RESOLUÇÃO Nº 07, DE 26 DE MARÇO DE 2013.

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE GOIÁS, no uso de suas atribuições legais e regimentais, considerando a decisão do Conselho Superior em reunião realizada no dia 26 de março de 2013 e, ainda, tendo como base legal a publicação da Lei nº 11.892, de 29 de dezembro de 2008, e o Estatuto do Instituto Federal de Goiás, resolve:

Art. 1º - Aprovar a Política de Segurança da Informação e das Comunicações - PoSIC do Instituto Federal de Educação, Ciência e Tecnologia de Goiás, nos termos do documento em anexo.

Art. 2º - Esta Resolução entra em vigor na data de sua publicação

PAULO CÉSAR PEREIRA
Presidente do Conselho Superior

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES

- PoSIC –

CAPÍTULO I

DOS OBJETIVOS

Art. 1º - A Política de Segurança da Informação e das Comunicações (PoSIC) do Instituto Federal de Educação, Ciência e Tecnologia de Goiás (IFG) tem por objetivo estabelecer diretrizes, normas e procedimentos com vistas à manutenção do bom uso da informação em todos os seus aspectos bem como dos recursos de comunicação.

Art. 2º - A PoSIC-IFG deve obedecer aos preceitos constitucionais, ao arcabouço legal vigente e aos documentos normativos e administrativo que regem a Administração Pública Federal.

Parágrafo único - Os fundamentos legais e normativos referentes à segurança da informação e das comunicações, considerados para a elaboração desta PoSIC, estão referenciados no Anexo III.

CAPÍTULO II

DA ABRANGÊNCIA

Art. 3º - As diretrizes, normas, procedimentos, manuais e quaisquer outras documentos advindos desta PoSIC aplicam-se a servidores, corpo discente, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, execute atividades vinculadas ao IFG.

Parágrafo Único - Todos são responsáveis e devem estar comprometidos com a Segurança da Informação e das Comunicações (SIC).

Art. 4º - Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo IFG devem atender a esta PoSIC.

Art. 5º - Esta política também se aplica, no que couber, ao relacionamento do IFG com outros órgãos e entidades públicos ou privados.

CAPÍTULO III

ESTRUTURA DA POSIC

Art. 6º - A PoSIC-IFG será composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

I - Política de Segurança da Informação e das Comunicações (PoSIC): constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação e das Comunicações;

II - Normas de Segurança da Informação e das Comunicações: estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da PoSIC-IFG, a serem seguidos em diversas instâncias em que a informação é tratada. Cada Norma deverá fazer referência ao ponto que pretende atender na PoSIC-IFG. A cada Norma será associado um conjunto de Procedimentos destinados a orientar sua implementação. A elaboração das Normas seguirá as orientações contidas em um documento do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI/PR), intitulado Atividade de Normatização;

III - Procedimentos de Segurança da Informação e das Comunicações: instrumentalizam o disposto nas Normas, permitindo a direta aplicação nas atividades do IFG. As Normas determinarão os responsáveis pela definição dos procedimentos, que poderão ainda ser detalhado em instruções. Os procedimentos e as instruções são de uso interno, não sendo obrigatória a sua publicação;

Parágrafo único - O IFG poderá lançar mão de outros documentos como manuais, jornais, folders e quaisquer outros instrumentos que puderem ser utilizados no cumprimento das diretrizes traçadas nesta PoSIC;

Art. 7º – Os conceitos utilizados na definição desta PoSIC estão expressos no Anexo II.

CAPÍTULO IV

DAS INSTÂNCIAS

Art. 8º - São instâncias de implementação, fiscalização e atualização desta PoSIC:

I - Comitê Gestor de Tecnologia da Informação (CGTI): instituído pela Portaria IFG nº 937, de 08 de novembro de 2011, é uma instância de natureza consultiva do Colégio de Dirigentes e tem por finalidade o alinhamento das ações de Tecnologia da Informação e das Comunicações, disposto no Plano de Desenvolvimento Institucional do IFG.

II - Comitê Gestor da Segurança da Informação e das Comunicações (CGSIC) do IFG, instituído pela Portaria nº 1437, de 29 de agosto de 2012, é um órgão de assessoramento da Reitoria, tendo natureza deliberativa nas questões concernentes às suas atribuições específicas.

III - Diretoria de Tecnologia da Informação (DTI): instância administrativa/executiva responsável por propor as políticas e programas do IFG na área de informática e telecomunicações, bem como por sua implementação e gestão.

