

Matriz de Gerenciamento de Riscos

1. Informações Básicas

Número da Matriz de Alocação de Riscos
9/2024

Responsável pela Edição
JULIANA VIEIRA DE LIMA

Data de Criação
11/04/2024 08:58

Objeto da Matriz de Riscos
AQUISIÇÃO DE SOFTWARES

2. Histórico de Revisões

Nenhuma Revisão encontrada.

3. Riscos Identificados

Número	Risco	Causa do Risco	Fase	Alocado para	Nível do Risco (I x P)	Nº Item
R-01	Impugnações	Impugnações ao edital ou ao processo licitatório podem paralisar o trâmite do planejamento da contratação.	Seleção do Fornecedor	Administração	Alto	
Impactos						
1	Paralisação do processo licitatório.					
Ações Preventivas						
P-01	Validação das Especificações Técnicas			Responsável: BENONI DE OLIVEIRA PIRES		
P-02	Consulta a processos de contratações correlatas finalizadas com sucesso.			Responsável: JAMES HILTON BECKER		
Ações de Contingência						
C-01	Resposta fundamentada à impugnação no prazo estipulado.			Responsável: JAMES HILTON BECKER		
Número	Risco	Causa do Risco	Fase	Alocado para	Nível do Risco (I x P)	Nº Item
R-02	Ausência de recursos orçamentários ou financeiros.	Indisponibilidade de recursos orçamentários ou financeiros para a execução da contratação.	Gestão de Contrato	Administração	Alto	
Impactos						
1	Prejuízo às atividades de ensino, pesquisa, extensão e gestão.					
Ações Preventivas						
P-01	Certificar-se da dotação orçamentária no planejamento da contratação			Responsável: BENONI DE OLIVEIRA PIRES		
Ações de Contingência						
C-01	Fomentar junto ao ordenador de despesas alternativas de orçamento .			Responsável: BENONI DE OLIVEIRA PIRES		
Número	Risco	Causa do Risco	Fase	Alocado para	Nível do Risco (I x P)	Nº Item
R-03	Volumetria da contratação incompatível com a realidade do órgão.	Utilização de critérios não condizentes com a realidade do órgão para elaboração da análise de custo total de propriedade (TCO), levando a um subdimensionamento ou superdimensionamento do quantitativo do objeto licitado.	Planejamento	Administração	Médio	
Impactos						
1	Não atendimento as demandas apresentadas pelos câmpus para o desenvolvimento do ensino, pesquisa e extensão.					
Ações Preventivas						
P-01	Realizar levantamento de estimativas de acordo com a necessidade mais urgente.			Responsável: BENONI DE OLIVEIRA PIRES		
Ações de Contingência						
C-01	Utilizar ferramenta alternativas compatíveis com as demandas apresentadas.			Responsável: BENONI DE OLIVEIRA PIRES		
Número	Risco	Causa do Risco	Fase	Alocado para	Nível do Risco (I x P)	Nº Item
R-04	Especificação imprecisa da solução.	Especificação de softwares que não contemplem a totalidade da necessidade apresentada devido as opções disponíveis no mercado.	Planejamento	Administração	Médio	
Impactos						
1	Não atendimento as demandas apresentadas pelos câmpus para o desenvolvimento do ensino, pesquisa e extensão.					
Ações Preventivas						
P-01	Elaborar as especificações técnicas a partir de modelos de licitações nacionais e com base nas tecnologias atuais de mercado.			Responsável: BENONI DE OLIVEIRA PIRES		

Ações de Contingência						
C-01	Revisão das especificações elaboradas.			Responsável: BENONI DE OLIVEIRA PIRES		
Número	Risco	Causa do Risco	Fase	Alocado para	Nível do Risco (I x P)	Nº Item
R-05	Licitação Frustrada	Em caso das propostas apresentadas consignarem preços manifestamente superiores aos praticados no mercado nacional ou incompatíveis com os fixados pelos órgãos oficiais competentes, ou critérios de habilitação incompatíveis com as necessidades do serviço e com o mercado.	Planejamento	Administração	Médio	
Impactos						
1	Não atendimento as demandas apresentadas pelos câmpus para o desenvolvimento do ensino, pesquisa e extensão.					
Ações Preventivas						
P-01	Especificações Técnicas bem elaboradas, de modo a estimular a competitividade.			Responsável: BENONI DE OLIVEIRA PIRES		
P-02	Validação das especificações em comparação às características usuais de mercado.			Responsável: BENONI DE OLIVEIRA PIRES		
P-03	Consulta aos fornecedores e elaboração de formação de preços, compatível aos praticados no mercado.			Responsável: BENONI DE OLIVEIRA PIRES		
P-04	Consulta a outras compras públicas do mesmo objeto para definições dos serviços, valores e critérios de julgamento e habilitação.			Responsável: BENONI DE OLIVEIRA PIRES		
Ações de Contingência						
C-01	Revisar o termo de referência.			Responsável: BENONI DE OLIVEIRA PIRES		
C-02	Revisão do Estudo Técnico Preliminar.			Responsável: BENONI DE OLIVEIRA PIRES		

Número	Risco	Causa do Risco	Fase	Alocado para	Nível do Risco (I x P)	Nº Item
R-06	Ataques cibernéticos através de software/SO	Pacotes de softwares desatualizados.	Planejamento	Administração	Alto	
Impactos						
1	Furto de dados e/ou ações que danifiquem sistemas e soluções de TI em geral.					
Ações Preventivas						
P-01	Atualização/substituição de softwares desatualizados (SOs)			Responsável: KARI DE SOUZA SOARES		
Ações de Contingência						
C-01	Implantar as versões mais atualizadas de sistemas legados.			Responsável: KARI DE SOUZA SOARES		
C-02	Suspender o uso de sistemas sem suporte ou substituir por sistemas equivalentes (SO)			Responsável: KARI DE SOUZA SOARES		

4. Acompanhamento das Ações de Tratamento de Riscos

Nenhum acompanhamento incluído.

