança da informação e comunicação cujo objetivo seja a redução de risco, a conformidade com as leis e regulamentos existente e a garantia da continuidade operacional, da integridade e da confidencialidade da informação;

II - que a informação no âmbito do IF Catarinense é essencial para viabilizar o alcance dos objetivos e metas da instituição, e que é crescente a interconectividade, expondo a informação a um crescente número e uma grande variedade de ameaças e vulnerabilidades;

III - que a Segurança da Informação, e todos os seus processos, não está somente atrelada à Segurança relacionada à Tecnologia da Informação;

IV - que a NBR ISO/IEC 27002:2005, norma que estabelece boas práticas em segurança da informação, recomenda revisões periódicas da política de segurança da informação das instituições;

V - as constatações da CGU na RA 201108759, que recomendou constituir comitê gestor de segurança da informação do IF Catarinense, para atuação de forma integrada, envolvendo as atividades da Reitoria em conjunto com seus Câmpus.

RESOLVE Aprovar:

Art. 1º - A Política de Segurança da Informação e Comunicações - PoSIC do Instituto Federal de Educação Ciência e Tecnologia Catarinense – IF Catarinense observará os princípios, objetivos e diretrizes estabelecidos nesta Resolução.

CAPÍTULO I

CONCEITOS E DEFINIÇÕES

Art. 2° No âmbito da PoSIC, considera-se:

I - agente responsável pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR: servidor do IF Catarinense ocupante de cargo efetivo incumbido de chefiar e gerenciar a ETIR;

II - ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

III - ativos de informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

V - capacitação em SIC: saber o que é segurança da informação e comunicações, aplicando em sua rotina pessoal e profissional, servindo como multiplicador do tema e aplicando os conceitos e procedimentos na organização como gestor de SIC;

VI - classificação da informação: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;

VII - Comitê de Segurança da Informação e Comunicações - CSIC: colegiado de caráter deliberativo responsável pela normatização e supervisão da segurança da informação e comunicações no âmbito do IF Catarinense;

VIII - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

IX - conscientização em SIC: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema;

X - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XI - CTIR.GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República DSIC/GSI/PR;

XII - custodiante do ativo de informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

XIII - disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade;

XIV - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR: colegiado com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no âmbito do IF Catarinense;

XV - especialização em SIC: saber o que é segurança da informação e comunicações, aplicando em sua rotina pessoal e profissional, servindo como multiplicador sobre o tema, aplicando os conceitos e procedimentos na organização como gestor de SIC e tornando-se referência na pesquisa de novas soluções e modelos de SIC;

XVI - Estrutura de GSIC: grupo responsável pela gestão e execução da SIC;

XVII - gestão de ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

XVIII - gestão de continuidade dos negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

XIX - gerenciamento de operações e comunicações: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporta, satisfazendo os acordos de níveis de serviço;

XX - gestão de riscos de segurança da informação e comunicações - GRSIC: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XXI - gestão de segurança da informação e comunicações - GSIC: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações;

XXII - gestor dos ativos de informação: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;

XXIII - Gestor de SIC: servidor nomeado pelo Reitor como responsável pela gestão de segurança da informação e comunicações no âmbito do IF Catarinense;

XXIV - incidente de SIC: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XXV - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XXVI - infraestrutura de TI: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica;

XXVII - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXVIII - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXIX - recursos criptográficos: sistemas, programas, processos e equipamento isolado ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

XXX - risco de SIC: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XXXI - segurança física e do ambiente: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;

XXXII - sensibilização em SIC: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional;

XXXIII - sistema estruturante: conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente;

XXXIV - terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao IF Catarinense;

XXXV - tratamento de incidentes: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XXXVI - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas; e

XXXVII - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO II

ESCOPO

Seção I
Objetivos da Política de Segurança da Informação e Comunicação

Art. 3° A PoSIC é uma declaração formal que objetiva a preservação da confidencialidade, da integridade, da disponibilidade e autenticidade das informações produzidas ou custodiadas pelo IF Catarinense.

Art. 4° O IF Catarinense deve observar as diretrizes, normas, procedimentos, mecanismos, competências e responsabilidades estabelecidos nesta PoSIC.

Art. 5° Integram também a PoSIC as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

Art. 6° As diretrizes de Segurança da Informação e Comunicações - SIC devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e estrutura organizacional do IF Catarinense.

Art. 7° A Gestão de Segurança da Informação e Comunicações - GSIC deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de SIC.