IV – A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): instância responsável a dar tratamento de primeiro nível aos incidentes de segurança da informação e das comunicações.

V - Gerência de Desenvolvimento, Administração e Manutenção de Tecnologia da Informação do IFG: instância responsável pelo desenvolvimento, implantação e manutenção dos recursos e serviços de tecnologia da informação e comunicações no âmbito do IFG.

VI - Coordenação de Tecnologia da Informação de cada câmpus: instância que tem como atribuição principal o gerenciamento da rede local, bem como dos recursos de tecnologia da informação e das comunicações do câmpus a ela conectados, direta ou indiretamente.

VII - Unidade: qualquer instância administrativa do IFG, a exemplo dos câmpus, unidades ligadas aos câmpus, núcleos de pesquisa e centros com funcionalidades específicas.

CAPÍTULO IV

DAS DIRETRIZES-GERAIS

Art. 9º - O cumprimento desta política de segurança e os documentos delas advindos deverão ser avaliados periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente constituído pelo CGSIC-IFG, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Art. 10 - Deverão ser instituídos programas permanentes e regulares de conscientização, sensibilização e capacitação em SIC buscando, se for o caso, parcerias com outros órgãos e entidades.

Art. 11 - O CGSIC-IFG, a DTI e a ETIR constituirão Força-Tarefa, doravante designada simplesmente de FTSIC, e serão solidariamente responsáveis pelas seguintes atividades:

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

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

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 das comunicações e promover a melhoria contínua nos processos e controles de Gestão de Segurança da Informação e das Comunicações.

Art. 12 - O CGSIC-IFG deve auxiliar o CGTI 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 IFG e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

Art. 13 - O CGSIC-IFG deve planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança.

Art. 14 - O IFG, 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. 15 - É vetado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas ou custodiadas pelo IFG.

Art. 16 - Os contratos firmados pelo IFG devem conter cláusulas que determinem a observância desta PoSIC e seus respectivos documentos.

Art. 17 - Para cada uma das diretrizes constantes dos artigos deste capítulo devem ser elaboradas Normas específicas e procedimentos.

CAPÍTULO V

DA GESTÃO DOS ATIVOS DE INFORMAÇÃO

Art. 18 - O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação. A não designação pressupõe que o gestor é o próprio custodiante.

Art. 19 - 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 entrada e saída nas dependências do IFG 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.

Art. 20 - O IFG deve criar, gerir e avaliar critérios de tratamento e identificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 21 - 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. 22 - Os sistemas de informação e os aplicativos do IFG devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

Art. 23 - O acesso dos usuários externos aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado à ciência e ao aceite desta PoSIC.

CAPÍTULO VI

DA GESTÃO DE RISCOS

Art. 24 - A FTSIC 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. 25 - A GRSIC é um processo contínuo e deve ser aplicado na implementação e operação da Gestão de Segurança da Informação e das Comunicações, levando em consideração o planejamento, a execução, análise crítica e melhoria da SIC no IFG.

Art. 26 - As proteções devem estar alinhadas aos riscos identificados.

CAPÍTULO VII

DA SEGURANÇA FÍSICA E DO AMBIENTE

Art. 27 - A FTSIC deve estabelecer mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências.

CAPÍTULO VIII

DA SEGURANÇA EM RECURSOS HUMANOS

Art. 28 - Os usuários devem ter ciência das ameaças e preocupações relativas à SIC e de suas responsabilidades e obrigações no âmbito desta PoSIC.

Art. 29 - Todos os usuários devem difundir e exigir o cumprimento desta PoSIC e da legislação vigente acerca do tema.

Art. 30 - Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários do IFG.

Art. 31 - É de responsabilidade da Diretoria de Desenvolvimento de Recursos Humanos do IFG estabelecer, para os servidores do IFG, controles de perfis, permissões e procedimentos necessários à salvaguarda da SIC, observadas as atribuições e competências de cada servidor.

Art. 32 - É de responsabilidade da Diretoria de Administração Acadêmica do IFG estabelecer, para o corpo discente, controles de perfis, permissões e procedimentos necessários à salvaguarda da SIC, observadas as atividades acadêmicas desenvolvidas pelos alunos.

CAPÍTULO IX

DA GESTÃO DE OPERAÇÕES E DAS COMUNICAÇÕES

Art. 33 - A FTSIC 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 IFG. Os acordos de nível de serviço devem ser compatíveis com padrões de mercado e requisitos de segurança.