5. Responsáveis / Assinantes

Equipe de Planejamento

KARI DE SOUZA SOARES
Membro da comissão de contratação

EDERSON DANTAS DE ALMEIDA
Membro da comissão de contratação

JULIANA VIEIRA DE LIMA

Equipe de apoio

BENONI DE OLIVEIRA PIRES

Autoridade competente

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Política_Segurança_Informação_Resoluo_08_Deز_2022assinado.pdf (842.02 KB)

**Anexo I -
Política_Segurança_Informação_Resoluo_08_Dez_2022
pdf**



**RESOLUÇÃO Nº 08, DE 05 DE DEZEMBRO DE 2022,
DO COMITÊ DE GOVERNANÇA DIGITAL**

Dispõe sobre a Política de Segurança da Informação do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

O PRESIDENTE DO COMITÊ DE GOVERNANÇA DIGITAL DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, no uso das atribuições que lhe foram conferidas pelo Art. 6º, inciso IV e Art. 9º, deste comitê.

RESOLVE:

Art. 1º Aprovar a Política de Segurança de Informação do IFSC.

Art. 2º Esta Resolução entra em vigor na data de 22 de dezembro de 2022.



Documento assinado digitalmente

JESUE GRACILIANO DA SILVA

Data: 15/12/2022 12:05:46-0300

CPF: 110.559.078-07

Verifique as assinaturas em <https://v.ifsc.edu.br>

Jesué Graciliano da Silva

Presidente do Comitê de Governança Digital

Súmula da reunião do CGD disponível em:

<https://sigrh.ifsc.edu.br/sigrh/downloadArquivo?idArquivo=2500594&key=6430c6f12ae57875d1fa0fd3c95d2da6>

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



**INSTITUTO
FEDERAL**
Santa Catarina



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

COMITÊ DE GOVERNANÇA DIGITAL

Presidência

Jesué Graciliano da Silva – Pró-reitor de Desenvolvimento Institucional

Secretário-Executivo

Benoni de Oliveira Pires – Diretor de TIC

Membros do CGD

Titulares

Aloísio Silva Júnior – Pró-reitora de Administração

Adriano Larentes da Silva – Pró-reitor de Ensino

Valter Vander de Oliveira – Pró-reitor de Extensão e Relações Externas

Flávia Maia Moreira – Pró-reitor de Pesquisa, Pós-Graduação Inovação

Tiago Semprebom – Colégio de Dirigentes (São José)

Daniel Fernando Carossi – Colégio de Dirigentes (São Lourenço do Oeste)

Volnei Velleda Rodrigues – Encarregado do Tratamento dos Dados Pessoais

Suplentes

Eliana Cristina Bar – Colégio de Dirigentes (Palhoça)

José Roberto Machado – Colégio de Dirigentes (Jaraguá do Sul)

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
10/2016	Versão 1.0	Documento final aprovado pelo Conselho Superior do IFSC através da RESOLUÇÃO CONSUP Nº 52, DE 24 DE OUTUBRO DE 2016.
06/2021	Versão 1.1	Alteração do “título” da política para Política de Segurança da Informação. Atendimento a INSTRUÇÃO NORMATIVA Nº 1, DE 27 DE MAIO DE 2020 Aprovação da Política de Segurança da Informação de acordo com a RESOLUÇÃO CONSUP Nº 09, DE 26 DE MARÇO DE 2021.
12/2022		Revogação da resolução 52/2016 pela resolução CONSUP Nº 61, DE 30 DE NOVEMBRO DE 2022 ;

CAPÍTULO I

DO ESCOPO, DOS PRINCÍPIOS E DA ABRANGÊNCIA

Art. 1º A Política de Segurança da Informação (PSI) está alinhada às estratégias do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina (IFSC), que objetiva garantir a autenticidade, a integridade, a confidencialidade e a disponibilidade das informações produzidas ou sob sua custódia.

Art. 2º A segurança da informação no IFSC abrange aspectos físicos, tecnológicos e humanos da organização e orienta-se pelos seguintes princípios:

- I. confidencialidade: garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal;
- II. disponibilidade: garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido;
- III. integridade: garante a não violação das informações, com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital; e
- IV. autenticidade: assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria.

Art. 3º A PSI provê diretrizes estratégicas, responsabilidades e apoio necessário para implementar a Gestão da Segurança da Informação - GSI, observando as disposições constitucionais, legais e regimentais vigentes.

Parágrafo único. Integram, também, essa Política, as normas gerais e específicas de segurança da informação, bem como os procedimentos complementares, destinados à proteção da informação e à disciplina de sua utilização.

Art. 4º A PSI aplica-se a todos aqueles que, direta ou indiretamente, possuem acesso às informações do IFSC.

Parágrafo único. Todos são responsáveis pela segurança da informação, pela segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas respectivas identificações.