Seção II
Abrangência

Art. 8° As diretrizes, normas complementares e manuais de procedimentos da PoSIC do IF Catarinense aplicam-se a servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, execute atividades vinculadas a este Instituto.

Parágrafo único. Todos são responsáveis e devem estar comprometidos com a segurança da informação e comunicações.

Art. 9° Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo IF Catarinense devem atender a esta PoSIC.

Art. 10 Esta política também se aplica, no que couber, ao relacionamento do IF Catarinense com outros órgãos e entidades públicas ou privadas.

CAPÍTULO III

PRINCÍPIOS

Art. 11. A PoSIC deve obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal.

CAPÍTULO IV

DIRETRIZES GERAIS

Art. 12. O cumprimento desta política de segurança e de suas normas complementares deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente constituído pelo Comitê de Segurança da Informação e Comunicações - CSIC, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Art. 13. Cabe ao CSIC instituir programas permanentes e regulares de conscientização, sensibilização e capacitação em SIC, buscando parcerias com outros órgãos e entidades.

Art. 14. Os órgãos e entidades do Sistema de Administração dos Recursos de Informação e Informática - SISP podem adotar ou utilizar esta PoSIC e suas normas complementares como modelos de referência para elaboração dos seus documentos.

Art. 15. Fica instituída a Estrutura de GSIC do IF Catarinense, composta pelo Comitê de Segurança da Informação e Comunicações - CSIC e pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, os quais serão solidariamente responsáveis pelas seguintes atividades:

I - executar os processos de segurança da informação e comunicações;

II - desenvolver, implementar e monitorar estratégias de segurança que atendam aos objetivos estratégicos do IF Catarinense;

III - avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação;

IV - desenvolver ações de conscientização dos usuários a respeito da implementação desses controles;

V - fornecer subsídios visando à verificação de conformidade de segurança da informação e comunicações; e

VI - promover a melhoria contínua nos processos e controles de GSIC.

Parágrafo único. A Estrutura de GSIC deve definir um Plano de SIC para o IF Catarinense.

Art. 16. As unidades administrativas que contam com corpo técnico e infraestrutura de tecnologia da informação próprios possuem autonomia para sua estrutura de GSIC, desde que submetidas e aderentes a esta PoSIC.

Art. 17. A estrutura central de SIC do IF Catarinense e as estruturas descentralizadas de Gestão de SIC devem compartilhar o sistema de registro de incidentes de SIC.

Art. 18. Os membros da Estrutura da GSIC devem receber regularmente capacitação especializada nas disciplinas relacionadas à SIC.

Art. 19. A GSIC do IF Catarinense deve auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias do Instituto Federal e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

Art. 20. A Estrutura de GSIC deve planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança.

Art. 21. O IF Catarinense, além das diretrizes estabelecidas nesta PoSIC, deve também se orientar pelas melhores práticas e procedimentos de SIC recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 22. É vetado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo IF Catarinense.

Art. 23. O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação.

Parágrafo único. A não designação pressupõe que o gestor é o próprio custodiante.

Art. 24. Os contratos firmados pelo IF Catarinense devem conter cláusulas que determinem a observância da PoSIC e seus respectivos documentos.

Art. 25. A utilização da computação em nuvem deve ser regulamentada pelo CSIC por norma específica.

CAPÍTULO V

DIRETRIZES ESPECÍFICAS

Art. 26. Para cada uma das diretrizes constantes das seções deste capítulo devem ser elaboradas normas táticas específicas, manuais e procedimentos.

Seção I

Da Gestão de Ativos da Informação

Art. 27. Os ativos de informação devem:

I - ser inventariados e protegidos;

II - ter identificados os seus proprietários e custodiantes;

III - ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV - ter a sua a entrada e saída nas dependências do IF Catarinense autorizadas e registradas por autoridade competente;

V - ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

VI - ser regulamentados por norma específica quanto a sua utilização; e

VII - ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 28. Os gestores da informação devem estabelecer regras e mecanismos que visem à manutenção de uma base de conhecimento sobre a realização de atividades no IF Catarinense, observadas as normas de SIC.

Art. 29. O IF Catarinense deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 30. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 31. Os sistemas de informação e as aplicações do IF Catarinense devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

Art. 32. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

Seção II
Da Gestão de Riscos

Art. 33. A Estrutura de GSIC deve estabelecer processos de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC que possibilitem identificar ameaças e reduzir vulnerabilidades e impactos dos ativos de informação.

Art. 34. A GRSIC é um processo contínuo e deve ser aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações, levando em consideração o planejamento, execução, análise crítica e melhoria da SIC no âmbito do IF Catarinense.