CAPÍTULO X

DO CONTROLE DE ACESSO AOS SERVIÇOS

Art. 34 – Todo usuário dos serviços de informática e comunicações deverá ser autenticado em uma base única.

Art. 35 – Todo acesso à informação deve ser registrado para efeito de auditoria.

Art. 36 – A DTI deve criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 37 – Os usuários do IFG são responsáveis por todos os atos praticados com suas identificações, tais como: nome de usuário/senha, crachá, carimbo, correio eletrônico e assinatura digital.

Art. 38 – 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.

Parágrafo único – A transferência do recurso de identificação constitui violação desta PoSIC.

Art. 39 – A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário.

Parágrafo único - Qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação.

Art. 40 – Todos os sistemas de informação do IFG, automatizados ou não, devem ter um gestor, formalmente designado pelo Reitor, que deve definir os privilégios de acesso às informações.

Art. 41 – Sempre que houver mudança nas atribuições de determinado usuário, o seu perfil de acesso às informações e aos recursos computacionais deve ser adequado imediatamente, devendo ser cancelados em caso de desligamento do IFG.

Parágrafo único – O responsável pela operacionalização da mudança de perfil deverá comunicá-la ao gestor do sistema de informação.

Art. 42 – O IFG deve 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. 43 – O IFG deve possuir mecanismos para:

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

II - bloquear as contas de acesso do servidor a funcionalidades dos sistemas, exceto conta de e-mail, nos casos de licença, afastamento e cessão; e

III - tratar os casos de remoção e redistribuição do servidor.

Art. 44 – É responsabilidade do gestor do Sistema Integrado de Administração de Recursos Humanos (SIAPE) disponibilizar os registros de todas as movimentações de pessoal ocorridas.

CAPÍTULO XI

DA CRIPTOGRAFIA

Art. 45 – Recursos criptográficos deverão ser utilizados sempre que as informações em trânsito ou armazenadas assim o requererem, em conformidade com orientações contidas em norma específica.

Parágrafo Único - A implementação dos recursos descritos ficará a cargo da DTI.

Art. 46 – O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Responsabilidade pelo seu uso.

CAPÍTULO XII

DA AQUISIÇÃO, DO DESENVOLVIMENTO E DA MANUTENÇÃO DE SISTEMAS

Art. 47 – A FTSIC deve estabelecer, em norma específica, 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. 48 – O processo de aquisição de sistemas e aplicações corporativas deve atender requisitos de segurança previstos em norma específica.

CAPÍTULO XIII

DO TRATAMENTO DE INCIDENTES

Art. 49 – O CGSIC-IFG deverá constituir a ETIR.

Parágrafo Único – A ETIR deverá possuir um regimento interno próprio e que deverá ser referendado pelo CGSIC-IFG.

Art. 50 – A FTSIC deve instituir metodologias ou normas que estabeleçam processos de gestão para tratamento e resposta a incidentes de segurança, de forma a observar o disposto no arcabouço técnico normativo do Centro de Tratamento de Incidentes de Segurança de Redes de Computador da Administração Pública Federal (CTIR Gov).

CAPÍTULO XIV

CONFORMIDADE

Art. 51 – Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de SIC do IFG com esta PoSIC e suas normas e procedimentos complementares, bem como com a legislação específica de SIC.

Art. 52 – A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados pelo IFG.

Art. 53 – A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pelo CGSIC-IFG.

Art. 54 – O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos percebidos pela FTSIC.

Art. 55 – Nenhuma unidade administrativa poderá permanecer sem verificação de conformidade de suas práticas de SIC por período superior a 2 (dois) anos.

Art. 56 – 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. 57 – Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado ao Gestor da unidade administrativa verificada, para ciência e tomada das ações cabíveis.

CAPÍTULO XV

PLANO DE INVESTIMENTO EM SIC

Art. 58 – Os investimentos em SIC serão realizados de forma planejada e consolidados em um plano de investimentos, respeitado o planejamento orçamentário do IFG.

Art. 59 – 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 e que será submetido ao CGTI.

CAPÍTULO XVI

PROPRIEDADE INTELECTUAL

Art. 60 – Na condição de propriedade intelectual, protegida por lei, nenhum aplicativo poderá ser utilizado no IFG sem a devida aquisição da licença de uso.