Art. 5º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo IFSC devem atender esta PSI.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 6º Para efeitos desta PSI e das normas complementares e procedimentos operacionais de Segurança da Informação criados para o âmbito do IFSC, serão adotados os conceitos e definições descritos no Anexo I.

CAPÍTULO III

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 7º A PSI do IFSC observa a legislação e as demais normas específicas descritas no Anexo II.

CAPÍTULO IV

DA ESTRUTURA NORMATIVA

Art. 8º A PSI e as normas de segurança da informação devem ser divulgadas a toda comunidade do IFSC e dispostas de maneira que seus conteúdos possam ser consultados a qualquer momento.

Parágrafo único. Os procedimentos de segurança da informação devem ser cumpridos pelas áreas diretamente envolvidas na sua aplicação.

Art. 9º A estrutura normativa da Segurança da Informação do IFSC é composta por um conjunto de documentos interdependentes:

- I. Política de Segurança da Informação: define as diretrizes, as competências e as responsabilidades referentes à Segurança da Informação;
- II. Normas de Segurança da Informação: estabelecem os conceitos, detalhando os passos a serem executados, e as obrigações a serem observadas para o cumprimento da Política; e
- III. Planos de Segurança da Informação: instrumentalizam o disposto nas normas, permitindo sua direta aplicação no âmbito do IFSC.

CAPÍTULO V

DAS DIRETRIZES GERAIS

Art. 10. A segurança da informação tem como principal diretriz a proteção da informação, garantindo a continuidade do negócio, minimizando seus riscos, maximizando o retorno sobre os investimentos e as oportunidades pertinentes.

Art. 11. As diretrizes de segurança da informação devem considerar, prioritariamente, a missão, a visão, os valores, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do IFSC.

Art. 12. As diretrizes de segurança da informação descritas nesta PSI devem ser observadas por todos os usuários que executem atividades direta ou indiretamente relacionadas ao IFSC durante todas as etapas do tratamento da informação, a saber: produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Art. 13. O cumprimento desta PSI, bem como dos normativos que a complementam, deverá ser avaliado periodicamente por meio de verificações de conformidade, respeitando os requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Parágrafo único. O Comitê de Governança Digital deverá criar os mecanismos de avaliação da PSI.

Art. 14. O IFSC deve observar as diretrizes estabelecidas nesta PSI e deve se orientar pelas melhores práticas e procedimentos de segurança da informação e comunicação recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 15. A Diretoria de Gestão do Conhecimento deve criar, gerir e avaliar critérios de tratamento da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 16. É vedado comprometer a disponibilidade, a integridade, a confidencialidade e autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo IFSC.

Parágrafo único. As cópias de documentos classificados deverão sofrer o mesmo processo de classificação de seu original.

Art. 17. 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 do ativo de informação é o próprio custodiante.

Art. 18. Os contratos, convênios, acordos e instrumentos congêneres firmados pelo IFSC devem conter cláusulas que determinem a observância desta PSI e seus documentos complementares.

CAPÍTULO VI

DAS DIRETRIZES ESPECÍFICAS

Art. 19. Para cada uma das diretrizes constantes das seções deste capítulo deve ser observada a pertinência de elaboração de políticas, procedimentos, normas, orientações e/ou manuais que disciplinem ou facilitem o seu entendimento.

Seção I

DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 20. A Gestão da Segurança da Informação - GSI deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de segurança da informação e comunicação.

Art. 21. A GSI deve compreender ações e métodos que visem a estabelecer parâmetros adequados, relacionados à segurança da informação e comunicação, 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 IFSC.

Parágrafo único. De forma a promover a gestão e fomentar os aspectos de segurança da informação, o Comitê de Governança Digital deve:

- I. definir uma estrutura adequada para a GSI;

- II. instituir Equipe de Tratamento e Respostas a Incidentes Cibernéticos (CSIRT);
- III. criar e manter um portal eletrônico que contenha um repositório de leis, normas, procedimentos e outros artefatos que colaborem para a manutenção, a divulgação e a auditoria da segurança da informação, bem como instrumentos para capacitação dos usuários interessados.

Seção II

DA PROPRIEDADE DA INFORMAÇÃO

Art. 22. As informações geradas, adquiridas ou custodiadas sob a responsabilidade do IFSC são consideradas parte do seu patrimônio intelectual não cabendo a seus criadores qualquer forma de direito autoral, salvo aqueles direitos garantidos no âmbito da Lei de Inovação e outros dispositivos legais, e devem ser protegidas segundo as diretrizes descritas nesta PSI, em seus documentos complementares e demais regulamentações em vigor.

Art. 23. É vedada a utilização de informações produzidas por terceiros para uso exclusivo do IFSC em quaisquer outros projetos ou atividades de uso diverso ao originalmente estabelecido, salvo autorização específica emitida pelo gestor do ativo de informação, nos processos e documentos de sua competência, ou pelo Reitor, nos demais casos, observando a legislação em vigor.

Seção III

DOS CONTROLES DE ACESSO

Art. 24. Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.

Art. 25. Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 26. Todos os sistemas de informação do IFSC, automatizados ou não, devem ter um custodiante do ativo da informação, formalmente designado pelo gestor do ativo de informação, que deve definir os privilégios de acesso às informações, observando a legislação em vigor.

Art. 27. O usuário é responsável por todos os atos praticados com suas identificações, entre as quais se destacam: nome do usuário na rede, carimbo, crachá, endereço de correio eletrônico e assinatura digital.