Seção III
Da Segurança Física e do Ambiente

Art. 35. A Estrutura de GSIC deve estabelecer mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências.

Art. 36. As proteções devem estar alinhadas aos riscos identificados.

Seção IV
Da Segurança em Recursos Humanos

Art. 37. Os usuários devem ter ciência:

I - das ameaças e preocupações relativas à SIC; e

II - de suas responsabilidades e obrigações no âmbito desta PoSIC.

Art. 38. Todos os usuários devem difundir e exigir o cumprimento da PoSIC, das normas de segurança e da legislação vigente acerca do tema.

Art.39. Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários do IF Catarinense, de acordo com suas competências funcionais.

Art. 40. Os usuários devem ser sensibilizados e conscientizados para apoiar esta PoSIC durante os seus trabalhos normais.

Art. 41. O controle de pessoal:

I - é de responsabilidade do titular da unidade administrativa juntamente com a Diretoria de Gestão de Pessoas; e

II - deve estabelecer controles de perfis, permissões e procedimentos necessários para a salvaguarda da SIC.

Seção V
Da Gestão de Operações e Comunicações

Art. 42. A Estrutura de GSIC deve estabelecer parâmetros adequados, relacionados à SIC, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais do IF Catarinense.

Seção VI
Dos Controles de Acessos

Art. 43. Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.

Art. 44. Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 45. Os usuários do IF Catarinense são responsáveis por todos os atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e assinatura digital.

Art. 46. A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

Art. 47. A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribui-

ções de cada usuário e qualquer outra forma de uso ou acesso, além do necessário depende de prévia autorização do gestor da área responsável pela informação.

Art. 48. Todos os sistemas de informação do IF Catarinense, automatizados ou não, devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações.

Art. 49. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento do IF Catarinense.

Art. 50. Os sistemas estruturantes devem possuir normas específicas, no âmbito de sua atuação, que regrem o controle de acesso quanto:

I - ao acesso às suas bases de dados;

II - à extração, carga e transformação de dados; e

III - aos serviços acessíveis via linguagem de programação.

Art. 51. Os sistemas estruturantes devem possuir mecanismos automáticos para:

I - revogar as concessões e desativar as contas de acesso do servidor nos casos de exoneração, demissão, aposentadoria e falecimento do servidor;

II - bloquear as contas de acesso do servidor nos casos de licença, afastamento, cessão e disponibilidade do servidor; e

III - tratar os casos de remoção e redistribuição do servidor, segundo as definições constantes na norma de controle de acesso ao sistema.

Art. 52. É responsabilidade do gestor do Sistema Integrado de Administração de Recursos Humanos - SIAPE disponibilizar, com periodicidade mensal, os registros de todas as movimentações de pessoal referenciadas no Art. 51 ocorridas no período, na forma definida por norma complementar.

Seção VII
Da Criptografia

Art. 53. O uso de recursos criptográficos interfere na confidencialidade, integridade, disponibilidade e autenticidade das informações, sendo, portanto, responsabilidade do Gestor de SIC a implementação dos procedimentos relativos ao seu uso, no âmbito das informações produzidas e custodiadas no IF Catarinense, em conformidade com as orientações contidas em norma específica.

Art. 54. O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Responsabilidade pelo seu uso.

Seção VIII

Da Aquisição, do Desenvolvimento e da Manutenção de Sistemas

Art. 55. A Estrutura de GSIC deve estabelecer critérios e metodologia de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção.

Art. 56. O processo de aquisição de sistemas e aplicações corporativas deve atender requisitos de segurança previstos em norma específica.

Seção IX

Do Tratamento de Incidentes

Art. 57. A Estrutura de GSIC deve instituir metodologias ou normas que estabeleçam processos de gestão para tratamento e respostas a incidentes de segurança, de forma a observar o disposto no arcabouço técnico normativo do CTIR.GOV.

Art. 58. Deve ser instituída a Equipe de Tratamento e Resposta a Incidentes de Segurança.

Seção X

Da Gestão de Continuidade

Art. 59. A Estrutura de GSIC deve instituir metodologias ou normas que estabeleçam a Gestão de Continuidade do Negócio.

Seção XI

Da Conformidade

Art. 60. Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de SIC do IF Catarinense e de suas unidades administrativas com esta PoSIC e suas normas e procedimentos complementares, bem como com a legislação específica de SIC.

Art. 61. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o IF Catarinense.

Art. 62. A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pela Estrutura de GSIC e aprovado pelo CSIC.

Art. 63. O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos.