Parágrafo único – A gestão das licenças de uso dos aplicativos será de responsabilidade do gestor de tecnologia da informação (TI) de cada unidade.

CAPÍTULO XVII

CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES

Art. 61 – Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta PoSIC.

Art. 62 – O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta PoSIC e suas normas complementares aos seus empregados e prepostos envolvidos em atividades no IFG.

Art. 63 – 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. 64 – Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

CAPÍTULO XVIII

GESTÃO DE MUDANÇAS

Art. 65 – Deve ser definido um processo adequado/objetivo de gestão de mudanças, que será detalhado em norma específica.

CAPÍTULO XIX

GESTÃO DE DESCARTE

Art. 66 – Nenhuma mídia armazenadora de dados deve ser descartada sem o devido tratamento, objetivando a segurança das informações nela contidas.

Parágrafo único – Entende-se por mídia qualquer dispositivo físico capaz de armazenar dados, a exemplo de mídias magnéticas, ópticas, eletrônicas e papel.

Art. 67 – Caberá ao custodiante da informação, em função da criticidade da informação, decidir pela destruição física da mídia ou por seu reaproveitamento.

CAPÍTULO XX

PENALIDADES

Art. 68 – Ações que violem esta PoSIC ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SIC serão devidamente apuradas e aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor.

CAPÍTULO XXI

COMPETÊNCIAS E RESPONSABILIDADES

Art. 69 – Cabe ao CGSIC-IFG:

I - Desenvolver a cultura de segurança da informação e das comunicações na Instituição;

II – Coordenar as ações de segurança da informação e das comunicações;

III – Propor, aprovar e publicar normas e procedimentos complementares à PoSIC;

IV – Dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PoSIC;

V – Avaliar criticamente a PoSIC, visando a sua aderência aos objetivos institucionais do IFG e à legislação vigente, e propor sua revisão, quando necessário;

VI – Eleger, dentre seus membros, o Gestor de Segurança da Informação e das Comunicações;

VII – Elaborar e aprovar seu Regimento Interno e modificá-lo, quando julgar necessário;

VIII – Instituir e implementar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), supervisionar suas ações e referendar o seu Regimento Interno;

IX – Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e das comunicações;

X – Constituir grupo de trabalho para realizar auditoria de segurança da informação e das comunicações;

XI – Receber e consolidar os resultados dos trabalhos de auditoria de segurança da informação e das comunicações e remetê-los à Reitoria;

XII – Responder às demandas dos órgãos de controle quando referentes à segurança da informação e das comunicações no IFG;

XIII – Realizar e/ou acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e das comunicações;

XIV – Elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação e das comunicações;

XV – Propor ao CGTI o Plano de Investimentos em Segurança da Informação e das Comunicações do IFG;

XVI – Desenvolver o Plano de Continuidade de Negócios para o IFG, dentro de sua área de competência;

XVII – Assessorar a Reitoria nos assuntos relativos à segurança da informação e das comunicações.

Art. 70 – 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 IFG;

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;

IX - Participar em fóruns, redes nacionais e internacionais relativos à SIC;

X – Aprovar o seu regimento interno.

Art. 71 – Cabe ao Gestor do Ativo de Informação:

I - Promover 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;

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

Art. 72 – Cabe ao custodiante do ativo de informação proteger e manter as informações, bem como controlar o acesso de execução/alteração, de acordo com os requisitos definidos pelo gestor da informação e em conformidade com esta PoSIC.

Parágrafo único – O acesso de leitura às informações obedecerá ao disposto na Lei de Acesso à Informação Pública (Lei nº 12.527/2012).

Art. 73 – Cabe ao titular da unidade administrativa:

I - Corresponsabilizar-se pelas ações realizadas por aqueles que estão sob sua subordinação;

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

III - Incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;

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

V - Realizar o tratamento e a identificação 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. 74 – 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;

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

Art. 75 – 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;

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

CAPÍTULO XXII

ATUALIZAÇÃO

Art. 76 – Esta PoSIC, bem como os documentos gerados a partir dela, deverão ser revisados anualmente, ou por deliberação do CGSIC.

ANEXO I

SIGLAS

(por ordem de citação)

1- PoSIC – Política de Segurança da Informação e das Comunicações.

2 - IFG – Instituto Federal de Educação, Ciência e Tecnologia de Goiás.

3 - SIC – Segurança da Informação e das Comunicações.

4 - DISC/GSI/PR – Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República.