§ 1º O usuário responderá pela segurança dos ativos; dos processos que estejam sob sua responsabilidade e por todos os atos executados com suas identificações, salvo se comprovado que o fato ocorreu sem o conhecimento ou consentimento do usuário.

§ 2º A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo o reconhecimento do usuário de maneira clara e irrefutável.

Art. 28. A autorização, o acesso e o uso da informação e dos recursos de tecnologia da informação e comunicação devem ser controlados e limitados ao necessário para o cumprimento das atividades de cada usuário.

§ 1º Qualquer outra forma de autorização, acesso ou uso necessitará de prévia autorização do gestor do ativo de informação, observando-se a legislação em vigor.

§ 2º A autorização de que trata o caput poderá ser delegada ao custodiante do ativo de informação.

Art. 29. Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, pelo gestor do ativo de informação ou sempre que for possível, de forma automatizada, devendo ser revogados em caso de desligamento do IFSC.

Seção IV

DA GESTÃO DE ATIVOS DA INFORMAÇÃO

Art. 30. As diretrizes quanto à gestão e mapeamento de ativos da informação, as responsabilidades e eventuais procedimentos devem ser disponibilizadas em normativas aprovadas pelo Comitê de Governança Digital e em conformidade com as diretrizes desta PSI.

Art. 31. Os recursos tecnológicos, os sistemas de informação e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 32. O acesso dos usuários aos ativos de informação e a sua utilização deve estar condicionado à assinatura do Termo de Responsabilidade, observando a legislação em vigor.

Seção V

DA GESTÃO DO USO DOS RECURSOS OPERACIONAIS E DE COMUNICAÇÕES

Art. 33. O uso da internet, e-mail corporativo e das redes sociais, no âmbito do IFSC, deve ser detalhado em normas específicas em conformidade com as diretrizes desta PSI.

Seção VI

DA GESTÃO ARQUIVÍSTICA DE DOCUMENTOS

Art. 34. Os documentos arquivísticos, independente da natureza de suporte ou formato, terão garantias de organicidade, unicidade, confiabilidade, autenticidade e acessibilidade, nos termos da lei.

Art. 35. Os documentos digitais, por suas especificidades, deverão ser criados de forma confiável e mantidos autênticos, preservados e acessíveis por todo o ciclo de vida, por meio de um sistema informatizado de gestão arquivística de documentos.

Seção VII

DA PRESERVAÇÃO DOS DOCUMENTOS ARQUIVÍSTICOS

Art. 36. O tratamento arquivístico – inclusive descarte – de documentos eletrônicos deve observar procedimentos definidos na legislação.

Parágrafo único. A gestão de documentos eletrônicos orienta-se pelos critérios da integridade e da disponibilidade das informações produzidas e custodiadas no âmbito do

IFSC, respeitados os requisitos legais e os princípios de segurança da informação e comunicação.

Art. 37. Os documentos constantes da base de dados corporativa devem ser armazenados em equipamentos e mídias que permitam acesso com celeridade compatível com as necessidades do negócio no âmbito do IFSC.

Art. 38. O Comitê de Governança Digital deverá aprovar a Política de Backup, Retenção e Restauração de Dados, a partir de proposta formulada pela Diretoria de Tecnologia da Informação e Comunicação (DTIC).

Parágrafo único. A Política de Backup, Retenção e Restauração de Dados deve conter, entre outros elementos, a política de cópias de segurança (backup) e de recuperação em casos de perda de informação, bem como de retenção de versões de documentos eletrônicos, definição de tabela de temporalidade para descarte e processos de eliminação de documentos que tenham sua utilidade superada.

Seção VIII

DA CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 39. As informações geradas, adquiridas ou custodiadas pelo IFSC deverão ser classificadas para indicar a necessidade, a prioridade e o nível esperado de proteção quanto ao seu tratamento e quando classificadas serão observadas as exigências das atividades da instituição, considerando as implicações que um determinado grau de classificação trará para os seus objetivos institucionais e observando a legislação em vigor.

§ 1º Todo usuário deve ser capaz de identificar a classificação atribuída a uma informação tratada pelo IFSC e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

§ 2º Não havendo norma específica, a classificação dos ativos de informação será realizada pelo próprio gestor do ativo.

Seção IX

DA GUARDA E TRAMITAÇÃO DE ATIVO DE INFORMAÇÃO CLASSIFICADA

Art. 40. Ativos de informação sob restrição de acesso devem ser armazenados em local que garanta sua acessibilidade apenas a usuário autorizado.

§ 1º Se o ativo estiver em meio físico, deverá ser armazenado em arquivo com proteção de acesso.

§ 2º Se o ativo estiver em meio eletrônico, deverá ser armazenado e movimentado de forma criptografada.

Seção X

DA SEGURANÇA FÍSICA E DO AMBIENTE

Art. 41. O Comitê de Governança Digital deve estabelecer mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências.

Parágrafo único. Os mecanismos de proteção estabelecidos devem estar alinhados aos riscos identificados.

Seção XI

DA SEGURANÇA EM RECURSOS HUMANOS

Art. 42. Todos os usuários devem ter ciência das ameaças e preocupações relativas à segurança da informação, bem como de suas responsabilidades e obrigações no âmbito desta PSI.