Art. 64. Nenhuma unidade administrativa poderá permanecer sem verificação de conformidade de suas práticas de SIC por período superior a 2 (dois) anos.

Art. 65. A execução da verificação de conformidade será realizada pela Estrutura de GSIC, podendo, com a prévia aprovação do CSIC, ser subcontratada no todo ou em parte.

Art. 66. É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

Art. 67. A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

Art. 68. Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Gestor de SIC ao Gestor da unidade administrativa verificada, para ciência e tomada das ações cabíveis.

Seção XII
Do Plano de Investimentos em SIC do IF Catarinense

Art. 69. Os investimentos em SIC serão realizados de forma planejada e consolidados em um plano de investimentos.

Art. 70. O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco.

Art. 71. Os investimentos em SIC constituirão ação orçamentária específica e permanente na Lei Orçamentária Anual - LOA, distinta das ações orçamentárias relativas a investimentos em segurança da informação destinados à Administração Pública Federal como um todo.

Art. 72. O plano de investimentos, assim como a correspondente proposta orçamentária, será aprovado pelo CSIC, mediante recomendação elaborada pela Estrutura de GSIC.

Art. 73. Caso a dotação concedida na LOA seja inferior à solicitada na proposta orçamentária, ou haja limitação na execução orçamentária, caberá ao CSIC realizar a correspondente revisão do plano de investimentos.

Seção XIII
Da Propriedade Intelectual

Art. 74. As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual do IF Catarinense e não cabe a seus criadores qualquer forma de direito autoral.

§ 1º Quando as informações forem produzidas por terceiros para uso exclusivo do IF Catarinense, instrumento próprio obrigará os criadores ao sigilo permanente do conteúdo dos produtos.

§ 2º É vedada a utilização das informações a que se refere o parágrafo anterior em quaisquer outros projetos ou atividades de uso diverso ao estabelecido pelo IF Ca-

tarinense, salvo autorização específica pelos titulares das unidades administrativas, nos processos e documentos de sua competência, ou pelo Reitor, nos demais casos.

Seção XIV

Dos Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 75. Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 76. Os acordos com terceiros podem também envolver outras partes.

Parágrafo único. Os acordos que concedam o acesso a terceiros podem incluir, quando necessário e justificado, permissão para designação de outras partes autorizadas e condições para os seus acessos desde que expressamente autorizadas pelo IF Catarinense.

Art. 77. Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta PoSIC.

Art. 78. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar a PoSIC e suas normas complementares aos seus empregados e prepostos envolvidos em atividades no IF Catarinense.

Art. 79. Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

Art. 80. Deve ser definido um processo adequado/objetivo de gestão de mudanças que será detalhado em norma específica.

CAPÍTULO VI

PENALIDADES

Art. 81. A não-observância aos dispositivos da PoSIC ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SIC do IF Catarinense pode acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

CAPÍTULO VII

COMPETÊNCIAS E RESPONSABILIDADES

Art. 82. Cabe ao Gestor de SIC:

I - promover cultura de segurança da informação e comunicações;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - propor recursos necessários às ações de SIC;

IV - coordenar o CSIC e a ETIR;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;

VI - manter contato direto com o DSIC/GSI/PR para o trato de assuntos relativos à segurança da informação e comunicações; e

VII - propor normas relativas à SIC.

Art. 83. Cabe ao CSIC:

I - normatizar e supervisionar a SIC no âmbito do IF Catarinense;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

III - propor alterações na PoSIC;

IV - solicitar apurações quando da suspeita de ocorrências de quebras de SIC;

V - avaliar, revisar e analisar criticamente a PoSIC e suas normas complementares, visando a sua aderência aos objetivos institucionais do IF Catarinense e às legislações vigentes;

VI - dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PoSIC do IF Catarinense;

VII - constituir grupo de trabalho para realizar verificações de conformidade;

VIII - aprovar o plano de investimentos em SIC do IF Catarinense;

IX - monitorar e avaliar periodicamente o plano de SIC de que trata o parágrafo único do Art. 15, assim como determinar os ajustes cabíveis; e

X - definir e atualizar seu Regimento Interno.

Art. 84. Cabe à ETIR:

I - facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

II - promover a recuperação de sistemas;

III - agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

IV - realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

V - analisar ataques e intrusões na rede do IF Catarinense;

VI - executar as ações necessárias para tratar quebras de segurança;

VII - obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

VIII - cooperar com outras equipes de Tratamento e Resposta a Incidentes; e

IX - participar em fóruns, redes nacionais e internacionais relativos à SIC.