5 - CGTI – Comitê Gestor de Tecnologia da Informação.

6 - CGSIC – Comitê Gestor de Segurança da Informação e das Comunicações.

7 - DTI – Diretoria de Tecnologia da Informação.

8 - ETIR – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

9 - FTSIC – Força-Tarefa de Segurança da Informação e das Comunicações.

10 - GRSIC – Gestão de Riscos de Segurança da Informação e Comunicações.

11 - SIAPE – Sistema Integrado de Administração de Recursos Humanos.

12 - CTIR Gov – Centro de Tratamento de Incidentes de Segurança de Redes de Computador da Administração Pública Federal.

13 - TI – Tecnologia da Informação.

ANEXO II

TERMOS E DEFINIÇÕES

(por ordem alfabética)

1 Autenticidade: princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação.

2 Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Instituição [ISO/IEC 13335-1:2004].

3 Análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco.

4 Avaliação de riscos: processo onde se compara o risco estimado com critérios de riscos predefinidos para determinar a importância do risco.

5 Ativo de informação: qualquer informação que tenha valor para a Instituição [ISO/IEC 13335-1:2004].

6 Ciência: Todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço devem ter ciência das normas, procedimentos, orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança.

7 Comunicação informal: tráfego de documentos, informações ou formulários que não estejam incluídos no conceito de que trata o ponto anterior, emitidos via caixas postais eletrônicas individuais de autoridade, servidor, estagiário ou fornecedor de bens e/ou serviços.

8 Comunicação oficial: tráfego de documentos, informações ou formulários emitidos por caixas postais eletrônicas do IFG, de atividades especiais ou ainda de projetos específicos.

9 Confidencialidade: somente pessoas devidamente autorizadas pelo gestor da informação devem ter acesso à informação não pública.

10 Contingência: indisponibilidade ou perda de integridade da informação que os controles de segurança não tenham conseguido evitar.

11 Continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável e previamente definido.

12 Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Controle também é usado como sinônimo para proteção ou contramedida.

13 Criticidade: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição.

14 Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado.

15 Ética: Todos os direitos e interesses legítimos de servidores, colaboradores, estagiários, prestadores de serviço e usuários do sistema de Informação do IFG devem ser respeitados.

16 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 pra a segurança da informação [ISO/IEC TR 18044:2004].

17 Gestão da continuidade de negócios: processo contínuo de gestão e governança suportado pela alta direção com recursos apropriados para garantir que as ações necessárias sejam executadas de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento dos serviços.

18 Gestão de riscos de Segurança da Informação e Comunicações: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para mitigar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

19 Gestor: agente da Instituição responsável pela definição de critérios de acesso, classificação, tempo de vida e normas específicas do uso da informação.

20 Identificação de riscos: processo para localizar, listar e caracterizar elementos do risco.

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

22 Integridade: somente operações de alteração, supressão e adição autorizadas pelo IFG devem ser realizadas nas informações.

23 Legalidade: além de observar os interesses do IFG, as ações de Segurança da Informação e Comunicações levarão em consideração leis, normas, políticas

organizacionais, administrativas, técnicas e operacionais, padrões, procedimentos aplicáveis e contratos com terceiros, dando atenção à propriedade da informação e direitos de uso.

24 Não-Repúdio: garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação.

25 Plano de Continuidade: É constituído de um conjunto de medidas, regras e procedimentos definidos, que serão adotados para assegurar que as funções ou atividades críticas da Instituição possam ser mantidas ou recuperadas após falha ou interrupção na operação normal dos sistemas direta ou indiretamente envolvidos com a gestão das informações.

26 Plano de continuidade de negócios: conjunto de procedimentos que devem ser adotados quando a Instituição deparar-se com problemas que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

27 Plano de gerenciamento de incidentes: plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente e que explicite as pessoas, recursos, serviços e outras ações que forem necessárias para implementar o processo de gerenciamento de incidentes.

28 Proporcionalidade: O nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações no IFG serão adequados ao entendimento administrativo e ao valor do ativo a proteger.

29 Quebra de segurança:- ação ou omissão, intencional ou acidental, que resulta no comprometimento da Segurança da Informação e das Comunicações.

30 Recursos de processamento da informação: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem.

31 Responsabilidade: As responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas. Todos os servidores do IFG são responsáveis pelo tratamento da informação e pelo cumprimento das Normas de Segurança da Informação e Comunicações advindas desta política.