Art. 43. Todos os usuários devem difundir e exigir o cumprimento desta PSI, de seus documentos complementares, das normas de segurança e da legislação vigente acerca do tema.

Art. 44. O Comitê de Governança Digital deve estabelecer processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários do IFSC, de acordo com suas competências funcionais.

Seção XII

DA GESTÃO DE RISCOS

Art. 45. As áreas responsáveis por ativos de informação devem implantar processos contínuos de gestão de riscos, os quais serão aplicados na implementação e operação da gestão da segurança da informação.

Parágrafo único. A gestão de riscos de TI deve avaliar os riscos relativos à segurança dos ativos de informação e à conformidade com exigências regulatórias ou legais.

Seção XIII

DA CONTINUIDADE DE NEGÓCIO

Art. 46. O Comitê de Governança Digital deverá instituir e manter um plano de continuidade de negócio, para atender as necessidades da instituição.

§ 1º O plano de continuidade de negócio deve propor, manter e, periodicamente, testar medidas de gestão da continuidade e recuperação da informação, visando reduzir para um nível aceitável ou previamente definido a possibilidade de interrupção ou o impacto causado por desastres nos recursos de informação que suportam os processos vitais do IFSC, até que se retorne à normalidade.

§ 2º O plano de continuidade deve ter acesso restrito e ser controlado pelo Comitê de Governança Digital.

Seção XIV

DA GESTÃO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO

Art. 47. O Comitê de Governança Digital deverá instituir uma Equipe de Tratamento e Respostas a Incidentes Cibernéticos (CSIRT), em conformidade com normas e procedimentos específicos.

Seção XV

DA CRIPTOGRAFIA

Art. 48. O uso de recursos criptográficos interfere na disponibilidade, integridade, confidencialidade e autenticidade das informações, sendo, portanto, responsabilidade do gestor e/ou custodiante consultar o Comitê de Governança Digital sobre a possibilidade do uso e recursos disponíveis para a implantação da criptografia.

Seção XVI

DA AUDITORIA E CONFORMIDADE

Art. 49. A autorização, o acesso e o uso da informação e dos procedimentos de auditoria devem ser executados nos recursos de informação.

Art. 50. Deve ser realizada a verificação de conformidade das práticas de segurança da informação do IFSC com esta PSI, com suas normas e com seus procedimentos complementares, bem como com a legislação específica de segurança da informação.

Parágrafo único. Cabe ao gestor ou custodiante do ativo de informação, com periodicidade máxima de acordo com o inventário dos ativos de informações, avaliar a conformidade e remeter os resultados ao Comitê de Governança Digital.

Art. 51. A verificação de conformidade deve, também, ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o IFSC.

Art. 52. A verificação da conformidade ampla será realizada pelo Comitê de Governança Digital, de forma planejada, mediante calendário de ações aprovado.

Art. 53. O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos.

Art. 54. Nenhum órgão ou unidade, abrangidos por esta PSI, poderá permanecer sem verificação de conformidade de suas práticas de segurança da informação e comunicação por período superior a 3 (três) anos.

Art. 55. A execução da verificação de conformidade será realizada por grupo de trabalho formalmente instituído pelo Comitê de Governança Digital.

Parágrafo único. A unidade de Auditoria Interna do IFSC poderá realizar trabalhos independentes de avaliação da PSI em conformidade com seu planejamento anual, com prévia comunicação ao Comitê de Governança Digital.

Art. 56. É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

Art. 57. 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. 58. Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo gestor ou custodiante do ativo para Comitê de Governança Digital, para ciência e tomada das ações cabíveis.

Seção XVII

DO PLANO DE INVESTIMENTOS EM SEGURANÇA DA INFORMAÇÃO

Art. 59. Os investimentos em Segurança da Informação serão realizados de forma planejada e consolidados no Plano Diretor de Tecnologia da Informação (PDTI) e no Plano de Desenvolvimento Institucional (PDI).

Art. 60. Os investimentos serão planejados com base nas necessidades institucionais e considerando os riscos a serem tratados, a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco.

Seção XVIII

DA RELAÇÃO COM TERCEIROS

Art. 61. Nos editais de licitação, nos contratos, convênios, acordos e instrumentos congêneres de cooperação técnica com entidades prestadoras de serviços para o IFSC, deverá constar cláusula específica sobre a obrigatoriedade de observância a esta PSI, bem como deverá ser exigida, da entidade contratada, a assinatura do Termo de Responsabilidade.

Art. 62. No contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta PSI, bem como suas normas e procedimentos complementares aos seus empregados e prepostos envolvidos em atividades no IFSC.

CAPÍTULO VII

DAS SANÇÕES

Art. 63. A não observância desta PSI e/ou de seus documentos complementares, bem como a quebra de controles de segurança da informação, poderá acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Parágrafo único. As normas e procedimentos poderão detalhar sanções aplicáveis a incidentes previamente definidos, inclusive indicando a participação em curso de capacitação.