Art. 85. Cabe ao Gestor do Ativo de Informação:

I - garantir a segurança dos ativos de informação sob sua responsabilidade;

II - definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta PoSIC;

III - conceder e revogar acessos aos ativos de informação;

IV - comunicar à ETIR a ocorrência de incidentes de SIC; e

V - designar custodiante dos ativos de informação, quando aplicável.

Art. 86. Cabe ao custodiante do ativo de informação proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta PoSIC.

Art. 87. Cabe ao titular da unidade administrativa:

I - conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SIC;

II - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;

III - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;

IV - informar à DGP a movimentação de pessoal de sua unidade;

V - realizar o tratamento e a classificação da informação;

VI - autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;

VII - comunicar à ETIR os casos de quebra de segurança; e

VIII - manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores.

Art. 88. Cabe aos terceiros e fornecedores, conforme previsto em contrato:

I - tomar conhecimento desta PoSIC;

II - fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e

III - fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

Art. 89. Cabe aos usuários:

I - conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta PoSIC, bem como os demais normativos e resoluções relacionados à SIC;

II - obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação; e

III - comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações à ETIR.

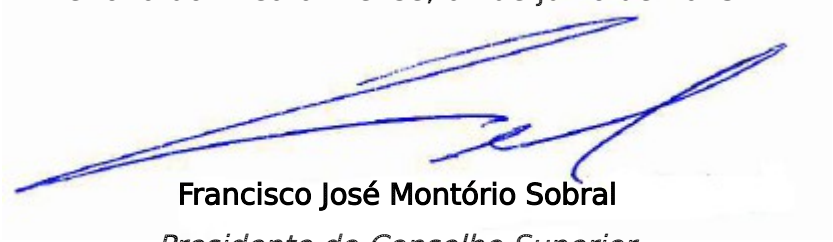
CAPÍTULO VIII

ATUALIZAÇÃO

Art. 90. Esta PoSIC, bem como os documentos gerados a partir dela, deverão ser revisados no máximo a cada cinco anos ou por deliberação do CSIC, de modo a atualizar a política frente a novos requisitos institucionais.

Parágrafo único. O CSIC formalizará a proposta de revisão da PoSIC por meio de Resolução, a qual deve ser, sucessivamente, apreciada pela Conselho Superior e aprovada pelo Reitor.

Reitoria do IF Catarinense, 02 de julho de 2013.



Francisco José Montório Sobral

Presidente do Conselho Superior

REFERÊNCIAS LEGAIS E NORMATIVAS

I – Quadro dos dispositivos legais de caráter federal, aplicáveis à Segurança da Informação:

Dispositivo	**Aspecto da SI**
Constituição Federal, Art. 5º, inciso X.	Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
Constituição Federal, Art. 5º, inciso XII.	Sigilo dos dados telemáticos e das comunicações privadas.
Constituição Federal, Art. 5º, inciso XIV.	Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
Constituição Federal, Art. 5º, inciso XXXIII e Art. 37, § 3º, inciso II.	Disponibilidade das informações constantes nos órgãos públicos.
Constituição Federal, Art. 5º, inciso XXXIV.	Disponibilidade das informações constantes nos órgãos públicos.
Constituição Federal, Art. 23, incisos III e IV.	Proteção da integridade, da autenticidade e da disponibilidade das informações pelo Estado.
Constituição Federal, Art. 216, § 2º.	Proteção da integridade, da autenticidade, da disponibilidade e do sigilo das informações constantes nos órgãos e entidades integrantes da Administração Pública.
Constituição Federal, Art. 37, caput.	Quanto melhor a gestão das informações, mais eficiente será o órgão ou entidade, daí a necessidade de implantação de uma Política de Segurança da Informação.
Constituição Federal, Art. 37, § 6º e Código Civil, Art. 43.	Responsabilidade objetiva do Estado por dano decorrente da má gestão das informações pelos órgãos e entidades da Administração Pública e pessoas de direito privado prestadoras de serviços públicos.
Constituição Federal, Art. 37, § 7º.	Necessidade de regulamentação do acesso a informações privilegiadas.
Consolidação das Leis do Trabalho - CLT, Art. 482, alínea "g".	Proteção das informações sigilosas acessadas no exercício de emprego público (empresas públicas e sociedades de economia mista).
Código de Conduta da Alta Administração, Art. 5º, § 4º.	Sigilo das informações fiscais e tributárias das autoridades públicas (sigilo perante terceiros e não em face da Administração Pública).
Código de Conduta da Alta Administração, Art.14, inciso II.	Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.
Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "h" do inciso XV da Seção II.	Proteção da integridade das informações públicas.
Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "I" do inciso XV da Seção II.	Proteção da disponibilidade das informações públicas.
Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso X da Seção I.	Proteção da disponibilidade das informações públicas.
Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso VII da Seção I.	Proteção da disponibilidade das informações públicas e garantia da publicidade das informações de interesse da coletividade.
Decreto nº 1.171/1994 (Código de Ética do Servidor Público), inciso IX da Seção I.	Proteção da integridade do patrimônio público, a exemplo de equipamentos, materiais, áreas e instalações.
Decreto nº 1.171/1994 (Código de Ética do Servidor Público), alínea "e" do inciso XIV da Seção II.	Disponibilidade das comunicações.
Código de Propriedade Industrial, Art. 75.	Sigilo das patentes de interesse da defesa nacional.
Código de Defesa do Consumidor, arts. 43 e 44.	Garantia da integridade e disponibilidade das informações dos consumidores arquivadas em bancos de dados.
Código Penal, Art. 151.	Proteção do sigilo, integridade e disponibilidade das informações de caráter pessoal veiculadas através dos meios de comunicação.
Código Penal, Art. 152.	Proteção do sigilo e da disponibilidade das informações dos estabelecimentos comerciais.