32 Risco: combinação da probabilidade de ocorrência de um evento e de suas consequências.

33 Segurança da informação: preservação da confidencialidade, da integridade e da disponibilidade da informação, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidos.

34 Termo de responsabilidade: acordo de confidencialidade e não divulgação de informações que atribui responsabilidades ao servidor e administrador de serviço quanto ao sigilo e a correta utilização dos ativos de propriedade ou custodiados da Instituição. Prestadores de serviços que, por força de contratos de suporte e manutenção de sistemas, ficam sujeitos às mesmas condições.

35 Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

36 Tratamento dos riscos: processo e implementação de ações de Segurança da Informação e Comunicações para evitar, reduzir, reter ou transferir um risco.

37 Usuário externo: qualquer pessoa física ou jurídica que faça uso de informações e que não esteja vinculada administrativamente ao IFG.

38 Usuário interno: qualquer pessoa física ou unidade interna que faça uso de informações e que esteja vinculada administrativamente ao IFG.

39 Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

ANEXO III

FUNDAMENTAÇÕES LEGAIS E NORMATIVAS

As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicações do IFG são:

1 Constituição Federal de 1988, reformada em 2008.
1.1 Art. 5º Incisos X e XIV. Sigilo das informações relacionadas à intimidade ou à vida privada.
1.2 Art. 5º, inciso XII. Sigilo dos dados telemáticos e das comunicações privadas.
1.3 Art. 5º, inciso XXXIII e Art. 37, § 3º, inciso II. Disponibilidade das informações constantes nos órgãos públicos.
1.4 Art. 5º, inciso XXXIV. Disponibilidade das informações constantes nos órgãos públicos.
1.5 Constituição Federal.
1.6 Art. 23, incisos III e IV. Proteção da integridade, da autenticidade e da disponibilidade das informações pelo Estado.
1.7 Art. 216, § 2º. Proteção da integridade, da autenticidade, da disponibilidade e do sigilo das informações constantes nos órgãos e entidades integrantes da Administração Pública.
1.8 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.
1.9 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.
1.10 Art. 37, § 7º. Necessidade de regulamentação do acesso a informações privilegiadas.
2 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).
3 Decreto nº 1.171/1994 (Código de Ética do Servidor Público):
3.1 alínea "h" do inciso XV da Seção II. Proteção da integridade das informações públicas.
3.2 alínea "I" do inciso XV da Seção II. Proteção da disponibilidade das informações públicas.
3.3 inciso X da Seção I. Proteção da disponibilidade das informações públicas.

3.4 inciso VII da Seção I. Proteção da disponibilidade das informações públicas e garantia da publicidade das informações de interesse da coletividade

3.5 inciso IX da Seção I. Proteção da integridade do patrimônio público, a exemplo de equipamentos, materiais, áreas e instalações.

3.6 alínea "e" do inciso XIV da Seção II. Disponibilidade das comunicações.

4 Código de Propriedade Industrial, Art. 75. Sigilo das patentes de interesse da defesa nacional.

5 Código de Defesa do Consumidor, Arts. 43 e 44. Garantia da integridade e disponibilidade das informações dos consumidores arquivadas em bancos de dados.

6 Código Penal:

6.1 Art. 151. Proteção do sigilo, integridade e disponibilidade das informações de caráter pessoal veiculadas através dos meios de comunicação.

6.2 Art. 152. Proteção do sigilo e da disponibilidade das informações dos estabelecimentos comerciais.

6.3 Art. 153. Proteção do sigilo das informações classificadas constantes nos sistemas ou bancos de dados da Administração Pública.

6.4 Art. 154. Proteção do sigilo das informações conhecidas em razão de função, ministério, ofício ou profissão.

6.5 Art. 184, § 3º. Proteção da autenticidade.

6.6 Art. 297. Proteção da integridade e autenticidade dos documentos públicos.

6.7 Art. 298. Proteção da integridade e autenticidade dos documentos particulares.

6.8 Art. 305. Proteção da disponibilidade e integridade das informações constantes nos órgãos e entidades públicos.

6.9 Art. 307. Proteção da autenticidade.

6.10 Art. 313-A. Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.

6.11 Art. 313-B. Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.

6.12 Art. 314. Proteção da disponibilidade das informações constantes nos órgãos e entidades públicos;

6.13 Art. 325. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

7 Código Processo Penal:

7.1 Art. 20. Proteção de informações sigilosas.

7.2 Art. 207. Proteção do sigilo profissional.

7.3 Art. 745. Proteção de informações sigilosas relacionadas ao condenado.

8 Código Tributário Nacional, Art. 198. Proteção do sigilo fiscal.

9 Código de Processo Civil, Art. 347, inciso II c/c Art. 363, inciso IV. Proteção da privacidade de seus clientes.

10 Código de Processo Civil, Art. 406, inciso II c/c Art. 414, §2º. Proteção da privacidade de seus clientes.

11 Instrução Normativa nº 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.

12 Lei nº 6.538/1978, Art. 41. Proteção da privacidade de correspondência.

13 Lei nº 7.170/1983, Art. 13. Proteção das informações sigilosas relacionadas à segurança nacional.

14 Lei nº 7.232/1984, Art. 2º, inciso VIII. Sigilo dos dados relacionados à intimidade, vida privada e honra, especialmente dos dados armazenados através de recursos informáticos.

15 Lei nº 7.492/1986, Art. 18. Proteção das informações sigilosas no âmbito das instituições financeiras ou integrantes do sistema de distribuição de títulos mobiliários.

16 Lei nº 8.027/1990, artigo 5º, inciso I. Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública e parágrafo único, inciso V, proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

17 Lei nº 8.112/1990, Art. 116, inciso VIII. Sigilo das informações produzidas ou conhecidas no exercício de cargo ou função pública e inciso IX, proteção das informações sigilosas acessadas no exercício de cargo ou função pública.

18 Lei nº 8.137/1990, Art. 3º, inciso I. Proteção da disponibilidade de informações para manutenção da ordem tributária.

19 Lei nº 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.

20 Lei nº 8.429/1992, Art. 13. Disponibilidade de informações pessoais do agente público para o Poder Público e veracidade dos dados.

21 Lei nº 8.443/1992, Art. 86, inciso IV. Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.

22 Lei Complementar nº 75/1993, Art. 8º incisos II e VIII, §§ 1º e 2º. Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.

23 Lei nº 8.625/1993, Art. 26, inciso I, alínea "b" e inciso II. Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.

24 Lei nº 8.906/1994, Art. 7º, inciso XIX. Proteção da privacidade do cliente do advogado.

25 Lei nº 9.100/1995, Art. 67, incisos VII e VIII. Proteção da integridade e autenticidade dos sistemas informatizados e das informações neles armazenadas.

26 Lei nº 9.279/1996, Art. 195, inciso XI. Proteção da privacidade das pessoas jurídicas, relacionado ao sigilo de suas informações.

27 Lei nº 9.296/1996, Art. 10. Sigilo dos dados e das comunicações privadas.

28 Lei nº 9.472/1997, Art. 3º, inciso V. Sigilo das comunicações.

29 Lei nº 9.472/1997, Art. 3º, inciso VI. Proteção de informações pessoais de caráter sigiloso.

30 Lei nº 9.472/1997, Art. 3º, inciso IX. Proteção de informações pessoais de caráter sigiloso.

31 Lei nº 9.504/1997, Art. 72. Proteção da integridade das informações de caráter eleitoral e dos equipamentos.

32 Lei nº 9.605/1998, Art. 62. Disponibilidade e integridade de dados e informações.

33 Lei nº 10.683/2003, Art. 6º. Todos os aspectos da segurança da informação.

34 Lei nº 10.703/2003, Arts. 1º, 2º e 3º. Disponibilidade de dados cadastrais para fins de investigação criminal e sigilo nas demais hipóteses.

35 Decreto nº 4.801/2003, Art. 1º, inciso X. Todos os aspectos da segurança da informação.

36 Decreto nº 5.483/2005, Arts. 3º e 11. Disponibilidade de informações pessoais do agente público para o Poder Público e dever de sigilo por parte da Controladoria-Geral da União.

37 Decreto nº 5.687/2006, Arts. 10 e 13 do Anexo. Disponibilidade das informações públicas ou administrativas e sigilo das informações pessoais constantes nos registros públicos.

38 Decreto nº 6.029/2007, inciso II do Art. 1º. Disponibilidade das informações constantes nos registros públicos.

39 Decreto nº 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.

40 Decreto nº 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.

41 Decreto nº 6.029/2007, Art. 22. Disponibilidade, integridade e autenticidade das informações constantes no banco de dados mantido pela Comissão de Ética Pública.

42 Lei nº 7.232/1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências.

43 Lei nº 8.248/1991. Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.

44 Lei nº 9.296/1996. Regulamenta o inciso XII, parte final, do Art. 5º da Constituição Federal que dispõe sobre a violação do sigilo de dados e das comunicações telefônicas.

45 Lei nº 9.472/1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais.

46 Lei nº 9.507/1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data.

47 Lei nº 9.609/1998. Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.

48 Lei nº 9.883/1999 Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN e dá outras providências.

49 Lei nº 8.159/1991. Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências.

50 Lei Complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

51 Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

52 Lei nº 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.

53 Lei nº 11.111, de 05 de maio de 2005. Regula o direito à informação e ao acesso aos registros públicos.

54 Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências.

55 Decreto nº 2.295, de 04 de agosto de 1997. Regulamenta o disposto no Art. 24, inciso IX, da Lei nº 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.

56 Decreto nº 2.556, de 20 de abril de 1998. Regulamenta o registro previsto no Art. 3º da Lei nº 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.

57 Decreto nº 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.

58 Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

59 Decreto s/nº, de 18 de outubro de 2000. Cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, e dá outras providências.

60 Decreto nº 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 nº 2.954, de 29 de janeiro de 1999, e dá outras providências.

61 Decreto nº 3.996, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

62 Decreto nº 4.073, de 03 de janeiro de 2002. Regulamenta a Lei nº 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.

63 Decreto nº 4.376, de 13 de setembro de 2002. Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, e dá outras providências.

64 Decreto nº 4.522, de 17 de dezembro de 2002. Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências.

65 Decreto nº 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.

66 Decreto nº 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.

67 Decreto nº 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.

68 Lei nº 9.983, de 14 de julho de 2000. Altera o Decreto Lei nº 2848/40 – Código Penal - tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

69 Decreto nº 1.171, de 24 de junho de 1994. Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências;

70 Lei nº 3.689, de 03 de outubro de 1941, atualizado até as alterações introduzidas pela Lei nº 11.900, de 08 de janeiro de 2009;

71 Lei nº 5.869, de 11 de janeiro de 1973;

72 Lei nº 7.232, de 29 de Outubro de 1984. Política Nacional de Informática, e dá outras providências;

73 Lei nº 8.027, de 12 de abril de 1990. Normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências;

74 Lei nº 8.112, de 11 de dezembro de 1990. Regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

75 Lei nº 8.429, de 2 de junho de 1992. Sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências;

76 Decreto nº 6.029, de 1º de fevereiro de 2007. Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências;

77 Lei nº 8.159, de 8 de janeiro de 1991. Política nacional de arquivos públicos e privados e dá outras providências;

78 Decreto nº 1.048, de 21 de janeiro de 1994. Sistema de Administração dos Recursos de Informação e Informática, da Administração Pública Federal, e dá outras providências;

79 Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

80 Decreto nº 4.553, de 27 de dezembro de 2002, que 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;

81 Normas e Resoluções do Gabinete de Segurança Institucional da Presidência da Republica:

81.1 Instrução Normativa GSI nº 01, de 13 de Junho de 2008;

81.2 Norma Complementar nº 02/IN01/DSIC/GSIPR, de 14 de outubro de 2008;

81.3 Norma Complementar nº 03/IN01/DSIC/GSIPR, de 03 de julho de 2009;

81.4 Norma Complementar nº 04/IN01/DSIC/GSIPR, de 17 de agosto de 2009;

81.5 Norma Complementar nº 05/IN01/DSIC/GSIPR, de 17 de agosto de 2009;

81.6 Norma Complementar nº 06/IN01/DSIC/GSIPR , de 23 de novembro de 2009;

82 Acórdão nº. 1603/2008, do Plenário do Tribunal de Contas da União – TCU;

83 ABNT NBR ISO 17799: 2005 - Código de Práticas para a Gestão da Segurança da Informação;

84 ABNT NBR ISO Guia 73: 2002 - Gestão de Riscos / Vocabulário;

85 ABNT NBR ISO/IEC 27001:2005 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gerência da Segurança da Informação – Requisitos;

86 ABNT NBR ISO/IEC 27002:2005 – Código de Prática para a Gestão de Segurança da Informação;

87 ISO/IEC TR 13335-3: 1998 - 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;

88 ISO/IEC GUIDE 51: 1999 - Fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos.

Goiânia, 26 de março de 2013

PAULO CÉSAR PEREIRA
Reitor