CAPÍTULO VIII

DAS COMPETÊNCIAS E DAS RESPONSABILIDADES

Seção I

DO COMITÊ DE GOVERNANÇA DIGITAL

Art. 64 As competências do Comitê de Governança Digital do IFSC estão descritas em regulamento próprio, a saber:

- I. Ser responsável pela governança e pelo alinhamento dos investimentos de Tecnologia da Informação e Comunicação com os objetivos estratégicos e apoio a priorização de projetos a serem atendidos.
- II. Aprovar políticas, normas e planos de Tecnologia da Informação e Comunicação;
- III. Aprovar políticas, normas e planos de Segurança da Informação;
- IV. Aprovar políticas, normas e planos relacionados aos dados abertos;
- V. Aprovar o Plano Estratégico de Tecnologia da Informação e Comunicação – PETIC e zelar pelo seu cumprimento;
- VI. Aprovar o Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC e zelar pelo seu cumprimento;
- VII. Analisar, supervisionar e priorizar, em conformidade com o PETIC e PDTIC, o planejamento anual de aquisições, contratações e serviços de Tecnologia da Informação e Comunicação;
- VIII. Promover a cultura de segurança da informação e comunicações;
- IX. Instituir e implementar a equipe de tratamento e resposta aos incidentes computacionais;
- X. Propor alterações em seu Regimento Interno.

DO COMITÊ TÉCNICO DE SEGURANÇA DA INFORMAÇÃO

Art. 65 As competências do Comitê de Técnico de Segurança da Informação estão descritas em regulamento próprio, a saber:

- I. Propor as políticas e normas gerais de segurança da informação;
- II. Tratar questões ligadas à segurança da informação e propor soluções específicas;
- III. Incentivar regulamentação das rotinas de segurança para uso e administração dos recursos da TIC, de forma a garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações;
- IV. Realizar e acompanhar estudos de novas tecnologias, quanto aos possíveis impactos na segurança da informação;
- V. Analisar e emitir parecer sobre as propostas encaminhadas ao comitê pela DTIC;
- VI. Subsidiar o Comitê de Governança Digital quando demandado.

Seção II

DOS USUÁRIOS

Art. 66. Compete aos usuários do IFSC:

- I. apropriar-se e cumprir fielmente as políticas, as normas, os procedimentos e as orientações de segurança da informação do IFSC;
- II. buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
- III. proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pelo IFSC;
- IV. assegurar que os recursos de informação que estejam à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo IFSC; e
- V. comunicar imediatamente ao Comitê de Governança Digital sobre qualquer descumprimento ou violação desta PSI e/ou de seus documentos complementares.

Art. 67. A partir do ingresso no IFSC, o usuário aceita esta PSI, sem a necessidade de assinatura de termos ou compromissos.

CAPÍTULO IX

DA APROVAÇÃO, DA VIGÊNCIA E DA ATUALIZAÇÃO

Art. 68. Esta PSI, bem como o conjunto de instrumentos normativos gerados a partir dela, serão revisados de forma periódica, conforme estrutura normativa, ou sempre que se fizer necessário, não excedendo o período máximo de 04 (quatro) anos.

ANEXO I - CONCEITOS E DEFINIÇÕES

I - Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

III - Análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco;

IV - Assinatura eletrônica: geração, por computador, de qualquer símbolo ou série de símbolos executados, adotados ou autorizados por um indivíduo para ser um laço, legalmente, equivalente à assinatura manual do indivíduo. A assinatura eletrônica está amparada pela LEI Nº 14.063, DE 23 DE SETEMBRO DE 2020 que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

V - Ativo: qualquer coisa que tenha valor para a organização;

VI - Ativo de informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio. Inclui meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VII - Ativo de informação classificada: ativo de informação com informação classificada;

VIII - Auditabilidade: atributo que garante a rastreabilidade dos diversos passos de um processo informatizado, identificando os participantes, ações e horários de cada etapa;

IX - Auditoria: atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais, com o intuito de verificar sua conformidade com os objetivos e políticas institucionais, orçamentos, regras normas e padrões;

X - Autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

XI - Avaliação de riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

XII – Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

XIII - 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 de informação das atividades críticas, de forma a manter suas operações em um nível aceitável previamente definido;

XIV - 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. NOTA: Controle é, também, usado como um sinônimo para proteção ou contramedida;

XV - Custodiante: entidade detentora da posse, mesmo que transitória, de informação produzida ou recebida pelo Instituto.

XVI - Desastre: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo da recuperação;

XVII - Disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

XVIII - Documento: unidade de registro de informações, qualquer que seja o formato ou suporte;

XIX - Documento de domínio público: documento ou obra (artística, invenção, desenho industrial, etc.) que pode ser livremente reproduzido, apresentado ou explorado sem necessidade de autorização ou de pagamento de direitos autorais, por esgotamento do prazo previsto em lei ou por outro motivo que tenha feito expirar a propriedade intelectual;

XX - Documento de natureza pública: documento relativo ou pertencente à coletividade, de uso comum a todos, universalmente, conhecido ou sem restrição de acesso a qualquer pessoa;

XXI - Evento de segurança da informação: uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação, previamente, desconhecida que possa ser relevante para a segurança da informação;

XXII - Gestão Arquivística de Documentos: conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento dos documentos em fase corrente e intermediária, visando sua eliminação ou recolhimento para guarda permanente.

XXIII - Gestão de riscos: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos.

XXIV - Gestão de segurança da informação: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade de negócios, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional dos processos institucionais estratégicos, operacionais e táticos, não se limitando portanto, à tecnologia da informação;

XXV - Gestor de ativo da informação: autoridade legal responsável pela concessão de acesso a terceiros.

XXVI - Incidente de segurança da informação: um simples ou uma série de eventos de segurança da informação, indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

XXVII - 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 veiculada;

XXVIII - Informação sigilosa: aquela submetida, temporariamente, à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

XXIX - Informação pessoal: aquela relacionada à pessoa identificada ou identificável;

XXX - Integridade: qualidade da informação não modificada, inclusive quanto ao trânsito e destino;

XXXI - Não-repúdio: propriedade da informação que não possa ter seu envio ou contestados, rejeitados ou repudiados por seu emissor ou por seu receptor;

XXXII - Política: intenções e diretrizes globais formalmente expressas pela direção;

XXXIII - Primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações;

XXXIV - Princípios: são ideias centrais que estabelecem diretrizes a um dado sistema, conferindo-lhe um sentido lógico, harmonioso e racional;

XXXV - Recursos de processamento da informação: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem;

XXXVI - Risco: combinação da probabilidade de um evento e de suas consequências;

XXXVII - Rótulo: identificação física ou eletrônica da classificação atribuída à informação;

XXXVIII - Segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como, autenticidade, responsabilidade, não repúdio e confiabilidade, também, podem estar envolvidas;

XXXIX - Segurança institucional: conjunto de ações integradas destinadas à proteção de pessoas, processos de negócio e ativos da Instituição;

XL - Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, avaliação, eliminação, destinação ou controle da informação;

XLI - Tratamento do risco: processo de seleção e implementação de medidas para modificar um risco;

XLII - Usuário: agente público, auditores e quaisquer outros entes que podem acessar ativos de informação do IFSC, mediante autorização de gestores de ativos;

XLIII - Verificação de conformidade em segurança da informação: procedimentos que fazem parte da avaliação de conformidade que visam identificar o cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação da Instituição;

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

ANEXO II - REFERÊNCIAS LEGAIS E NORMATIVAS

I – Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e privados e dá outras providências;

II – Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

III – Lei nº 8.745, de 9 de dezembro de 1993, que dispõe sobre a contratação por tempo determinado para atender à necessidade temporária de excepcional interesse público, nos termos do inciso IX do art. 37 da Constituição Federal, e dá outras providências;

IV - Lei nº 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre os direitos autorais e dá outras providências;

V - Lei nº 9.962, de 22 de fevereiro de 2000, que disciplina o regime de emprego público do pessoal da Administração Federal direta, autárquica e fundacional, e dá outras providências;

VI - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159 de 1991, e dá outras providências;

VII - Lei nº 12.682, de 9 de julho de 2012, que dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos;

VIII - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

IX - Lei nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

X - Decreto nº 2.556, de 20 de abril de 1998, que 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;

XI - Decreto nº 3.714, de 3 de janeiro de 2001, que 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;

XII - Decreto nº 4.073, de 3 de janeiro de 2002, que regulamenta a Lei nº 8.159/1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados;

XIII - Decreto nº 4.829, de 3 de setembro de 2003, que dispõe sobre criação do Comitê Gestor da Internet no Brasil – CCIbr, sobre o modelo de governança da Internet no Brasil e dá outras providências;

XV - Decreto nº 6.605, de 14 de outubro de 2008, que dispõe sobre o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva – COTEC;

XVI - Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527/2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;

XVII - Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527/2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;

XVIII - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo e dispõe sobre o Núcleo de Segurança e Credenciamento;

XIX - Decreto nº 8.539, de 8 de outubro de 2015, que dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional;

XX - Decreto nº 8.771, de 11 de maio de 2016, que regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações;

XXI - Decreto nº 8.777, de 11 de maio de 2016, que institui a Política de Dados Abertos do Poder Executivo Federal;

XXII - Decreto nº 9.283, de 07 de fevereiro de 2018, que Regulamenta a Lei nº 10.973, de 2 de dezembro de 2004, a Lei nº 13.243, de 11 de janeiro de 2016, o art. 24, § 3º, e o art. 32, § 7º, da Lei nº 8.666, de 21 de junho de 1993, o art. 1º da Lei nº 8.010, de 29 de março de 1990, e o art. 2º, caput, inciso I, alínea "g", da Lei nº 8.032, de 12 de abril de 1990, e altera o Decreto nº 6.759, de 5 de fevereiro de 2009, para estabelecer medidas de incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo, com vistas à capacitação tecnológica, ao alcance da autonomia tecnológica e ao desenvolvimento do sistema produtivo nacional e regional.

XXIV - Decreto nº 9.637, de 26 de dezembro de 2018, que Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, 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.

XXV - Decreto nº 10.024, de 20 de setembro de 2019, Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal.

XXVI - Decreto nº 10.332, de 28 de abril de 2020, que Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.

XXVII - Decreto nº 10.543, de 13 de novembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas na administração pública federal e regulamenta o art. 5º da Lei nº 14.063, de 23 de setembro de 2020, quanto ao nível mínimo exigido para a assinatura eletrônica em interações com o ente público.

XXVIII - Resolução nº 20, de 16 de julho de 2004 do Conselho Nacional de Arquivos (CONARQ), que dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos;

XXIX - Resolução nº 32, de 17 de maio de 2010 do Conselho Nacional de Arquivos (CONARQ), que dispõe sobre a inserção dos metadados na Parte II do modelo de requisitos para sistemas informatizados de gestão arquivística de documentos – e-ARQ Brasil;

XXX - Câmara Técnica de Documentos Eletrônicos (CTDE). Conselho Nacional de Arquivos (CONARQ). E-ARQ Brasil: modelo de requisito para sistemas informatizados de gestão arquivística de documentos. Rio de Janeiro: Arquivo Nacional, 2011;

XXXI - Instrução Normativa nº 1, de 04 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISIP do Poder Executivo Federal.

XXXII - Instrução Normativa PR nº 11, do INPI, de 18 de março de 2013, que estabelece normas e procedimentos relativos ao registro de programa de computador;

XXXIII - Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal direta e indireta e dá outras providências;

XXXIV - Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013, que dispõe o Credenciamento de Segurança para o tratamento de informação classificada, em qualquer grau sigilo, no âmbito do Poder Executivo Federal;

XXXV - Instrução Normativa GSI/PR nº 3, de 06 de março de 2013, que dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal;

XXXVI - Norma Complementar nº 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008, do Gabinete de Segurança Institucional da Presidência da República, que estabelece a Metodologia de Gestão de Segurança da Informação e Comunicações no âmbito da Administração Pública Federal, direta e indireta;

XXXVII - Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para a elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

XXXVIII - Norma Complementar nº 04/IN01/DSIC/GSPR, de 15 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta;

XXXIX - Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, do Gabinete de Segurança Institucional da Presidência da República, que disciplina criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR no âmbito da Administração Pública Federal, direta e indireta;

XL - Norma Complementar nº 06/IN01/DSIC/GSPR (Revisão 01), de 11 de novembro de 2009, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações no âmbito da Administração Pública Federal, direta e indireta;

XLI - Norma Complementar nº 07/IN01/DSIC/GSPR (Revisão 01), de 15 de julho de 2014, do Gabinete de Segurança Institucional da Presidência da República, que estabelece as Diretrizes para Implementação de Controles de Acesso relativos à Segurança da Informação e Comunicações no âmbito da Administração Pública Federal, direta e indireta;

XLII - Norma Complementar nº 08/IN01/DSIC/GSPR, de 19 de agosto de 2010, do Gabinete de Segurança Institucional da Presidência da República, que dispõe as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;

XLIII - Norma Complementar nº 09/IN01/DSIC/GSPR (Revisão 02), de 15 de julho de 2014, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações no âmbito da Administração Pública Federal, direta e indireta;

XLIV - Norma Complementar nº 10/IN01/DSIC/GSPR, de 30 de janeiro de 2012, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre o Inventário e Mapeamento de Ativos de Informação nos aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

XLV - Norma Complementar nº 11/IN01/DSIC/GSPR, de 30 de janeiro de 2012, do Gabinete de Segurança Institucional da Presidência da República, dispõe sobre as Diretrizes para Avaliação de Conformidade nos aspectos relativos à Segurança da Informação e Comunicações no âmbito da Administração Pública Federal, direta e indireta;

XLVI - Norma Complementar nº 12/IN01/DSIC/GSPR, de 30 de janeiro de 2012, do Gabinete de Segurança Institucional da Presidência da República, dispõe sobre o Uso de Dispositivos nos aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

XLVII - Norma Complementar nº 13/IN01/DSIC/GSPR, de 30 de janeiro de 2012, do Gabinete de Segurança Institucional da Presidência da República, dispõe sobre as Diretrizes para Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

XLVIII - Norma Complementar nº 14/IN01/DSIC/GSPR, de 30 de janeiro de 2012, do Gabinete de Segurança Institucional da Presidência da República, dispõe sobre as Diretrizes

Relacionadas à Segurança da Informação e Comunicações para o Uso de Computação em Nuvem nos órgãos e entidades da Administração Pública Federal;

XLX - Norma Complementar nº 15/IN01/DSIC/GSPR, de 11 de junho de 2012, do Gabinete de Segurança Institucional da Presidência da República, dispõe sobre as Diretrizes para o Uso Seguro das Redes Sociais na Administração Pública Federal;

L - Norma Complementar nº 16/IN01/DSIC/GSPR, de 21 de novembro de 2012, do Gabinete de Segurança Institucional da Presidência da República, dispõe sobre as Diretrizes para Desenvolvimento e Obtenção de Software Seguro nos órgãos e entidades da Administração Pública Federal;

LI - Norma Complementar nº 17/IN01/DSIC/GSPR, de 9 de abril de 2013, do Gabinete de Segurança Institucional da Presidência da República, dispõe sobre a Atuação e Adequações para Profissionais da Área de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

LII - Norma Complementar nº 18/IN01/DSIC/GSPR, de 9 de abril de 2013, do Gabinete de Segurança Institucional da Presidência da República, dispõe sobre as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

LIII - Norma Complementar nº 19/IN01/DSIC/GSPR, de 15 de julho de 2014, do Gabinete de Segurança Institucional da Presidência da República, dispõe sobre Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal;

LIV - Norma Complementar nº 20/IN01/DSIC/GSPR, de 15 de dezembro de 2014 (Revisão 01), do Gabinete de Segurança Institucional da Presidência da República, dispõe sobre as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e Entidades da Administração Pública Federal;

LV - Norma Complementar nº 21/IN01/DSIC/GSPR, de 8 de outubro de 2014, do Gabinete de Segurança Institucional da Presidência da República, dispõe sobre as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes;

LVI - ABNT NBR ISO/IEC 27001:2006: Tecnologia da Informação: Técnicas de Segurança da Informação: Sistemas de Gestão de Segurança da Informação; LVI - ABNT NBR ISO/IEC 27002:2007: Tecnologia da Informação: Código de Prática para a Gestão da Segurança da Informação;