Código Penal, Art. 153.	Proteção do sigilo das informações classificadas constantes nos sistemas ou bancos de dados da Administração Pública.
Código Penal, Art. 154.	Proteção do sigilo das informações conhecidas em razão de função, ministério, ofício ou profissão.
Código Penal, Art. 184, § 3º.	Proteção da autenticidade.
Código Penal, Art. 297.	Proteção da integridade e autenticidade dos documentos públicos.
Código Penal, Art. 298.	Proteção da integridade e autenticidade dos documentos particulares.
Código Penal, Art. 305.	Proteção da disponibilidade e integridade das informações constantes nos órgãos e entidades públicos.
Código Penal, Art. 307.	Proteção da autenticidade.
Código Penal, Art. 313-A.	Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, Art. 313-B.	Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, Art. 314.	Proteção da disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, Art. 325.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Código Processo Penal, Art. 20.	Proteção de informações sigilosas.
Código Processo Penal, Art. 207.	Proteção do sigilo profissional.
Código Processo Penal, Art. 745.	Proteção de informações sigilosas relacionadas ao condenado.
Código Tributário Nacional, Art. 198.	Proteção do sigilo fiscal.
Código de Processo Civil, Art. 347, inciso II c/c Art. 363, inciso IV.	Proteção da privacidade de seus clientes.
Código de Processo Civil, Art. 406, inciso II c/c Art. 414, § 2°.	Proteção da privacidade de seus clientes.
Instrução Normativa n° 4/2010.	Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal.
Lei n° 6.538/1978, Art. 41.	Proteção da privacidade de correspondência.
Lei n° 7.170/1983, Art. 13.	Proteção das informações sigilosas relacionadas à segurança nacional.
Lei n° 7.232/1984, Art. 2°, inciso VIII.	Sigilo dos dados relacionados à intimidade, vida privada e honra; especialmente dos dados armazenados através de recursos informáticos.
Lei n° 7.492/1986, Art. 18.	Proteção das informações sigilosas no âmbito das instituições financeiras ou integrantes do sistema de distribuição de títulos mobiliários.
Lei n° 8.027/1990, artigo 5°, inciso I.	Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.
Lei n° 8.027/1990, artigo 5°, parágrafo único, inciso V.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Lei n° 8.112/1990, Art. 116, inciso VIII.	Sigilo das informações produzidas ou conhecidas no exercício de cargo ou função pública.
Lei n° 8.112/1990, Art. 132, inciso IX.	Proteção das informações sigilosas acessadas no exercício de cargo ou função pública.
Lei n° 8.137/1990, Art. 3°, inciso I.	Proteção da disponibilidade de informações para manutenção da ordem tributária.
Lei n° 8.429/1992, Art.11, incisos III, IV e VII.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público, bem como garantia de publicidade das informações de interesse coletivo ou geral que devem ser divulgadas por ato oficial.
Lei n° 8.429/1992, Art. 13.	Disponibilidade de informações pessoais do agente público para o Poder Público e veracidade dos dados.
Lei n° 8.443/1992, Art. 86, inciso IV.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Lei Complementar n° 75/1993, Art. 8° incisos II e VIII, §§ 1° e 2°.	Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.
Lei n° 8.625/1993, Art. 26, inciso I, alínea "b" e inciso II.	Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.
Lei n° 8.906/1994, Art. 7°, inciso XIX.	Proteção da privacidade do cliente do advogado.

Lei n° 9.100/1995, Art. 67, incisos VII e VIII.	Proteção da integridade e autenticidade dos sistemas informatizados e das informações neles armazenadas.
Lei n° 9.279/1996, Art. 195, inciso XI.	Proteção da privacidade das pessoas jurídicas, relacionado ao sigilo de suas informações.
Lei n° 9.296/1996, Art. 10.	Sigilo dos dados e das comunicações privadas.
Lei n° 9.472/1997, Art. 3°, inciso V.	Sigilo das comunicações.
Lei n° 9.472/1997, Art. 3°, inciso VI.	Proteção de informações pessoais de caráter sigiloso.
Lei n° 9.472/1997, Art. 3°, inciso IX.	Proteção de informações pessoais de caráter sigiloso.
Lei n° 9.504/1997, Art. 72.	Proteção da integridade das informações de caráter eleitoral e dos equipamentos.
Lei n° 9.605/1998, Art. 62.	Disponibilidade e integridade de dados e informações.
Lei n° 10.683/2003, Art. 6°.	Todos os aspectos da segurança da informação.
Lei n° 10.703/2003, arts. 1°, 2° e 3°.	Disponibilidade de dados cadastrais para fins de investigação criminal e sigilo nas demais hipóteses.
Decreto n° 4.801/2003, Art. 1°, inciso X.	Todos os aspectos da segurança da informação.
Proteção da autenticidade. Decreto n° 5.483/2005, arts. 3° e 11.	Disponibilidade de informações pessoais do agente público para o Poder Público e dever de sigilo por parte da Controladoria-Geral da União.
Decreto n° 5.687/2006, arts.10 e 13 do Anexo.	Disponibilidade das informações públicas ou administrativas e sigilo das informações pessoais constantes nos registros públicos.
Decreto n° 6.029/2007, inciso II do Art. 1°.	Disponibilidade das informações constantes nos registros públicos.
Decreto n° 6.029/2007, Art. 10.	Sigilo da identidade do denunciante e sigilo do processo para proteção da honra e da imagem do investigado antes da prolação da decisão pela Comissão de Ética.
Decreto n° 6.029/2007, Art. 13.	Sigilo do processo administrativo por infração ética antes da prolação da decisão e publicidade após o término e aplicação das penalidades.
Decreto n° 6.029/2007, Art. 22.	Disponibilidade, integridade e autenticidade das informações constantes no banco de dados mantido pela Comissão de Ética Pública.

II – Quadro da legislação específica de caráter federal relacionada à Segurança da Informação:

Regulamento	**Assunto**
Lei n° 7.232/1984	Dispõe sobre a Política Nacional de Informática, e dá outras providências.
Lei n° 8.248/1991	Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.
Lei n° 9.296/1996	Regulamenta o inciso XII, parte final, do Art. 5° da Constituição Federal que dispõe sobre a violação do sigilo de dados e das comunicações telefônicas.
Lei n° 9.472/1997	Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais.
Lei n° 9.507/1997	Regula o direito de acesso a informações e disciplina o rito processual do habeas data.
Lei n° 9.609/1998	Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.
Lei n° 9.883/1999	Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.
Lei n° 8.159/1991	Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências.
Lei Complementar n° 105, de 10 de janeiro de 2001.	Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.
Medida Provisória n° 2.200-2, de 24 de agosto de 2001.	Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia

	da Informação em autarquia, e dá outras providências.
Lei n° 10.973, de 02 de dezembro de 2004.	Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências.
Lei n° 11.111, de 05 de maio de 2005.	Regula o direito à informação e ao acesso aos registros públicos.
Lei n° 11.419, de 19 de dezembro de 2006.	Dispõe sobre a informatização do processo judicial; altera a Lei n° 5.869, de 11 de janeiro de 1973 - Código de Processo Civil; e dá outras providências.
Decreto n° 2.295, de 04 de agosto de 1997.	Regulamenta o disposto no Art. 24, inciso IX, da Lei n° 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Neste caso o processo deverá ser sigiloso, excetuando-se a publicidade das compras governamentais.
Decreto n° 2.556, de 20 de abril de 1998.	Regulamenta o registro previsto no Art. 3° da Lei n° 9.609, de 19 de fevereiro de 1998, que dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.
Decreto n° 3.294, de 15 de dezembro de 1999.	Institui o Programa Sociedade da Informação, com objetivo de viabilizar a nova geração da Internet e suas aplicações em benefício da sociedade brasileira.
Decreto n° 3.505, de 13 de junho de 2000.	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
Decreto de 18 de outubro de 2000.	Cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, e dá outras providências.
Decreto n° 3.714, de 03 de janeiro de 2001.	Dispõe sobre a remessa por meio eletrônico de documentos a que se refere o Art. 57-A do Decreto n° 2.954, de 29 de janeiro de 1999, e dá outras providências.
Decreto n° 3.996, de 31 de outubro de 2001.	Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.
Decreto n° 4.073, de 03 de janeiro de 2002.	Regulamenta a Lei n° 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.
Decreto n° 4.376, de 13 de setembro de 2002.	Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, e dá outras providências.
Decreto n° 4.522, de 17 de dezembro de 2002.	Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências.
Decreto n° 4.553, de 27 de dezembro de 2002.	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.
Decreto n° 4.689, de 07 de maio de 2003.	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação - ITI, e dá outras providências.
Decreto n° 4.829, de 03 de setembro de 2003.	Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.
Decreto de 29 de outubro de 2003.	Institui Comitês Técnicos do Comitê Executivo do Governo Eletrônico e dá outras providências.
Decreto n° 5.301, de 09 de dezembro de 2004.	Institui a Comissão de Averiguação e Análise de Informações Sigilosas, dispõe sobre suas atribuições e regula seu funcionamento.
Decreto n° 5.450, de 31 de maio de 2005.	Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.
Decreto n° 5.563, de 11 de outubro de 2005.	Regulamenta a Lei n° 10.973, de dezembro de 2004, que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo, e dá outras providências.
Decreto n° 5.584, de 18 de novembro de 2005.	Dispõe sobre o recolhimento ao Arquivo Nacional dos documentos arquivísticos públicos produzidos e recebidos pelos extintos Conselho de Segurança Nacional - CSN, Comissão Geral de Investigações - CGI e Serviço Nacional de Informações - SNI, que estejam sob a custódia da Agência Brasileira de Inteligência - ABIN.
Decreto n° 5.772, de 08 de maio de 2006, Art. 8°.	Institui na estrutura regimental do Gabinete de Segurança Institucional da Presidência da República o Departamento de Segurança da Informação e Comunicações com diversas atribuições na área de segurança da informação e comunicações.

Decreto n° 6.605, de 14 de outubro de 2008.	Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC.
Instrução Normativa n° 1 do GSI, de 13 de junho de 2008.	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
Resolução n° 58 do INPI, de 14 de julho de 1998.	Estabelece normas e procedimentos relativos ao registro de programas de computador.
Resolução n° 59 do INPI, de 14 de julho de 1998.	Estabelece os valores das retribuições pelos serviços de registro de programas de computador.
Resolução n° 338 do STF, de 11 de abril de 2007.	Dispõe sobre classificação, acesso, manuseio, reprodução, transporte e guarda de documentos e processos de natureza sigilosa no âmbito do STF.
Resolução n° 140 do TST, de 13 de setembro de 2007.	Regulamenta, no âmbito da Justiça do Trabalho, a Lei n° 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial.
Resolução n° 22.718/2008 do TSE, arts. 18 e 19.	Regula a propaganda eleitoral na internet em campanha nas eleições de 2008.

III – Quadro de normas técnicas relacionadas à Segurança da Informação:

Regulamento	**Assunto**
ISO/IEC TR 13335-3:1998.	Esta norma fornece técnicas para a gestão de segurança na área de tecnologia da informação. Baseada na norma ISO/IEC 13335-1 e TR ISO/IEC 13335-2. As orientações são projetadas para auxiliar o incremento da segurança na TI.
ISO/IEC GUIDE 51:1999.	Esta norma fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos. É aplicável a qualquer aspecto de segurança relacionado a pessoas, propriedades, ao ambiente, ou a uma combinação de um ou mais destes (por exemplo, somente pessoas; pessoas e propriedades; pessoas, propriedades e o ambiente).
ISO/IEC GUIDE 73:2002.	Esta norma fornece definições genéricas de termos de gestão de riscos para a elaboração de normas. Seu propósito é ser um documento genérico de alto nível voltado para a preparação ou revisão de normas que incluam aspectos de gestão de riscos.
ABNT NBR ISO IEC 17799: 2005.	Esta norma é equivalente à ISO/IEC 17799:2005. Consiste em um guia prático que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos de controle e os controles definidos nesta norma têm como finalidade atender aos requisitos identificados na análise/avaliação de riscos.
ABNT NBR ISO/IEC 27001:2005.	Esta norma é usada para fins de certificação e substitui a norma Britânica BS 7799-2:2002. Aplicável a qualquer organização, independente do seu ramo de atuação, define requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação.